ROMA TRE
UNIVERSITÀ DEGLI STUDI

Scuola Dottorale EDEMOM

European **D**octorate in **E**lectronic Materials, **O**ptoelectronics and **M**icrosystems

Doctor of Philosophy Course In Electronic Engineering - XXV Ciclo

Hylemetric Techniques for Data and Information Security

Dr. Lorenzo Cozzella

Tutor

Prof. Giuseppe Schirripa Spagnolo

Coordinator

Prof. Giuseppe Schirripa Spagnolo

June 2013

命

エリサ

永

Acknowledgments

This work is dedicated to my family, always present and near to me, giving me the necessary force to go ahead along this hard walk. In particular I want to dedicate all the results to my wife Carla, who has made this journey with me, sharing all the successes and the defeats.

A special thanks to my Professor, and Tutor Schirripa Spagnolo, whom has given to me this opportunity and all his effort to support me in this adventure, becomes, in over ten years of collaborations, part of my family, allowing me to reach these professional goal, which I try to obtain with force and, sometimes, obstinacy. In particular I have to thanks the patience of Professor Schirripa when hundreds times I’ve requested to recheck formulas, figures and strange ideas which jump out of my mind.

Abstract

The proposed research is based on past years studies on innovation in biometric systems, which has led to verifying how, in all the biometry approach, exists a similar approach, defined in the research Biometry Paradigm, which is based on the identification and utilization of particular characteristics, having the properties to be univocal and measurable. Typical examples are fingerprint, iris, retina, hand geometry, face and so on. Starting from this consideration, we have tried to verify if a similar approach could be applied to valuable objects, such as banknotes, artworks, identification documents and, in general, to all the objects which have the necessity to be verified to fight against their counterfeiting. The research work was based on the identification of some characteristics, which can be measured in a non-destructive way, inside some notable case studies, such as banknotes, passports, drug packages, lithography, with the aim to create a method, starting from the past experience in the biometric analysis, which allows to verify with a great accuracy objects' authenticity. The methods developed in this research have been defined as Hylemetric Authentication, from Greek words *ΰλη* (hyle), for inanimate objects and *μετρον* (metros) for measurement.

The study started from the analysis of the existing solutions adopted to put in secureness banknotes, documents, artworks' certificates and drug packages. Starting from this analysis, in each case study, has been possible identify a set of different security systems and approach. In particular it is possible define two categories of security approach:

- Overt Authentication/Identification System, visible at human eye and verifiable in a simple manner by the final utilizer.

- Covert Authentication/Identification System, not simply visible or visible under particular environmental conditions and/or using particular instrumentations.

Typical examples of overt systems are holograms and intaglio printing on banknotes, shifting and changing inks, used on pharmacologic packages. Covert systems are typically ultraviolet inks, infrared patterns and so on, used always on banknotes.

Sometimes are also proposed mixed systems, such as 1D and 2D barcodes, which at first analysis can be considered as overt systems, but the necessity to use dedicated and sometimes also complex decoding systems, allows to catalogue it as mixed system; in fact its presence is sometimes considered as proof of originality, but in reality the originality can be proven only analyzing the content of the barcode, which sometimes results encrypted.

Focusing on research case studying, banknotes presents both overt and covert solutions, whereas drugs packages are in general characterized by overt or mixed ones. Lithography and artworks in general have been authenticated using only paper certificate of authenticity, without any automatic or semi-automatic verification system. In any case this approach can be categorized as overt, because the presence of a Certificate of Authenticity with signature and stamp on it, is generally considered sufficient to be sure on the artwork originality.

Starting from this state-of-art, the research has tried to verify the possibility to apply the biometric approach to these case studies, with the aim to enforce the authentication and anti-counterfeiting process with an innovative solution. For making this, the first step is the identification, for each case study, of at least one univocal characteristic, present on the analyzed object at priori (e.g. Banknotes security fibres), or added on it (e.g. white light speckles added on drug packages), which has the requested requirements to be categorized as Hylemetric

Characteristic. In particular a characteristic, to be considered as usable in the Hylemetric approach, has to have the following basic properties:

- Uniqueness: every objects should be identifiable and distinguishable from all others;
- Consistency: feature vector should be verifiable by multiple parties over the lifetime of the object;
- Conciseness: feature vector should be short and easily computable;
- Robustness: it should be possible to verify the feature vector even if the object has been subjected to harsh treatment;
- Resistance to Forgery: it should be very difficult and costly, or impossible for an adversary, to forge a document by coercing a second object to express the same feature vector as the original one.

For any of the case study analyzed during the research course, it has been possible to identify proper characteristics which have all these properties. The acquisition of them changes from object to object, has in biometry paradigm, depending on the object physical characteristics, but the verification approach is similar for all the analyzed ones.

In banknote case, we have used metallic security fibres as Hylemetric characteristic. They have the physical property to shine in the visible spectrum when illuminated by ultraviolet light at a precise wavelength. We have acquired the fibres distribution, creating a unique identification pattern based on them. This pattern has been encrypted and then coded in a bidimensional barcode, based on DataMatrix ECC 200 Standard. The proposed encryption has been made by means of Elliptic Curve, to reduce dimensions of pattern encrypted version and cope with DataMatrix maximum storage constraint.

For artworks in general, we have made some experiments on lithography and then on oil and statue. The proposed approach has to modify the Certificate of

Authenticity, introducing both new information on the paper version and a new digital version of it. All the modifications are based on the extraction of an Hylemetric characteristic from the artwork. In Lithography case, the typical stone impression leave a unique grain pattern, acquirable using a digital camera. For oil paints and statue using particular image manipulations and filters is possible from the acquired image obtaining a speckle-like pattern from the object structure.

Analyzing the pharmacologic products packaging, we have decided to add on them the Hylemetric characteristic, using the so called White Light Speckle technique. We have used ultraviolet ink sprayed on a package' particular area. In this way each package has been stamped with a different Speckle Pattern.

In any studied cases, independently from the acquired characteristic, has been possible defining a Hylemetric Template, which allows to authenticate the related object. In some cases the defined template has been converted into a 2D Barcode to be directly put on the object (e.g. banknotes, drug packages), or has been codified to be inserted in a Digital Certificate of Authenticity (e.g. artworks).

In the case of barcodes, we have used both standard DataMatrix, or a new 2D Barcode based on Computer Generated Holograms, defined HoloBarcode. In some case the barcode has been proposed to be put on the object using infrared ink, to maintain the original object aspect and to increase the system security as well. The usage of infrared ink starting from the necessity to put it on banknotes, plenty of visible and invisible security artefacts. The infrared band is empty on over the 80% of the banknote surface in both sides and it is possible to find the proper area where to put the barcode.

Otherwise, the introduction of a non-standard bidirectional barcode, based on CGH, has been proposed in such cases where the object to be analysed can be heavily manipulated and ruined. HoloBarcode has the great advantage to be highly resistant to loss of information (i.e. loss of part of the barcode area) and to offer the possibility to extract information also starting from only a little part of the barcode. However, the storage capacity of these barcodes is very poor, if compared with standard 2D Barcodes with same dimensions.

In conclusion, during this research we have analysed the state-of-art of security features applied to valuable objects. Then, starting from a biometric approach, has been proposed an Hylemetric paradigm, which allows to authenticate objects starting from their intrinsic characteristics. We have made tests on different type of objects, such as banknotes, passports, lithography, oil paints, drug packages, obtaining in any case the correct definition of a Hylemetric Procedure, similar in any case, and a Hylemetric Template to be used in verification phase. After that we have also proposed a new bi-dimensional barcode, based on Synthetic Holograms, to be used in particular cases instead of Standard ones to store the Hylemetric Template for offline verification activities.

Author’s Bibliography

The following bibliography lists all the papers written with the author contribution during PhD course. It is subdivided into two sections: papers strictly related to research activities, published on International Journals, International Congresses or National Journals as well; papers written with Author contribution, but on arguments near or out of the scope of the PhD research activities.

PhD Related Pubblications

- G. Schirripa Spagnolo, L. Cozzella, C. Simonetti, “Hylemetry versus Biometry: a new method to certificate the lithography authenticity”, Proceedings SPIE, 8084, 80840S, 2011.
- G. Schirripa Spagnolo, L. Cozzella, and C. Simonetti, “Banknote security using a biometric-like technique: a Hylemetric approach”’, Meas. Sci. Technol., Vol. 21, 055501, 2010.
- G. Schirripa Spagnolo, L. Cozzella, and C. Simonetti, “Currency Verification by 2D Infrared Barcode”, Meas. Sci. Technol., Vol. 21, 107002, 2010.
- L. Cozzella, C. Simonetti, and G. Schirripa Spagnolo, “It is possible to use biometric techniques as authentication solution for objects? Biometry vs.. Hylemetry”, IEEE Proc. of 5th International Symposium on Communications Control and Signal Processing (ISCCSP), 10.1109/ISCCSP.2012.6217753, 2012.
- M. De Santis, L. Cozzella, G. Schirripa Spagnolo, “New 2D Barcode solution based on Computer Generated Holograms: Hologhaphic Barcode”, IEEE Proc.

of 5th International Symposium on Communications Control and Signal Processing (ISCCSP), 10.1109/ISCCSP.2012.6217831, 2012.

- L. Cozzella, C. Simonetti, and G. Schirripa Spagnolo, "Banconote verifica tramite approccio biometrico", ICT Security Gennaio 2011, 2011.
- Lorenzo Cozzella, Carla Simonetti, and Giuseppe Schirripa Spagnolo, "Drug packaging security by means of white-light speckle", Optics and Lasers in Engineering, Vol. 50(11), 1359–1371, 2012.
- G. Schirripa Spagnolo, C. Simonetti, and L. Cozzella, "Watermarking di immagini tramite olografia sintetica", Proc. Elettrottica 2004, Pavia 15-17 giugno 2004, pp. 298-301, 8° convegno nazionale AEI "Strumentazione e metodi di misura elettroottici" Elettroottica 2004, 2004.
- G. Schirripa Spagnolo, C. Simonetti, and L. Cozzella, "Fragile digital watermarking by synthetic holography", Proc. Optics/Photonics in Security and Defence SPIE Symposium, London 24-28 October 2004, Proc. SPIE vol.5615, 173-182, 2004.
- G. Schirripa Spagnolo, C. Simonetti, and L. Cozzella, "Image authentication by means of fragile CGH watermarking", Proc. Optics and Optoelectronics SPIE Conference, Warsaw 29 August 2-September 2005, Proc. SPIE vol.5954, 2005.

Other Pubblications

- G. Schirripa Spagnolo, C. Simonetti, L. Cozzella, "IR Fringe Projection for 3D Face Recognition", Proceeding of International Conference on Advanced Phase Measurement Methods in Optics and Imaging, Locarno, 2010.
- G. Schirripa Spagnolo, C. Simonetti, L. Cozzella, "Autenticazione di documenti di identità tramite watermarking fragile", Safety and Security, 2010.

- L. Cozzella, C. Simonetti, D. Papalillo, G. Schirripa Spagnolo, “Designing of binary diffractive optical elements for beams performing”, Proc. SPIE 8306, 83060X, 2011, doi:10.1117/12.912311
- G. Schirripa Spagnolo, D. Papalillo, A. Martocchia, L. Cozzella, “Simple educational tool for digital speckle shearography”, Eur. J. Phys. 33 733 doi:10.1088/0143-0807/33/4/733, 2012.
- G. Schirripa Spagnolo, C. Simonetti, and L. Cozzella, “Superposed strokes analysis by conoscopic holography as an aid for a handwriting expert”, J. Opt. A: Pure Appl. Opt. 6, 869-874, 2004.
- G. Schirripa Spagnolo, C. Simonetti, and L. Cozzella, “Content fragile watermarking based on a computer generated hologram coding technique”, J. Opt. A: Pure Appl. Opt. 7, 333-342, 2005.
- G. Schirripa Spagnolo, L. Cozzella, and C. Simonetti, “Un Laser per il riconoscimento delle firme”, ICT Security Luglio-Agosto 2009, 19-23, 2009.
- G. Schirripa Spagnolo, L. Cozzella, and C. Simonetti, “Determination of the sequence of line crossings by means of 3D laser profilometry”, SPIE Conference, Warsaw 29 August 2-September 2005, Proc. SPIE vol.5954, 2005.
- G. Schirripa Spagnolo, L. Cozzella, and C. Simonetti, “Measurement of mass diffusion coefficients by digital moiré”, SPIE Conference, Warsaw 29 August 2-September 2005, Proc. SPIE vol.5954, 2005.
- Giuseppe Schirripa Spagnolo, Lorenzo Cozzella, Carla Simonetti, “Linear Conoscopic Holography as aid for Forensic Handwriting Expert”, Optik, Available online, 2012, doi: 10.1016/j.ijleo.2012.06.097.
- Giuseppe Schirripa Spagnolo, and Lorenzo Cozzella, “Laser speckle decorrelation for fingerprint acquisition”, J. Opt., Vol. 14(9), 094006, 2012, doi:10.1088/2040-8978/14/9/094006

Table of Contents

ACKNOWLEDGMENTS I

ABSTRACT III

AUTHOR'S BIBLIOGRAPHY IX

PHD RELATED PUBBLICATIONS IX

OTHER PUBBLICATIONS X

TABLE OF CONTENTS XIII

LIST OF FIGURES XIX

LIST OF TABLES XXIX

LIST OF ACRONYMS XXXI

CHAPTER 1 MOTIVATIONS 33

1.1 INTRODUCTION 34

1.1.1 TERMINOLOGY 37

1.1.1.1 Physical and Logical Access 37

1.1.1.2 Authentication and Identification 38

1.1.1.3 Physical and Behavioral Biometry 39

1.1.1.4 Interactive and Passive Biometry 39

1.1.1.5 Positive and Negative Verification 40

1.2 BIOMETRIC PROCESS PHASES 41

1.2.1 Biometric Data Registration (Enrollment) 42
1.2.2 Authentication Phase 43
1.2.3 Identification Phase 44
1.3 Performance Evaluation 44
1.3.1 FRR, FAR and ROC Curve 45
1.3.2 User Typology 48
1.3.3 Equal Error Rate (ERR) 49
1.3.4 Identification Rate Rk 54
1.4 Kinds of Biometric Systems 55
1.4.1 Fingerprints 55
1.4.2 Face 56
1.4.3 Hand Geometry 57
1.4.4 Palmprint 57
1.4.5 Iris 58
1.4.6 Retina 59
1.4.7 Keystroke 60
1.4.8 Signature 60
1.4.9 Voice 61
1.4.10 Gait 62
1.4.11 Biometry Comparison 63
1.5 Biometric paradigm applied to lifeless matter 65

CHAPTER 2 STATE OF THE ART 71

2.1 Introduction 72
2.1.1 Overt (or direct) Security 73
2.1.2 Covert (or indirect) Security 74
2.2 Banknote and Document Security Solution 74
2.2.1 Paper Watermarking 76
2.2.2 Security Printing 79
2.2.2.1 Intaglio Printing - Latent Image Effect 79
2.2.2.2 Letterpress 81
2.2.2.3 Guilloches 83

2.2.2.4 Rainbow printing 83
2.2.2.5 Printing Ink with Optically Variable Characteristics 84
2.2.2.6 Microprint 86
2.2.2.7 UV-Print 86
2.2.2.8 See-Through Register 87
2.2.2.9 Digital Security Print in a Photograph 88
2.2.3 PERFORATION 89
2.2.3.1 Mechanical Perforation and Laser Perforation 89
2.2.3.2 Micro-Perforation 90
2.2.3.3 Perforated Picture 91
2.2.4 DIFFRACTIVE SECURITY ELEMENTS 91
2.2.4.1 Holographic Elements 92
2.2.4.2 Kinegram® 94
2.2.5 SECURITY ELEMENTS INSERTION 95
2.3 ARTWORKS SECURITY 96
2.4 DRUG PACKAGE SECURITY FEATURES 98
2.4.1 OVERT (OR DIRECT) SECURITY SOLUTIONS 100
2.4.1.1 Holograms 101
2.4.1.2 Colour-Shift Inks 102
2.4.1.3 Barcoding 103
2.4.1.4 Radio Frequency Identification (RFId) 104
2.4.2 COVERT OR INDIRECT SECURITY SOLUTIONS 105
2.4.2.1 UV Inks and Print 105
2.4.2.2 Colour and UV Micro-text Print 106
2.4.2.3 Taggant Authentication 107
2.4.2.4 Laser Surface Authentication – LSA 108
2.4.2.5 Physical Unclonable Function – PUF 109
2.4.3 COMBINING OVERT AND COVERT TECHNOLOGIES 110

CHAPTER 3 HYLEMETRIC PARADIGM 111

3.1 INTRODUCTION 111
3.2 HYLEMETRIC CHARACTERISTICS 112

3.3 TEMPLATE DEFINITION 115

3.4 BIDIMENSIONAL BARCODE 116

3.4.1 PDF417 BARCODE 118

3.4.2 AZTEC CODE 122

3.4.3 QR CODE 130

3.4.4 DATA MATRIX ECC 200 137

3.4.4.1 Technical Characteristics 139

3.4.4.2 Error Correction in ECC 200 145

CHAPTER 4 HYLEMETRIC APPLICATIONS 147

4.1 INTRODUCTION 147

4.2 BANKNOTE VERIFICATION BY HYLEMETRIC APPROACH 148

4.2.1 BANKNOTE VERIFICATION ENHANCEMENT BY IR BARCODE 164

4.3 ARTWORKS HYLEMETRIC AUTHENTICATION 173

4.3.1 OIL PAINTING AUTHENTICITY CASE STUDY 182

4.3.2 LITHOGRAPHY DIGITAL CERTIFICATE OF AUTHENTICITY CASE STUDY 186

4.4 DRUG PACKAGE AUTHENTICATION 203

4.4.1 WHITE LIGHT SPECKLE HYLEMETRY 205

4.4.1.1 UV Speckle PUF Template 210

4.4.1.2 Verification Phase 217

4.4.1.3 Analysis and Results 220

4.4.2 HOLOGRAPHIC BARCODE 229

4.4.2.1 Experimental results 235

CHAPTER 5 CONCLUSION 241

5.1 INTRODUCTION 241

5.2 FUTURE PERSPECTIVES 242

APPENDIX A BIBLIOGRAPHY 243

APPENDIX B SYNTHETIC HOLOGRAMS 259

B.1 LEE'S DELAYED SAMPLING METHOD 262

List of Figures

FIGURE 1.1 – BIOMETRIC PROCESS SCHEMA. ENROLLMENT, IDENTIFICATION AND AUTHORIZATION PHASES ARE CLEARLY REPORTED AND LINKED EACH OTHER. 42

FIGURE 1.2 – BIOMETRIC SYSTEM PERFORMANCE CAN BE SUMMARIZED USING DET AND ROC CURVES. IN THESE TWO EXAMPLES ARE SHOWN IN (A) A DET CURVE RELATED TO FRR VS.. FAR, AND, IN (B) THE SAME RATIO EXPRESSED USING A ROC CURVE ON LINEAR SCALE. THE TWO EXAMPLES ARE RELATED TO FACE-G MATCHER SCORES PERFORMANCE TEST USING NIST BSSR1 DATABASE [11] 48

FIGURE 1.3 – PROBABILITY DISTRIBUTIONS FOR IMPOSTORS AND GENUINE USERS. IT HAS PUT IN EVIDENCE THAT, GIVEN A THRESHOLD Φ, IT IS POSSIBLE TO DEFINE THE GENUINE USERS PERCENTAGE REFUSED BY THE SYSTEM (FRR CYAN AREA) AND THE PERCENTAGE OF IMPOSTOR USERS WHICH GRANT ACCESS TO THE SYSTEM (FAR ORANGE AREA). THE INTERSECTION POINT BETWEEN THE TWO PROBABILITY CURVES IDENTIFIES THE THRESHOLD VALUE ABLE TO GIVE THE EER. ALSO D-PRIME (OR D’) IS CLEARLY IDENTIFIED IN THIS FIGURE. 53

FIGURE 1.4 – IN (A) FAR AND FRR ARE SHOWN AT THRESHOLD Φ VARYING. IT HAS TO BE NOTED THAT THE TWO CURVES INTERSECTION IDENTIFIES THE ERR, WITH THE RELATED Φ_{EER} THRESHOLD VALUE. IN (B) THE ROC CURVE RELATED TO THE PREVIOUS FAR AND FRR CURVES IS SHOWN. 53

FIGURE 1.5 – IRIS IMAGES ACQUIRED USING DIFFERENT SENSORS. IT HAS TO BE NOTED THE DETAIL OF THE HIGH DISTINCTIVE IRIS PATTERN. 59

FIGURE 1.6 – BANKNOTE IMAGE ACQUIRED UNDER ULTRAVIOLET ILLUMINATION. IT HAS SIMPLE TO NOTICE THE RANDOM SECURITY METALLIC FIBRE S DISTRIBUTION INSIDE THE IMAGE. 67

FIGURE 2.1 – MODERN DANDY ROLL EXAMPLE USED FOR PRINTING WATERMARKS ON PAPER IN LIGHT WAY. 78

FIGURE 2.2 – PAPER WATERMARKING EXAMPLES. IN PARTICULAR IN (B) 50 EURO BANKNOTE WATERMARK IS REPORTED. 78

Figure 2.3 – Example of intaglio printing shows a clearly visible and physically perceptible ink coating. 80

Figure 2.4 – The use of a corresponding design in association with intaglio print allows the printing and, as a result, the detection of a picture or text, which would otherwise remain hidden (latent image/ tilt effect in a Czech Republic passport). 81

Figure 2.5 – Picture of a "Novel" numbering box. 82

Figure 2.6 – Typical letterpress characteristics are dot fringes (left) and/or the relief-like impression in the paper (right). 82

Figure 2.7 – Guilloches on a Swiss banknote. 83

Figure 2.8 – Rainbow print allows a smooth transition of colours. 84

Figure 2.9 – The €50 banknote's denomination figure, printed in OVJ® ink, reflects different colours depending on the angle of the oblique light. 85

Figure 2.10 – Specific characteristic of Irisafe® is the pearly shine; seen here in an example of the Swiss Vehicle Registration document. 85

Figure 2.11 – Examples of a microprint in Kinegram® (left) and in intaglio print (right). 86

Figure 2.12 – The fluorescent overprint is often positioned over the biographical entries, to help recognition of spot manipulations. Here a photo of the Swiss ID card in daylight (left) and under UV-lighting (right). 87

Figure 2.13 – The front part of the subject under normal light (above left) is printed precisely over. The back side (below left) thus creating a whole motif. This is visible under transmitted light (right). 88

Figure 2.14 – A special digital print allows data to be encoded into an image. Without the use of a special device, the information is not seen (left). Using a decoding lens, the information becomes visible (right) 89

Figure 2.15 – The perforated numbers are punched out (left) or lasered (right) into the document in an exact pattern. 90

FIGURE 2.16 – IMAGES OF A SWISS BANKNOTE WITH MICROPERF^{TM} (LEFT) AND A BRITISH PASSPORT WITH DESTRIPERF^{TM} (RIGHT) SEEN UNDER TRANSMITTED LIGHT. 90

FIGURE 2.17 – THE *PERFORATED IMAGE* IS A VERY SOPHISTICATED SECURITY ELEMENT WHICH IS SIMPLE TO VERIFY IN TRANSMITTED LIGHT. THE SWISS PASSPORT BIOGRAPHICAL PAGE IN AN OVERVIEW (LEFT) AND IN A CLOSE-UP OF THE IMAGEPERF^{TM} PICTURE (RIGHT) 91

FIGURE 2.18 – EXAMPLE OF 100 € BANKNOTE HOLOGRAM. (A) IS THE IMAGE OF THE BANKNOTE AREA AND (B) IS THE SAME AREA WITH THE HOLOGRAM HIGHLIGHTED, AFTER BANKNOTE ILLUMINATED WITH A DIFFERENT ANGLE. 93

FIGURE 2.19 – TYPICAL FOR THE HOLOGRAM IS THE SUBJECT'S THREE-DIMENSIONAL REPRODUCTION. THE MASTERCARD EXAMPLE SHOWS AN ADDITIONAL COLOUR CHANGE WHEN THE ANGLE OF DIRECT LIGHT IS VARIED. 93

FIGURE 2.20 – METALLIC KINEGRAM® IN AN EXAMPLE OF THE SLOVENIAN PASSPORT. 94

FIGURE 2.21 – BY CHANGING THE ANGLE OF INCIDENT LIGHT OR VIEWING, A TWO-DIMENSIONAL PICTURE OF MOVING STRUCTURES AND CHANGING COLOURS CAN BE DEPICTED. 95

FIGURE 2.22 – THE DIFFERENCE BETWEEN REAL COLOUR SECURITY FIBRE S IN A CANADIAN PASSPORT (A) AND IMITATIONS IN THE FORGERY (B) CAN BE EASILY SEEN BY USING A MAGNIFYING GLASS. 96

FIGURE 3.1 – EXAMPLE OF QR CODE. 117

FIGURE 3.2 – EXAMPLE OF PDF417 CODEWORDS AREAS.. 120

FIGURE 3.3 – (A) EXAMPLE OF AZTEC BARCODE; (B) THE CORE OF THE FULL AZTEC CODE IS COMPOSED BY 40 BITS BETWEEN THE ORIENTATION MARKS FOR ENCODING PARAMETERS CODEWORDS AREAS. 123

FIGURE 3.4 – EXAMPLE OF CREATION OF AZTEC BARCODE DATA: MESSAGE DATA ARE PLACED IN A SPIRAL PATTERN AROUND THE CORE. THE MODE MESSAGE BEGINS “01011100”, INDICATING 01_2+1 2 LAYERS, AND 011100_2+1 = 29 DATA CODEWORDS (OF 6 BITS EACH).. 126

FIGURE 3.5 – 6-LAYER (41×41) AZTEC CODE SHOWING REFERENCE GRID. 129

FIGURE 3.6 – EXAMPLES OF DIFFERENT SIZE QR CODES: (A) 21X21; (B) 33X33; (C) 57X57; (D) 177X177. 132

FIGURE 3.7 – EXAMPLE OF QR CODE PRINTED ON PAPER AND RUINED. IT IS STILL POSSIBLE EXTRACTING INFORMATION FROM IT, DUE TO THE LEVEL OF ERROR CORRECTION. 134

Figure 3.8 – QR Code grid creation to determine error correction level pattern orientation and scale and pattern mask. 135
Figure 3.9 – Character position inside QR Code matrix. 136
Figure 3.10 – Management of great dimension symbols inside the QR code matrix, with the related error correction codes. 137
Figure 3.11 – (a) Finder Pattern uses for determine position, orientation and scale; (b) data pattern encoded following ECC 200 standard. 139
Figure 3.12 – Quantity of data encoded in a square Data Matrix in relation to the barcode dimension. 141
Figure 3.13 – Symbol Size vs.. Data region dimension. 144
Figure 4.1 – Experimental setup for detection of metallic color fibres. 151
Figure 4.2 – 10 Euro banknote image acquired using UV light source. It is possible to see the random distribution of metallic security fibers. 152
Figure 4.3 – Particular of the same 10 Euro banknote, with superposed a controlling grid. The algorithm assigns a value of 1 to each cell in which is present one or part of a fibre... 154
Figure 4.4 – FFR and FAR curves; EER identifies the threshold to be used in the verification procedure. It has to be noted that the FAR curve seems to have a non standard slope because our studies are limited at template difference under 2%. 156
Figure 4.5 – Specimens used in test step: (a) 5 Euro banknote with secure fibers high density; (b) 10 Euro banknote with some shadows; (c) 20 Euro banknote with high exposure; (d) 50 Euro banknote with secure fibers medium density. 159
Figure 4.6 – (a) a 20 € note UV image in grayscale; (b) the output of the morphologic transformation on the previous image; (c) the related controlling grid and (d) the superposition of image (b) and (c). 160
Figure 4.7 – A 10 Euro note with three increasing ruined areas: (a) and (b) are still recognized due to the tolerance introduced in the system, whereas (c) is considered not accepted. 161

Figure 4.8 – Two different 20 Euro note which show how different can be the security fibers distribution in similar banknotes. 163

Figure 4.9 – 20 Euro banknote image acquired using UV light source with superposed the control grid and the resulting decimal template. 167

Figure 4.10 – Virtual example of 20 Euro banknote with two IR 2D barcode superposition. 169

Figure 4.11 – Summarization of all the described method steps, both for creating the 2D barcode and verifying banknotes. 171

Figure 4.12 – The loss of the singular highlighted fiber leads to a different template, in one or more elements, from the information extracted by IR barcode. In this situation, the banknote can be recognized as genuine or not in relation with the selected verification threshold. 172

Figure 4.13 – (a) oil paint; (b) stone lithography (c) sculpture. Are highlighted the related verification areas and the extracted HHPs. 175

Figure 4.14 – (a) oil painting with highlighted the selected verification area; (b) authentication area with trust points; (c) area acquired during verification phase, with highlighted used trust points; (d) Hylemetric Hash Pattern related to (c) after geometrical corrections. 177

Figure 4.15 – Complete schema showing the artwork verification phase. 181

Figure 4.16 – Examples of extracted HHPs. (a) I_C image; (b) I_T image; (c) HPP_C; (d) HPP_T; (e) 2D correlation between HHPC and HHPT without geometrical correction; (f) 2D correlation between HHPC and HHPT with geometrical correction. 183

Figure 4.17 – Example of 2D correlation obtained with Test Image under "important" geometric distortions. It is possible to observe that the geometric corrections allow, also in this case, to correctly calculate the cross-covariance. 185

Figure 4.18 – Lithography used for testing our authentication method. These were made both in 1984 by Michele Cascella (famous Italian crepuscular landscapist; 1892-1989). The lithography are obtained from private collection. 187

Figure 4.19 – In (a) it is highlighted the area used for certification image (b) and test image (c). On certification and test images are also highlighted the used trusted points. 189

Figure 4.20 – Complete schema showing the lithography verification phase. It is highlighted the execution of verification program in a secure memory space. The data outside secure memory space or secure device are encoded for not allowing copy attack. 195

Figure 4.21 – Certificate Image (a) and Test Image (b). It could be noted that test image is a counter clockwise rotated and translated version of (a). 197

Figure 4.22 – Example of verification result with Salt and Pepper Noise addition. (a) Certificate Image; (b) Roto-traslated Test image with Gaussian Noise Added (0.3 distribution value); (c) Correlation result without Test image geometrical correction; (d) Correlation result after Test image geometrical correction using two trust points. 198

Figure 4.23 – (a) Cascella's Albero di Arancio Certification Image; (b); Test image scaled by 80% in both directions; (c) Resulting equal to 14.84 with geometrical transformation. 201

Figure 4.24 – (a) Test image rotate of 9 degree clockwise and scaled by 20% in both directions; (b); Test image after Geometrical Correction; (c) Resulting equal to 1.28 in case of no geometrical transformation; (d) Resulting equal to 24.01 in case of geometrical transformation. 202

Figure 4.25 – In (a), Drug package under white light illumination is shown, while in (b) the same package is acquired under UV illumination, showing the speckle pattern. 207

Figure 4.26 – Nine different speckle patterns acquired from nine different drug packages (Bayer® Aspirin©). The speckle patterns are created with the same method, using a UV spray ink from a distance of 10 cm, sprayed for 1 second. The speckle patterns reported in the nine images differ in number, dimension and distribution inside a similar package area. 209

Figure 4.27 – The speckle pattern sample shown in Fig. 2(a) is now subdivided into 64 blocks, using a grid with 128x128 pixels cells. 211

Figure 4.28 – (a) Acquired image with trust points superposition. The usage of ten points allows correction of geometrical distortion using third order polynomial function; (b) same

IMAGE UNDER UV ILLUMINATION; (C) ACQUIRED IMAGE WITH DATAMATRIX REFERENCE BOUNDING BOX SUPERPOSITION. THE USE OF THE DATAMATRIX BOUNDING BOX ALLOWS CORRECTION OF THE GEOMETRICAL DISTORTIONS WHEN THE ORIGINAL STANDARD REFERENCE INFORMATION IS KNOWN. 212

FIGURE 4.29 – THE SCHEMA FOR CREATING AN ENCODED 196 BIT STRING STARTING FROM A BLOCK IMAGE IS REPORTED. STARTING FROM A SPECKLE IMAGE BLOCK, A HISTOGRAM IS CREATED WITH INDICATION OF THE PERCENTAGE FOR EACH SIZE INTERVAL. EACH PERCENTAGE IS CONVERTED TO A 4 BIT STRING USING THE CONVERSION IN TABLE 2, CREATING A 32 BIT STRING RELATED TO THE SINGLE BLOCK. AFTER THAT, THE 32 BIT STRING IS ENCODED IN A 196 BIT STRING USING AN ECC PRIVATE KEY. 215

FIGURE 4.30 – FOUR DIFFERENT IMAGE BLOCKS ARE SHOWN IN (A), (B), (C) AND (D) TO SHOW THAT ANY BLOCK REPRESENTS A DIFFERENT SPECKLE PATTERN WITH A DIFFERENT SPECKLE STATISTIC, EVEN BETWEEN TWO CONTIGUOUS BLOCKS. EACH STATISTIC, AS USED IN THIS PAPER, IS REPORTED IN (E), (F), (G) AND (H) RESPECTIVELY. 216

FIGURE 4.31 – (A) ORIGINAL SPECKLE PATTERN; (B) SPECKLE PATTERN AFTER GEOMETRICAL DISTORTION PRODUCED BY ROTO-TRANSLATION AND PERSPECTIVE ERROR; (C) DISTORTED IMAGE REPORTED IN (B) AFTER AUTOMATIC GEOMETRICAL CORRECTION BY MEANS OF THIRD ORDER POLYNOMIAL TRANSFORMATION; (D) CORRELATION PEAK BETWEEN ORIGINAL IMAGE (A) AND CORRECTED ONE (C)....................... 219

FIGURE 4.32 – (A) ORIGINAL SPECKLE PATTERN IMAGE; (B) ACQUIRED IMAGE WITH PERSPECTIVE DISTORTION; (C) CORRELATION RELATED TO (A) AND (B) WITHOUT GEOMETRICAL CORRECTION. THE CORRELATION VALUE IS EQUAL TO 0.06 RELATED TO A STATISTICAL THRESHOLD OF 0.2; (D) CORRELATION RELATED TO (A) AND (B) WITH GEOMETRICAL CORRECTION. THE CORRELATION VALUE IS EQUAL TO 0.68 RELATED TO A STATISTICAL THRESHOLD OF 0.25. 221

FIGURE 4.33 – (A), (B) AND (C) SHOW THREE CONTIGUOUS BLOCKS EXTRACTED FROM SPECKLE PATTERN REPORTED IN FIGURE 4.26(A). IN (D), THE CORRELATION BETWEEN (A) AND (C) IS REPORTED; THE CORRELATION VALUE IS EQUAL TO 0.009 FOR A THRESHOLD OF 0.25. IN (E), THE CORRELATION BETWEEN (A) AND (B) IS REPORTED; THE CORRELATION VALUE IS EQUAL TO 0.008 FOR A THRESHOLD OF 0.25. (F) SHOWS THE CORRELATION BETWEEN (B) AND (C); THE CORRELATION VALUE IS EQUAL TO 0.008 FOR A THRESHOLD OF 0.25. 222

Figure 4.34 – (a) reports the original drug package, as shown in Figure 4.26(i); (b) the same package with a clockwise rotation of 5 degrees; (c) same package with a translation of 20 pixels down and 20 pixels right; (d) same package with reduced scale of 10% in both directions; (e) same package with perspective error of 7 degrees modification on both directions and 8 degrees rotation. 224

Figure 4.35 – (a) Drug package reported in Figure 4.26(a) with a hole in it; (b) Drug package reported in Figure 4.26(b) with right border folded; (c) Drug package reported in Figure 4.26(c) with massive ink writing; (d) Drug package reported in Figure 4.26(d) folded along horizontal axis in the centre of the package; (e) Drug package reported in Figure 4.26(e) with blue ball pen writing; (f) Drug package reported in Figure 4.26(g) with blue gel pen writing. 227

Figure 4.36 – FAR and FRR curves extracted from statistical analysis. The two thresholds used during the article are highlighted. 228

Figure 4.37 – HoloBarcode generation and subsequently string extraction. To implement these tests HoloBarcode has been positioned inside a finder pattern, equal to the one used in the ECC 200 Data Matrix, which is necessary for locating the data area. 234

Figure 4.38 – (a) Data Matrix Code without damage, (b) Readable Data Matrix with data loss correction , (c) and (d) not readable Data Matrix code. 235

Figure 4.39 – (a) HoloBarcode without damage, (b) HoloBarcode with data loss and data correctly recovered, (c) and (d) HoloBarcode readable, data partially recovered. 236

Figure 4.40 – Recovered data from HoloBarcodes of Figure 4.39 237

Figure 4.41 – (a) and (b) readable Data Matrix, (c) and (d) encoded information not readable. 238

Figure 4.42 – (a) ,(b) and (c) HoloBarcode readable without loss of encoded information, (d) HoloBarcode with information partially recovered. 239

Figure B.1 – Lee Hologram phasor decomposition schema. It shows a real and imaginary components related to a single cell to be transformed. 266

Figure B.2 – Lee Hologram phasor decomposition schema. It shows a real and imaginary components related to a single cell to be transformed. 267

List of Tables

TABLE 1.1 – COMPARISON AMONG MAIN BIOMETRY. THE RELATED CHARACTERISTIC LEVEL IS INDICATED WITH CHAR H (HIGH), M (MEDIUM), AND L (LOW), BASED ON AMERICAN STANDARD SCALE FOR BIOMETRIC SYSTEM EVALUATION. 63

TABLE 1.2 – IN THIS TABLE FAR AND FRR RESULTS FOR THE MOST USED BIOMETRY, FINGERPRINT, FACE, AND IRIS, ARE REPORTED. THE EVALUATED ACCURACY IS FUNCTION OF SOME FACTORS: SENSOR CHARACTERISTICS, USED ACQUISITION PROTOCOL, ENVIRONMENTAL CONDITIONS, SUBJECTS NUMBER, NUMBER OR ACQUIRED SAMPLES FOR EACH SUBJECT, SUBJECT HABITS, TIME BETWEEN EACH ACQUISITION AND SO ON. 64

TABLE 3.1 – VARIOUS POLYNOMIAL FUNCTIONS USED FOR LAYERS AND MESSAGE INSIDE AZTEC CODE. 126

TABLE 3.2 – NUMBER OF MAXIMUM CHARACTERS NECESSARY IN RELATION TO CODE TYPE.............................. 131

TABLE 3.3 – NUMBER OF MAXIMUM CODEWORDS THAT COULD BE RESTORED IN RELATION TO THE REED-SOLOMON ERROR CORRECTION LEVEL. 133

TABLE 3.4 – TABLE OF DATA MATRIX ECC 200 SYMBOL ATTRIBUTES (SQUARE FORM). 141

TABLE 4.1 – RELIABILITY OF THE SYSTEM VS.. BANKNOTES TYPE AND BANKNOTES MANIPULATION. 164

TABLE 4.2 – TYPE OF TRANSFORMATION IN RELATION TO DISTORTIONS [SEE REF. 107]. 192

TABLE 4.3 – CORRELATION VALUES FOR DIFFERENT ADDED NOISE, WITH RELATED NOISE PARAMETERS. IT HAS TO BE NOTED THAT STATISTICAL THRESHOLDS ARE CONSTRUCTED USING *CORRELATION FUNCTION MEAN VALUE* AND STANDARD DEVIATION AND ARE NOT DIRECTLY CONNECTED TO ANY NOISE FUNCTION MEAN VALUES AND VARIANCES. 199

TABLE 4.4 – SPECKLE SIZE INTERVAL DEFINITION. ALL SPECKLE INSIDES A SPECKLE FIELD ARE ANALYZED AND SUBDIVIDED INTO 10 INTERVALS IN RELATION TO THEIR SIZE, WHICH IS EXPRESSED IN PIXELS. THEN, THE INTERVALS IDENTIFIED WITH 0 AND 9 ARE REMOVED FOR ROBUSTNESS. 212

TABLE 4.5 – PERCENTAGE CONVERSION. EACH PERCENTAGE RELATED TO A SPECKLE SIZE INTERVAL IS CONVERTED TO A 4 BIT CODING FOLLOWING THIS TABLE. 213

TABLE 4.6 – HAMMING'S DISTANCES BETWEEN THE NINE SPECKLE PATTERNS REPORTED IN FIGURE 4.26........ 223

TABLE 4.7 – HAMMING'S DISTANCES BETWEEN SPECKLE PATTERNS AND THEIR RUINED VERSIONS. THE FIRST COLUMN REPORTS THE VALUES RELATED TO THE RUINED SPECKLE PATTERN ACQUIRED FROM THE ACQUISITION SYSTEM THE SECOND COLUMN REPORTS THE SAME VALUES FOR THE GEOMETRICALLY CORRECTED VERSIONS. 225

TABLE 4.8 – SYMBOLS USED FOR TRANSFORMING A BINARY STRING INTO A BITMAP IMAGE........ 230

List of Acronyms

AFIS	Automatic Fingerprint Identification System
CAS	Covert Authentication System
CGH	Computer Generated Holograms
CMC	Cumulative Match Characteristic
DET	Detection Error Trade-off
ECC	Elliptic Curves Cryptography
EER	Equal Error Rate
FAR	False Accept Rate
FFT	Fast Fourier Transform
FRR	False Rejection Rate
FTA	Failure To Acquire
FTC	Failure To Capture
FTE	Failure To Enroll
GAR	Genuine Accept Rate
HCCB	High Capacity Colour Barcode
IR	Infrared
OAS	Overt Authentication System
PUF	Physical Uncloneable Feature
QR	Quick Response (Code)
ROC	Receiver Operating Characteristic

SH	Synthetic Hologram
SHW	Synthetic Hologram Watermarking
UV	Ultraviolet

Chapter 1 Motivations

1.1 INTRODUCTION 34

1.1.1 TERMINOLOGY 37

1.2 BIOMETRIC PROCESS PHASES 41

1.2.1 BIOMETRIC DATA REGISTRATION (ENROLLMENT) 42

1.2.2 AUTHENTICATION PHASE 43

1.2.3 IDENTIFICATION PHASE 44

1.3 PERFORMANCE EVALUATION 44

1.3.1 FRR, FAR AND ROC CURVE 45

1.3.2 USER TYPOLOGY 48

1.3.3 EQUAL ERROR RATE (ERR) 49

1.3.4 IDENTIFICATION RATE RK 54

1.4 KINDS OF BIOMETRIC SYSTEMS 55

1.4.1 FINGERPRINTS 55

1.4.2 FACE 56

1.4.3 HAND GEOMETRY 57

1.4.4 PALMPRINT 57

1.4.5 IRIS 58

1.4.6 RETINA 59

1.4.7 KEYSTROKE 60

1.4.8 SIGNATURE 60

1.4.9 VOICE 61

1.4.10 GAIT 62

1.4.11 BIOMETRY COMPARISON 63

1.5 BIOMETRIC PARADIGM APPLIED TO LIFELESS MATTER 65

1.1 Introduction

Physical characteristics are used since human origin to identify each other. Face, voice, posture, are all typical and ancestral types of identification method, developed in the human history. Alphonse Bertillon [1], chief of Paris' Police crime identification division, has developed and used the idea to identify possible criminals by means of measurable physical characteristics, during investigation phase, since half of nineteenth century.

When his idea were starting to grow in popularity, it was obscured by a more simple and efficient solution, proposed in the same period: the measurable differences between fingerprint of different people [2]. This approach allowed (and allows also today), to clearly identify people, with a very low possibility to have two fingerprints, belong to two different people, so similar to be confused each other.

In very few time the majority of Police Department in different Nations started to collect criminal fingerprints, creating something similar to the modern database, but made on paper. In this way could be possible verifying the presence on the crime scene of a well-known criminal, comparing the acquired fingerprints with the collected ones.

From that time ahead, the usage of physical characteristics to identify people started to spread all around the world, first with the necessity to secure access to highly confidential information areas, than spreading to the consumer market, composed by non-government subjects, wide public and private institutions, law enforcement entities, but also to common people to access their personal data at home, without using pin and or password.

During the evolution of the physical characteristic usage for logical and physical security, it has been coined a new term, used to identify this approach: ***Biometry***. This term derives from two Greek words : *βιος* (bios), which means life, and *μετρον* (metron), which means measurement, so it is possible to be translate has measurement of life, such as of life characteristics, which allows to take apart one individual to another one.

Theoretically any human characteristic, both physical or behavioral, can be qualified as discriminant to identify a person. In practice a human characteristic can be considered as biometric discriminant only if cope with the following properties [3]:

- *Universality*: al the person should have the characteristic;
- *Permanence*: the characteristic should not vary over time;
- *Distinctiveness*: samples corresponding to different persons should be as different as possible, that is, the inter-class variability should be as large as possible;
- *Robustness*: samples corresponding to the same person should be as close as possible, that is, the intra-class variability should be as small as possible;

- *Accessibility*: the sample should be easy to present to the acquisition device;
- *Acceptability*: it should be perceived as nonintrusive by the user;
- *Hardness to circumvention*: it should be hard for an impostor to fool the system.

Some of these properties are not directly related to the physical characteristic, but to the acquisition system, in particular for acceptability and hardness to circumvention.

Nowadays, the complex international situation and the growing in security awareness, have introduced an enforcement in security controls on common citizens, promoting actions related to area and border control, based on biometric systems. The usage of biometry as security enforced is demonstrated by international initiatives, such as electronic passport, e-Visa and electronic personal identification documents (CIE – Carta di Identità Elettronica). All these solutions will have a common denominator the usage of biometric identifiers. New investments are also foreseen to empower AFIS (Automatic Fingerprint Identification System), based on fingerprint database to be used by international anti-crime structures (e.g. FBI, Interpool, CIA)

A Biometric Identification System is essentially based on the verification of claimed identity (Authentication), or on the individuation of an identity among a set of registered ones (Identification), matching an homogeneous set of data, extracted during verification phase, with the similar set of data maintained in a database. The two different phase in which a person gives its personal data to the acquisition system are called ***enrollment*** and ***matching***. The set of characteristics will be generated starting from the acquisition, and subsequent elaboration, of physical characteristics data (e.g. fingerprint, iris, hand geometry, retina), or behavioral data (e.g. posture, gait, keystroke, voice). In some cases, with the aim to increase identification/authentication system robustness, it is possible using different biometric characteristics, creating a ***multi-modal biometric system***. Some examples are identification system based on fingerprint, palmprint and hand geometry, fingerprint and iris scan. This approach request the definition of a homogeneous score, to be used for confronting different biometry in a unique system.

1.1.1 Terminology

In the following common definition are reported, which can be applied to all the biometric' families. In addition the definition for Enrollment and Verification phases are reported, with a sensor-independent approach, with the aim to arrive at the final definition of **Biometric Template** [3], such as, a uniform and unique data agglomeration, created by means of acquired biometric data, and used for easily verify person authentication.

1.1.1.1 Physical and Logical Access

In the biometric-based identification/authentication system study, exists two recurrent terms:

- ***Physical Access:*** verification procedure with the aim to check the authorization of a person to enter in a particular site, room, or building;
- ***Logical Access:*** verification procedure with the aim to check authorization of a person to use a particular information resource.

1.1.1.2 Authentication and Identification

One of the most important distinction in the biometric process is between authentication and identification.

In the ***Authentication Process***, also called "*one-to-one*", acquired data have to been compared with a unique biometric datum, gave from the same person during registration (i.e. Enrollment) Phase, and stored in a centralized Database. This procedure allows to verify if a person is whom she/he says to be. Frequently this kind of checking is made using also a support user identification token, such as personal id, password, username, pin and so on.

In the ***Identification Process***, the biometric acquired data are checked against an entire Database, to verify if exists at least one person with the "same" biometric template. This process is also called "one-to-many", and it does not requires additional information.

Sometimes, when it is not possible specifying if the verification phase is related to an authorization, or an identification process, it is used the term "***Biometric Identification***".

1.1.1.3 Physical and Behavioral Biometry

Referring to the generic term of biometric identification, it is possible distinguish among two different biometric families:

- ***Physical Biometry***, based on the usage of physical characteristics, such as fingerprint, iris, hand geometry, face, retina and so on;
- ***Behavioral Biometry,*** based on the usage of characteristics not strictly related to individual properties, such as, keystroke velocity, gait, voice, signature and so on.

In the following some information related to the more important and diffused biometric techniques will be reported, for sake of completeness.

1.1.1.4 Interactive and Passive Biometry

Biometric identification processes can be applied both in interactive way, or in passive one.

In the first case the interested person is aware of the system operability and gives her/his biometric data on voluntary basis (***Interactive Biometry).***

In the second case, the biometric data are acquired without person awareness and interaction with the system (***Passive Biometry).***

Typical examples of the first case is the fingerprint acquisition, whereas the second case is the gait or face at distance acquisition. Obviously the Passive Biometry is more linked with Identification problem, where Interactive one with Authentication processes.

1.1.1.5 Positive and Negative Verification

A Biometric system can work both in positive or negative identification; in the first case person declares (also implicitly) to be part of a well-known user group; in the second case person declares (also implicitly) to be not part of a well-known user group.

In a ***Positive Identification*** process it is clear the link between the person under biometric verification, with an identity present in the system, and the user request a positive process, such as a verification that she/he is whom he claim to be, referring to the selected user group[1]. In this approach both authentication and identification can be used. In case of correspondence between the acquired biometric data and the registered ones, an acceptance will be declared, otherwise a rejection. Typical examples are physical and logical access controls.

Negative identification has the aim to establish if a subject under identification does not belong to a well-known user group in the system. Some examples are the presence in the police databases, or if she/he has just one driving license. This procedure is the most used in USA Governance scope. This approach has been proposed to avoid the usage of different identities from a single person. In this case if the system find a correspondence in the databases, between the analyzing biometric data and all the available biometric templates, this become a rejection, whereas in negative case, the system gives an acceptance (i.e. the person requesting a document can have it, because she/he has not another one).

[1] Obviously the real user identity has to be clearly verified during registration phase, using also common paper documents and using identification processes not strictly related to biometric ones.

It has to be noted that, if positive verification can be made with or without biometric systems, negative verification can be carried out only using biometric data [5]. Negative identification can be made only with a one-to-many approach, where the “many” part can be or the entire content of a set of databases, or only one or more short lists.

1.2 Biometric Process Phases

Biometric process can be synthetized as a set of precise phases, independently from the type of biometry and the nature of the acquired data as clearly reported in Figure 1.1.

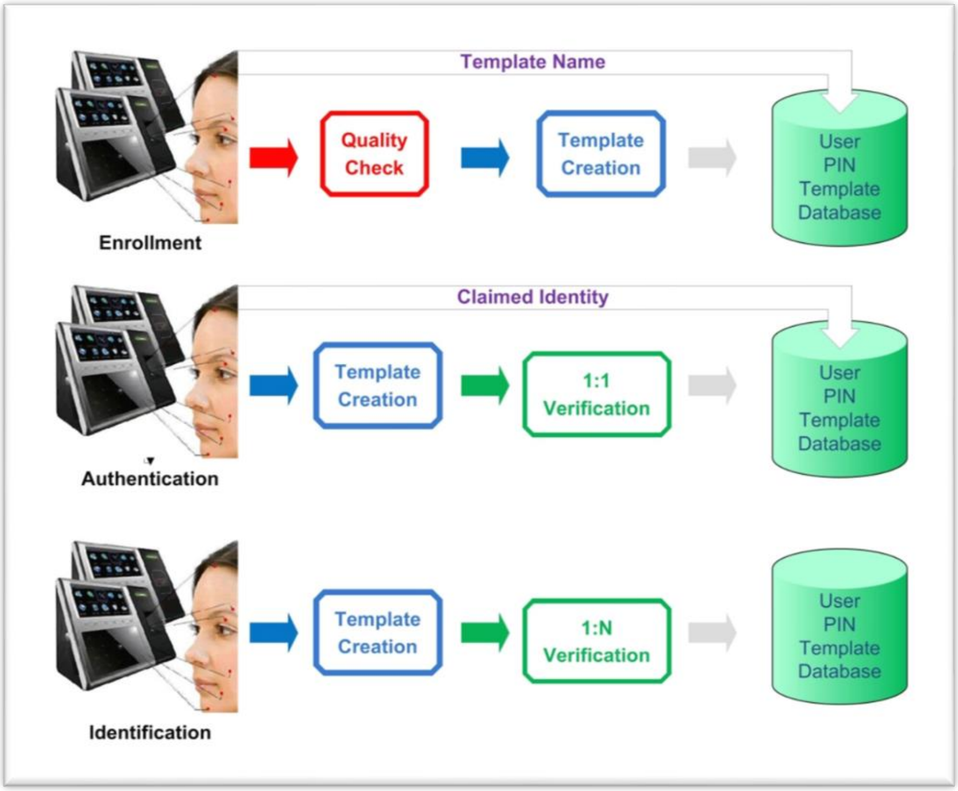


Figure 1.1 – Biometric Process schema. Enrollment, identification and authorization phases are clearly reported and linked each other.

1.2.1 Biometric Data Registration (Enrollment)

User's biometric data registration, also called ***Enrollment***, is the first phase of the biometric paradigm. A user, which would be grant to access to a system or site, has to register her/his biometric characteristics, using an appropriate acquisition system.

Generally the acquired sample has to be undertake a set of quality checks; in case of negative quality results, the Enrollment process has to be reiterated. After this stage, the system has to perform a procedure known as “***feature extraction***”, which is based on the extraction, from the acquired sample, of some numerical characteristics, which will be used to create a uniform numerical set called ***Biometric Template***. Registration phase is concluded with the template storage on a secure database. Sometimes could happen that the storage biometric data is not a numeric template, but the acquired image itself.

In the following, to take into consideration both the proposed situation, we refers to “biometric identifier” or “biometric data”, instead of biometric template.

1.2.2 Authentication Phase

Authentication phase starts with the acquisition of a new biometric sample, in the same way used during Enrollment one, but not necessary using an identical acquisition system. After that the biometric features have been extracted and compared with the one stored in the database(s), or in a storage media, such as a smart card (match on card example).

The verification result is in true/false form or in percentage of similarity (matching score) between the extracted template and the stored one.

1.2.3 Identification Phase

During identification phase the user cannot use storing media, nor insert an identification information (e.g. pin, username, token), but the system checks the acquired template with all the templates present in its databases. The verification result is a set of matching scores, one in the best case, assuring that the person has been identified or can belongs to a set of possible identity, or a “not-identified” message.

All the verification phases are made on the basis of the existence of a matching threshold. The presence of a threshold is due to the differences that can be exist between the acquired image in Enrollment phase and in verification one. These differences can be due to different sensors, different environmental conditions, different acquisition conditions (e.g. rotated fingerprint), and so on. In the following more details on the verification threshold selection and related verification errors will be explained.

1.3 Performance Evaluation

Biometric system performance evaluation i based on statistical analysis, related on the number of correct identification respect with total number of tentative identification. In the following the main performance statistics are reported.

1.3.1 FRR, FAR and ROC Curve

A classical access system, based on a pin, password or token, request a *perfect* match between the claimed characteristic and the stored one. In a Biometric system this situation is near impossible and the verification is based on similarity instead of identity. This assertion is more valid more the biometric system is ***open***. With the term open is identified a biometric system where acquisition sensors can have different capabilities and performance, environmental characteristics can widely change and so the acquired sample can differs a lot from the registered one. In addition, greater the storage database is, greater the probability to fail the identification/authorization is.

It ha also to be taken into consideration that the near impossibility to have two biometric data set identical is on the basis of the ***anti-replay*** technique in biometric systems. If a set identical to the registered one is submitted to the system, it is automatically discharged, because is considered not secure.

All the differences presented till now, can lead to a distinction between the possible template variations, known in literature as ***intra-class variations***, such as differences inside the same biometric characteristic belonging to the same person, acquired in different time.

Differences related to the same biometric characteristic belonging to different people are called ***inter-class variations.*** A biometric dataset to be used in a authentication/identification system should have a low intra-class variation value and a high inter-class one. In this way the differences among different acquisition of the same characteristic from the same person are minimized, whereas the difference among the same characteristic of different people are maximized. In this way it is also achieved the aim to minimized the false negatives (rejections of authorized people), and to maximized false positive (acceptance of unauthorized people).

The similitude grade between two biometric datasets (i.e. biometric templates) is valorised using a ***similitude score***, or simply score. To determine if a score is sufficient to grant the user authentication/identification, it is necessary define a threshold φ. If it is defined "*Genuine Score*" the value S_G associated to the matching between two different templates belong to the same person and "*Impostor Score*" the value S_I, associated to two templates belong to two different person, it is possible writing:

$$\begin{cases} \text{if } S_G \geq \varphi & \text{Genine User correctly recognized} \\ \text{if } S_G < \varphi & \text{Genuine User erroneusly rejected} \\ \text{if } S_I < \varphi & \text{Impostor correctly rejected} \\ \text{if } S_I \geq \varphi & \text{Impostor erroneusly recongized} \end{cases} \tag{1.1}$$

The ***False Accept Rate (FAR)***, also defined False Match Rate (FNMR)[2] is the percentage of impostor users recognized by the system as genuine ones (i.e. $S_I \geq \varphi$), calculated on the total number of verification attempts.

[2] It has to be noted that FMR and FNMR are not exactly synonyms of FRR and FAR (see [9] and [10]), but in this work we will refer to FRR and FAR in this meanings, due to the fact that this choice, even if not completely correct, does not alter the proposed results and considerations.

Similarly , the ***False Reject Rate (FRR)***, also called False Non Match Rate (FNMR) of an identification system, can be considered the percentage of genuine scores which fail the correct identification (i.e. $s_G < \varphi$).

The ***Genuine Accept Rate (GAR)***, is the part of genuine scores which are over the selected threshold (i.e. $s_G \geq \varphi$) and is equal to:

$$GAR = 1 - FRR. \tag{1.2}$$

It is simple saying that, analysing Eq. (1.1) and the above-reported definitions, that varying the threshold value φ, it is impossible that both FAR and FRR increase or decrease together.

The FAR and FRR variation analysis varying φ can be made by means of the so called DET (*Detection Error Tradeoff*) Curves [7],which represent the FRR referred to FAR, varying the threshold φ in a normally deviated reference scale. When the used scale is linear, logarithmic or semi-logaritmic, the resulting curves are called ***Receiver Operating Characteristic (ROC) Curve*** [8]. In many cases ROC curves represents GAR vs.. FAR, instead of FRR vs.. FAR.

The main difference in the usage of ROC curve instead of DET ones is the necessity to use a linear or logarithmic scale, instead of a normally deviated one.

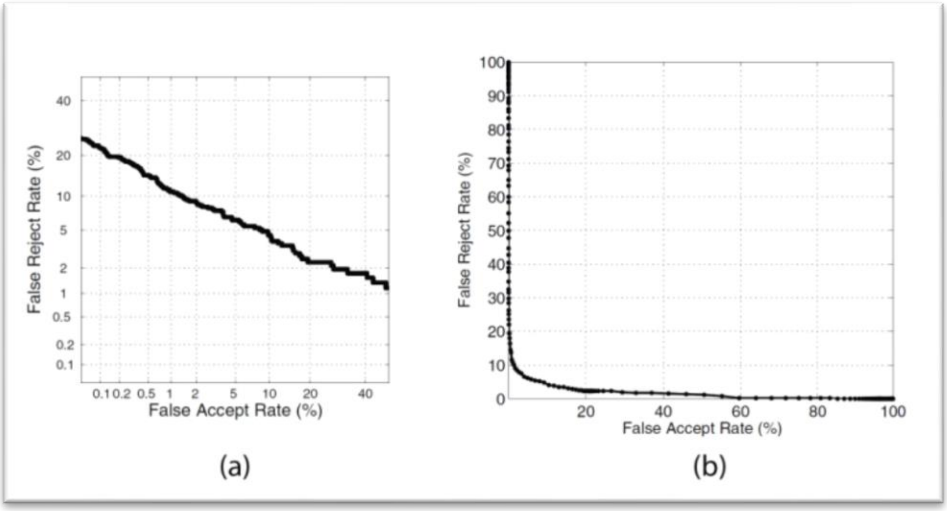


Figure 1.2 – Biometric system performance can be summarized using DET and ROC curves. In these two examples are shown in (a) a DET Curve related to FRR vs.. FAR, and, in (b) the same ratio expressed using a ROC Curve on linear scale. The two examples are related to Face-G matcher scores performance test using NIST BSSR1 database [11]

1.3.2 User Typology

An interesting analysis is the distribution of false positive and false negative among the entire user typologies. Doddington [12] has made a study demonstrating that all the users can be divided in four categories and the distribution of false positive and negative is not uniform among all of them.

These four categories are based on the "recognisability" of a user. In particular the four recognisability category proposed by Doddington in relation with their intrinsic characteristics are[3]:

[3] Even if this categorization has been thought to be applied to voice, it can be applied to all the biometric system, independently from the used characteristics.

- *Sheep:* ir represents users with a biometric dataset highly distinctive, with a related low intra-class variation values, and related high inter-class variation values. This category presents a low value in both false acceptance and false rejection.
- *Goats:* it represents all the users prone to high FRR values due to their intrinsic characteristics, having high values of intra-class variations.
- *Lambs:* it represents users having biometric datasets highly superposed to the ones belong to different people. These sets show low values of inter-class variations, lead to high FAR values.
- *Wolf:* are people which have success to manipulate their biometric data (in particular the behavioural ones) with the aim to pretend to be another person, regularly registered the system. In this way this typology of person, try to gain access at the system in fraudulent way. This lead to artificially increase the FAR value.

1.3.3 Equal Error Rate (ERR)

In addition to the FAR and FRR, a biometric system can be characterised on the basis of other error categories.

The ***Failure to Acquire (FTA) rate***, also known as **Failure to Capture (FTC)** is the percentage of a biometric acquisition system to fail the user biometric data acquisition. This kind of errors happen when the system is not able to acquire a signal with an adequate quality (e.g. user face in a too much dark environment, fingerprint with low level of details).

The ***Failure to Enroll (FTE) rate*** is the percentage of users which fails to register in the system using a specified acquisition sensor.

A trade-off exists between the FTE, which requests a system with a low accuracy, and the FAR/FRR, which request the contrary. Typically errors having an high impact on FTE happen when the system has an high threshold and refuse low quality acquired images. Consequently, having a high quality threshold leads to have a database containing only templates related to high quality images. In this way the system accuracy is increased and the FAR and FRR both decrease, because are reduced the verification error possibility. Having a low quality threshold, allows to have templates related to poor quality images, increasing the possibility to have false positive and false negative results.

Due to quality (FTE, FTC) and accuracy (FAR, FRR) factors dependency, it is important define a unique threshold value, which has the capability to summarise Biometric Systems performances. This value is called ***Equal Error Rate (EER)***. ERR corresponds to the point on DET Curve where FAR and FRR are equal. Value lower than EER are related to more accurate systems.

It is also interesting note that low threshold values lead to maximize the FAR values, because also biometric data very different from original ones will be recognized as genuine, but minimize the FRR, because became very difficult to be not recognised. Otherwise high values of threshold leads to an high percentage of false negative, but also to a low percentage of false positive. A system with a high threshold is useful for the access to strictly reserved areas, where is better having a false rejection, when an unauthorised person that grants illegal access. Low threshold values can be useful for end-user systems, which grants access to the authorised person with an high rate is more important when data reservation.

Another value used to evaluate system performance is the so called ***d-prime (d')***. It measures the separation between the median values of genuine and impostor probability distributions, calculated in standard deviation units:

$$d' = \frac{\sqrt{2}\left|\mu_{genuine} - \mu_{impostor}\right|}{\sqrt{\sigma_{genuine}^2 - \sigma_{impostor}^2}}, \tag{1.3}$$

where μ and σ are the median and standard deviation values respectively. Higher values of d' indicates better performance systems, because the two distributions are more distant and only few cases can be misinterpreted by the system (i.e. few false acceptance and false rejections).

If the two distributions have a normalized Gaussian profile, with equal variance (this last hypothesis is not so common in biometric system), then $d'$is equal to the standard deviation [13].

Poh and Bengio have introduced [14] another value for measuring system performances, knows as F-ratio, and defined as:

$$F - ratio = \frac{\mu_{genuine} - \mu_{impostor}}{\sigma_{genuine} - \sigma_{impostor}}, \tag{1.4}$$

If the two distributions are Gaussian-like, a relation exists between ERR and F-ratio:

$$EER = \frac{1}{2} - \frac{1}{2} erf\left(\frac{F - ratio}{\sqrt{2}}\right), \tag{1.5}$$

where

$$erf\ \ x\ \ = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt\ . \tag{1.6}$$

In Figure 1.3 classical individual distributions are shown, with highlighted also the ERR Threshold value and the d-prime distribution distance. In Figure 1.4 (a) are shown FAR and FRR distributions related to Threshold variation, with highlighted the related ERR. In In Figure 1.4 (b) the ROC curve of the same distributions is reported. It is possible notice has the ERR in the ROC curve is equal to the secondary diagonal.

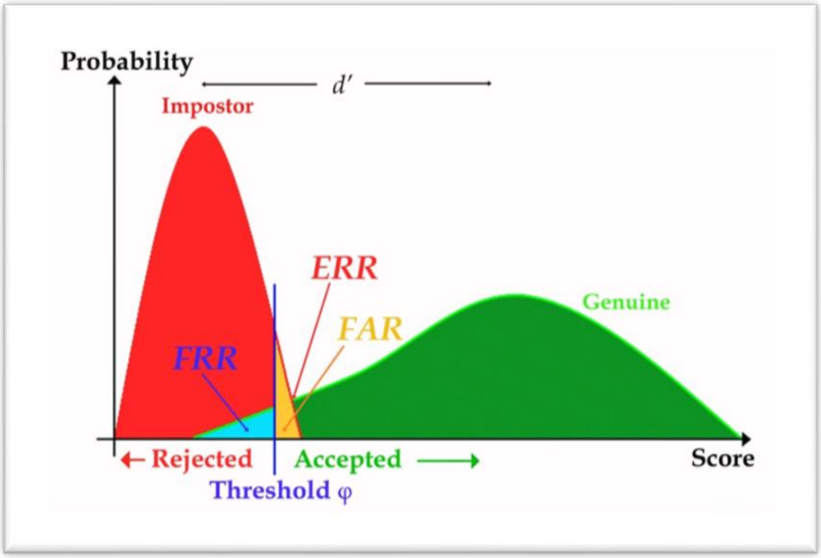


Figure 1.3 – Probability distributions for Impostors and Genuine Users. It has put in evidence that, given a threshold φ, it is possible to define the genuine users percentage refused by the system (FRR cyan area) and the percentage of impostor users which grant access to the system (FAR orange area). The intersection point between the two probability curves identifies the threshold value able to give the EER. Also d-prime (or d’) is clearly identified in this figure.

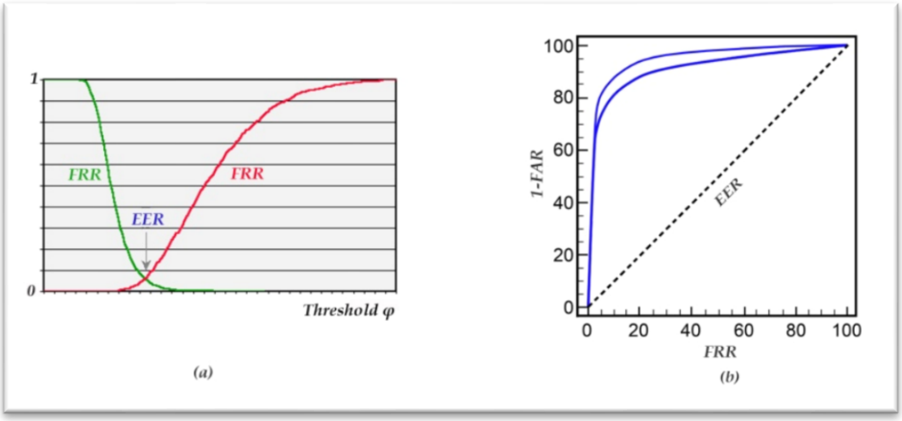


Figure 1.4 – In (a) FAR and FRR are shown at threshold φ varying. It has to be noted that the two curves intersection identifies the ERR, with the related φ_{EER} threshold value. In (b) the ROC curve related to the previous FAR and FRR curves is shown.

1.3.4 Identification Rate Rk

In case of identification, the acquired biometric dataset is compared with all the templates resident in the database, with the aim to determine the "***Best Match***". The best match can be determine comparing all the obtained matching scores and reporting only the best one, such as the most one related to the most similar data sets. The ***Identification Rate*** is the percentage of correct identification made by the system for a particular user. This analysis is made using the ***rank-k*** $\boldsymbol{R_K}$, which indicates the percentage of correct identification made by the system inside the range of maximum scores achieved, for the k-esim user. For better understanding if a particular user is correctly identified 100 times, and the maximum score range is between 96% and 100% of similitude, with a threshold of 90% of similitude, the rank-k will be not 100, but the number of times, among these 100, where the identification score was equal or greater than 96. SO, for example the rank.k in this case could be 20, indicating that only in the 20% of cases the identification has been made in the proper way. Greater the rank-k is, better the system works, for that user.

To define the performance of the system referring to all the k users, it is possible referring to the ***Cumulative Match Characteristic (CMC)*** curve, which represents the value R_k with k from 1 to M, where M is the number of users registered in the database [15].

Relation between CMC curves and ROC/DET curves has been widely described in literature by Grother and Phillips [16] and by Bolle and others [17].

1.4 Kinds of Biometric Systems

In the following chapters will be presented the main physical and behavioral biometrics. It has to be noted that, referring to the performance parameters reported in the previous, it is possible affirm that the perfect biometry does not exist. On other hands it is possible say that many of them can be considered acceptable.

1.4.1 Fingerprints

Fingerprints are used for person identification for more than a century. The capability to verify (identify) person using fingerprint images is very high [18].

A fingerprint can be reduced to a ridge and valley pattern presents on fingers' surface since the seventh month of pregnancy and no more modified by natural events for the rest of the person life.

Some studies have demonstrate also that any finger has a different pattern, also on the same person and also between twins [9].

Nowadays fingerprint scanners have a very low cost, allowing also normal people to use this solution to access their notebook or netbook.

The offered accuracy is suitable to use fingerprint systems in authentication and identification systems, also in case of forensic applications. In particular, multi-finger systems, which allow to acquire all the 10 fingers, grant a high level of uniqueness, also in complex identification cases. In addition, the high level of inter-class diversification, allows to use fingerprint not only as authentication method, but also as identification one.

1.4.2 Face

Face recognition is a non-invasive biometry and, face attributes are probably the more common biometric elements used by human being for person identification. Face recognition can be made using manned statistical approaches, till unmanned dynamic systems, typical of video-surveillance systems used to verify black-listed person inside dynamic crowd (e.g. airports).

The most popular approaches to face recognition are [19]:

- Determination of shape and position for face characteristics, such as eyes, nose, mouth, inter-pupillary distance, nose-mouth distance.
- Global face image analysis made on the basis of a normalized faces set (i.e. eigenfaces).

Face recognition systems performances are suitable, like fingerprint ones, for commercial purposes [20], even if are highly impacted by environmental (e.g. illumination) and acquisition factors (e.g. rotation, acquisition distance). It has to be noted that this biometric systems can have difficulties to check face images acquired with different angles.

A face recognition system, for working properly, have to automatically do the following steps:

1. Identify face presence inside a picture;

2. Localise face position, if present.
3. Recognise a face from a generic point of view, under any possible environmental conditions.

1.4.3 Hand Geometry

Hand biometry is based on acquisition of a set of geometric measures made on the hand itself, including also length and wide of each finger [21]. It is a very simple technique, not much evolved since its introduction and widely accepted as is. In addition it is not affected by environmental humidity problems or skin sweating.

In any case hand geometry it is documented as low distinctive and it is used exclusively for authentication and not identification purposes. Another limitation is that acquired information varies along time, in particular during growing age or for arthritis problems. Also rings of other objects present on the analysed hand can give an identification issue. Finally, acquiring sensors have great dimensions, limiting the usage on some particular objects like notebooks or tablets and smartphones.

1.4.4 Palmprint

Human palm contains a huge information usable for person identification, in a way similar to fingerprint one. In fact a ridges and valleys pattern can be identified on it. Due to the high acquisition area, it is envisaged to be more distinctive than fingerprint case [22].

Palmprint scanner have, similar to hand geometry, a problem due to the high area to be acquired, which limits the use of this biometry.

In any case this biometry, if added to the less distinctive hand geometry one, allows to overcome the limits of this last one. Some distinctive features can be acquired also using low resolution scanner, typical of hand geometry acquisition, improving authentication performance.

1.4.5 Iris

Iris is an eye annular region, enclosed b pupil and sclera (the eye white part). The iris visual texture is formed during foetus formation and is stabilised until the second year of life, even if, can change in the following years in relation to the iris pigment. Iris texture complexity allows to obtain an high distinctive biometry, usable both in authentication and identification phases [23].

Current iris biometric system accuracy and acquisition performance allow to use iris as large scale identification system, similarly with fingerprint biometric ones. In fact also in iris case two iris of twin subjects are different each other. In addition it is possible also identify the usage of contact lens with false iris superposition with liveness testing [24] based on the rapid unconscious iris dimension modification.

It has to be noted that, even if an iris biometric system has a FAR highly lower than other biometric ones, its FRR value is still too much high [25].

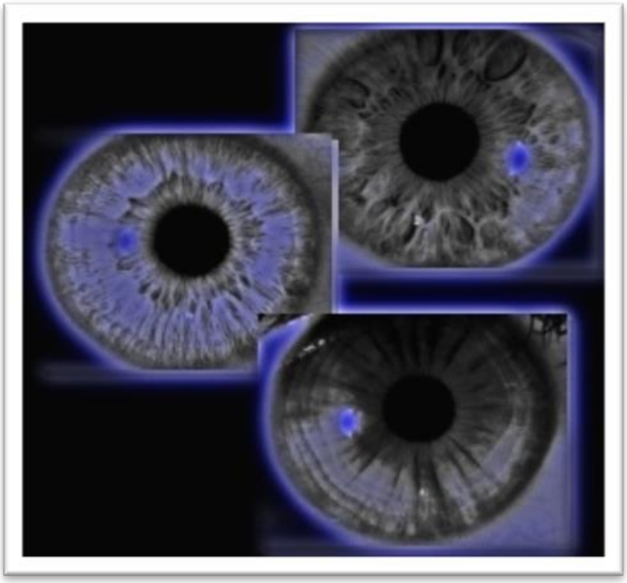


Figure 1.5 – Iris images acquired using different sensors. It has to be noted the detail of the high distinctive iris pattern.

1.4.6 Retina

Retina vascular structure is rich of information absolutely distinctive, able to characterize any human eye in a unique way. Retina biometry is the most secure, but also one of the most invasive.

Retina scan are based on vascular pattern acquisition by means of a ocular-shape system. This is the reason way this biometry is considered too much invasive and it is used only in particular (generally military) applications.

All the installed Retina scans have a false accept percentage equal to 0[4] [26].

The usage of these dispositive has the inconvenience to reveal also medial problems, such as hypertension, and so, for privacy matter, are not usable in civilian application.

1.4.7 Keystroke

The *"keystroke dynamic"* is based on the concept that any person has a proper keystroke style, characterised by speed, delay intervals, pressure value associated to any single key. This biometry has not been introduced with the aim to be highly distinctive, but for identity verification with a low number of false rejection [27].

This biometry is the first not-physical biometry, because the keystroke dynamic is highly influenced by personal habit modifications. It is possible verifying the presence of high intra-class variations, due to emotional motivations, or keyboard different position.

This biometry has the advantage, respect with the other ones, to be monitored also after identification completion, adding another security level to an access made, for example, using classical fingerprint methods.

1.4.8 Signature

The signature apposition method is universally recognised as characteristic and distinctive [28-30]. Even if this biometry requires the contact with a writing media

[4] Even if the false negative currently registered is a not-known value [26].

and the user participation (i.e. active biometry), it has recognised as authentication method both at legal and government level.

Using PDA and graphic tablets, it is possible verifying in real time the signature authenticity, using the pressure profile dynamic. It is also possible to verify signature off-line, with the aim to verify a transaction or an individual identity in a second time after signature apposition [30].

Also this one is considered a behavioural biometry, due to the fact that signature tends to modify itself during life or due to the used writing media, attitude, physical or mental status.

1.4.9 Voice

The voice is a combination of physical and behavioural characteristics [31]. Physical characteristics are based on shape and dimension of speaking appendixes, such as lips, throat, vocal chords, nose cavity, all simultaneously used to generate sounds. Those characteristics are invariant in a single person, but behavioural and emotional aspects can deeply change also during the same speech.

In addition, voice is considered not extremely distinctive, and so not usable in large scale identification systems.

A biometric speech recognition system is based on the lecture of a predetermined phrase, used during Enrollment phase, or in a free identification.

This last one is obviously more difficult to achieve, but it results more robust against frauds.

The principal disadvantage of this system is the high sensitivity to background noise. For this reason it is widely used in phone recognition systems, even if the limited bandwidth reduce the distinctness.

1.4.10 Gait

Gait biometry is related to the walking way of a person and is one f the few usable for distant biometry recognition. It is for this reason widely used in video surveillance systems.

Due to the high changeability of the acquired gait, a lot of recognition algorithms exists, based on the definition of the person silhouette, with the aim to determine space-temporal features linked to the gait itself. For this reason is essential to have a good human body model.

Some algorithms are based on the extraction of dynamic variation of predetermined points, such as the alternation of right and left part of feet during the walking gesture [32].

This biometry is highly impacted by external factors, such as shoes, clothes, rheumatics disease, walking surface and so on.

1.4.11 Biometry Comparison

The Table 1.1 summarizes some consideration reported on the previous sections, highlighting the main characteristics of each technique, both from a technical and a social point of view. In fact not all the biometric approaches reported here have the same level of acceptability from the final user. It has to be noted that not all the existing biometry have been reported in the previous sections and also not all are reported in the following Table 1.1, due to the growing interested in biometry, which leads to research new approach every day.

Table 1.1 – Comparison among main biometry. The related characteristic level is indicated with char H (High), M (Medium), and L (Low), based on American standard scale for biometric system evaluation.

Indicatore Biometrico	**Universalità**	**Distintività**	**Permanenza**	**Collezionabilità**	**Prestazioni**	**Accettabilità**	**Circonvenzione**
Impronte Digitali	M	H	H	M	H	M	M
Volto	H	L	M	H	L	H	H
Iride	H	H	H	M	H	L	L
Retina	H	H	M	L	H	L	L
Geometria della Mano	M	M	M	H	M	M	M
Palmprint	M	H	H	M	H	M	M
Andatura	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Firma	L	L	L	H	L	H	H
Voce	M	L	L	M	L	H	H
Orecchio	M	M	H	M	M	H	M
Pattern venoso della mano	M	M	M	M	M	M	L
Termografia del Volto	H	H	L	H	M	H	L
DNA	H	H	H	L	H	L	L
Odore	H	H	H	L	L	M	L

In Table 1.2 are reported FAR and FRR values for some of the previous discussed biometric approaches, referred to official testing databases, and stressing test conditions.

Table 1.2 – In this table FAR and FRR results for the most used biometry, fingerprint, face, and iris, are reported. The evaluated accuracy is function of some factors: sensor characteristics, used acquisition protocol, environmental conditions, subjects number, number or acquired samples for each subject, subject habits, time between each acquisition and so on.

Caratteristica Biometrica	***Test***	***Condizione di Test***	***FRR***	***FAR***
Impronte Digitali	FVC 2004 [33]	Distorsione esagerata della pelle, rotazione	2%	2%
Impronte Digitali	FpVTE 2003 [18]	Dati operative governativi US	0.1%	1%
Volto	FRVT 2002 [20]	Variazione della luce, outdoor/indoor, tempo	10%	1%
Voce	NIST 2004 [34]	Contesto independente, multilingua	5-10%	2-5%
Iride	ITIRT 2005 [25]	Condizioni ambientali indoor, accessi multipli	0.99%	0.94%

As it is simple to demonstrate analysing the previous Table 1.1 and Table 1.2, it is not always true that the most secure and reliable biometric solution is also the most accepted by common users. A classic example is the retina biometry, which offers the highest levels of distinctiveness and universality, but the lowest value of acceptability, due to its invasive acquisition method. On the other hands, DNA has an accuracy level similar to the retina one, but it is heavily limited in collectability.

In conclusion it is possible assert that does not exists the “perfect biometry”, usable in any possible circumstance. Sometimes, the best solution, in particular situation, could be a combination of two or more biometry (e.g. fingerprint, palmprint and face).

1.5 Biometric paradigm applied to lifeless matter

The traditional methods for establishing the authenticity of documents, credit card, banknotes, packaging and high value products rely on secret identifiers or on manufacturing process which is difficult to reproduce. Typical examples are holograms, bar code, RFID, security paper, intaglio printing, etc. However difficult to reproduce, it is never equal to impossible to reproduce: "*what one man can make, another can copy*" [39]. Note that traditional RFIDs with encoded digital information could be easily replicated and thus, are not capable of resolving the problem or tag authenticity [40, 41].

On the contrary, the modern technologies used for person's identification are based on non-reproducible physiological or behavioural characteristics. In other words, a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, retina and iris patterns, voice waves, DNA, signatures, etc.; this approach is called biometric authentication [42].

Biometric authentication is based on the acquisition of specific human characteristics, to be used to create an identification/verification template (feature vector), as described in the previous sections. This template is compared with one extracted during verification phase for determining if a human being is whom he claims to be. Obviously, due to difficulties to acquire in different phases, and with different acquisition systems, the "identical" features pattern, a thresholded verification method is envisaged. The threshold, in biometric system, is essential, due to the fact that it deeply influences the system reliability.

Since the biometric identification has given excellent results, it comes naturally to apply similar criteria to uniquely identify “lifeless matter”.

Analysing the previous sections, it is clear that, any biometry, independently from its nature, both physical and behavioural, are characterised by common features, below-summarized:

- Identification of one or more features having the property to be able to uniquely identify a person. These features have to be some additional properties, such as collectability, persistence and so on.
- Creation of a vector biometric template to be used in verification phase, on the basis of the extracted feature.
- Check made using a predefined threshold between acquired template and extracted one
- Use of encryption systems to maintain in a secure way the biometric template database.

If we analyse common use object, such as banknotes, it is possible noting that exist also in this case some characteristics, which can be assimilated to the one identified in human biometric paradigm. For example, banknotes shows, under ultraviolet light, to have metallic security fibre s inside them, having different colours, shapes and positions. These fibre s are put inside paper pulp during banknotes paper preparation; in this way any banknote has a different fibre s set, in number, position and dimension. This distribution can be considered similar to fingerprint minutiae one. In this way it is possible think to apply a method similar to the fingerprint one, and to biometry in general, also to banknotes, to tell part one to another one, on the basis of their intrinsic characteristic. This approach allows also to determine banknotes authenticity, due to the fact that a counterfeited banknote has to have a fibre s distribution identical to the original one for using the same template. If we encrypt the template, using a PKI approach, it is also impossible to extract it from an original banknote and using on a counterfeited one. The following Figure 1.6 shows this feature distribution, in a twenty euros banknote under ultraviolet illumination. Security fibre s result to be fluorescent in visible spectrum under this kind of illumination.

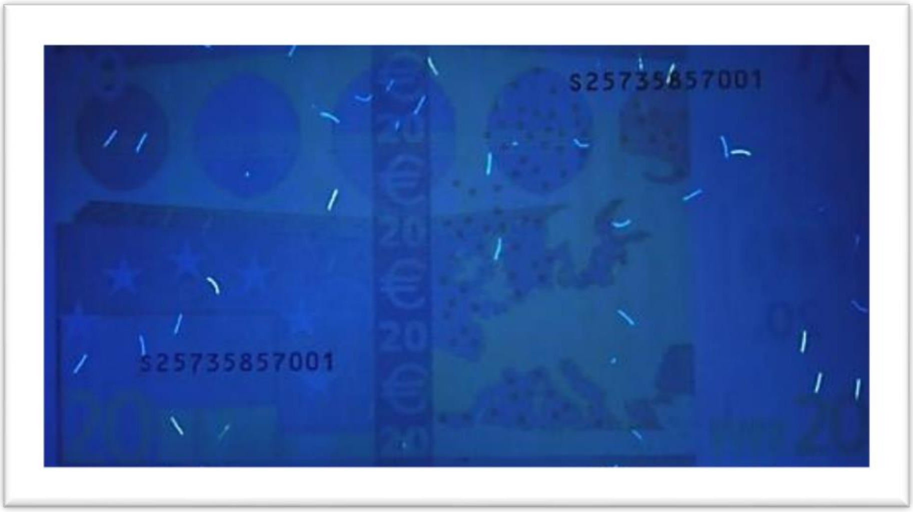


Figure 1.6 – Banknote image acquired under ultraviolet illumination. It has simple to notice the random security metallic fibre s distribution inside the image.

As for biometric authentication, it is possible to coin a word in order to identify this new method of authentication of nonliving matter. The term Biometrics derives from two Greek words: βιος (bios) “life” and μετρον (metron) “measurement”; so it is possible to literally translate Biometrics in “life measurement”. For Aristotle the term $\breve{\upsilon}\lambda\eta$ (hyle) meant nonliving matter [35]; therefore, the Hylemetric authentication may identify the procedure for the identification of inanimate objects.

Any pattern made with a specified design can be duplicate using an identical technology. On the contrary, every pattern produced by random processes is an irreproducible characteristic that can be used in Hylemetric identification [43-45]. There are a large number of applications that could benefit from the ability to uniquely identify inanimate objects. Currency, ticket, and art counterfeit detection, as well as verification of product are some of application where authentication of inanimate objects is desirable.

In biometric authentication the sampled characteristic should have the following properties:

- ***Universality:*** all the person should have the characteristic;
- ***Permanence:*** the characteristic should not vary over time;
- ***Distinctiveness:*** samples corresponding to different persons should be as different as possible, that is, the inter-class variability should be as large as possible;
- ***Robustness***: samples corresponding to the same person should be as close as possible, that is, the intra-class variability should be as small as possible;

- ***Accessibility***: the sample should be easy to present to the acquisition device;
- ***Acceptability***: it should be perceived as nonintrusive by the user;
- ***Hardness to circumvention***: it should be hard for an impostor to fool the system.

Similar proprieties must to be found in characteristics to be used for authenticating the inanimate objects (Hylemetric authentication). In particular, in Hylemetric authentication the sampled characteristic should have the following properties [36, 46]:

- ***Uniqueness***: every objects should be identifiable and distinguishable from all others;
- ***Consistency***: feature vector should be verifiable by multiple parties over the lifetime of the object;
- ***Conciseness***: feature vector should be short and easily computable;
- ***Robustness***: it should be possible to verify the feature vector even if the object has been subjected to harsh treatment;
- ***Resistance to Forgery***: it should be very difficult and costly, or impossible for an adversary, to forge a document by coercing a second object to express the same feature vector as the original one.

Each texture that is highly random and difficult/impossible to reproduce can be potentially used as Hylemetric characteristic. Obviously, good Hylemetric characteristics have to satisfy the following additional requirements:

- it has to be simple repeatable and reliable to implement the feature vector (template);
- the cost of creating and signing the feature vector has to be small, in relation with a desired level of security;
- the cost of exact or near-exact replication of the unique and random physical structure used as Hylemetric characteristic has to be greater of the value of the object under forgery;
- the cost of verifying the authenticity of a signed feature vector has to be small, if compared with a desired level of security.

Chapter 2 State of the Art

2.1 INTRODUCTION 72

2.1.1 OVERT (OR DIRECT) SECURITY 73

2.1.2 COVERT (OR INDIRECT) SECURITY 74

2.2 BANKNOTE AND DOCUMENT SECURITY SOLUTION 74

2.2.1 PAPER WATERMARKING 76

2.2.2 SECURITY PRINTING 79

2.2.2.1 Intaglio Printing - Latent Image Effect 79

2.2.2.2 Letterpress 81

2.2.2.3 Guilloches 83

2.2.2.4 Rainbow printing 83

2.2.2.5 Printing Ink with Optically Variable Characteristics 84

2.2.2.6 Microprint 86

2.2.2.7 UV-Print 86

2.2.2.8 See-Through Register 87

2.2.2.9 Digital Security Print in a Photograph 88

2.2.3 PERFORATION 89

2.2.3.1 Mechanical Perforation and Laser Perforation 89

2.2.3.2 Micro-Perforation 90

2.2.3.3 Perforated Picture 91

2.2.4 DIFFRACTIVE SECURITY ELEMENTS 91

2.2.4.1 Holographic Elements 92

2.2.4.2 Kinegram® 94

2.2.5 SECURITY ELEMENTS INSERTION 95

2.3 ARTWORKS SECURITY 96

2.4 DRUG PACKAGE SECURITY FEATURES 98

2.4.1 OVERT (OR DIRECT) SECURITY SOLUTIONS 100

2.4.1.1 Holograms 101

2.4.1.2 Colour-Shift Inks 102

2.4.1.3 Barcoding 103

2.4.1.4 Radio Frequency Identification (RFId) 104

2.4.2 COVERT OR INDIRECT SECURITY SOLUTIONS 105

2.4.2.1 UV Inks and Print 105

2.4.2.2 Colour and UV Micro-text Print 106

2.4.2.3 Taggant Authentication 107

2.4.2.4 Laser Surface Authentication – LSA 108

2.4.2.5 Physical Unclonable Function – PUF 109

2.4.3 COMBINING OVERT AND COVERT TECHNOLOGIES 110

2.1 Introduction

High value object security has an important impact in the security countermeasure field from a long time. A typical example is banknote, which, for their intrinsic value, are characterised by a very high number of security and anti-counterfeiting measures. Other examples are artworks, counterfeited since ancient history. In this last case a classic security method is adopted: the certificate of authenticity, issued by a certified expert. Lithography, sculptures, pictures in general are all sold with a paper-made certificate of authenticity. Also gems, such as diamonds, have implemented this solution to the originality issue.

In the following a panoramic of the state of the art of anti-counterfeiting systems applied to lifeless object of particular intrinsic value is reported. Then the study point out on two important family of objects security methods: banknotes and pharmaceutical packaging.

2.1.1 Overt (or direct) Security

Overt features enable instant authentication of packaging through visual inspection by the user without requiring expert knowledge. Optically variable features such as holographic devices within the design and colour shift inks are the most common and effective overt security features, enabling packaging to be validated both quickly and easily. Another case is the certificate of authenticity issued with artworks, to state the originality of the related object of art.

Some solution, considered at first sight as overt, are in reality mixed, such as barcode, because its only presence does not grant the originality of the object. In fact a common person cannot decipher the barcode content without an appropriate instrument. On the other hand, the visibility of one and two dimensional barcode does not allow to include then into covert solution.

Another typical overt solution are banknotes or drug packages holograms, which grant object authenticity with their only presence.

2.1.2 Covert (or indirect) Security

In some cases, for example banknotes and drug packages, it is possible to use an increased security solution, by the introduction of covert and forensic features. Covert techniques such as infrared (IR) and Ultraviolet (UV) pigments, micro-text and microscopic tagging are invisible, and they are difficult to detect and replicate without specialist detection equipment. The first level of security is the impossibility to view at human sight. The second level consist of protecting methods after covert solution has been discovered, to avoid its copy. Examples are banknote security fibre s, visible only under ultraviolet illumination only, or chemical tracer.

Forensic solutions include molecular markers and biological tracers. These features can only be identified using laboratory equipment, offering complete confidence in packaging authentication. In addition Laser Surface Authentication has arisen as an interesting solution for authenticating drug packaging using a biometric-like approach, based on package surface characteristics [45, 48, 50].

2.2 Banknote and Document Security Solution

Identity document and banknote counterfeiting is a market which, differently from the “canonical” markets, never goes in crisis. Banknotes counterfeiting is a centuries-old reality, as identity document one. This two situation go head-to-head for some simply reasons [37]:

- Both have an high value for the parallel market controlled by criminals.

- Both are object of advanced security solution application.
- Counterfeiting solutions to bypass security ones are very often applicable to both the situations.

Counterfeiting makes any year great technological steps in advance, head-to-head with security innovation introduced to contrast it. Now faking expertise is changed from artistic to high technology.

Document and banknote faking can be divided into six different categories; some are interesting for this study, in particular the last two:

- **Improper Document Use** (***Imposter***): in this case, we are dealing with a real, uncorrupted document. The person using the document to identify himself is, however, not the proper holder. The person often looks similar to the official document holder (compare holder's picture, holder's description).
- **Counterfeit Document** (***Complete Forgery***): a counterfeit document is forged in all parts. The model for the production of the forged document is usually an authentic document.
- **Fantasy Product**: this is a document of a nation, for ex., which no longer exists or a document void of any identifying/legit imaging character (i.e. “World Service Authority Passport”). Other kind of documents, such as securities, may also appear as fantasy products.
- **Falsification** (***Content Forgery***): this is a real document on which unauthorized manipulations were done. Often official entries are erased or

partially/totally replaced by secondary entries. In personal documents, it is often the picture that is replaced.

- **Blank Document Forgery**: in a blank forgery the original material of a real document is used. The content entries, however, were not made by a proper authority. Blank documents are usually obtained in a burglary.
- **Fraudulently Obtained Document**: applicants try to obtain a genuine document, using forged documents or documents not rightfully theirs, and/or not correctly filled-in application forms. This mostly occurs when the applicant presents a false identity and/or has not fulfilled certain requirements (i.e. fraudulently obtaining a genuine driver's license by using a forged personal document).

Al fine di effettuare una panoramica completa sulle soluzioni ad oggi disponibili per proteggere documenti e le banconote dalle possibili falsificazioni.

2.2.1 Paper Watermarking

With the aim to protect a paper document (i.e. both document and/or banknote), the first step consist in protecting the document support, such as the paper itself. A possible technique is the so called paper watermarking, implemented by means of particular images or writings.

The watermark is a characteristic manufacturing feature of high quality paper. It can take the form of a portrait, drawing, signet, which is created on the wire of the paper machine during production. It is identifiable as a series of shadow and chiaroscuro areas, viewable when the object is illuminated in reflection or transmission [38].

We can differentiate:

- Light watermarks (light or negative watermarks)
- Shadow watermarks (shaded or positive watermarks)
- Duo-tone watermarks (combination of light and shadow watermarks)
- Halftone watermarks (half-shadowed or portrait watermarks)

False or so-called “Molette” watermarks (not to be confused with forgeries) are made by impressing the finished, still damp paper with a mould called a Molette roller.

Two principal methods for creating paper watermarks exists:

- Dandy roll process
- Mould cylinder technology

Due to the high complexity of both the processes, there are applied only to high quality paper.

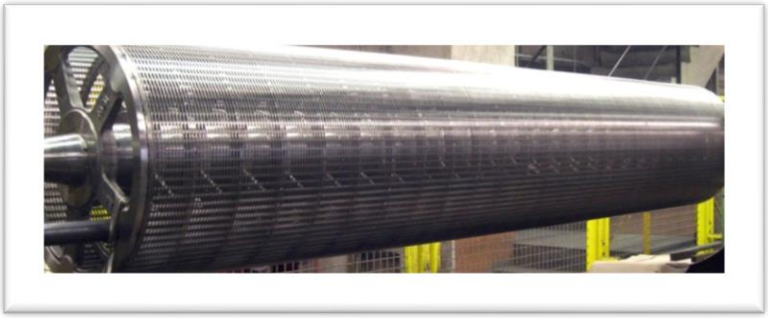


Figure 2.1 – Modern dandy roll example used for printing watermarks on paper in light way.

Light, shadow and duo-tone watermarks are created by enriching (shadow watermarks) or displacing (light watermarks) pulp fibre s on the wire belt section of the paper machine, on which a watermark-building “egoutteur” (dandy roll) is found. Half-tone watermarks are made using cylinder mould technology, in which the watermark-producing motif is found directly on the cylinder mould.

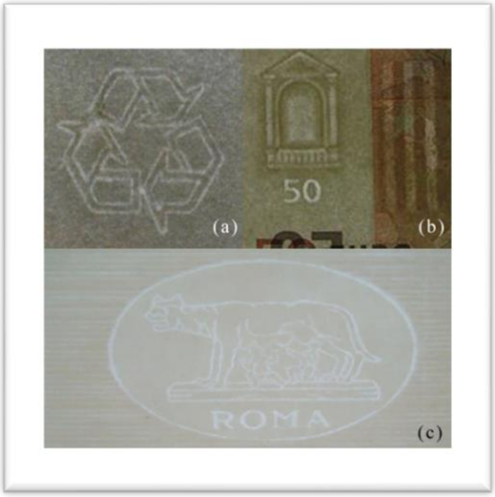


Figure 2.2 – Paper watermarking examples. In particular in (b) 50 Euro banknote watermark is reported.

2.2.2 Security Printing

Another method family, widely used for protecting documents and banknotes are based on different printing techniques. In the following a brief review of these methods is reported, with an highlight on the intrinsic security offered and the indication of the typology (i.e. overt or covert).

2.2.2.1 Intaglio Printing - Latent Image Effect

Intaglio print, also known as relief print, is an exclusive method reserved for security printing. In the printing mould, the printed areas lie lower than the non-printed areas. Characteristics of this printing technique are: the raised, tactilely-perceptible ink coating (relief structure) and the reproduction of finest details (i.e. microprint), which are perceptible in the whole print.

The three-dimensional structure of intaglio print can be used to conceal a message (i.e. word or logo) that is only readable from a specific direction. When the document is held towards the light at an oblique angle, it is possible to read such latent images (also known as tilt effect). This allows to categorize this method as an overt one.

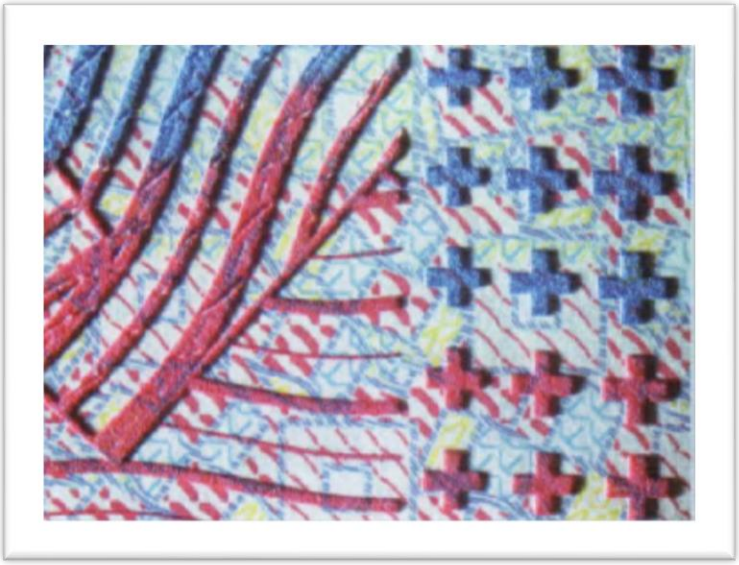


Figure 2.3 – Example of intaglio printing shows a clearly visible and physically perceptible ink coating.

In some cases it is possible using the intaglio printing as a covert technique. In fact it is possible using a specific design, which allows the intaglio image to be viewed only under a predetermined angle, and to be hidden in all the other ones, as shown in Figure 2.4.

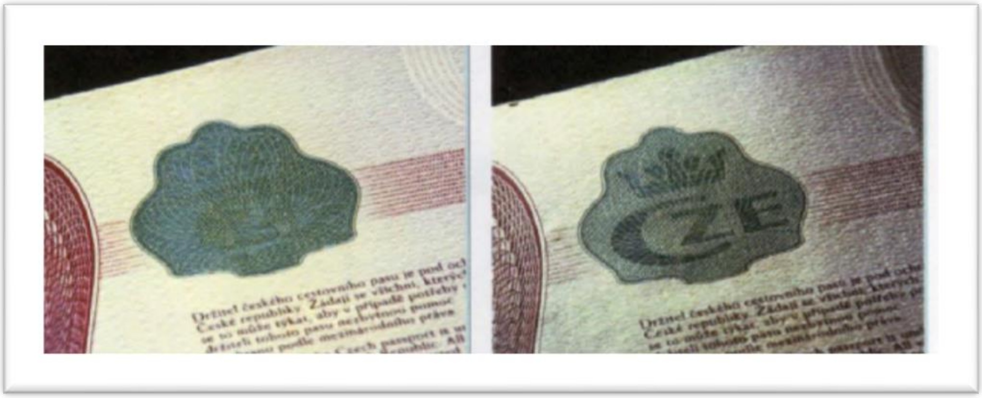


Figure 2.4 – The use of a corresponding design in association with intaglio print allows the printing and, as a result, the detection of a picture or text, which would otherwise remain hidden (latent image/ tilt effect in a Czech Republic passport).

2.2.2.2 Letterpress

Personal documents, securities, bank notes and other documents in danger of being forged are most often individualized by being given form numbers. These numbers are normally affixed using a numbering machine. The number stamp used automatically shifts after each number entry. Numbers which are affixed through the use of such an apparatus display the typical letterpress characteristics, such as dot fringes (squashed edges and additional ink at the number margins) and/or a slight embossed indentation. An example of the used apparatus is shown in Figure 2.5, where in Figure 2.6 the typical letterpress result is shown.

This is also known as direct book printing method.

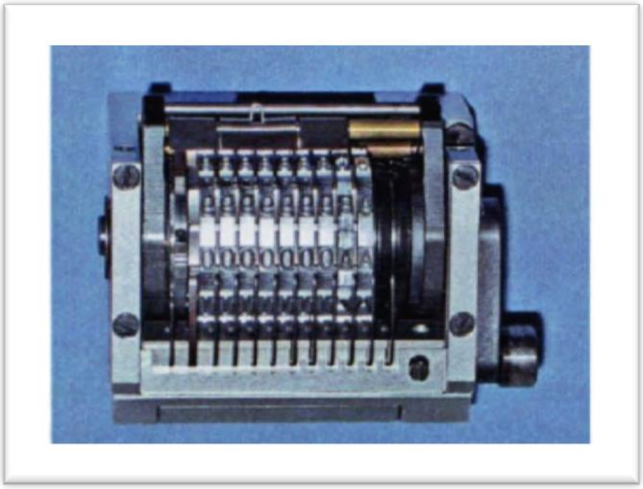


Figure 2.5 – Picture of a “Novel” numbering box.

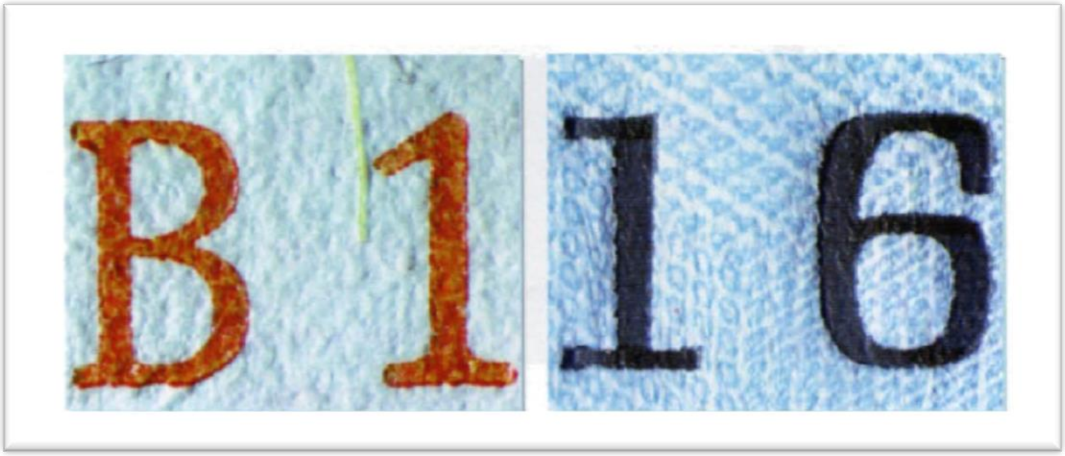


Figure 2.6 – Typical letterpress characteristics are dot fringes (left) and/or the relief-like impression in the paper (right).

2.2.2.3 *Guilloches*

Guilloches are fine, intertwined geometric line patterns or ornaments. Guilloches are usually printed in at least two colours in order to protect banknotes, securities and personal documents from reproduction. An example is reported in Figure 2.7.

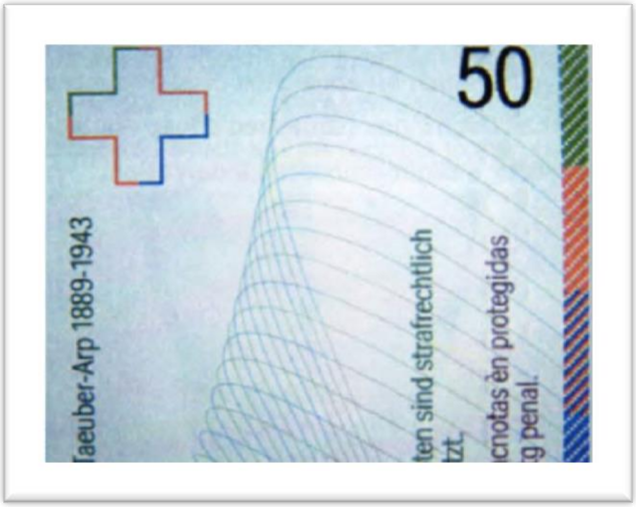


Figure 2.7 – Guilloches on a Swiss banknote.

2.2.2.4 *Rainbow printing*

This print with flowing colour changes is produced in a single printing step. In order to achieve this, the printing machine or the colouring apparatus, respectively, requires a special attachment. In following Figure 2.8 is shown a typical rainbow printing for Republic of Ghana banknotes.

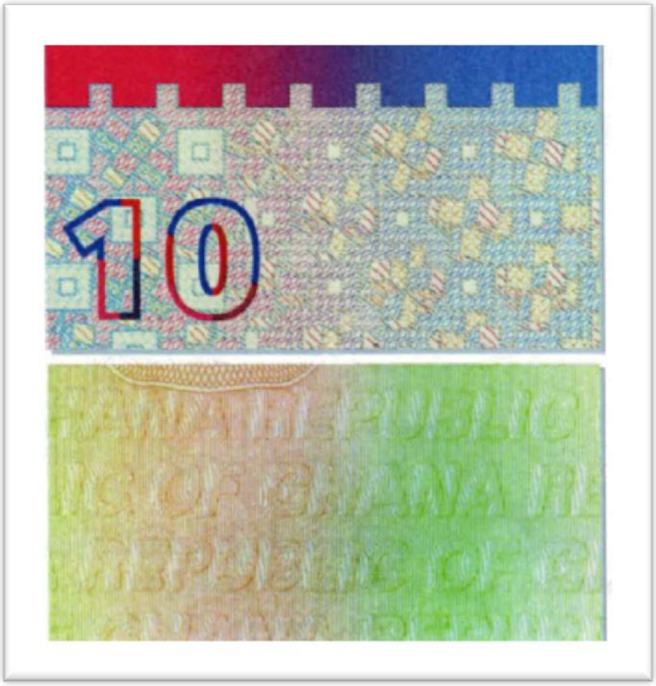


Figure 2.8 – Rainbow print allows a smooth transition of colours.

2.2.2.5 Printing Ink with Optically Variable Characteristics

These are special printing colours not readily available for public purchase, like, i.e. OVI® (optically variable ink) or SicpaStar® which have a defined, clear colour-change. The colour effect of the printed subject can be detected when the angle of the incoming light is varied by tilting the document, as shown in Figure 2.9.

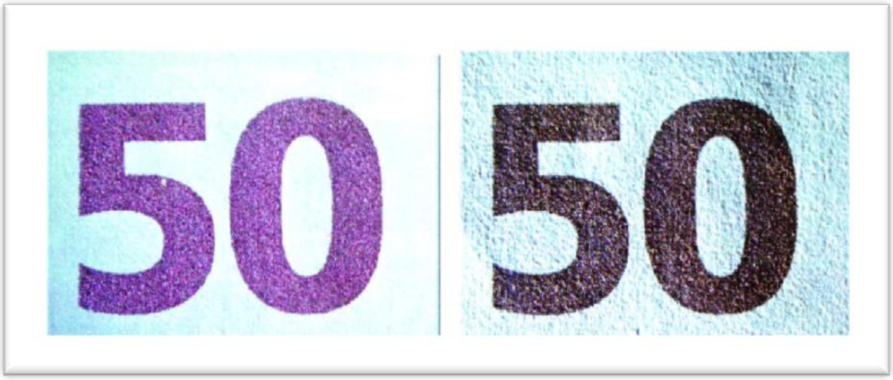
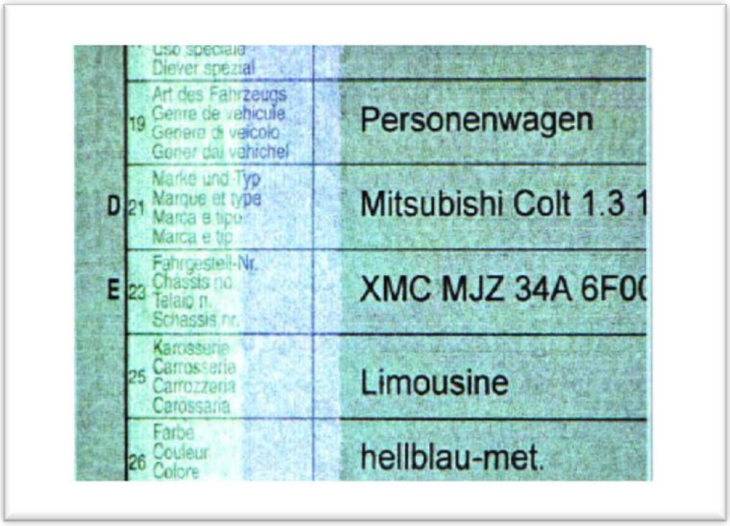


Figure 2.9 – The €50 banknote's denomination figure, printed in OVJ® ink, reflects different colours depending on the angle of the oblique light.

A further security element often used, having optically variable characteristics, is the "iridescent print" (Irisafe®), shows in following Figure 2.10.



		Uso speciale Diever spezial	
	19	Art des Fahrzeugs Genre de vehicule Genere di veicolo Gener dal vehichel	Personenwagen
D	21	Marke und Typ Marque et type Marca e tipo Marca e tip	Mitsubishi Colt 1.3 1
E	23	Fahrgestell-Nr. Chassis no Telaio n. Schassis nr.	XMC MJZ 34A 6F0(
	25	Karosserie Carrosserie Carrozzeria Carossaria	Limousine
	26	Farbe Couleur Colore	hellblau-met.

Figure 2.10 – Specific characteristic of Irisafe® is the pearly shine; seen here in an example of the Swiss Vehicle Registration document.

2.2.2.6 Microprint

These are very small characters (approx. 0.2 - 0.3 mm), which are only legible with the help of a magnifying glass. Microprint often takes the form of an endless text and is printed using intaglio, offset or letterpress methods.

Holographic elements (i.e. hologram or Kinegram®) also often possess microprints.

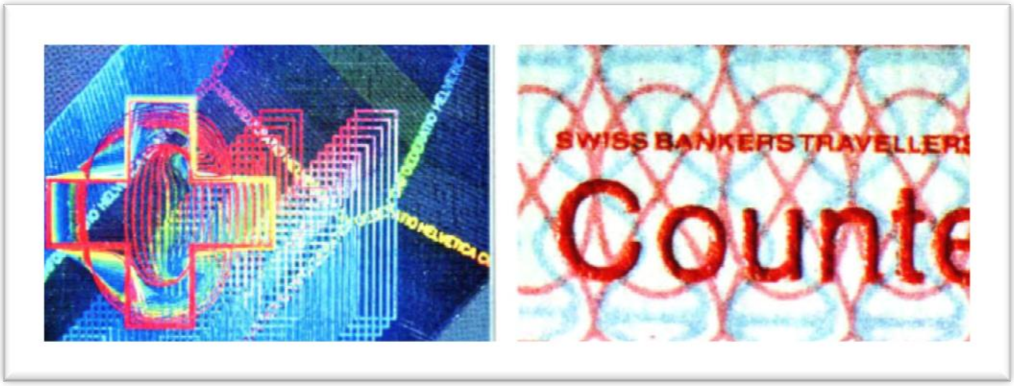


Figure 2.11 – Examples of a microprint in Kinegram® (left) and in intaglio print (right).

2.2.2.7 UV-Print

These are overprints made with special ink, which reveal fluorescing elements under UV-Iight (motifs, text, form numbers, etc.). One or more fluorescent colours can be used. The UV-ink colours used fluoresce in the light range of 254 and/or 366 nm.

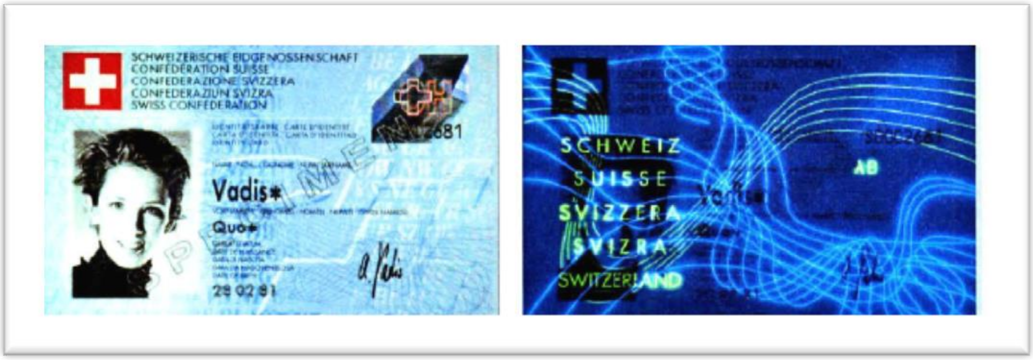


Figure 2.12 – The fluorescent overprint is often positioned over the biographical entries, to help recognition of spot manipulations. Here a photo of the Swiss ID card in daylight (left) and under UV-lighting (right).

2.2.2.8 See-Through Register

These are different parts of a subject or motif, which are printed and positioned on the front and back side of a document, so that they lie exactly over one-another and portray a whole motif when viewed under transmitted light. In order to print see-through registers with an exact fit, special printing machines must be used which simultaneously print all colours on the front and back side.

Figure 2.13 shows a typical example, used in Swiss personal identification cards.

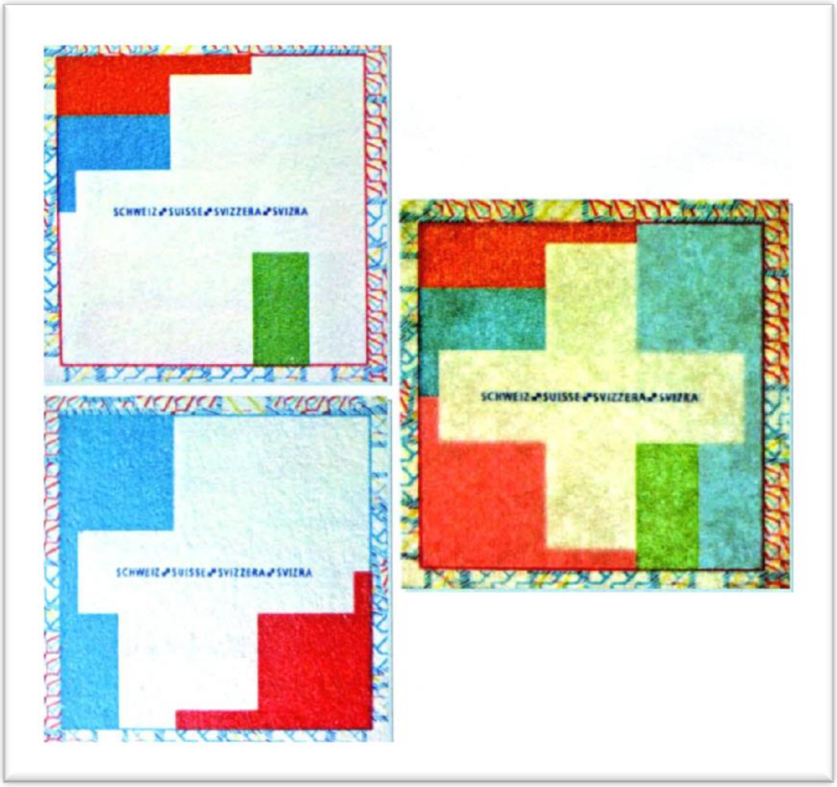
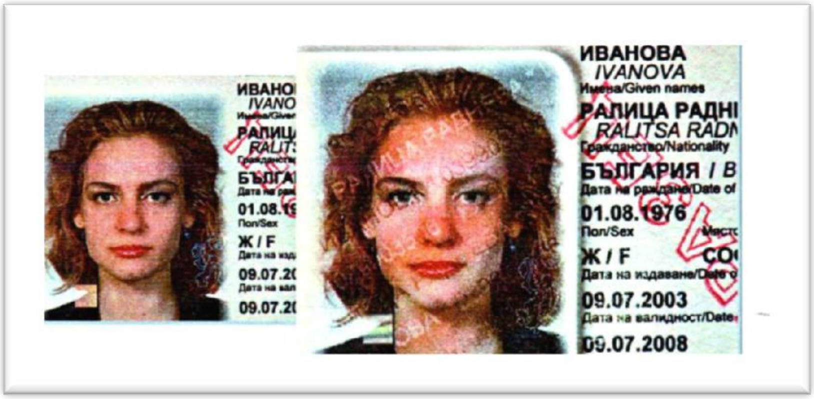

SCHWEIZ SUISSE SVIZZERA SVIZRA
SCHWEIZ SUISSE SVIZZERA SVIZRA
SCHWEIZ SUISSE SVIZZERA SVIZRA

Figure 2.13 – The front part of the subject under normal light (above left) is printed precisely over. The back side (below left) thus creating a whole motif. This is visible under transmitted light (right).

2.2.2.9 Digital Security Print in a Photograph

This security element is integrated into a digitally produced picture (i.e. Scrambled Indicia®, V.I.P.™, or Variable Information Personalization). This personalization uses laser engraving, ink jet and toner-based systems.

To verify the digital security print, a special decoding lens is necessary. This device is very difficult to come by and is therefore found almost exclusively at specialized inspection points. This allows to categorize this technique as covert one. In following Figure 2.14, the example related to Russia identification cards is reported.



ИВАНО
IVANO
Имена/Giver
РАЛИЦ
RALIT
Гражданств
БЪЛГА
Дата на ражд
01.08.19
Пол/Sex
Ж / F
Дата на изд
09.07.20
Дата на вал
09.07.20

ИВАНОВА
IVANOVA
Имена/Given names
РАЛИЦА РАДН
RALITSA RADN
Гражданство/Nationality
БЪЛГАРИЯ / B
Дата на раждане/Date of
01.08.1976
Пол/Sex
Място
Ж / F
СО
Дата на издаване/Date o
09.07.2003
Дата на валидност/Date
09.07.2008

Figure 2.14 – A special digital print allows data to be encoded into an image. Without the use of a special device, the information is not seen (left). Using a decoding lens, the information becomes visible (right)

2.2.3 Perforation

2.2.3.1 Mechanical Perforation and Laser Perforation

Form numbers in the form of perforations are used in passports and also in some other documents. We differentiate between mechanical perforation and laser perforation. Mechanical perforations are pierced or punched holes. The compressed margins of these perforations can be felt on one side of the paper.

Laser perforations are burnt into the paper. Characteristics of laser perforation

are burn marks (yellow-brown discolouration of the media in margins around the holes) .

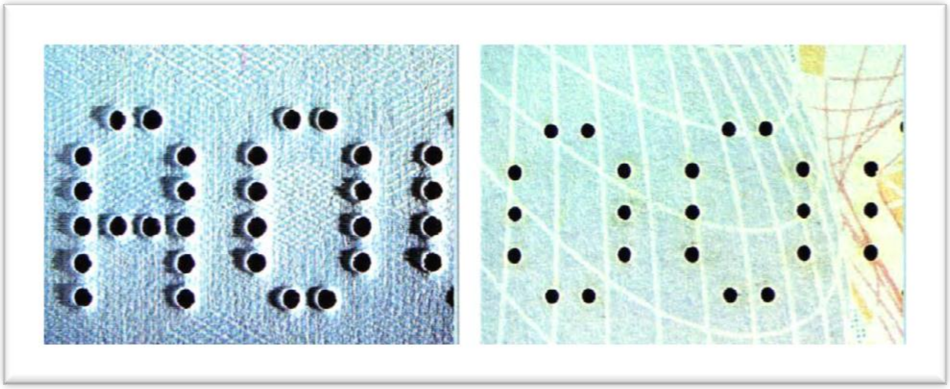


Figure 2.15 – The perforated numbers are punched out (left) or lasered (right) into the document in an exact pattern.

2.2.3.2 *Micro-Perforation*

A similar technique is the so-called *Micro-perforation* (i.e. MicroPerf™, DestriPerf™), which is based on a fine hole or line pattern, which is burned into the relevant paper by using a laser, has shown in Figure 2.16.

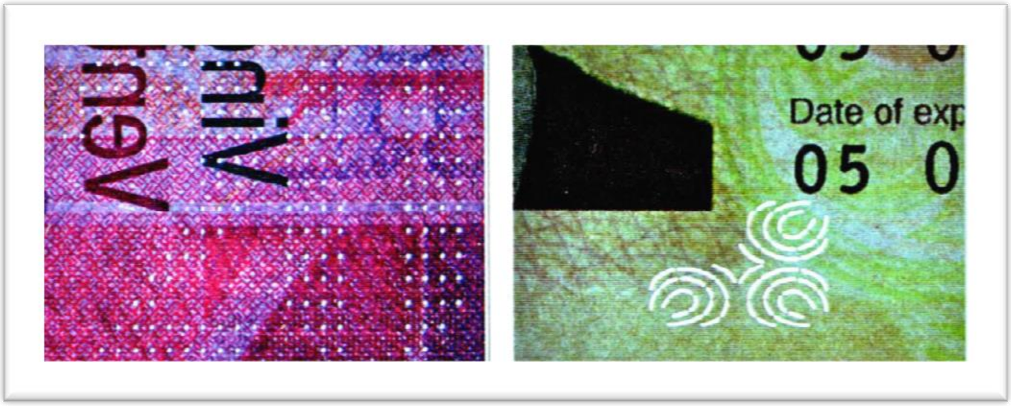
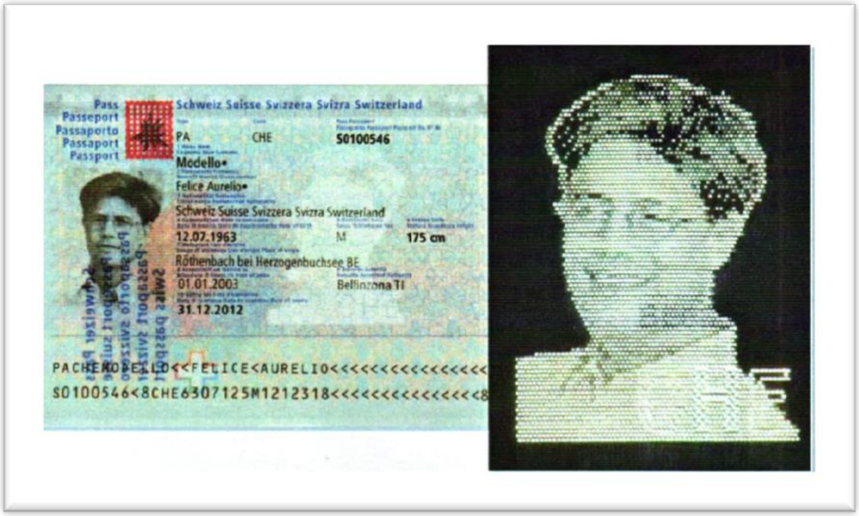


Figure 2.16 – Images of a Swiss banknote with MicroPerf^{TM} (left) and a British Passport with DestriPerf^{TM} (right) seen under transmitted light.

It has to be noted that this kind of perforation has the characteristic to be visible under transmission illumination.

2.2.3.3 *Perforated Picture*

The photograph of the document holder is perforated into the biographical page as a perforated image (ImagePerf^{TM}) with the use of a special laser. ImagePerf^{TM} must hereby correspond with the picture on the identification document, as shown in Figure 2.17.



Pass
Passeport
Passaporto
Passaport
Passport

Schweiz Suisse Svizzera Svizra Switzerland

PA CHE S0100546

Modello

Felice Aurelio

Schweiz Suisse Svizzera Svizra Switzerland

12.07.1963 M 175 cm

Röthenbach bei Herzogenbuchsee BE

01.01.2003 Bellinzona TI

31.12.2012

```
PACHEMODELLO<<FELICE<AURELIO<<<<<<<<<<<<<<<<
S0100546<8CHE6307125M1212318<<<<<<<<<<<<<<<8
```

Figure 2.17 – The *perforated image* is a very sophisticated security element which is simple to verify in transmitted light. The Swiss passport biographical page in an overview (left) and in a close-up of the ImagePerf^{TM} picture (right) .

2.2.4 Diffractive Security Elements

Diffractive elements, used as security features, introduce an high level of security, due to the intrinsic difficulties existing in counterfeiting this elements.

The typical, and most known, examples are holograms, present on a very large kind of products, such as banknotes, drug packages, passports, certificate of originality.

2.2.4.1 Holographic Elements

Hologram is the definition of a laser-made photographic shot (holography) which is a true, three-dimensional reproduction of the original picture. The white light hologram is a variation, which does not require laser-light for production. Compared to the "normal" hologram, the production is more complex. For this reason, it is used in forgery security on banknotes, credit cards, identity cards and similar documents.

Holograms are quite counterfeit-proof and are employed for the purpose of forgery prevention. It is not possible to duplicate them with any known copying technique.

In Figure 2.18 an image of 100 € banknote is shown, on which, under a different illumination angle, it is possible to view the appearance of the hologram.

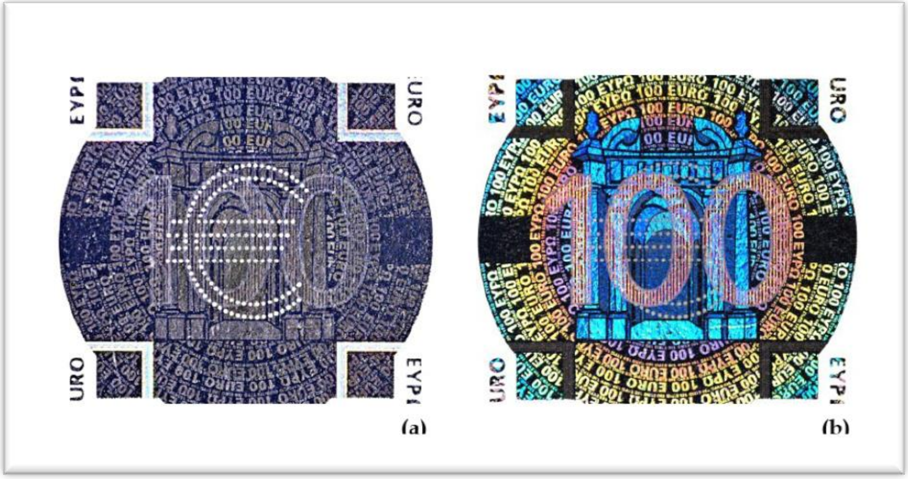


Figure 2.18 – Example of 100 € banknote hologram. (a) is the image of the banknote area and (b) is the same area with the hologram highlighted, after banknote illuminated with a different angle.

Another example of hologram applied to document security is the MasterCard solution, which shows an additional colour change under different angles of direct light illumination (see Figure 2.19).

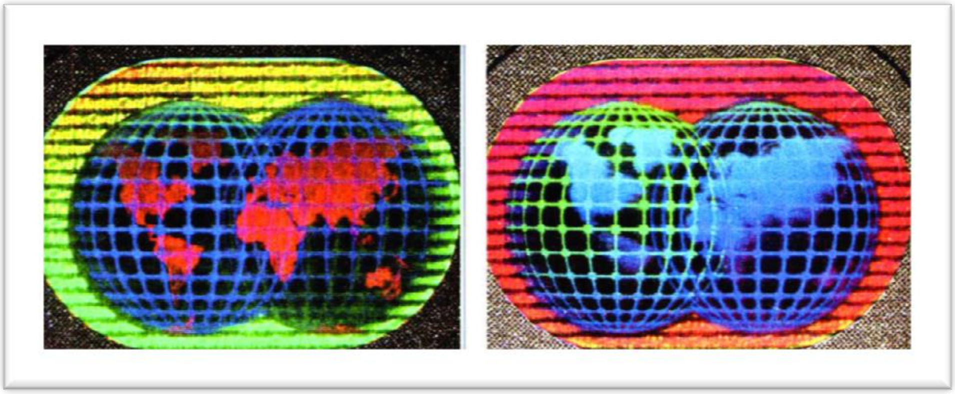


Figure 2.19 – Typical for the hologram is the subject's three-dimensional reproduction. The MasterCard example shows an additional colour change when the angle of direct light is varied.

2.2.4.2 Kinegram®

The Kinegram® contains a combination of different computer-generated micro-structures, which reflect incoming light in different, defined directions. A picture of moving structures and changing colours is seen when the angle of incoming light or viewing is changed. A Kinegram® does not give a three dimensional reproduction of a picture as is the case with the hologram.

Kinegrams are used exclusively to protect highly valuable documents (personal documents, banknotes, visas).

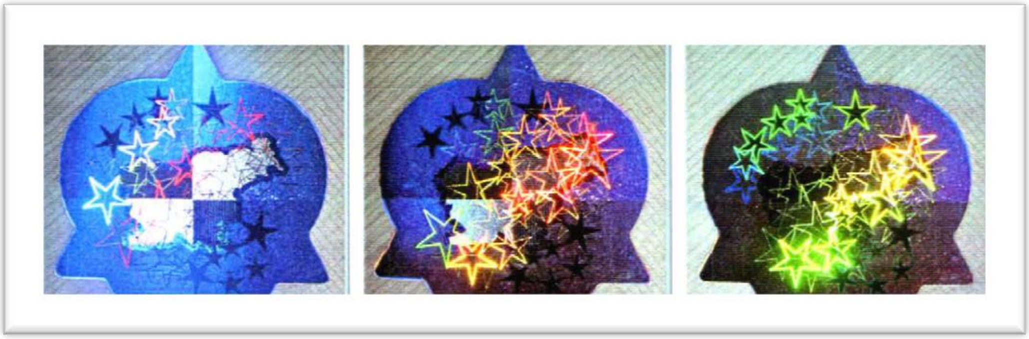


Figure 2.20 – Metallic Kinegram® in an example of the Slovenian passport.

In the following Figure 2.21, there is an example of a different kind of Kinegram® , present on Swiss passport, called *Trasparent Kinegram®*.

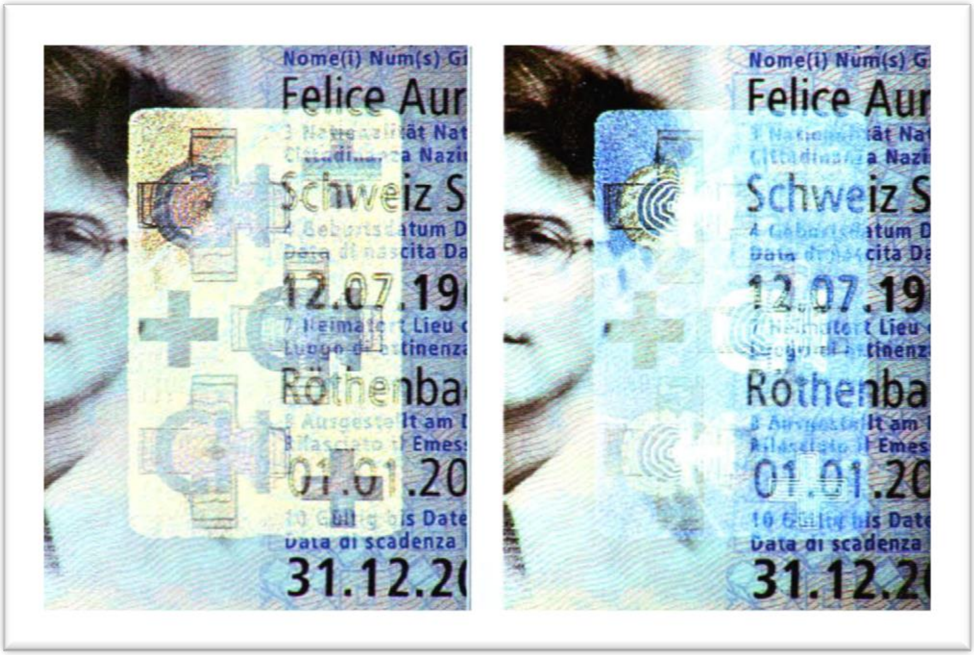


Figure 2.21 – By changing the angle of incident light or viewing, a two-dimensional picture of moving structures and changing colours can be depicted.

2.2.5 Security Elements insertion

Another method to protect documents to be counterfeited is the insertion directly inside paper support of security elements. The most famous method is the use of metallic security fibre s.

Security fibre s are mixed into the raw material mass (paper pulp) during paper production and are therefore found within the paper as well as on its surface. However, the fibre s of counterfeit documents are printed or manually imitated.

The authenticity of security fibre s is often detectable by simply using a magnifying glass.

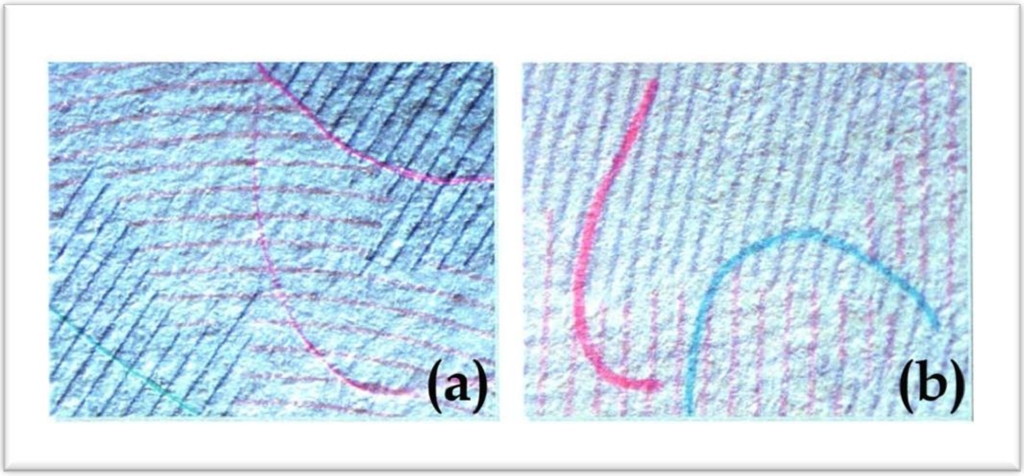


Figure 2.22 – The difference between real colour security fibre s in a Canadian passport (a) and imitations in the forgery (b) can be easily seen by using a magnifying glass.

2.3 Artworks Security

The main problem when we buy an artwork object consists in getting a certificate of authenticity, in particular for the artwork bought through a seller and not at first hand from artist.

There is a tremendous abuse in the “certificate of authenticity” business because, unless it is originated and signed directly by the artist, but by the publisher of the art (in the case of limited editions), a confirmed dealer or agent of the artist (not a third party or reseller), or an acknowledged expert on the artist, all those certificates are pretty much meaningless.

A legitimate one must contain specific details about the artwork, such as when and how it was produced, the names of people or companies involved in its production, dimensions, and the names of reference books or similar resources that contain either specific or related information about either that work of art and/or the artist. It should also state the qualifications and full contact information of the individual or entity that authored the certificate, and include his or her complete and current contact information.

Unfortunately, often these certificates are exchanged between similar artworks: the same document is supplied by the seller to certificate the originality of more than one single artwork. In this way the buyer could have a copy of an original certificate to attest that the “not original artwork” is, instead, an original one. Unfortunately, most people believe that art with a certificate is automatically genuine, but that’s not even close to truth [54]. It happens because does not exist a law rules who is (or is not) qualified to produce certificates of authenticity, or what types of statement, information or documentation a certificate of authenticity must contain. In other words, anyone can write a certificate whether they are qualified or not. As if that is not bad enough, unscrupulous sellers forge false certificates of authenticity and use them to either sell outright fakes or to misrepresent existing works of art as being more important or valuable than they actually are [55]. A possible fraud can be put the following way into effect: an art merchant, starting from an original lithography and its original certificate of authenticity, duplicates both and sells false artwork as genuine using false certificate of authenticity as clue of originality.

2.4 Drug Package Security Features

One of the more sensible counterfeiting object categories is pharmaceutics products, and the counterfeiting rate continues to increase. The global pharmaceutical supply chain is at growing risk from counterfeit drugs, which cost companies billions and endanger the health of patients. Currently, parallels markets that claim to offer the same pharmacological product at a lower price than the normal distribution channels are appearing. In many cases, the offered product is only a copy in packaging nearly identical to that of the authentic product. These copies have no real effect (or, in the worst case, have significant side effects). Secure packaging is an important factor in countering fake products. This requirement has led to the enforcement of stringent legislation to ensure that pharmaceutical packaging cannot be easily imitated. Through the usage of new anti-counterfeiting technology, pharmaceutical packaging manufacturers can easily produce secure packaging and fulfill the requirements of government policies. The World Health Organization (WHO) estimates that the global trade in counterfeit drugs is experiencing continuous growth [56], about 1% of prescribed drugs in the developed world and 30% in parts of the developing world can be fakes. The threat is even greater on the internet, where 50% of drugs bought on illegal online pharmacies are thought to be counterfeit.

As the forged trade grows and becomes more profitable, criminals are becoming increasingly sophisticated and capable in the way that they package their products. In addition to manufacturing fake drugs, counterfeiters are seeking to infiltrate the legal supply chain. This approach allows them to steal authentic shipments and redirect them to other markets, reselling them for their own profit. Another emerging threat to the security of the pharmaceutical supply chain is ‘third shift’ packaging production. This process involves contractors or their staff carrying out extra hidden production runs and selling the resulting genuine packaging to counterfeiters. As a result, global regulatory bodies have introduced strict legislation to ensure maximum security of pharmaceutical packaging. The WHO Expert Committee on Specifications for Pharmaceutical Preparations has stressed the importance of implementing a quality assurance program. In the relevant report [57], the committee focuses on the role of packaging in relation to the stability of pharmaceuticals and the potential for counterfeiting. It is specified that the design of the packaging must prevent tampering with or counterfeiting of the enclosed medicinal products. Packaging must also carry the correct information and identification of the product.

The US Food and Drug Administration (FDA) enforces rule 21 CFR Part 211 [58], which specifies current good manufacturing practices for finished pharmaceuticals. Within this framework, the rule mandates that tamper-evident packaging should be used for over-the-counter (OTC) human drug products. According to the regulation, which aims to protect drug packaging against counterfeiting, it should not possible to duplicate the packaging using commonly available materials or processes.

In 2003, in response to the increasing number of counterfeiting incidents, the US FDA formed a Counterfeit Drug Task Force, which has released an annual report related to the global drug counterfeiting situation through 2006 [59]. The task force also aims to create a comprehensive system of modern protective measures against counterfeit drugs. One of the measures is to ensure the security of packaging. Recently, many solutions have been proposed to meet this goal. The best-known such solution is the usage of a barcode containing standard information related to the drugs and package, but tamper-resistant tapes, holograms and colour-shifting inks and dyes are also widely used.

Defeating counterfeiters demands a multi-level approach, an element of which is secure packaging. However, to ensure the optimal security of pharmaceutical packaging, both direct (also called overt) and indirect (also called covert) technologies must be used [60]. Direct technology refers to methods that easily allow the end user to verifying the packaging originality, while indirect technology refers to methods whose use require a certain level of expertise and, in some cases, require dedicated machines. Indirect technologies are also characterized by their invisibility; in other words, they use security mechanisms based on objects that are not visible, such as ultraviolet (UV) inks. In some cases the two solutions are both implemented in the same security methods or different solutions are combined in the same package.

2.4.1 Overt (or Direct) Security solutions

Overt features enable instant authentication of packaging through visual inspection by the user without requiring expert knowledge. Optically variable features such as holographic devices within the design and colour shift inks are the most common and effective overt security features, enabling packaging to be validated both quickly and easily.

2.4.1.1 Holograms

Introduced by Glaxo in 1989 on their Zantac® product, holographic packaging has grown to be a popular means of assuring consumers of genuineness [61]. Holograms have appealed to manufacturers over the ages because of their relatively low cost, flexibility in manufacturing process integration and instant primary feature identification by consumers, with obvious branding advantages. The most basic common hologram used in pharmaceutical packaging security is the rainbow hologram, which generates a rainbow-like radiance by diffracting white light into the spectrum of visible light. Stereograms are rainbow holograms composed of a number of images arranged to provide an animation upon tilting. Newer dot matrix digital holograms comprise microscopic pixels, each of which is a hologram itself, that combine to produce one coherent holographic image [62, 63].

By altering the holographic recording medium, hologram design can be integrated into transparent foils to produce distinct packing tape. Holographic designs can also be made on tamper-evident seals, protecting consumers from mal-handled or illegally refilled products. The conventional means of generating a hologram employs lasers that impinge on a recording medium, but high resolution holograms are typically made by more precise electron beams (e-beams) [64].

In general, holograms have two sets of security features: primary and secondary. The primary features consist of overt patterns that are easily inspected by the naked eye. These features include the general radiance of a rainbow hologram and intricate designs. Secondary (covert) features provide well-equipped authenticators with a means to obtain additional confidence about the hologram’s genuineness. This identification often entails the use of specialized readers such as polarizing sheets, ultraviolet radiation or chemical reagents. For instance, a newly commercialized hologram reacts to moisture, revealing a covert image – consumers can breathe onto the hologram to confirm a product’s genuineness [65, 66].

The success of basic holograms as an anti-counterfeiting measure has degraded over time because low-cost reproductive equipment and unregulated mass-suppliers are available over the internet. Jeff Allen asserts that almost anyone can now obtain a hologram printing machine, often for less than $10,000, or simply order duplicates of a master hologram from dozens of hologram-making companies throughout the world [67]. Counterfeiters are now applying knock-off holograms to their products, making it almost impossible for the average consumer to discern real drugs from fake drugs. However, pharmaceutical manufacturers widely continue to put their logo on a hologram as first level identification.

2.4.1.2 Colour-Shift Inks

Whilst holograms offer a high level of overt security on their own, they can also be used in combination with other security devices to provide another hurdle for would-be counterfeiters to overcome; these additional measures include colour shift inks. Colour-shift inks appear to have two or more distinct colours when viewed from differing viewing angles [68, 69]. These features are easily verified by tilting the item carrying the colour-shift so that the different colours can be observed.

Different colour combinations are available, and both strong opaque and subtle transparent effects can be created to complement the existing design of the packaging. Currently, only a limited number of security suppliers produce colour-shift inks because the process to create the colour-shift pigment is highly specialized and requires particular technical knowledge and bespoke equipment. The supply of colour-shift inks is tightly controlled to ensure that the products are used only in genuine circumstances and under strict codes of conduct, including end use agreements. This solution is also used in some national banknote security [37, 69].

2.4.1.3 Barcoding

Barcodes were developed for electronic control of products in the sale system chain. For this reason, they are not developed to fight counterfeiting; however, they are universally recognized as a sign of originality. This sense of originality can be easily overcome by means of simple copy attack. To resolve this limitation, 2D and 3D barcodes have been developed and standardized. Some of the most famous examples are QR codes [70] and DataMatrix [71], which presents a high level of error resilience and an additional capacity to load encrypted data. However, these codes are also weak to copy attacks; for this reason, Encrypted 2D barcodes with open standards linked to a centralized database have been developed. This solution has been considered as an alternative to Radio Frequency

Identification (RFId) for America's national drug track-and-trace system (ePedigree) because the legislature only specifies the use of an "electronically readable" technology [72].

2.4.1.4 Radio Frequency Identification (RFId)

RFId technology uses tiny electronic tags to identify products with specialized readers that can operate at a distance. With the advancement of technology, including the development of RFId, the U.S. Food and Drug Administration (FDA) launched ePedigree as a renewed effort to require drugs sold in the U.S. to contain complete pedigree information [72]. Although ePedigree does not require RFId, it has been promoted to the fore of technologies that are available to solve the problem, primarily by the FDA.

RFID is designed to operate with Electronic Product Codes (EPC), which support item-unique coding. Thus, with a global mass-serialized RFID scheme such as the Worldwide Track and Trace Bank (WTTB), products can be automatically tracked from raw materials to post-consumer waste. Such a system could also be used to fight product diversion and illegal parallel trade [73].

RFId has encountered some obstacles in its replacement of barcodes. The chief concerns revolve around privacy, tag costs, complicated logistics and poor read rates [74]. Innovative tag printing techniques using metal-organic materials may address the tag cost issue by directly printing tag antennas on product packaging [75].

As tag prices and read error rates decline, RFId could theoretically be implemented in developing nations. RFId readers could operate in areas with poor electrical supply by integrating them with cell phones. Upon reading the EPC, the cell phone could interrogate a central database to retrieve the drug’s pedigree. However, the industry’s response has not been encouraging. Although the first RFId phone kit was released in 2004, RFId-equipped mobile phones remain rare, despite predictions that up to 50% of mobile phones would be enabled with similar remote-sensing technology by 2009 [76, 77].

2.4.2 Covert or Indirect Security solutions

The level of packaging security can be further increased by the introduction of covert and forensic features. Covert techniques such as infrared (IR) and UV pigments, micro-text and microscopic tagging are invisible, and they are difficult to detect and replicate without specialist detection equipment. As a result, they provide a higher level of protection. Forensic solutions include molecular markers and biological tracers. These features can only be identified using laboratory equipment, offering complete confidence in packaging authentication. In addition Laser Surface Authentication has arisen as an interesting solution for authenticating drug packaging using a biometric-like approach, based on package surface characteristics [48, 50, 78].

2.4.2.1 UV Inks and Print

Images printed with UV ink are only visible under UV light illumination. UV inks are available in different frequencies. Depending on the formulation of the ink, investigators must use either long wave or short wave UV illumination to make the printed images or text visible. Images and text can be printed in a variety of UV colours, ranging from blue to yellow to red. Even UV ‘picture’ images can be printed in full colour or black and white, with grey scale or 'flesh tones' that are again only visible under a UV light source.

The level of security offered by UV inks and print is defined by the limited access to the inks and their component pigments, and a genuinely secure range of inks is only available under restricted use measures. By combining the colours to create photographic images, the level of security is further increased because of the highly specialized origination and printing techniques required. Sophisticated printing capabilities are also available for the creation of fine line designs, as well as colour and UV micro-text prints similar to those used on banknotes [37, 79].

2.4.2.2 Colour and UV Micro-text Print

Micro-text print creates text characters that cannot be observed with the naked eye; and consequently, they can be hidden within larger overt images such as text and pictures without the knowledge of the consumer or potential counterfeiter. These complex designs are difficult to reproduce and can be further validated using a magnifying lens or microscope to examine the detailed features and sophisticated print. This equipment is inexpensive, readily available and pocket-sized, making micro-text print a user-friendly technology. Because of the need for specialist printing equipment, materials and technical knowledge, this technique is extremely difficult to copy. Because the technology is covert, many counterfeiters simply do not attempt replication, and they create the overt image without the inclusion of the micro-text print.

Micro-text can also be printed using a UV ink. In that case, the finished image is only visible under UV light and with a magnifying lens. The invisibility of this printing technology enables it to be used without affecting other design elements. Although the text size is slightly larger than standard micro-text print, the use of UV invisible ink considerably enhances security [80].

2.4.2.3 Taggant Authentication

Taggant authentication technology provides a highly secure method for on-site or in-field applications. Pharmaceutical companies can integrate taggants to quickly protect and authenticate packaging in the market by using most standard printing and coating techniques. Authentication is a key factor for technologies that can reliably identify and distinguish genuine packaging from counterfeit packaging [81].

The most highly secure taggant systems can only be verified by special handheld readers that are in turn only available from a secure source, thus ensuring that any potential counterfeiter is not aware of the presence of an authentication technology. Handheld readers are relatively low-cost lightweight authentication tools that enable quick and easy authentication in different environments. Company personnel and authorized agents can simply and accurately determine whether packaging is authentic or not.

2.4.2.4 Laser Surface Authentication – LSA

Improvements in laser scanning techniques now allow brand managers to uniquely identify products by imaging microscopic deformations on the surface of their packages. The distinctive microscopic patterns are a result of minute manufacturing differences on a per-item basis. This “natural randomness” can be interpreted as a product’s fingerprint [43].

These surface fingerprints can be captured by measuring the speckle backscatter from an impingent laser beam scanned over the surface of interest. Upon rescanning the same section, a distinct spike (or the lack of a distinct spike) in the cross correlation can indicate positive authentication (or otherwise). This method is generally resilient to reasonable surface fatigue, but no authentication can take place if the scanned section is not delimited or is severely damaged. Developing nations typically offer a more challenging handling environment. Laser surface mapping is very rapid, and some vendors claim up to 300 scans per second [82].

Additionally, it requires no modifications to products packaged with flat surfaces. Because it is new, the technology’s efficacy has not yet been studied extensively. LSA is based on the possibility of acquiring paper (and packaging) surface roughness. Any paper surface has a different fibre pattern. By acquiring laser speckle scattering using a CCD camera, it is possible to reconstruct a detailed 3D image of the paper surface [51]. Starting from this 3D model, it is possible to create an LSA template related to the surface roughness that uniquely identifies the document or packaging. The described approach is similar to the one used in human biometry, with the exception of the great amount of data to be analyzed by the LSA approach. In fact, LSA requires the laser scanning of the entire package surface, as well as the scanning of a Machine Readable Zone (MRZ), with a high-detail resolution [83]. This approach requires dedicated machinery to correctly acquire the laser light scattering, and a high resolution must be obtained by subsequent acquisition of different package portions.

2.4.2.5 Physical Unclonable Function – PUF

One emerging approach to packaging security is based on the possibility of including a random pattern of chemical particles in the package itself, which would have specific characteristics [84, 85]. A possible solution is based on the introduction of a random distribution of phosphor particles, which scatter under UV illumination (a phosphorescence phenomenon). It is possible to acquire an image of these particles under UV illumination and create a barcode with the positions of the particles inside a predetermined frame after segmentation. With a properly designed acquisition device, the particle distribution can be acquired, and the recalculated barcode can be verified against the original by a secure internet connection or a barcode directly stamped on the package itself. This method offers the possibility to introduce the phosphor particles during package production, but the acquisition and segmentation is significantly impacted by the light source illumination, angle of acquisition, and possible geometric distortions.

2.4.3 Combining Overt and Covert Technologies

Overt and covert design features generally complement each other, and they are used jointly on packaging for maximum security. Security print techniques using highly defined print lines to create complex designs that are difficult to originate and print are also highly effective in the fight against counterfeiting. Sophisticated overt and covert security design features, which are created using the latest software, can be built into each design, protecting pharmaceutical packaging from counterfeiting. A wide variety of fine design techniques can be combined to build bespoke security solutions into packaging protection and authentication requirements. These techniques include engraved images, intaglio printing, relief images, warp grids, variable line width, guilloche designs, crystal patterns and special rasters (see for more details Ref. [68]).

Chapter 3 Hylemetric Paradigm

3.1 INTRODUCTION 111

3.2 HYLEMETRIC CHARACTERISTICS 112

3.3 TEMPLATE DEFINITION 115

3.4 BIDIMENSIONAL BARCODE 116

3.4.1 PDF417 BARCODE 118

3.4.2 AZTEC CODE 122

3.4.3 QR CODE 130

3.4.4 DATA MATRIX ECC 200 137

3.4.4.1 Technical Characteristics 139

3.4.4.2 Error Correction in ECC 200 145

3.1 Introduction

In §1.5 has been introduced the possibility to apply the biometric approach to the lifeless matter, such as banknotes, lithography, art works and so on. This approach, applied to lifeless matter has been called **Hylemetry Paradigm** [86].

On the basis, Hylemetric paradigm is an application of Biometry, as described in Chapter 1, to objects, starting from the determination of one or more features useful to clearly identify an object from another one. This step is based on the verification of the possibility to apply to an object characteristic all of the properties necessary to maximise inter-class value (i.e. possibility to separate one object from a similar one on the basis of that feature) and minimize intra-class one (i.e. the possibility to erroneously identify an object as a different one).

Due to the particularity of an inanimate object referring to human being, a characteristic to be classified as Hylemetric feature has to accomplish also to addition properties, more related to its object nature.

After the determination of the identification characteristics, the process follows the biometric one, with an acquisition of those ones, using different methods in relation to object nature (as in biometry) and the creation of a Hylemetric template, to be used for verification purposed and to be stored in a secured database.

During verification phase the hylemetry and biometry paradigms are identical and the approach is essentially based on the comparison of data templates and the usage of a threshold to discriminate among them in case of extraction errors. The usage of a threshold, like in biometry, allow to determine FAR and FRR for any Hylemetric system.

3.2 Hylemetric Characteristics

As summarized before, the basic step in the Hylemetric paradigm is the determination of one or more object characteristics, which can be used as Hylemetric ones in the authentication/identification process.

The principal properties that an lifeless matter has to have, are the same ones related to human identification:

- ***Universality****:* all the objects should have the characteristic;
- ***Permanence****:* the characteristic should not vary over time due to object usage;
- ***Distinctiveness****:* samples corresponding to different objects should be as different as possible, that is, the inter-class variability should be as large as possible;
- ***Robustness***: samples corresponding to the same object should be as close as possible, that is, the intra-class variability should be as small as possible;
- ***Accessibility***: the sample should be easy to present to the acquisition device;
- ***Acceptability***: it should be perceived as nonintrusive and not potentially destructive by the object owner;
- ***Hardness to circumvention***: it should be hard for a counterfeiter to fool the system using false copies of an original object.

In addition, in Hylemetric authentication the sampled characteristic should have also the following properties [46]:

- ***Uniqueness***: every objects should be identifiable and distinguishable from all others;

- ***Consistency***: feature vector should be verifiable by multiple parties over the lifetime of the object;
- ***Conciseness***: feature vector should be short and easily computable;
- ***Robustness***: it should be possible to verify the feature vector even if the object has been subjected to harsh treatment;
- ***Resistance to Forgery***: it should be very difficult and costly, or impossible for an adversary, to forge a document by coercing a second object to express the same feature vector as the original one.

Each texture that is highly random and difficult/impossible to reproduce can be potentially used as Hylemetric characteristic. Obviously, good Hylemetric characteristics have to satisfy the following additional requirements:

- it has to be simple repeatable and reliable to implement the feature vector (template);
- the cost of creating and signing the feature vector has to be small, in relation with a desired level of security;
- the cost of exact or near-exact replication of the unique and random physical structure used as Hylemetric characteristic has to be greater of the value of the object under forgery;
- the cost of verifying the authenticity of a signed feature vector has to be small, if compared with a desired level of security.

3.3 Template Definition

Another important aspect of Hylemetry approach is the definition of an appropriate Hylemetric template to be used during verification phase.

The template definition cannot be unique, but depends on the nature of the Hylemetric characteristics and varies from object to object. In any case it is always possible define a template for a specific object family, for example banknotes.

The usage of templates instead of the entire image of the acquired Hylemetric characteristics is due to some practical advantages. First of all the template can be defined following a unique standard, independently from the number of the identified characteristics or the acquisition quality offered by verification systems. In this way the verification phase can also be automatized, or, when this is not possible, can be standardized.

Secondarily, it is possible define a unique template also in presence of more than only one characteristic; in this case we can define multimodal Hylemetry templates.

An example of Hylemetric template can be the creation of a binary bitmap (i.e. a bit stream on which any bit has is significant) that synthetizes the position on a particular feature inside a predefined area of the analysed object. This template can be stored in local or remote way and, during verification phase, an automatic system can extract this template from the object under inspection and match it with the related template.

The template matching can be made in different ways. The most used one is the minimum Hamming Distance among two binary stream templates, verified against a verification threshold. This is the same approach used also in Iris Biometry [5, 23-24]. In other cases it is possible using a correlation approach between the two template images.

In any case the template standardization is on the basis of a possibility to automatize the verification process.

3.4 Bidimensional Barcode

Verification phase can be automatized including Hylemetric information inside a barcode to be checked by verification systems. In recent years, information exchange and the transmission of digital images have become more and more convenient, with the rapid development of the Internet and digital storage technology. However, these technologies also make it possible for unscrupulous people to duplicate and distribute unauthorized images with low cost. Methods that link advertising media on flat surfaces such as paper, as well as cyber-advertising media, have become universal. Numerous advertisements that incorporate URLs or Quick Response codes (QR code) on flat-surface advertisements are appearing everywhere. In Figure 3.1 is shown an example of a typical QR code [87].

Figure 3.1 – Example of QR code.

The QR code is a Matrix 2D Barcode that was developed by the Denso Company in Japan in September 1994. In addition to the advantages of 1D Barcode, it has specialties of rapid and wide identification, expresses Chinese and Japanese characters effectively, which other 2D Barcodes have been unable to do [88-89].

The increasing competition in the Mobile Marketing market indicates that Mobile Marketing platform providers will be forced to integrate identity and context information offered by the mobile network, in order to improve the efficiency of applications [90]. Mobile application can be defined as an Internet application that fits well in the mobile computing environment [91].The lines used to transmit images from cellular phones and computers are becoming broadband enabled, establishing an environment in which images can be easily sent at high speeds using terminals and networks. Digital watermarking technology is a technology for which linkage with existing media is highly anticipated in that it can directly embed information into picture images, video and sound media [92].

According to 2D Barcode anti-counterfeiting technology, combining the Computer Generate Holograms with the 2D Barcode greatly improves the depth and width of the application of the 2D barcode in the anti-counterfeiting field.

Nowadays 2D Barcodes, as the QR-code, are very used in all sort of advertising and packaging. Most of the time, 2D Barcodes appear printed on paper or as digital information over the Internet. Caused by malicious purposes or the wear and tear of the paper, the 2D Barcode could be found ruined. The presence of loss of information due to noise dots on the surface, as to the cropping of the 2D Barcode.

In the following it is presented a panoramic view of the more important barcodes, which can be used for Hylemetric verification, with a particular attention to DataMatrix one, the most used and the best standardised one.

3.4.1 PDF417 Barcode

The PDF417 is a stacked linear barcode symbol format used in a variety of applications, primarily transport, identification cards, and inventory management. PDF stands for Portable Data File. The 417 signifies that each pattern in the code consists of 4 bars and spaces, and that each pattern is 17 units long. The PDF417 symbology was invented by Dr. Ynjiun P. Wang at Symbol Technologies in 1991 [93]. It is represented by ISO standard 15438.

In addition to features typical of two dimensional bar codes, PDF417's capabilities include:

- **Linking** – PDF417 symbols can link to other symbols which are scanned in sequence allowing even more data to be stored.
- **User-specified dimensions** – The user can decide how wide the narrowest vertical bar (X dimension) is, and how tall the rows are (Y dimension).
- **Public domain format** – Anyone can implement systems using this format without any license.

The PDF417 bar code (also called a symbol) consists of 3 to 90 rows, each of which is like a small linear bar code. Each row has:

- a quiet zone. This is a mandated minimum amount of white space before the bar code begins.
- a start pattern which identifies the format as PDF417.
- a “row left” codeword containing information about the row (such as the row number and error correction level)
- 1-30 data codewords: Codewords are a group of bars and spaces representing one or more numbers, letters, or other symbols.
- a “row right” codeword with more information about the row.
- a stop pattern.
- a quiet zone.

All rows are the same width; each row has the same number of codewords. The following Figure 3.2 shows the barcode zones on a typical PDF417.

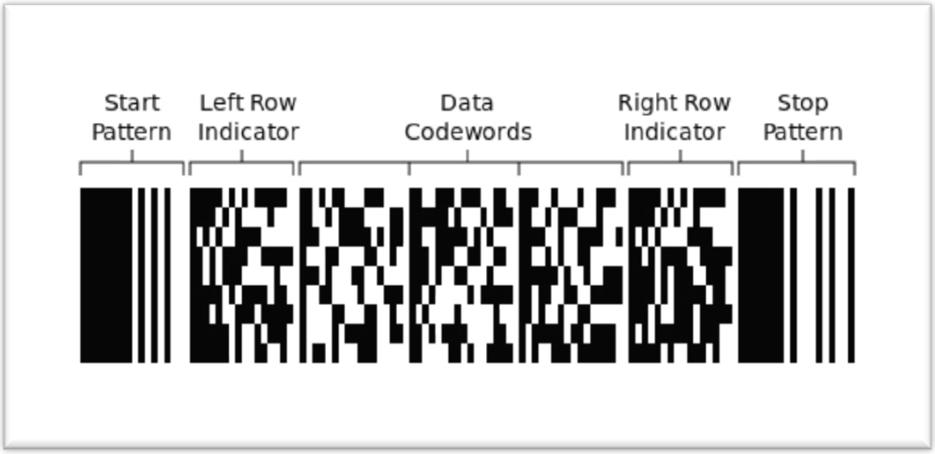


Figure 3.2 – Example of PDF417 codewords areas.

PDF417 uses a base 929 encoding. Each codeword represents a number between 0 and 928 inclusive.

The codewords are represented by patterns of dark (bar) and light (space) regions. Each of these patterns contains four bars and four spaces (where the 4 in the name comes from). The total width is 17 times the width of the narrowest allowed vertical bar (the X dimension); this is where the 17 in the name comes from. Each pattern starts with a bar and ends with a space.

The row height must be 3 times the minimum width: $Y \geq 3X$.

There are three distinct bar-space patterns used to represent each codeword. These patterns are organized into three groups known as clusters. The clusters are labelled 0, 3, and 6. No bar-space pattern is used in more than one cluster. The rows of the symbol cycle through the three clusters, so row 1 uses patterns from cluster 0, row 2 uses cluster 3, row 3 uses cluster 6, and row 4 again uses cluster 0. Which cluster can be determined by an equation:

$$K = \left(b_1 - b_2 + b_3 - b_4 + 9\right)_9 \tag{3.1}$$

Where K is the cluster number and the bi refer to the width of the i-th bar in the symbol character (in X units). The round parenthesis indicates the module 9 operation.

Alternatively, it is possible also:

$$K = \left(E_1 - E_2 + E_5 - E_6 + 9\right)_9 \tag{3.2}$$

Where E_i is the *i-th* edge-to-next-same-edge distance. Odd indices are the leading edge of a bar to the leading edge of the next bar; even indices are for the trailing edges. The round parenthesis indicates the module 9 operation.

One purpose of the three clusters is to determine which row (mod 3) the codeword is in. The clusters allow portions of the symbol to be read using a single scan line that may be skewed from the horizontal. For instance, the scan might start on row 6 at the start of the row but end on row 10. At the beginning of the scan, the scanner sees the constant start pattern, and then it sees symbols in cluster 3. When the skewed scan straddles rows 6 and 7, then the scanner sees noise. When the scan is on row 7, the scanner sees symbols in cluster 1. Consequently, the scanner knows the direction of the skew. By the time the scanner reaches the right, it is on row 10, so it sees cluster 1 patterns. The scanner will also see a constant stop pattern.

Of the 929 available codewords, 900 are used for data, and 29 for special functions. Three different encoding schemes are defined and can be mixed as necessary within a single symbol.

- **Text**: each codeword represents one or two characters.
- **Byte**: each group of 5 codewords represents 6 bytes.
- **Numeric**: groups of up to 15 codewords represent as many as 44 decimal digits.

When the PDF417 symbol is created, from 2 to 512 error detection and correction codewords are added. PDF417 uses Reed–Solomon error correction. When the symbol is scanned, the maximum number of corrections that can be made is equal to the number of codewords added, but the standard recommends that two codewords be held back to ensure reliability of the corrected information.

3.4.2 Aztec Code

Aztec Code is a type of 2D barcode invented by Andrew Longacre, Jr. and Robert Hussey in 1995.[94] The code was published by AIM, Inc. in 1997. Although the Aztec code is patented,[94] it has been released to the public domain and published as ISO/IEC 24778:2008 standard.

Named after the resemblance of the central finder pattern to an Aztec pyramid, Aztec code has the potential to use less space than other matrix barcodes because it does not require a surrounding blank “quiet zone”.

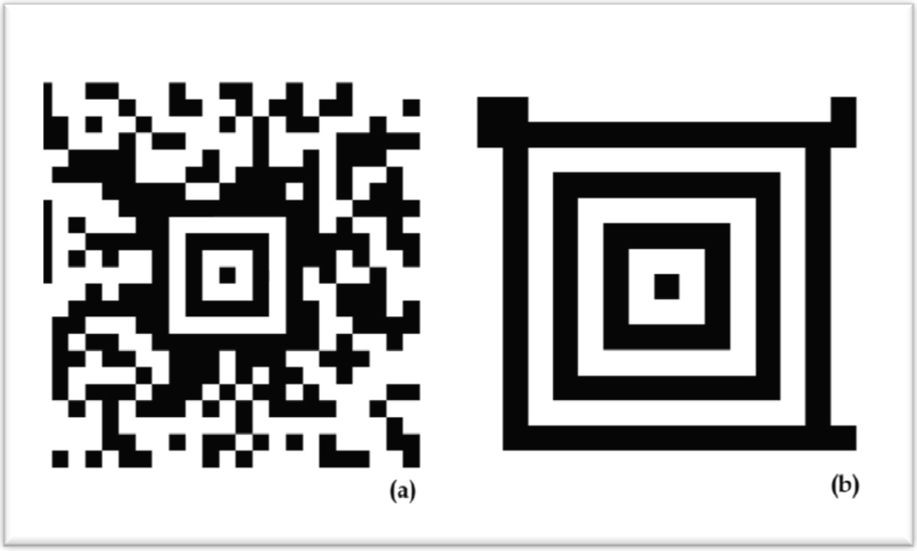


Figure 3.3 – (a) Example of Aztec barcode; (b) the core of the full Aztec code is composed by 40 bits between the orientation marks for encoding parameters codewords areas.

The symbol is built on a square grid with a bullseye pattern at its centre for locating the code. Data is encoded in concentric square rings around the bulls-eye pattern. The central bulls-eye is 9×9 or 13×13 pixels, and one row of pixels around that encodes basic coding parameters, producing a “core” of 11×11 or 15×15 squares. Data is added in “layers”, each one containing two rings of pixels, giving total sizes of 15×15, 19×19, 23×23, etc.

The corners of the core include orientation marks, allowing the code to be read if rotated or reflected. Decoding begins at the corner with three black pixels, and proceeds clockwise to the corners with two, one, and zero black pixels. The variable pixels in the central core encode the size, so it is not necessary to mark the boundary of the code with a blank “quiet zone”, although some bar code readers require one (see Figure 3.3).

Generating an Aztec code The encoding process consists of the steps of:

- Converting the source message to a string of bits;
- Computing the necessary symbol size and mode message, which determines the Reed-Solomon codeword size;
- Bit-stuffing the message into Reed-Solomon codewords;
- Padding the message to a codeword boundary;
- Appending check codewords;
- Arranging the complete message in a spiral around the core.

All conversion between bits strings and other forms is performed according to the big-endian (most significant bit first) convention. All 8-bit values can be encoded, plus two escape codes:

- FNC1, an escape symbol used to mark the presence of an application identifier, in the same way as in the GS1-128 standard.
- ECI, an escape followed by a 6-digit extended channel interpretation code, which specifies the character set used to interpret following bytes.

By default, codes 0–127 are interpreted according to ANSI X3.4 (ASCII), and 128–255 are interpreted according to ISO 8859-1: Latin Alphabet No. 1. This corresponds to ECI 000003.

Bytes are translated into 4- and 5-bit codes, based on a current decoding mode, with shift and latch codes for changing modes. Byte values not available this way may be encoded using a general “binary shift” code, which is followed by a length and a number of 8-bit codes.

For changing modes, a shift affect only the interpretation of the single following code, while a latch affects all following codes. Most modes use 5-bit codes, but Digit mode uses 4-bit codes.

The mode message encodes the number of layers (L layers encoded as the integer L−1), and the number of data codewords (D codewords, encoded as the integer D−1) in the message. All remaining codewords are used as check codewords.

For compact Aztec codes, the number of layers is encoded as a 2-bit value, and the number of data codewords as a 6-bit value, resulting in an 8-bit mode word. For full Aztec codes, the number of layers is encoded in 5 bits, and the number of data codewords is encoded in 11 bits, making a 16-bit mode word.

The mode word is broken into 2 or 4 4-bit codewords in GF(16), and 5 or 6 Reed-Solomon check words are appended, making a 28- or 40-bit mode message, which is wrapped in a 1-pixel layer around the core.

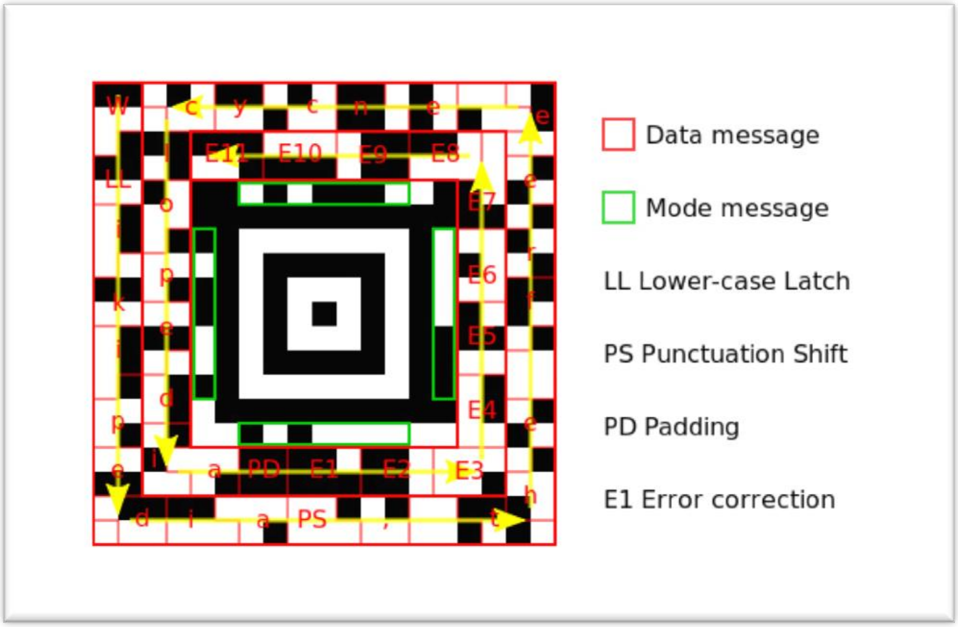


Figure 3.4 – Example of creation of Aztec Barcode data: message data are placed in a spiral pattern around the core. The mode message begins "01011100", indicating 01_2+1 2 layers, and 011100_2+1 = 29 data codewords (of 6 bits each).

Because an L+1-layer compact Aztec code can hold more data than an L-layer full code, full codes with less than 4 layers are rarely used. Most importantly, the number of layers determines the size of the Reed-Solomon codewords used. This varies from 6 to 12 bits following the Table 3.1:

Table 3.1 – Various polynomial functions used for layers and message inside Aztec Code.

Bits	Fields	Polynomial	Used for
4	GF(16)	$x^4 + x + 1$	Mode Message
6	GF(64)	$x^6 + x + 1$	Layer 1-2
8	GF(256)	$x^8 + x^5 + x^3 + x^2 + 1$	Layer 3-8
10	GF(1024)	$x^{10} + x^3 + 1$	Layer 9-22
12	GF(4096)	$x^{12} + x^6 + x^5 + x^3 + 1$	Layer 23-32

The codeword size b is the smallest even number which ensures that the total number of codewords in the symbol is less than the limit of 2^b-1 which can be corrected by a Reed-Solomon code.

As mentioned above, it is recommended that at least 23% of the available codewords, plus 3, are reserved for correction, and a symbol size is chosen such that the message will fit into the available space.

The data bits are broken into codewords, with the first bit corresponding to the most significant coefficient. While doing this, code words of all-zero and all-ones are avoided by bit stuffing: if the first $b-1$ bits of a code word have the same value, an extra bit with the complementary value is inserted into the data stream. This insertion takes place whether or not the last bit of the code word would have had the same value or not.

Also note that this only applies to strings of $b-1$ bits at the beginning of a code word. Longer strings of identical bits are permitted as long as they straddle a code word boundary. When decoding, a code word of all zero or all one may be assumed to be an erasure, and corrected more efficiently than a general error.

This process makes the message longer, and the final number of data codewords recorded in the mode message is not known until it is complete. In rare cases it may be necessary to jump to the next-largest symbol and begin the process all over again to maintain the minimum fraction of check words.

After bit stuffing, the data string is padded to the next codeword boundary by appending 1 bits. If this would result in a code word of all ones, a stuff bit may need to be inserted. On decoding, the padding bits may be decoded as shift and latch codes, but that will not affect the message content. The reader must accept and ignore a partial code at the end of the message, as long as it is all-ones.

Additionally, if the total number of data bits available in the symbol is not a multiple of the codeword size, the data string is prepended with an appropriate number of 0 bits to occupy the extra space. These bits are not included in the check word computation.

Both the mode word, and the data, must have check words appended to fill out the available space. This is computed by appending K check words such that the entire message is a multiple of the standard Reed-Solomon polynomial (x−1)(x−2)(x−4)...(x−2K−1). Note that check words are not subject to bit stuffing, and may be all-zero or all-one. Thus, it is not possible to detect erasure of a check word. A full Aztec code symbol has, in addition to the core, a "reference grid" of alternating black and white pixels occupying every 16th row and column. These known pixels allow a reader to maintain alignment with the pixel grid over large symbols. For up to 4 layers (31×31 pixels), this consists only of single lines extending outward from the core, continuing the alternating pattern. Inside the 5th layer, however, additional rows and columns of alternating pixels are inserted ±16 pixels from the centre, so the 5th layer is located ±17 and ±18 pixels from the centre, and a 5-layer symbol is 37×37 pixels.

Likewise, additional reference grid rows and columns are inserted ±32 pixels from the centre, making a 12-layer symbol 67×67 pixels. In this case, the 12th layer occupies rings ±31 and ±33 pixels from the centre. The pattern continues indefinitely outward, with 15-pixel blocks of data separated by rows and columns of the reference grid.

One way to construct the symbol is to delete the reference grid entirely, and begin with a 14×14-pixel core centred on a 2×2 pixel white square. Then break it into 15×15 pixel blocks and insert the reference grid between them.

Referring to Figure 3.5, the mode message begins at the top-left corner of the core, and wraps around it clockwise in a 1-bit thick layer. It begins with the most significant bit of the number of layers, and ends with the check words. For a compact Aztec code, it broken into four 7-bit pieces to leave room for the orientation marks. For a full Aztec code, it is broken into four 10-bit pieces, and those pieces are each divided in half by the reference grid.

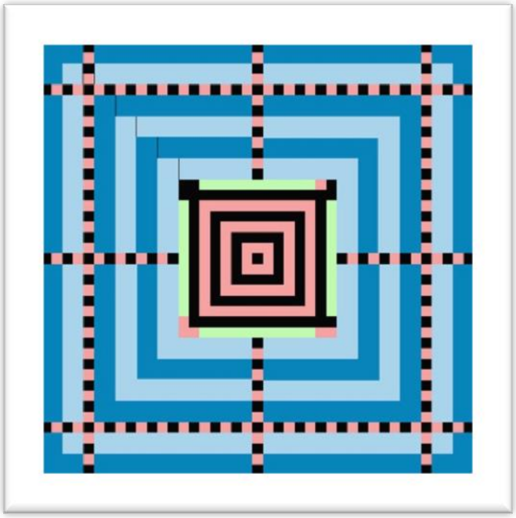


Figure 3.5 – 6-layer (41×41) Aztec code showing reference grid.

The main message begins at the outer top-left of the entire symbol, and spirals around it counter clockwise in a 2-bit thick layer, ending directly above the top-left corner of the core. This places the bit-stuffed data words, for which erasures can be detected, in the outermost layers of the symbol, which is most prone to erasures. The check words are stored closer to the core.

With the core in its standard orientation, the first bit of the first data word is placed in the upper-left corner, with additional bits placed in a 2-bit-wide column left-to-right and top-to-bottom. This continues until 2 rows from the bottom of the symbol, when the pattern rotates 90 degrees, and continues in a 2-bit high row, bottom-to-top and left-to-right. After 4 equal-sized quarter layers, the spiral continues with the top-left corner of the next-inner layer, finally ending one pixel above the top-left corner of the core.

Finally, 1 bits are printed as black squares, and 0 bits are printed as white squares.

3.4.3 QR Code

QR Code (abbreviated from Quick Response Code) is the trademark for a type of two-dimensional code first designed for the automotive industry. More recently, the system has become popular outside the industry due to its fast readability and large storage capacity compared to standard UPC barcodes. The code consists of black modules (square dots) arranged in a square pattern on a white background. The information encoded can be made up of four standardized kinds (“modes”) of data (numeric, alphanumeric, byte/binary, Kanji), or through supported extensions, virtually any kind of data.

Invented in Japan by the Toyota subsidiary Denso Wave in 1994 to track vehicles during the manufacturing process, the QR Code is one of the most popular types of two-dimensional barcodes. It was designed to allow its contents to be decoded at high speed.

Unlike the old barcode that was designed to be mechanically scanned by a narrow beam of light, the QR code is detected as a 2-dimensional digital image by a semiconductor image sensor and is then digitally analyzed by a programmed processor. The processor locates the three distinctive squares at the corners of the image, and normalizes image size, orientation, and angle of viewing, with the aid of a smaller square near the fourth corner. The small dots are then converted to binary numbers and validity checked with an error-correcting code.

The amount of data that can be stored in the QR Code symbol depends on the datatype (mode, or input character set), version (1,...,40, indicating the overall dimensions of the symbol), and error correction level.

The maximum storage capacities occur for 40-L symbols (version 40, error correction level L), and are as follows (where character refers to individual values of the input mode/datatype, as indicated):

Table 3.2 – Number of maximum characters necessary in relation to code type.

Code	**Charachter**
Numeric only	*Max. 7,089 characters (0, 1, 2, 3, 4, 5, 6, 7, 8, 9)*
Alphanumeric	*Max. 4,296 characters (0–9, A–Z [upper-case only], space, $, %, *, +, -, ., /, :)*

Code	Charachter
Binary/byte	*Max. 2,953 characters (8-bit bytes) (23624 bits)*
Kanji/Kana	*Max. 1,817 characters*

Here are some sample QR Code symbols:

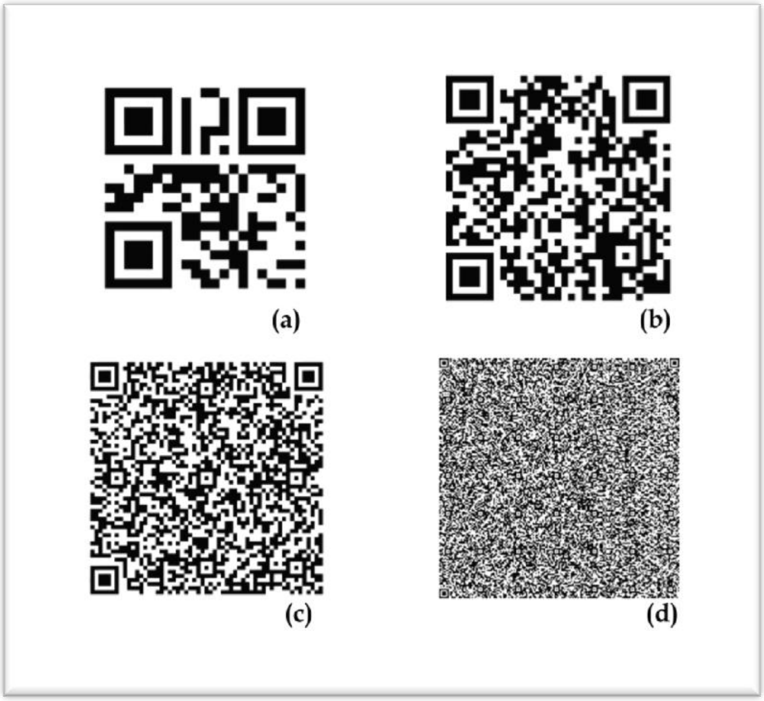


Figure 3.6 – Examples of different size QR Codes: (a) 21x21; (b) 33x33; (c) 57x57; (d) 177x177.

Encrypted QR Codes, which are not very common, have a few implementations. For example, Japanese immigration use encrypted QR Codes when placing visas in passports.

Codewords are 8 bits long and use the Reed–Solomon error correction algorithm with four error correction levels. The higher the error correction level, the less storage capacity. The following table lists the approximate error correction capability at each of the four levels:

Table 3.3 – Number of maximum codewords that could be restored in relation to the Reed-Solomon error correction level.

Correction Level	Character
Level L (Low)	7% of codewords can be restored
Level M (Medium)	15% of codewords can be restored
Level Q (Quartile)	25% of codewords can be restored
Level H (High)	30% of codewords can be restored

Due to the design of Reed–Solomon codes and the use of 8-bit codewords, an individual code block cannot be more than 255 codewords in length. Since the larger QR symbols contain much more data than that, it is necessary to break the message up into multiple blocks. The QR specification does not use the largest possible block size, though; instead, it defines the block sizes so that no more than 30 error-correction symbols appear in each block. This means that at most 15 errors per block can be corrected, which limits the complexity of certain steps in the decoding algorithm. The code blocks are then interleaved together, making it less likely that localized damage to a QR symbol will overwhelm the capacity of any single block.

Thanks to error correction, it is possible to create artistic QR Codes that still scan correctly, but contain intentional errors to make them more readable or attractive to the human eye, as well as to incorporate colours, logos and other features into the QR Code block.

In following Figure 3.7 a damaged, but still readable QR Code is shown.

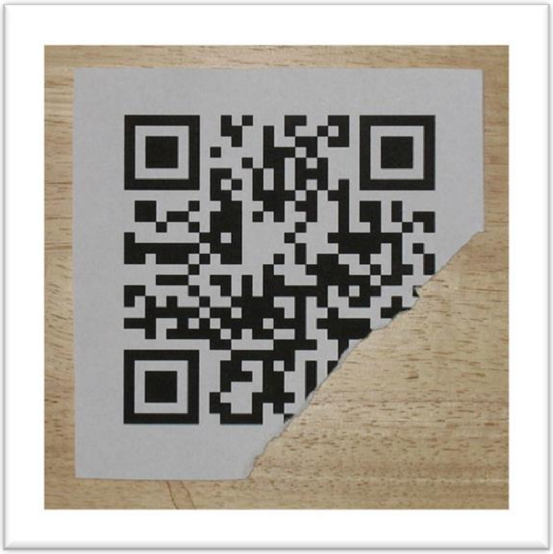


Figure 3.7 – Example of QR code printed on paper and ruined. It is still possible extracting information from it, due to the level of error correction.

The format information records two things: the error correction level and the mask pattern used for the symbol. Masking is used to break up patterns in the data area that might confuse a scanner, such as large blank areas or misleading features that look like the locator marks. The mask patterns are defined on a 6×6 grid that is repeated as necessary to cover the whole symbol. Modules corresponding to the dark areas of the mask are inverted.

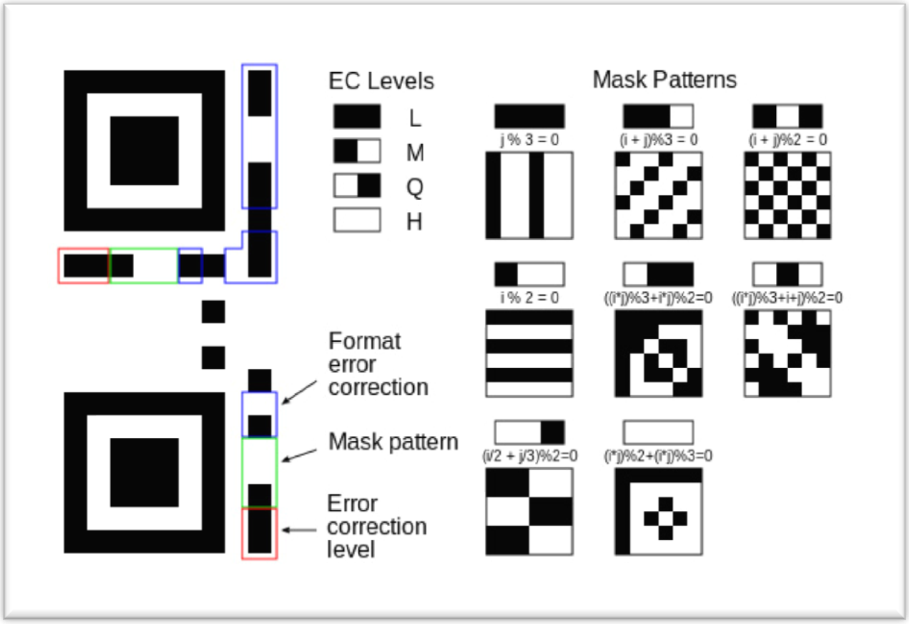


Figure 3.8 – QR Code grid creation to determine error correction level pattern orientation and scale and pattern mask.

The format information is protected from errors with a BCH code, and two complete copies are included in each QR symbol.

The message data is placed from right to left in a zigzag pattern, as shown in Figure 3.9.

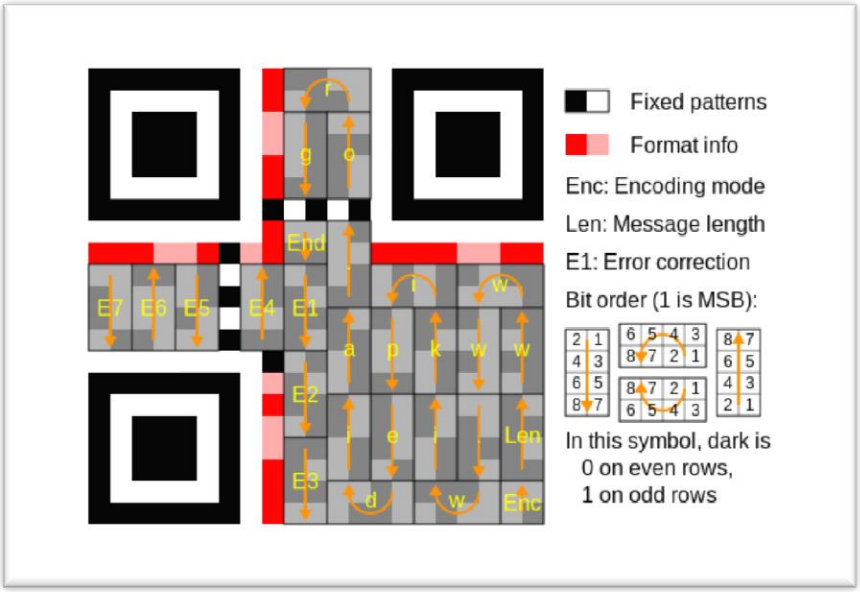


Figure 3.9 – Character position inside QR Code matrix.

In larger symbols, this is complicated by the presence of the alignment patterns and the use of multiple interleaved error-correction blocks. This solution is reported in the following schema in Figure 3.10.

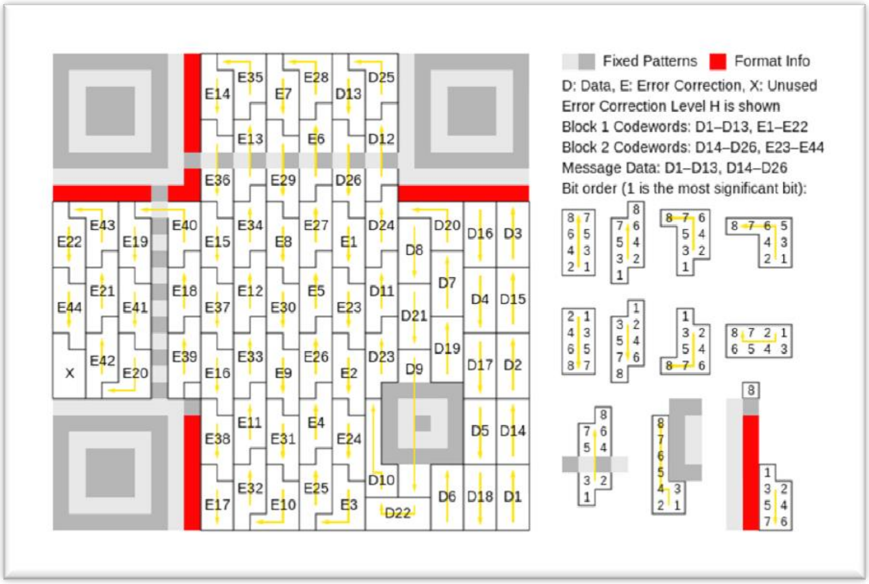

Fixed Patterns
Format Info
D: Data, E: Error Correction, X: Unused
Error Correction Level H is shown
Block 1 Codewords: D1–D13, E1–E22
Block 2 Codewords: D14–D26, E23–E44
Message Data: D1–D13, D14–D26
Bit order (1 is the most significant bit):
E35 E28 D25
E14 E7 D13
E13 E6 D12
E36 E29 D26
E43 E40 E34 E27 D24 D20 D16 D3
E22 E19 E15 E8 E1 D8
D7
E21 E18 E12 E5 D11 D4 D15
E44 E41 E37 E30 E23 D21
D19
E42 E39 E33 E26 D23 D17 D2
X E20 E16 E9 E2 D9
E11 E4 D5 D14
E38 E31 E24
D10
E32 E25 D6 D18 D1
E17 E10 E3 D22

Figure 3.10 – Management of great dimension symbols inside the QR code matrix, with the related error correction codes.

3.4.4 Data Matrix ECC 200

Data Matrix is a matrix (2D or two-dimensional) bar code which may be printed as a square or rectangular symbol made up of individual dots or squares. This representation is an ordered grid of dark and light dots bordered by a finder pattern. The finder pattern is partly used to specify the orientation and structure of the symbol. The data is encoded using a series of dark or light dots based upon a pre-determined size. The minimum size of these dots is known as the ***X-dimension***.

Data Matrix ECC 200 is composed of two separate parts (see figure below): the finder pattern, which is used by the scanner to locate the symbol, and the encoded data itself.

The finder pattern defines the shape (square or rectangle), the size, X-dimension and the number of rows and columns in the symbol. It has a function similar to the Auxiliary Pattern (Start, Stop and Centre pattern) in an EAN-13 [95] Bar Code and allows the scanner to identify the symbol as a Data Matrix.

- The solid dark is called the "***L finder pattern***". It is primarily used to determine the size, orientation and distortion of the symbol.
- The other two sides of the finder pattern are alternating light and dark elements, known as the "***Clock Track***". This defines the basic structure of the symbol and can also help determine its size and distortion.

The data is then encoded in a matrix within the Finder pattern. This is a translation into the binary Data Matrix symbology characters (numeric or alphanumeric).

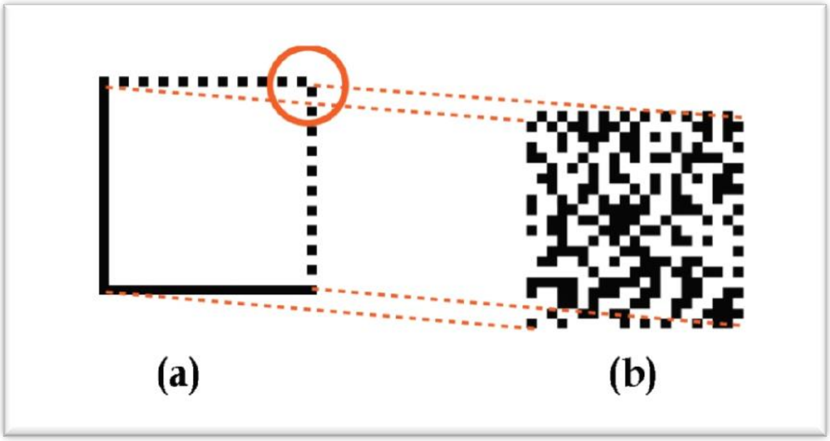


Figure 3.11 – (a) Finder Pattern uses for determine position, orientation and scale; (b) data pattern encoded following ECC 200 standard.

Just like linear (1D) bar codes Data Matrix has a mandatory Quiet Zone. This is a light area around the symbol which must not contain any graphic element which may disrupt reading the bar code. It has a constant width equal to the X-dimension of the symbol on each of the 4 sides.

Each Data Matrix symbol is made up of number of rows and columns. In version ECC 200, the number of rows and columns is always an even number. Therefore ECC 200 always has a light "square" in the upper right hand right corner (circled in the figure above). Obviously, this corner will be dark if the Data Matrix symbol is printed in negative (complementary colours).

3.4.4.1 Technical Characteristics

When implementing Data Matrix, a choice of symbol form must be made (based upon configuration support, available space on the product type, amount of data to encode, the printing process, etc.). It is possible encode the same data in two forms of Data Matrix: Square and Rectangle.

The square form is the most commonly used and enables the encoding of the largest amount of data according to ISO / IEC 16022 Information technology – Automatic Identification and data capture techniques – Data Matrix bar code symbology specification.

However, the rectangle form may be selected to meet the constraints of speed of printing on the production line. Indeed, the rectangle form with the limited height of the symbol is well suited to some high speed printing techniques.

Data Matrix is capable of encoding variable length data. Therefore, the size of the resulting symbol varies according to the amount of data encoded. Accordingly, this section can only estimate the size of a given Data Matrix approximately based on this parameter.

The figure below is extracted from ISO/IEC 16022. It provides a useful guide to estimating the size of the symbol but the exact size of the Data Matrix symbol depends on the exact encoded data. What we mean here is that Data Matrix is composed of fields which have a ladder shape (L shape). See the figure below for the size and capacity graph.

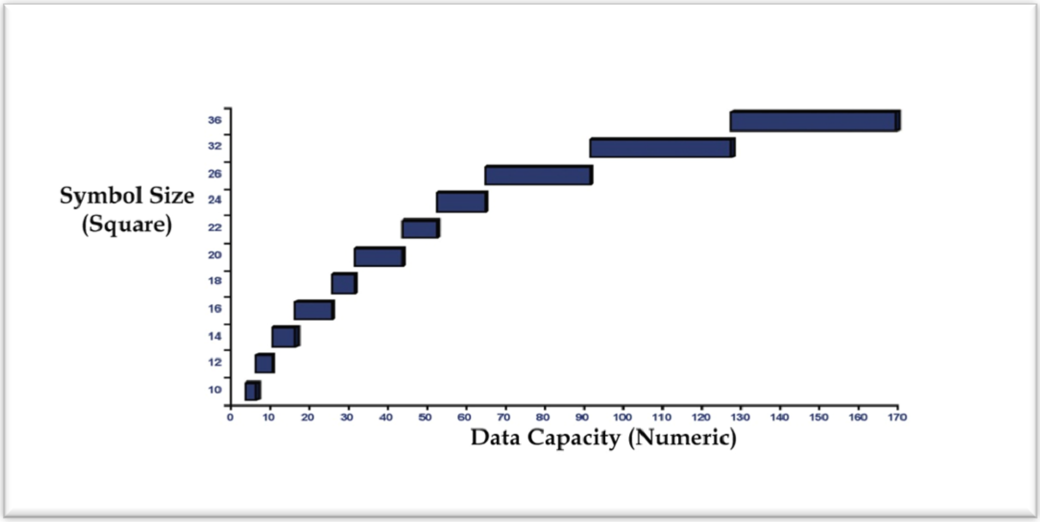


Figure 3.12 – Quantity of data encoded in a square Data Matrix in relation to the barcode dimension.

The following Table 3.4 shows the maximum number of data could be inserted in a square Data Matrix in relation with symbol size and Data Area dimensions.

Table 3.4 – Table of Data Matrix ECC 200 Symbol Attributes (Square form).

Symbol Size		*Data Region*		*Mapping Matrix Size*	*Total Codewords*		*Maximum Data Capacity*		*% of codewords used for Error Correction*	*Max. Correctable Codewords*
							Num	*Alph*		
Row	*Col*	*Size*	*N°*		*Data*	*Error*	*Cap*	*Cap*		*Error/Erasure*
10	10	8x8	1	8x8	3	5	6	3	62.5	2/0
12	12	10x10	1	10x10	5	7	10	6	58.3	3/0
14	14	12x12	1	12x12	8	10	16	10	55.6	5/7
16	16	14x14	1	14x14	12	12	24	16	50	6/9
18	18	16x16	1	16x16	18	14	36	25	43.8	7/11

Symbol Size		***Data Region***		***Mapping Matrix Size***	***Total Codewords***		***Maximum Data Capacity***		***% of codewords used for Error Correction***	***Max. Correctable Codewords***
							Num	***Alph***		
Row	***Col***	***Size***	***N°***		***Data***	***Error***	***Cap***	***Cap***		***Error/Erasure***
20	20	18x18	1	18x18	22	18	44	31	45	9/15
22	22	20x20	1	20x20	30	20	60	43	40	10/17
24	24	22x22	1	22x22	36	24	72	52	40	12/21
26	26	24x24	1	24x24	44	28	88	64	38.9	14/25
32	32	14x14	4	28x28	62	36	124	91	36.7	18/33
36	36	16x16	4	32x32	86	42	172	127	32.8	21/39
40	40	18x18	4	36x36	114	48	228	169	29.6	24/45
44	44	20x20	4	40x40	144	56	288	214	28	28/53
48	48	22x22	4	44x44	174	68	348	259	28.1	34/65
52	52	24x24	4	48x48	204	84	408	304	29.2	42/78
64	64	14x14	16	56x56	280	112	560	418	28.6	56/106
72	72	16x16	16	64x64	368	144	736	550	28.1	72/132
80	80	18x18	16	72x72	456	192	912	682	29.6	96/180
88	88	20x20	16	80x80	576	224	1152	862	28	112/212
96	96	22x22	16	88x88	696	272	1392	1042	28.1	136/260
104	104	24x24	16	96x96	816	336	1632	1222	29.2	168/318
120	120	18x18	36	108x108	1050	408	2100	1573	28	204/390
132	132	20x20	36	120x120	1304	496	2608	1954	27.6	248/472
144	144	22x22	36	132x132	1558	620	3116	2335	28.5	310/590

The sizes provided above are given in terms of numbers of rows and columns. For the Data Matrix ECC 200 square-form, the number of rows and columns can vary between 10 and 144 providing 24 different potential symbol sizes.

By contrast for the Data Matrix rectangle-form, however, the number of rows is between 8 and 16 and the number of columns between 18 and 48. The Data Matrix in rectangle-form allows six sizes (the square form has 24) and its use is less widespread than the square-form.

The dimensions refer to the area used by the Data Matrix symbol, when printed. When printing a Data Matrix ECC 200 the image size is dependent upon the following factors:

- The amount and format (numeric or alphanumeric) of the encoded information:
    - numbers and characters are encoded in terms of bits, represented by dark or light;
    - "dots" of an identical size. The larger the amount of bits required, the larger the symbol will be.
- The size of the X-dimension (see techniques for details);
- The choice of form: square or rectangular.

The Table 3.4 shows the maximum amount of data that can be encoded in the square and rectangular form of Data Matrix. At most, the Data Matrix can encode up to:

- 2,335 alphanumeric characters;
- 3,116 numbers.

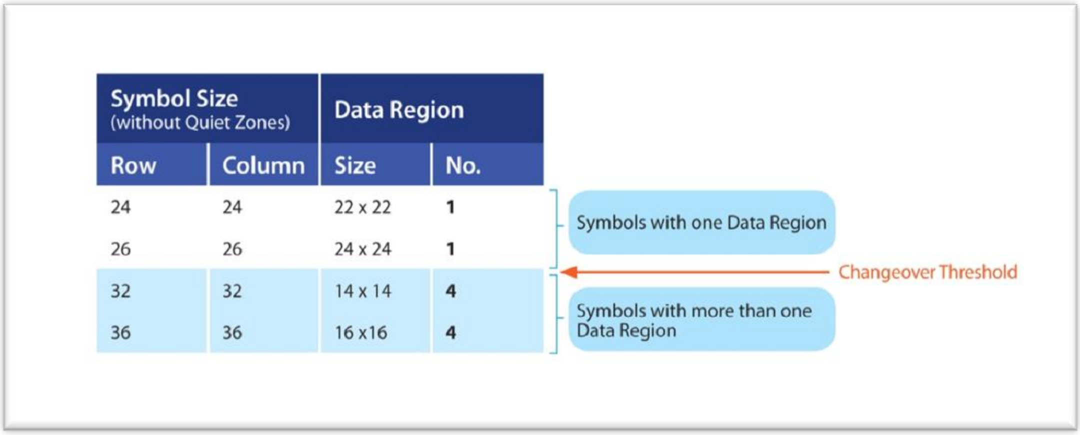
This maximum is based upon a square-form symbol made up of 144 rows and 144 columns divided into 36 Data Regions of 22 rows and 22 columns each.

For the Data Matrix in the rectangle-form, the maximum capacity is:

- 72 alphanumeric characters;
- 98 numbers.

The matrix symbol (square or rectangle) will be composed of several areas of data (or: Data Regions), which together encode the data.

The following Figure 3.13 shows an extract of ISO/IEC 16022, which gives details on how the Data Regions are composed. For example a symbol consists of 32 rows and 32 columns, including 4 sub-arrays of 14 rows and 14 columns. The number and size of "sub matrices" within the Data Matrix symbol are shown in the column "Data Region".



Symbol Size (without Quiet Zones)		Data Region	
Row	Column	Size	No.
24	24	22 x 22	1
26	26	24 x 24	1
32	32	14 x 14	4
36	36	16 x16	4

Symbols with one Data Region
Changeover Threshold
Symbols with more than one Data Region

Figure 3.13 – Symbol Size vs.. Data region dimension.

3.4.4.2 Error Correction in ECC 200

There are several methods of error detection. An example is the **check-digit** used by many linear bar codes, which use an algorithm to calculate the last digit of the number encoded. Check-digits can confirm if the string of data is encoded correctly according to the specified algorithm. In the case of a mistake, however, it can’t indicate where the mistake was made.

Another example is to repeat data encoded within a symbol, which will help to obtain a successful read even if the symbol is damaged. This is called **redundancy** and can lead to some confusion when applied to Data Matrix: for Data Matrix we will talk about “level of security”.

Indeed, the encoding of data in a Data Matrix symbol can be done using multiple ***security levels***. The two-dimensional structure allows the encoding of the data and mechanisms for correcting errors should they occur. These mechanisms enable the scanner to reconstitute some of the information in the event of a damaged or difficult to read Data Matrix symbol.

Several security levels are described in the Data Matrix standard ISO/IEC 16022 (Information technology - International Symbology Specification). Each of the Data Matrix code types: ECC 000; ECC 050; ECC 080; ECC 100; and ECC 140 has some form of error detection and correction.

Data Matrix ECC 200 is the only Data Matrix configuration which employs *Reed-Solomon error correction*. This feature allows, to a certain extent, the location of errors and, where possible, their correction.

The Reed-Solomon error correction:

- Calculates complementary codes and add-ins during the creation of the symbol,
- Reconstitutes the original encoded data by recalculating the data from the complementary codes and add-ins. The recalculation regenerates the original data by locating errors at the time of scanning. Such errors may be the result of printing problems, specular reflection or degradation of the printed surface.

Chapter 4 Hylemetric Applications

4.1 INTRODUCTION 147
4.2 BANKNOTE VERIFICATION BY HYLEMETRIC APPROACH 148
4.2.1 BANKNOTE VERIFICATION ENHANCEMENT BY IR BARCODE 164
4.3 ARTWORKS HYLEMETRIC AUTHENTICATION 173
4.3.1 OIL PAINTING AUTHENTICITY CASE STUDY 182
4.3.2 LITHOGRAPHY DIGITAL CERTIFICATE OF AUTHENTICITY CASE STUDY 186
4.4 DRUG PACKAGE AUTHENTICATION 203
4.4.1 WHITE LIGHT SPECKLE HYLEMETRY 205
4.4.1.1 UV Speckle PUF Template 210
4.4.1.2 Verification Phase 217
4.4.1.3 Analysis and Results 220
4.4.2 HOLOGRAPHIC BARCODE 229
4.4.2.1 Experimental results 235

4.1 Introduction

In this section the application of the Hylemetric paradigm to different object to ensure authenticity is presented. In particular the solution applied to banknotes, lithography and artworks in general, and drug packages, with indication of the necessary modification to be compliant with the different usage requirements.

In any case, all the proposed applications, proven in laboratory using optical systems and numerical simulations, follow the Hylemetric paradigm and for each object family a precise Hylemetric characteristic has been found or created ad hoc, to be used for template generation.

4.2 Banknote verification by Hylemetric Approach

There are many security features found in important documents (such as to banknotes, credit cards and so on) and used to defeat fraudsters. Several security features have been incorporated into the euro banknotes so that, upon careful examination, their authenticity can be reliably determined. They are integrated in the substrates of paper or added on it, and they are not commercially available to ordinary people [37, 97 – 98]. Since banknotes are a national product, their counterfeiting is a serious problem which affects everybody to some degree. The threat of counterfeiting is increasing, mainly because of the advancements in reprographic technologies that are currently available, or are in the development stage. Professionals can draw on sophisticated technologies such as colour photocopying and graphic scanning, allowing them to easily craft plausible notes. This type of counterfeiting, though limited, is swiftly growing and questions the value of print as a security feature on banknotes. A solution to this problem could be the use of a system uniquely linked to the banknote itself. To do this, it is necessary for a single banknote to find unique, unrepeatable, and unchangeable characteristics. If these features are present, it is possible to identify the banknote and to distinguish it from the others.

Using this approach, we think it is possible for mass products like banknotes to have a high security element, which remains secure for a long period of time, easy to produce and to use [37]. As a matter of fact, there are security features that are incorporated in the substrates of paper during its manufacture. Paper consists of a mixture of cellulose fibres and various chemical additives. The fibres are derived from wood, cotton, or pure cellulose in the case of superior papers; in the case of banknotes there are also metallic colour fibres in the paper pulp. In the banknotes, the paper fibre structure, and specifically the position of the above mentioned metallic colour fibres, are microscopic random features which are very hard to copy. These fibres can only be observed under ultraviolet light; when the banknotes are observed under ultraviolet light, they do not shine. On the contrary, the imitation banknotes do shine.

The key idea is not to create new features inside the banknotes [48], but to use this random distribution as biometry uses the random distribution of "minutiae" inside a fingerprint image. The position of these metallic fibres can be transformed into a binary pattern, which can be encoded using a cryptographic algorithm.

The method used for protecting banknotes against counterfeits essentially consists of three main steps:

- the banknote has to pass under the ultraviolet light to show the real random position of the metallic colour fibres;
- the metallic fibres have to be detected by using a video microscope, then digitized.

- The digitalized image has to be enhanced in order to distinguish the maximum number of fibres from the background, then encoded using a RSA algorithm (or a digital signature) to certify it [99].

All these steps are detailed here below in order to highlight how to obtain a secure code (template) from a banknote image.

The first step is the acquisition of a banknote image lightened by an ultraviolet lamp. The use of an UV light source is necessary to visualize where the metallic security fibres are, and to determine their positions inside the banknote area. In fact, these fibres are observable only via a UV light since they become fluorescent. For instance, euro notes contain red, green and blue fluorescent fibres. Imitations are frequently made by means of drawing or printing techniques, and quite a few of these are truly deceptive. In some cases all the three fluorescent fibres colours are present on counterfeits notes, since the fluorescent inks are commercially available, and preparing printable fluorescent inks is not so difficult an effort. Imitations are crafted with fluorescent inks that are visible in white light. Another indication of the originality of banknotes is that the security fibres are embedded in the paper pulp during their manufacture; this crafting method helps recognizing them from false fibres, since the original ones have a depth which is missing in the false ones. The distribution of these metallic fibres is random and inimitable (such as for fingerprints' minutiae). Each banknote can be told apart from the others using this random distribution. Due to the paper process followed to insert the security fibres, a different part of them is visible on each side of the banknote. For this reason the UV Light is used in transparency. The UV source is made using a panel (200 mm wide, 100 mm high), composed by 200 UV LEDs; each LED has dominant wavelength of 400 nm and luminous intensity of 350 mcd.

The setup for the second step is made by a digital camera which acquires the banknote image lighted from behind by the UV LEDs matrix. A possible set-up is shown in Figure 4.1, which highlights the relative simplicity of the security code creation system. The acquired image shows the metallic fibres in random position.

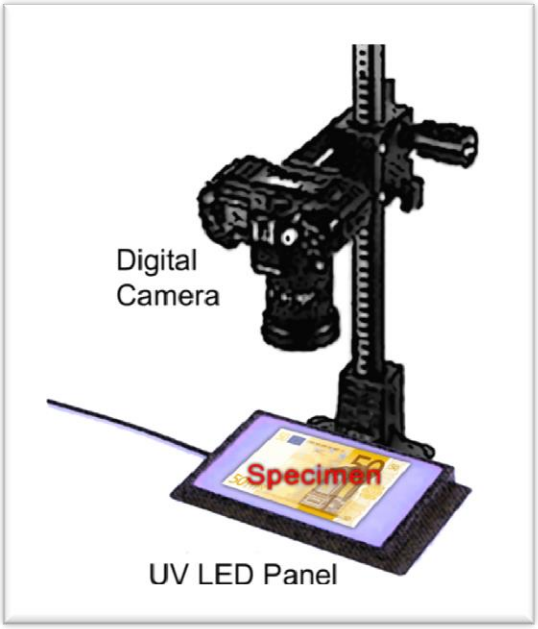


Figure 4.1 – Experimental setup for detection of metallic color fibres.

Finally, the UV image is enhanced using morphological transformations [107] with the aim of putting in evidence security fibres in respect to the note's background (see Figure 4.2). The morphological operation selected in this work is the Opening Top-Hat for its intrinsic characteristic to enhance lighter small details (i.e. fibres) from the darker background of a grayscale image. In particular the selected window has dimensions 3x3 pixels; this choice allow to better identify fibre objects inside the banknote image. From the resulting image after the morphological transformation it is clear that, as in biometry, the critical step is the selection of an adequate threshold in order to decide if a pixel belongs to a security fibre or to note’s background. Depending on the selected threshold, the number of false-positives (background pixels tagged as fibres) and false-negatives (fibres pixels tagged as background) varies.

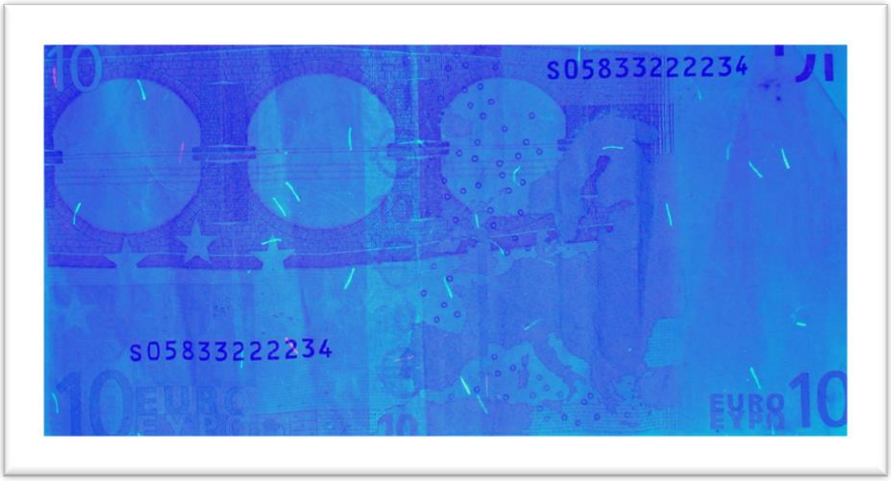


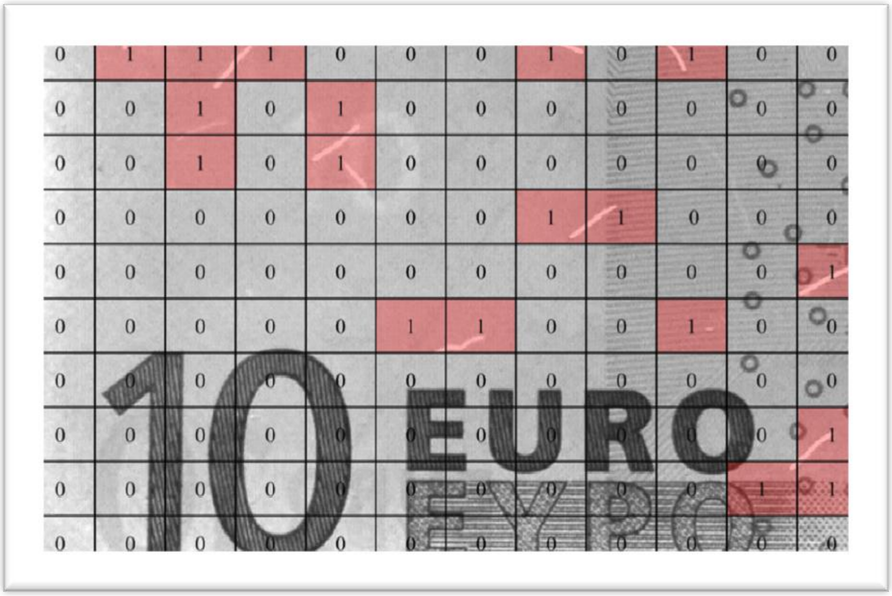
Figure 4.2 – 10 Euro banknote image acquired using UV light source. It is possible to see the random distribution of metallic security fibers.

The output of the Opening Top-Hat transformation is divided into cells of 32x32 pixels. The Image is resized, using standard bicubic method, in order to obtain image dimensions multiple of cells dimensions. The result is an image to be processed having, for the same banknote type, fixed dimensions. For instance, in our set-up, acquired 10 Euro banknote image has dimensions of 1111x2171 pixels, and the resized one is 1120x2176 pixels. To each cell we associate a value 0 or 1, obtaining a binary template (i.e. security code) related to the specific banknote type (i.e. 10 Euro) with fixed dimensions of 35x68 pixels.

In our experiments we have used the following fixed templates, one for each banknote type:

- 29x54 pixels for the 5 Euro notes;
- 35x68 pixels for the 10 Euro notes;
- 49x92 pixels for the 20 Euro notes;
- 57x106 pixels for the 50 Euro notes.

If one 32x32 pixel cell does not contain a security fibre, we associate the value 0 (i.e. lack of metallic fibres) to the corresponding template element, otherwise, we associate to it the value 1 (i.e. presence of at least a part of a metallic fibre) (see Figure 4.3).



0	1	1	1	0	0	0	1	0	1	0	0
0	0	1	0	1	0	0	0	0	0	0	0
0	0	1	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	1	1	0	0	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	0	0

Figure 4.3 – Particular of the same 10 Euro banknote, with superposed a controlling grid. The algorithm assigns a value of 1 to each cell in which is present one or part of a fibre.

The decision method used for setting a template element to 0 or 1, is based on a statistic approach. For each cell we have calculated the mean value and the standard deviation and, for this, we have set the binarization threshold to the mean value plus twice the standard deviation. This choice is based on the fact that fibres pixels are lighter than background ones. After that, we have matched each pixel of a cell with the related threshold: if more than the 1% of the pixels (in our system 10 pixels) results to be greater than the threshold, we set the template value related to that cell to 1, otherwise to 0.

Obviously, other techniques for best segmentation are present in literature [100]. In any case the proposed technique, for this application, allows obtaining very good results.

The choice of the best threshold value in the Hylemetric approach is similar to the determination of the best biometric threshold value, used for optimizing the False Acceptance Rate (FAR – the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percentage of invalid inputs which are incorrectly accepted) and the False Rejection Rate (FRR – the probability that the system fails to detects a match between the input pattern and a matching template in the database. It measures the percentage of valid inputs which are incorrectly rejected), with the aim to obtain the Equal Error Rate (EER – the rate at which both accept and reject errors are equal. The lower the EER is, more accurate the system is considered to be).

For determine the segmentation threshold used in this paper we have conducted a set of tests with the aim to determine the experimental FAR and FRR curves for each type of banknote. First of all we have acquired 20 exemplars of 20 € banknote and we have verified the possibility that one of the 19 non correct banknote can be erroneously identified as the last one, for each acquired notes (i.e. 380 tests in total). The result is the False Acceptance Rate curve for 20 € banknotes.

After that we have acquired a 20 € banknote in perfect conditions; after the acquisition we have ruined the banknotes in different ways (i.e. creased, punched, folded, written, washed) and them are acquired several times after each ruining treatment, obtaining a new set of 10 ruined images for each perfect note to be used for determine the False Rejection Rate for the 20 € notes (i.e. 200 tests in total).

The resulting FAR and FRR curves are shown in Figure 4.4. The two curves allow to determine the threshold with identify the Equal Error Rate (EER) for the 20 € notes. In our case the identified value is 1% of template difference, which gives optimum results in any test.

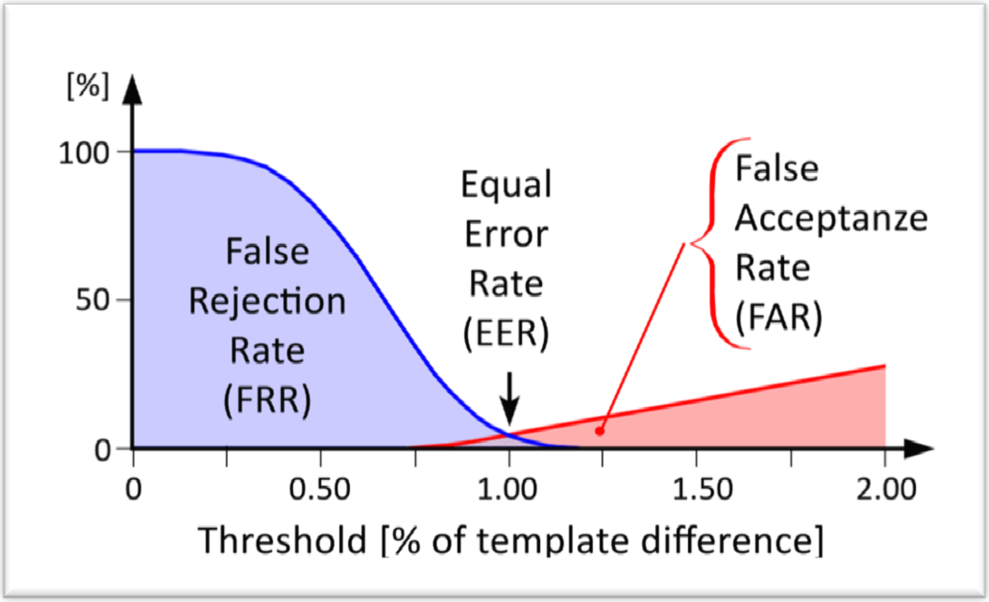


Figure 4.4 – FFR and FAR curves; EER identifies the threshold to be used in the verification procedure. It has to be noted that the FAR curve seems to have a non standard slope because our studies are limited at template difference under 2%.

The last step consists in the encryption of the binary controlling grid using an appropriate cryptographic system. The encrypted encryption minutiae can be stored by the National Central Bank Authority, originator also of the banknote itself. This signature (made by the binary code of the minutiae positions) can be stored in a central database, associated to the banknote numerical code. If someone wants to verify if a banknote is original or counterfeited, it has to extract the digital signature from the interested banknote and compare it with the ones obtained from the central Bank Database in a secure and encrypted way.

In the following the steps an authorized entity has to follow to verify the authenticity of a banknote are detailed. First of all, it has to log to the central database, as depicted before, send the banknote numerical code and retrieve the digital signature file, in a secure way. Secondarily the verification entity has to create its own controlling template, following the same steps described in the previous paragraphs,. Eventually it has to confront the extracted template code with the decoded one. Due to possible note physical problems (e.g. banknote ruined, creased, folded, wrinkled, with holes etc.), it is possible that the controlling template created in verifying phase could be quite similar, but not identical, to the extracted one, even if using the same codifying threshold. For this reason, it is proposed a XOR approach between the two template, which allow to check the coincidence bit at bit. The result will be a numerical value equal or less then (in the previous 10 € case) 35x68 = 2380 (template dimensions). The originality is verified if the computed template differs from the extracted one for less than 1% of bits (EER value previously determined); so the verifying threshold in the 10 Euro case is set to 2356. The solution is obviously depending on the implementing choices made in this paper. The described situation is related to the 10 Euro banknote, as before mentioned. Due to different dimensions of other banknotes (in particular 200 and 500 Euro), we have different image dimensions, and so different template dimensions.

The set-up for verifying the originality of a banknote, due to the relative simplicity of the proposed approach, could be made in a compact way, and similar to the one used for the controlling code creation.

The experimental results are related to 5, 10, 20 and 50 Euro notes, in perfect case and in simulated ruined ones. All the results demonstrate the validity of the proposed *Hylemetric* approach, in particular in case of a high security fibres distribution.

The following Figure 4.5shows a subset of used banknotes as acquired after UV illumination. Different secure fibre distributions among different notes are clearly visible in this figure.

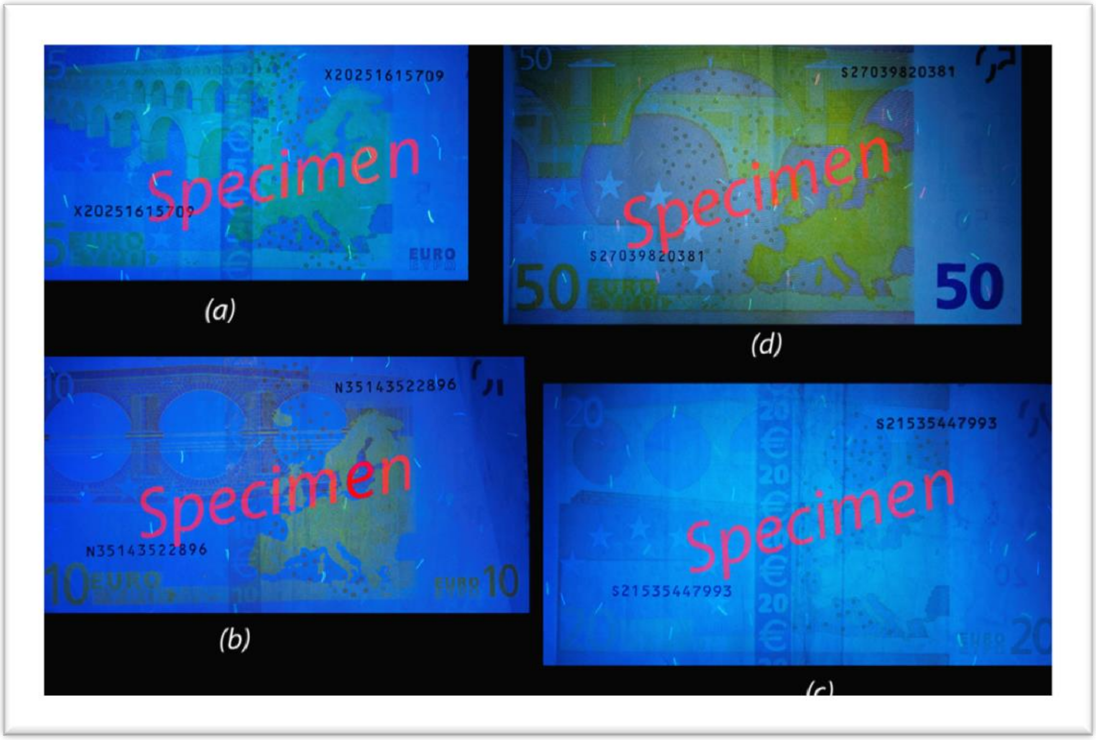


Figure 4.5 – Specimens used in test step: (a) 5 Euro banknote with secure fibers high density; (b) 10 Euro banknote with some shadows; (c) 20 Euro banknote with high exposure; (d) 50 Euro banknote with secure fibers medium density.

The first test case is made on a 20 Euro banknote acquired as described before. First of all, the RGB acquired image is greyscaled, to allow best result with the used Opening Top Hat transformation. The result is shown in Figure 4.6(a). After this step, Top-Hat morphological transformation is applied, obtaining a black and white image representing only the security fibres distribution. Obviously, due to the process and to the not homogeneous intensity of each fibre, some of them are lost. The result is shown in Figure 4.6(b). After having applied the macro-cells algorithm, the obtained schema is the one shown in Figure 4.6(c). Eventually in

Figure 4.6(d) is shown the extracted template, which correctly identifies the majority of security fibres; only the less visible ones are discharged. It has to be noted that there are also some few controlling cells which match no fibres: this phenomenon is due to the statistical threshold used.

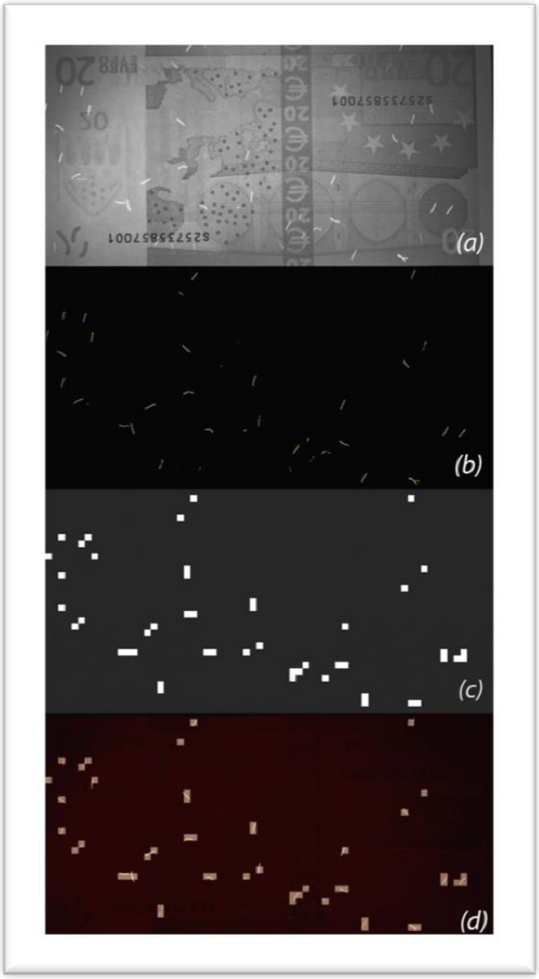


Figure 4.6 – (a) a 20 € note UV image in grayscale; (b) the output of the morphologic transformation on the previous image; (c) the related controlling grid and (d) the superposition of image (b) and (c).

Another test demonstrates the possibility to extract and verify the template from a banknote digitally ruined; this test simulates the real situation of banknote verification in case of loss of security fibre information. A 10 € banknote is acquired and its UV image is digitally ruined in different ways (Figure 4.7(a), (b) and (c)). In the first two cases the banknote is still recognized, due to the tolerance introduced in the verification system to manage these situations. In the last case (Figure 4.7(c)) the banknote is discharged, due to the great missing area (more than 15% of the original one).

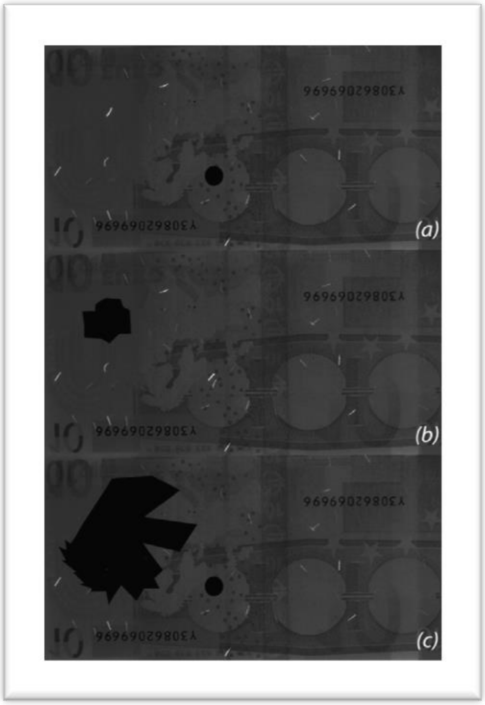


Figure 4.7 – A 10 Euro note with three increasing ruined areas: (a) and (b) are still recognized due to the tolerance introduced in the system, whereas (c) is considered not accepted.

In order to demonstrate that different banknotes have different security fibre distribution, it is proposed a test on two different 20 € notes (see Figure 4.8(a)(b)). Due to the random distribution, if a 32x32 cell is used to extract the template values, it is not possible having two banknote with the same template. This assertion is true if the cells dimension is not too much wide, allowing a lot of security fibres to have their local position inside a unique cell.

This situation leads to a great probability to obtain two template related to two different banknotes to much similar; in this case the verification system could recognize the two banknote as the same. In our approach the problem is a bi-dimensional one, due to the fact that the proposed system has two different “thresholds”, which needs the identification of two different EER: cells dimension threshold and binarization threshold. In our approach is clear that the same cell dimension is needed for similar banknotes (e.g. 32x32 pixels for 5 and 10 €), but good results are also achieved using greater cells (50x50 or 64x64 pixels in particular on 20 and 50 €). Cells with lower dimensions not introduce false positive/negative cases, but the necessary computational resources are higher respect to the related advantages, so it is decided to use always cells with dimensions equal to 32x32 pixels, which allow having good fibres recognition with a relatively low computational effort.

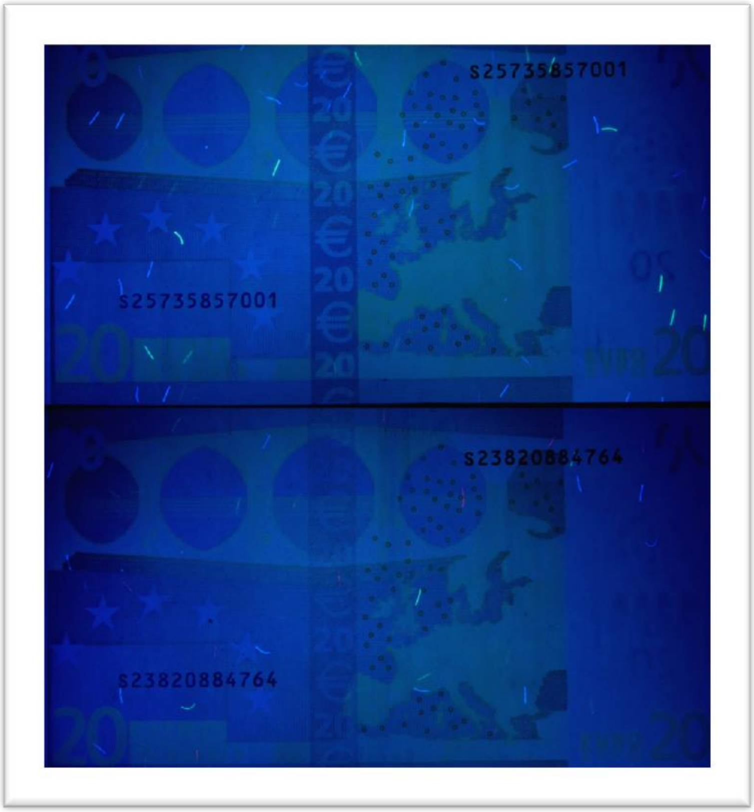


Figure 4.8 – Two different 20 Euro note which show how different can be the security fibers distribution in similar banknotes.

The question related to the threshold used for binarizing the extracted image by means of the proposed morphological transformations has been yet deeply discussed. Eventually, to verify the reliability of the proposed technique we have tested the system with 10 banknotes of 5 €, 10 banknotes of 10 €, 10 banknotes of 20 € and 10 banknotes of 50 €, using the threshold value statistically determined as above-described, both with new notes, ruined ones and digitally destroyed ones, and the results are reported in Table 4.1.

Table 4.1 – Reliability of the system vs.. banknotes type and banknotes manipulation.

Notes	Test description	Number of tests	Number of Errors
5€	“original” vs.. “fake”	90	0
	“original” vs.. “original ruined”	20	2
	“original” vs.. “fake ruined”	20	0
	“original ruined” vs.. “fake”	20	1
	“original ruined” vs.. “fake ruined”	20	0
10€	“original” vs.. “fake”	90	0
	“original” vs.. “original ruined”	20	1
	“original” vs.. “fake ruined”	20	0
	“original ruined” vs.. “fake”	20	0
	“original ruined” vs. “fake ruined”	20	0
20€	“original” vs. “fake”	90	1
	“original” vs. “original ruined”	20	1
	“original” vs. “fake ruined”	20	0
	“original ruined” vs. “fake”	20	1
	“original ruined” vs. “fake ruined”	20	0
50€	“original” vs. “fake”	90	0
	“original” vs.. “original ruined”	20	1
	“original” vs. “fake ruined”	20	0
	“original ruined” vs. “fake”	20	0
	“original ruined” vs. “fake ruined”	20	0

4.2.1 Banknote verification enhancement by IR Barcode

The main drawback of the proposed method is the necessity to have an active security connection with the related central bank for verifying the extracted information with the recorded ones. In this paper, for overcoming this limitation, a Hylemetry approach is integrated with asymmetric cryptography, allowing distinguishing counterfeited banknotes from the genuine ones using only information present on the notes themselves.

The necessity of a secure connection with a central bank database has some obvious disadvantages:

- The central bank has to store a great amount of data (at least one for each banknote);
- The verification authority has to have always available a secure connection;
- The secure connection has high cost for neglecting any "man in-the-middle" attack.

For these reasons, a solution which allows verifying a banknote using only information present in the notes itself is presented as enhancement of the previous approach. This proposal has the necessity to introduce a public key cryptographic schema, which allows avoiding the secure connection with the central bank, granting in any case a high security level. The encoded information now are directly printed on the banknote itself and are intrinsically connected with the physical and security characteristics of the related note (i.e. florescent security fibre s position).

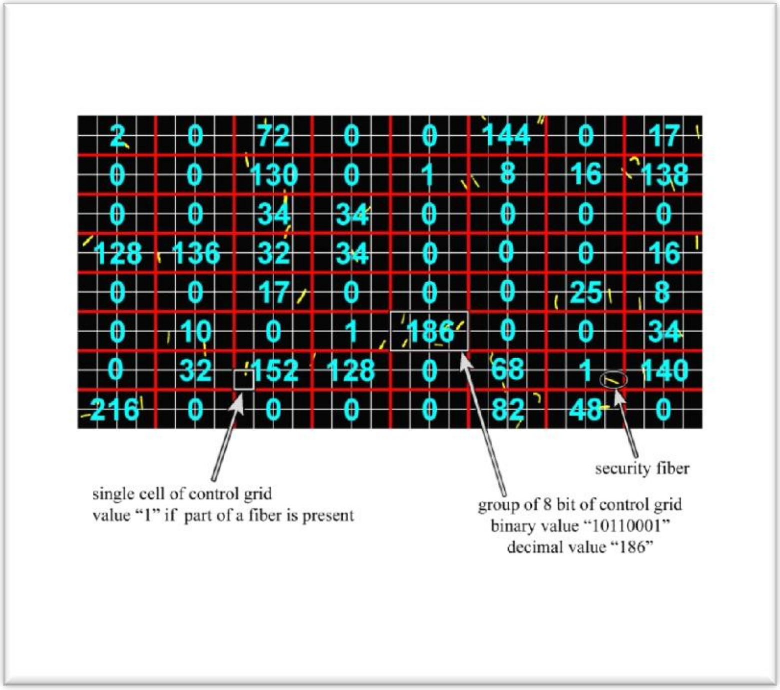
The first step consists in the acquisition of a banknote image lightened by an ultraviolet source. The use of an UV light source is necessary to visualize where the metallic security fibre s are, and to determine their positions inside the banknote area. In fact, these fibre s are observable only via a UV light since they become fluorescent under this kind of illumination. The distribution of these metallic fibre s is random and not reproducible (such as for fingerprints' minutiae). Each banknote can be told apart from the others using this random distribution.

Due to the paper process following insertion of the security fibre s, a different part of them is visible on each side of the banknote. In this paper the UV source is made up using four UV lamps, composed by 41 UV LEDs each; any LED has dominant wavelength of 355 nm and luminous intensity of 50 mcd. The four lamps set-up is made for creating approximately uniform illumination and the possibility of acquiring good quality images (obviously other method of illumination can be used – the illumination system is not a critical point for the proposed schema). The image is then digitally acquired using a Lumenera 105M camera, and a UV cut-off filter. The choice of this camera is due to its high sensitivity from UV to FIR. In this particular case, we use also a filter for eliminating the dominant UV high energy information, which interferes with the extraction of fibre s in the visible spectrum.

From the digitalized image, using segmentation processes described in the previous section, it is then possible to extract a binary template, which is a binary representation of the security fibre s position (a kind of banknote fingerprint).

The last step consists in the encryption of the binary control grid using an asymmetric cryptographic system and the creation of a 2D barcode containing the encoded information.

In our method banknote is divided in a control grid with dimensions 16x32, obtaining a template of 512 bit, which corresponds to a string of 64 decimal numbers, from 0 to 255, converting each group of 8 bit from binary to decimal base. Figure 4.9 shows the digitalized UV-lighted banknote image with superposed the control grid and the resulting decimal template.



2	0	72	0	0	144	0	17
0	0	130	0	1	8	16	138
0	0	34	34	0	0	0	0
128	136	32	34	0	0	0	16
0	0	17	0	0	0	25	8
0	10	0	1	186	0	0	34
0	32	152	128	0	68	1	140
216	0	0	0	0	82	48	0

single cell of control grid
value "1" if part of a fiber is present

group of 8 bit of control grid
binary value "10110001"
decimal value "186"

security fiber

Figure 4.9 – 20 Euro banknote image acquired using UV light source with superposed the control grid and the resulting decimal template.

It has to be noted that, if in verification phase we obtain a template different from the original one only for the position of one single fibre (or part of it) the encoded version of the template results completely different and the system refuse the banknote. If we encode separately any fibre information (or a group of them) it is possible recognize a genuine note, introducing a threshold based on minimum number of recognized fibres (or group of them). To create a system robust to data loss (banknote deterioration) we encrypt any number one by one. If we use as asymmetric cryptographic a typical 1024 RSA algorithm [99, 101], the resulting encoded string is 65536 bit long. In practice, it is very difficult insert such a great amount of data in a standard 2D barcode, which is the output of our scheme. This problem can be overcome using Elliptic Curve Cryptography (ECC) [102] instead of RSA; in particular it possible obtaining better security robustness then 1024 RSA algorithm using a 192 bit key length ECC [103].

We have decided, in our approach, to use a standard 144x144 Data Matrix barcode, as defined in ref. [71], it is possible enclose up to 1558 byte of binary information. This capacity is sufficient for our use. In fact, starting from a 512 bit template it is possible using a 2x4 mobile mask, which allows encoding 8 pixels in a decimal number from 0 to 255, obtaining a 64 number string. The ECC 192 coding gives as result an encoded binary string of 1536 bytes, compatible with the max amount of storable information in the selected barcode.

After that, we have to select the banknote area in which we will put the barcode. Analysing the IR banknote image is clear that there is very few information in this spectrum. Therefore, we have decided to put the IR barcode on one side of the banknote, doubling it in both the right and left part, allowing extracting information also having only part of the note itself. Due to the dimension of the selected area, it is possible enclose in the note a 2D square barcode with 45x45 mm side dimensions, allowing having no interference with the note's serial number (which is also visible in the IR spectrum).

This barcode can now be printed on the banknote as described before, using an IR ink; in this way it can be controlled only using an infrared scanner, similar to the ones used for verifying other banknote's infrared security features.

In Figure 4.10is possible view a virtual example of the banknote IR information barcode superposition, with near the barcode position inside note and highlighted a portion of Data Matrix barcode used in this work.

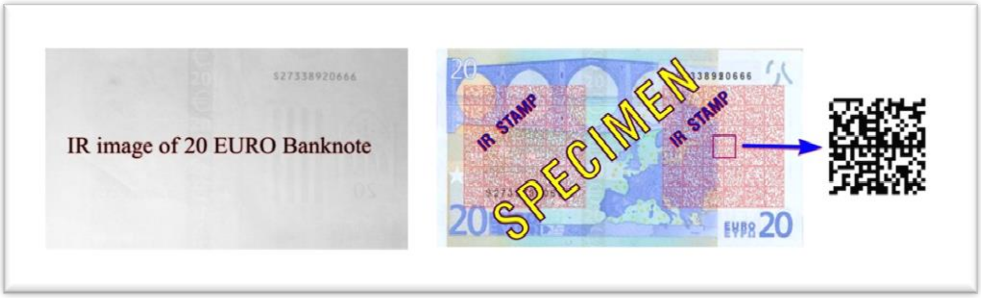


Figure 4.10 – Virtual example of 20 Euro banknote with two IR 2D barcode superposition.

In the following, steps an authorized entity has to follow to verify a banknote authenticity are detailed. Due to the introduction of the 2D Data Matrix Barcode, it is not necessary to the verification authority logs into a secure database, but it has only to extract UV security fibres, construct the new control grid, convert it in a numerical string as described before and verifying it with the encoded string presents in the IR 2D barcode.

The only information needed outside the banknote is the public keys used for decode string extracted from the barcode. So now the central bank authority has to maintain only a couple of 160 bit keys for each banknote (or banknote group), instead of 2x1024 bit RSA keys and a 2664 bit controlling grid to be sent in an encrypted form. It is also possible having a unique set of public keys, stored in the verification system, which eliminates any connection with central bank servers. Obviously only the Central Bank, which officially emits banknotes, has the private 196 bit ECC key necessary to create the encoded barcode.

Also in this new approach, due to possible note physical problems (e.g. banknote ruined, creased, folded, wrinkled, with holes etc.), it is possible that the controlling template created in verifying phase could be quite similar, but not identical, to the extracted one. For this reason, it is proposed a correlation approach between the two controlling codes (i.e. numerical strings converted in binary strings), which allow to check the coincidence bit at bit. The originality is verified if the computed controlling code differs from the extracted one for less than a threshold of the bits value (EER value previously determined).

Figure 4.11 summarizes all the described steps, both for creating the 2D barcode and verifying banknotes.

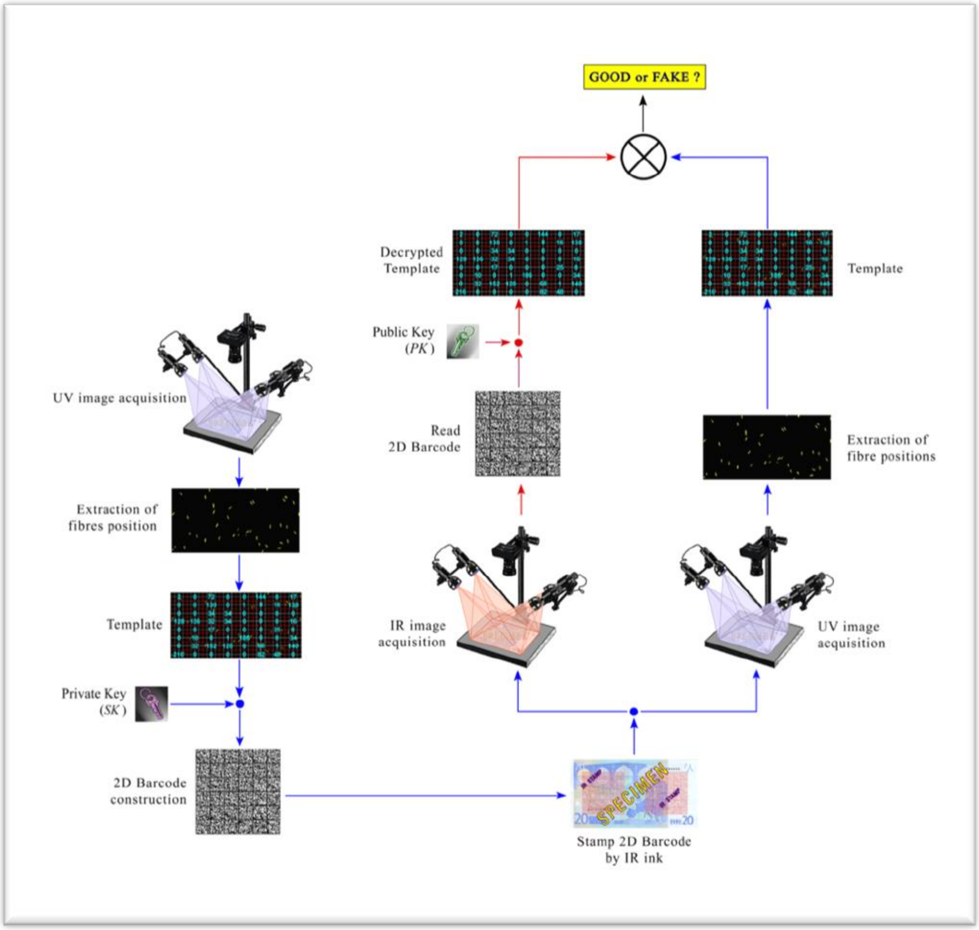
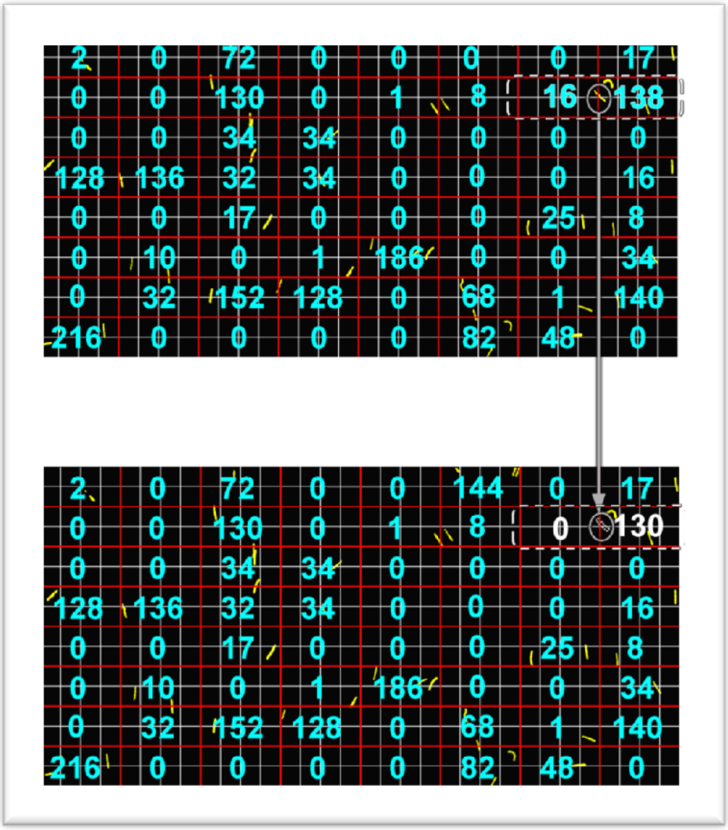


Figure 4.11 – Summarization of all the described method steps, both for creating the 2D barcode and verifying banknotes.

Obviously, during the fibres position acquisition and template extraction, it is possible that one or more fibres, (cause noise or deterioration of the banknote), are not detected. As shown in Figure 4.12, the loss of a singular fibre leads to a different decimal value, respect with the template extracted from the IR barcode one. In this situation, the banknote can be recognized as genuine or not in relation with the selected verification threshold. High thresholds lead to severe systems, which becomes fragile to banknote normal corruption, whereas low thresholds leads to systems that can recognize as genuine also fake banknotes. In our experiments, we had used a threshold equal to 1% of code difference, allowing recognizing banknotes also after wearing to normal banknote usage and manipulation.



2	0	72	0	0	0	0	17
0	0	130	0	1	8	16	138
0	0	34	34	0	0	0	0
128	136	32	34	0	0	0	16
0	0	17	0	0	0	25	8
0	10	0	1	186	0	0	34
0	32	152	128	0	68	1	140
216	0	0	0	0	82	48	0

2	0	72	0	0	144	0	17
0	0	130	0	1	8	0	130
0	0	34	34	0	0	0	0
128	136	32	34	0	0	0	16
0	0	17	0	0	0	25	8
0	10	0	1	186	0	0	34
0	32	152	128	0	68	1	140
216	0	0	0	0	82	48	0

Figure 4.12 – The loss of the singular highlighted fiber leads to a different template, in one or more elements, from the information extracted by IR barcode. In this situation, the banknote can be recognized as genuine or not in relation with the selected verification threshold.

4.3 Artworks Hylemetric Authentication

The main problem when we buy an artwork object consists in getting a certificate of authenticity, in particular for the artwork bought through a seller and not at first hand from artist. There is a tremendous abuse in the “certificate of authenticity” business because, unless it is originated and signed directly by the artist, but by the publisher of the art (in the case of limited editions), a confirmed dealer or agent of the artist (not a third party or reseller), or an acknowledged expert on the artist, all those certificates are pretty much meaningless. A legitimate one must contain specific details about the artwork, such as when and how it was produced, the names of people or companies involved in its production, dimensions, and the names of reference books or similar resources that contain either specific or related information about either that work of art and/or the artist. It should also state the qualifications and full contact information of the individual or entity that authored the certificate, and include his or her complete and current contact information.

Unfortunately, often these certificates are exchanged between similar artworks: the same document is supplied by the seller to certificate the originality of more than one single artwork. In this way the buyer could have a copy of an original certificate to attest that the “not original artwork” is, instead, an original one. Unfortunately, most people believe that art with a certificate is automatically genuine, but that’s not even close to truth [96]. It happens because does not exist a law rules who is (or is not) qualified to produce certificates of authenticity, or what types of statement, information or documentation a certificate of authenticity must contain. In other words, anyone can write a certificate whether they are qualified or not. As if that is not bad enough, unscrupulous sellers forge false certificates of authenticity and use them to either sell outright fakes or to misrepresent existing works of art as being more important or valuable than they actually are [104]. A possible fraud can be put the following way into effect: an art merchant, starting from an original lithography and its original certificate of authenticity, duplicates both and sells false artwork as genuine using false certificate of authenticity as clue of originality.

A solution for this problem would be put in action a system that links together a certificate to a specific artwork. In this way the inappropriate usage will not be possible and the buyer will be able to verify the originality by himself. To do this it is necessary, for a single artwork, to find unique, unrepeatable, and unchangeable characteristics. If these characteristics are present, we have the possibility to identify the artwork and to distinguish it from another one.

Many works defined different approaches to identify objects unique characteristics in a way similar to biometry, choosing the opportune characteristic [43, 48, 51, 83, 85].

In any artwork is possible finding a characteristic, which match with the previous reported lists. In particular, artworks, due to the way on which they are produced, have an intrinsic randomness, due to the hand-made process. Analysing some different example, reported in Figure 4.13, it is possible identifying speckle-like structures in all of them. In particular Figure 4.13(a) reports an oil paint, with highlighted the certificate area, Figure 4.13(b) shows the same information related to a sculpture, and Figure 4.13(c) related to a lithography.

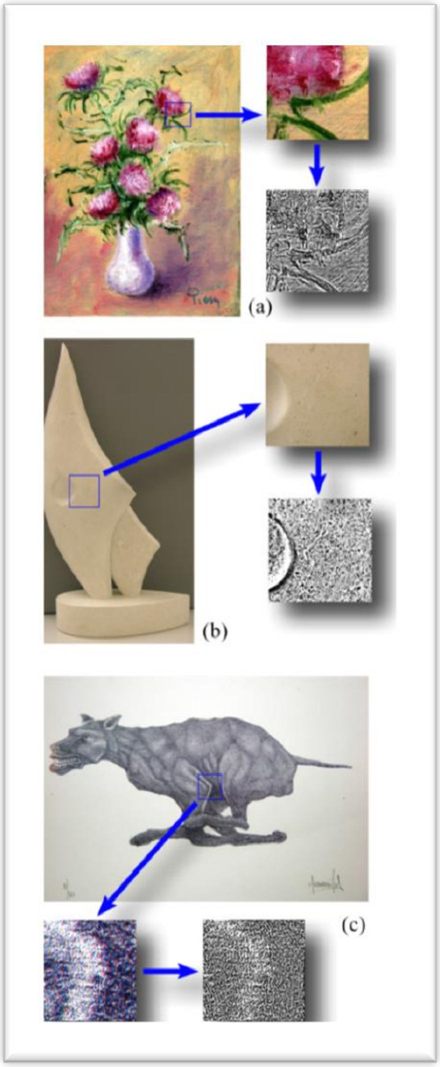


Figure 4.13 – (a) oil paint; (b) stone lithography (c) sculpture. Are highlighted the related verification areas and the extracted HHPs.

The process for creating a Hylemetric digital certificate of authenticity, is based on the extraction, from a specific area of an artwork, a random pattern difficult/impossible to reproduce. This allows defining the Hylemetric approach as a one-way function, defined in the following as Hylemetric Hash Pattern (HHP). The HHPs extracted from the reported examples are shown in Figure 4.13 too.

If we refer, for sake of simplicity, only to Oil paint, reported in Figure 4.13(a), the first step is identifying an acquisition area and, inside it, defining a set of trust points. The trust points are used to allow the correction of geometrical distortion that can be introduced in verification phase. Figure 4.14(a) shows oil painting and related identified authentication area. On the authentication area (Figure 4.14(b)) are reported selected trust points (four in this example). Figure 4.14(c) shows the area acquired during verification phase and the related trust points used to geometrically correct this image before matching phase. The next step, is the creation of a HHP based on the acquired area. In the reported example, the HHP is carrying out with a grey-levelling, high pass filtering, normalization, and subsequent thresholding (see Figure 4.14(d)). The result has speckle-like appearance, allowing to applying, in verification phase, typical speckle metrology techniques, as described in the following sections.

The image shown in Figure 4.14(b) in reported (with low resolution) in a digital authenticity certificate. On the digital authenticity certificate will be also present the HHP related to the authentication area. To avoid certificate digital counterfeiting, it has to be digitally signed, using a classic Digital Signature approach (Digital Signature Standard - DSS), based on PKI infrastructure [105].

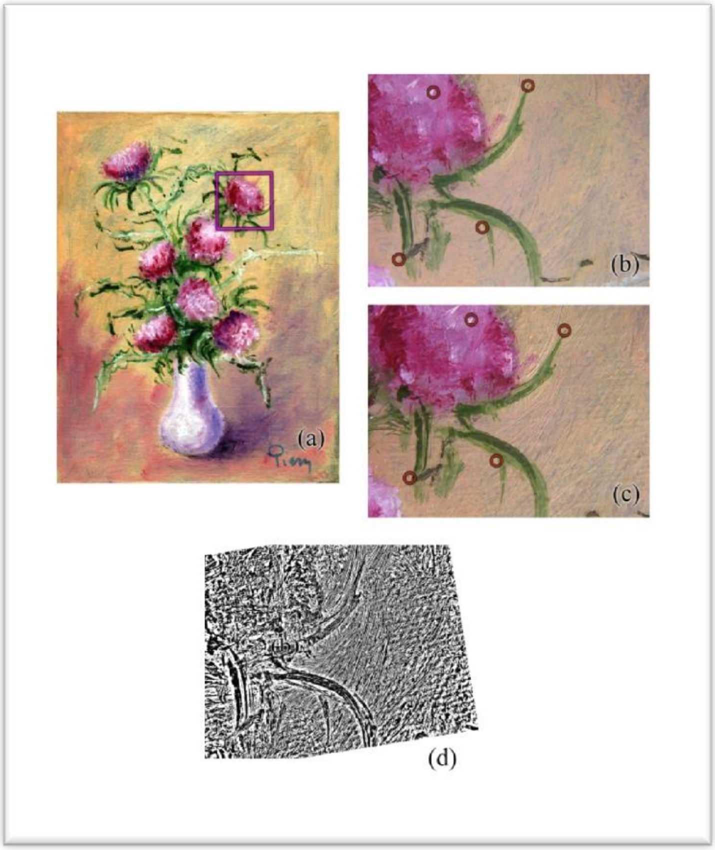


Figure 4.14 – (a) oil painting with highlighted the selected verification area; (b) authentication area with trust points; (c) area acquired during verification phase, with highlighted used trust points; (d) Hylemetric Hash Pattern related to (c) after geometrical corrections.

Referring to Figure 4.13, it easy notice that the three HHPs, even if extracted from three different artworks, produced with different instruments and techniques, are very similar.

Summarizing, the digital certification of authenticity contains: the low resolution image of the verification area; clear indication of trust points; HHP pattern. In addition, digital certificate is signed by a DSS approach.

The first step to verify the authenticity of artworks (in our example oil paint) consists of acquiring the image of the verification area (I_T - Test Image). During this process of acquisition it is not possible acquiring a portion perfectly identical to the one present in the certificate of authenticity. Besides, some geometric distortions can be introduced. In other words, during the acquisition of the authentication area with a typical digital camera, it is easy that we get a bigger or smaller portion of image around the interested zone (with consequent scale error introduction), with some roto-translations (referred to original certification image), and can be also affected by some acquisition distortion, due to lens system used (e.g. barrel). To correct all the reported distortions, the system, by means of trust points, applies image transformations (e.g. affine, polynomial, reflective, etc.) so that Test Image (I_T) becomes very similar to the image of the verification area inside the digital certificate of authenticity (I_C).

As described in [106 – 107] is possible correcting a great amount of errors selecting trust points on the two figures. Trust points are points present in both the two images, which clearly identifying the same real point. In this work we have used, in particular, affine transformations.

Verification software, after having acquired trust points, automatically applies the correct transformation, which allows obtaining a corrected version of I_T to be used during matching phase.

After having applied geometrical transformation, it is possible extracting the HHP from the transformed image $I_T^{'}$. The process is the same used for creating the HHP related to certificate image.

The last step consists in matching HHP_C and HHP_T, the Hylemetric Hash Patterns extracted from the digital authenticity certificate (and related to I_C), and from the geometrically corrected test image $I_T^{'}$ respectively.

Due to possible residual geometrical distortion and presence of noise, it is still possible that HHP_T could be little different from HHP_C, even if in case of original artwork and related certificate. Therefore, considering also that all the *HHPs* have a random structure, the comparison among HHP_T and HHP_C, is based on digital cross-covariance calculation, similar to the one used in speckle field measurement [108]. In particular, the cross-covariance formula used in this work is:

$$C_\alpha(\Delta x, \Delta y) = F^{-1}\left[\frac{F^*(HHP_C)F(HHP_T)}{\left|F^*(HHP_C)F(HHP_T)\right|^\alpha}\right]. \tag{4.1}$$

In Eq. (4.1), $(\Delta x, \Delta y)$ are the correlation peak coordinates, F and F^{-1} are the forward and backward Fourier Transform operators respectively, and * means the complex conjugate. Eq.(4.1) is efficiently calculated using a Fast Fourier

Algorithm. The coefficient α controls the correlation peak width. Optimum values range is from $\alpha = 0$, for images characterized by high spatial frequency content and high noise level, to $\alpha = 0.5$, for low noise image with less fine structure. For α values greater than 0.5, the high frequency noise is magnified. In our experiment we have always used $\alpha = 0.5$ values, also in case of noisy test images, obtaining in any case good results.

As in biometric approach, also Hylemetry introduce a correlation threshold, necessary to define if the two HHPs are similar enough to be considered the same. The threshold used in this case is defined as follow:

$$\begin{cases} C_\alpha < T_\alpha & \text{false artwork} \\ C_\alpha \geq T_\alpha & \text{genuine artwork} \end{cases}. \tag{4.2}$$

The selection of the appropriate threshold is based on the minimization of False Acceptance Ratio, such as the percentage of false artworks recognized as true, respect the total amount of verification tests (it has to be noted that the introduction of geometrical correction has highly reduced False Rejection Ratio, due to genuine lithography recognized as counterfeited).

The following Figure 4.15 shows the previously described process.

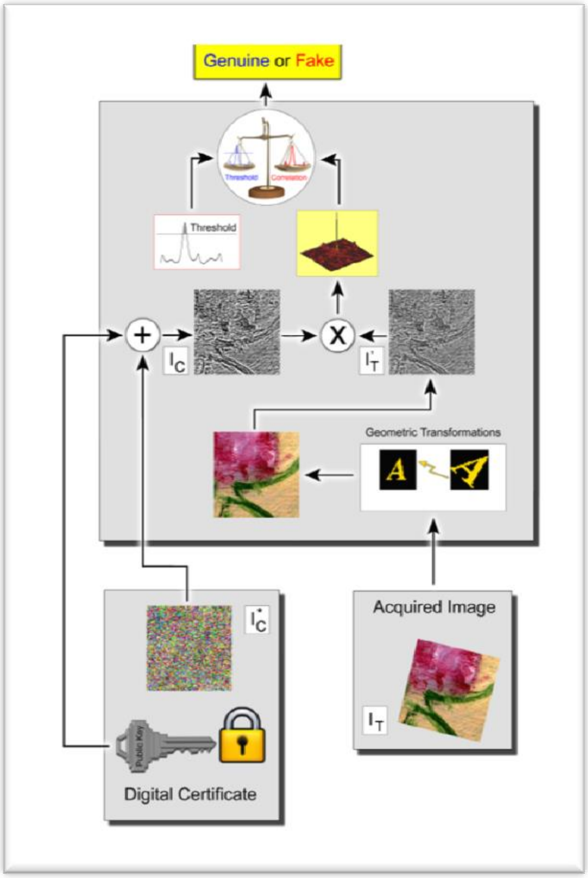


Figure 4.15 – Complete schema showing the artwork verification phase.

In the following sections some artworks cases are reported, with relevant results. In particular the cases of Oil Painting and Stone Lithography have been analysed, due to their large presence in the artworks market, and the highly percentage of counterfeited copies widely diffused.

4.3.1 Oil Painting Authenticity Case Study

In this section some experiments made on real oil paint are reported. For their execution we have create a dedicated Matlab$^{©}$ program, which allows the human verifier to select verification areas among the two images, to input the trust points, having also a help system for selecting the same points on the two images. Obviously the software does not implement any automatic solution, which is a possible enhancement to the previously described procedure.

In this work, the acquisition was made using a commercial Nikon Coolpix 8700 Camera, with embedded Nikkor ED 8.9-71.2 mm objective, staying in front of the interested artwork area at ≈ 10 cm with macro function.

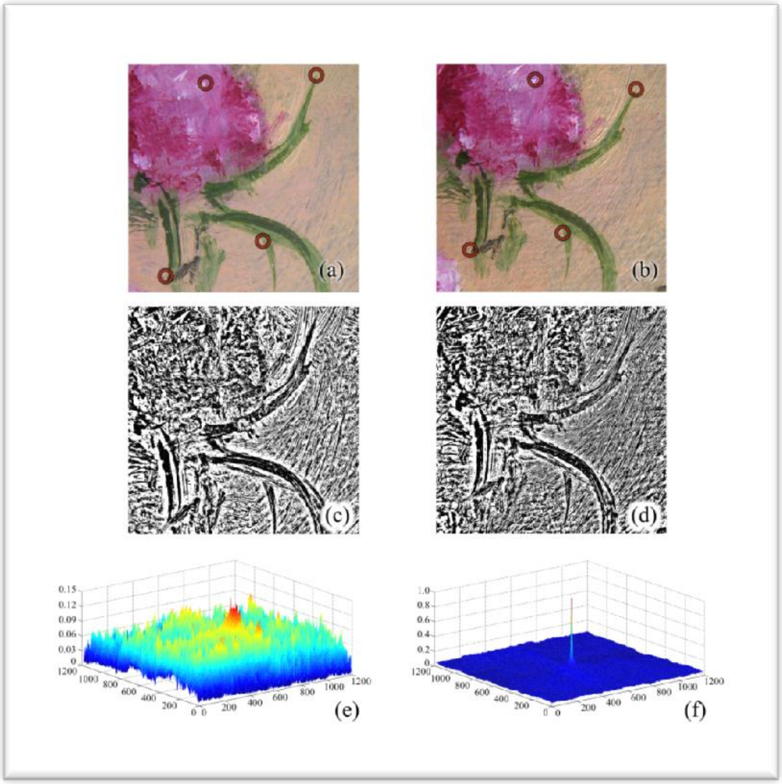


Figure 4.16 – Examples of extracted HHPs. (a) I_C image; (b) I_T image; (c) HPP_C; (d) HPP_T; (e) 2D correlation between HHPC and HHPT without geometrical correction; (f) 2D correlation between HHPC and HHPT with geometrical correction.

Figure 4.16 reports an example of extracted HHPs. In Figure 4.16(a) we have the image of the original verification area (I_C, here brought in High Definition, we take into account that on the Authenticity Certificate this image is memorized in Low Definition inhibiting copy attack). In Figure 4.16(b) we have the verification area acquired for matching purposes (I_T). In Figure 4.16(c) HHP_C is reported, while in Figure 4.16(d) is shown HHP_T. Now, we report 2D correlation between HHP_C and HHP_T, before (Figure 4.16(e)) and after (Figure 4.16(e)) geometrical correction.

In Figure 4.16, the 2D correlation has been calculated using Eq. (4.1). Figure 4.16(e) underlines how critic the geometrical distortions are for the proposed system. In particular respect to a statistical Threshold equal to $T_\alpha = 0.31$, the normalized correlation peak is equal to $C_\alpha = 0.095$. On the contrary, with geometrical correction application, we have a normalized correlation peak equal to $C_\alpha = 0.75$, where the threshold is equal to $T_\alpha = 0.34$, very similar to the previous one.

In Figure 4.17 is reported a similar example, where the test image, reported in Figure 4.17(b) has acquired with 20% downscaling in both dimensions (i.e. acquisition from a distance greater than the original one), a 7 degrees clockwise rotation, a translation of 111 pixels horizontally and 36 pixels vertically, and a reduced acquired area. This extreme case allows testing the robustness of the system, which reports a 2D Normalized Correlation that still highlights a correct identification ($C_\alpha = 0.72$ versus $T_\alpha = 0.36$).

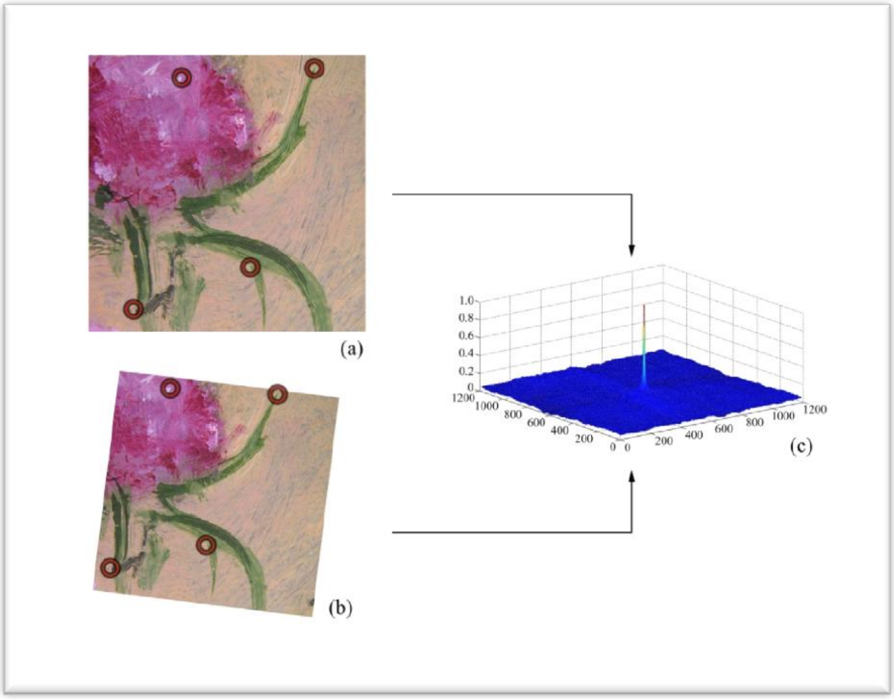


Figure 4.17 – Example of 2D correlation obtained with Test Image under "important" geometric distortions. It is possible to observe that the geometric corrections allow, also in this case, to correctly calculate the cross-covariance.

The threshold T_α used in this paper, for any reported results, is:

$$T_\alpha = 3 \cdot \sqrt{\bar{m}_C + \sigma_C}. \tag{4.3}$$

where $\bar{m}_C$ is the mean value of the correlation function and σ_C the related standard deviation. It has to be noted that is possible defining alternative statistical thresholds. We have used in our experiments also different thresholds, with similar results, such as three times the mean value plus once standard deviation, three times the standard deviation plus once mean value and so on. The choice of the threshold in Eq. (4.3) is due to the very low variance of its values among different image distortions.

4.3.2 Lithography Digital Certificate of Authenticity Case Study

The term lithograph or lithography comes from Greek, meaning “writing with stone”. It was invented in 1798 by German Alois Senefelder [109]. Technical process of lithography is based on the principle that limestone is naturally attracted to oil, and that oil and water have a natural antipathy, refusing to mix. A simplified version of the process is the follow:

1) The artist draws the image on lithographic stone with a greasy substance such as a waxy or greasy crayon.

2) The stone is moistened with water. Parts of the stone not protected by the grease soak up the water.

3) Oil based ink is rolled onto the stone. The greasy parts of the stone pick up the ink, while the wet parts do not.

4) A piece of paper is pressed onto the stone, and the ink transfers from the stone to the paper [110].

Colour hand-made lithographs require the production of a new plate (stone) for each colour. It is not uncommon to print more colours, so the artist can become involved in a long process of production. Although lithography after World War II was generally considered a commercial medium, in reality, the Lithography is an important artistic medium [111]. Figure 4.18 shows two Lithography made by artist Michele Cascella.

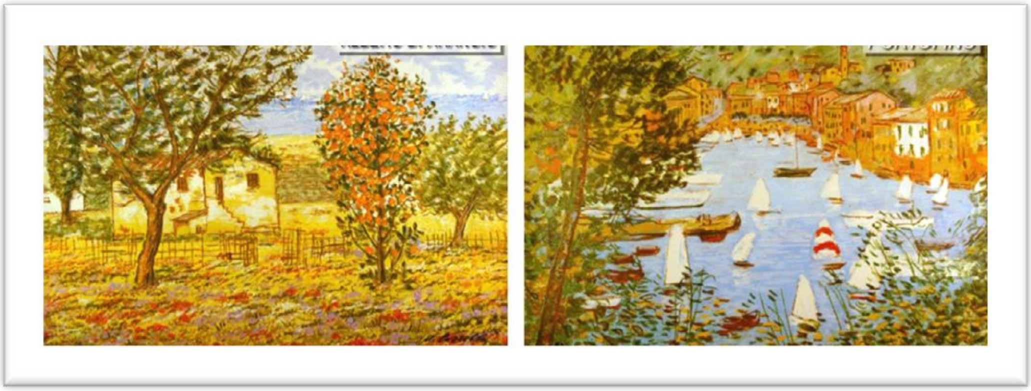


Figure 4.18 – Lithography used for testing our authentication method. These were made both in 1984 by Michele Cascella (famous Italian crepuscular landscapist; 1892-1989). The lithography are obtained from private collection.

To certify a lithography authenticity by means of Hylemetric Identification it is necessary to find a unique, non-reproducible and immutable characteristic. For instance, we could use the distribution of colourful "stains", which composes a feature of the image. In this way the method exploits ownership of lithography, because it is made using limestone' porosity.

The image is drawn on slab of porous limestone with a greasy crayon. Following the entire surface of the stone is wet with a nitric acid emulsified with gum Arabic. The function of this emulsion is to create a hydrophilic layer of calcium nitrate salt and gum Arabic on all non-image surfaces. The gum solution penetrates into the pores of the stone, completely surrounding the original image with a hydrophilic layer that will not accept a grease-based ink (the printing ink)

[112 – 114]. Because grease and water do not mix, the ink did not transfer to the moist blank area. When a sheet of paper is pressed against the surface of stone, a print of the design is made.

Every stone has different distribution of pores and it shines through the print. This is to distinguish lithographs of dissimilar runs, because the porosity changes with changing the stone; but if we have the same run, the differences between each print are in the corrosion of the stone or in the various piles of colour that is deposited on the paper when the print is made. So the methods that we use to distinguish the lithography are the same because also in this case there will be different distributions of colourful "stains".

The idea consists to choose from the artwork a nuance, for instance a little recognizable zone, and use it to identify the lithography. The portion of lithography is acquired by a digital high definition camera and it is physically printed on the certificate to help the user to find the area to be used in verification phase.

Due to possible rotation, translation, distortion and scale errors, which can lead to a misinterpretation, is necessary indicates on this image impressed on the original certificate also the trust points (from two to six) to be used for correcting any possible image distortion. Summarizing, the paper version of the certification of authenticity is now enriched with the image of the verification area, with the clear indication of all the possible trust points to be used in verification phase. This new certificate will be called "***Digital Certificate of Authenticity".***

During verification phase the verifier has to acquire a similar image zone and correct any possible distortion and acquisition error before correlate the two images for verifying the lithography authenticity.

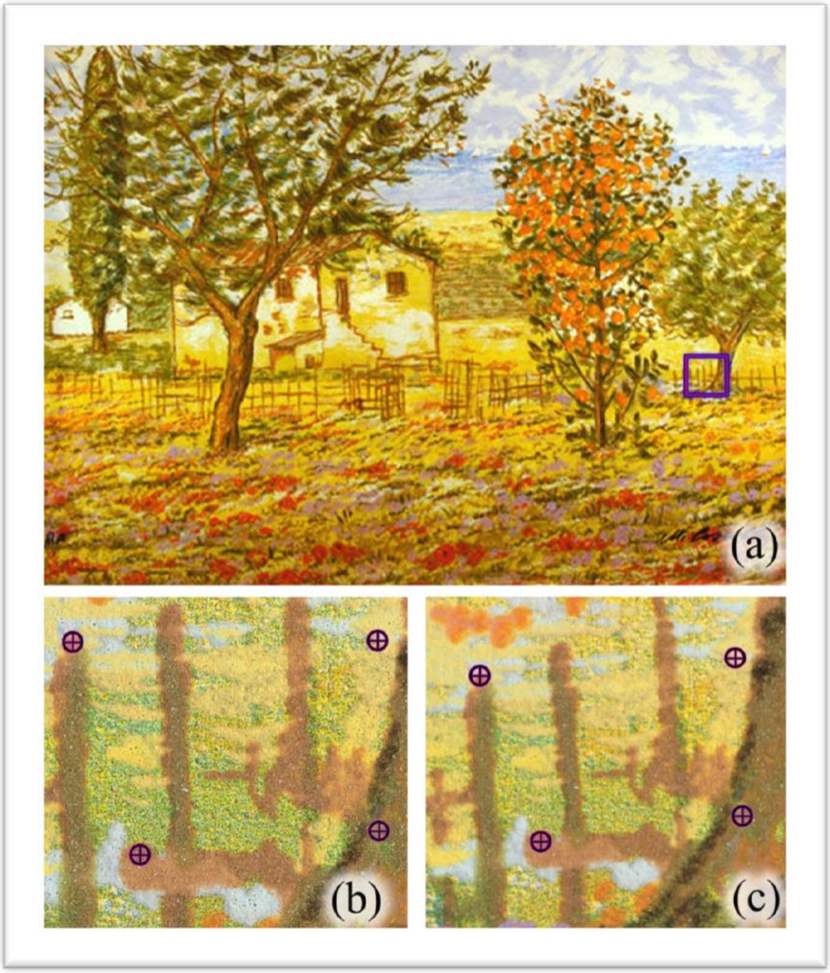


Figure 4.19 – In (a) it is highlighted the area used for certification image (b) and test image (c). On certification and test images are also highlighted the used trusted points.

With reference to Figure 4.19, we consider image shown in Figure 4.19(b) as the certification one and image shown in Figure 4.19(c) as the acquired one to be verified, called in the following test image, for sake of simplicity.

In the following we enter in deep in the necessary steps to correctly evaluate image and certificate connection, which certifies the originality of the artwork itself.

The first step, as for the Oil Painting case, is the correction, as much as possible, of any acquisition distortion, which can lead to a misidentification of original certification image. In fact, when acquired with a digital camera, the test image A can contain a bigger portion of image around the same zone, can have some roto-translation (referred to original certification image to compare with), and can be affected by some acquisition distortion, due to lens system used. In addition it also be possible having additional noise on it, due to not perfect cleaning on camera lens. The proposed method is able to correct all these problems and it results robust to added noise of various origins (e.g. Gaussian, salt and pepper, median, etc.).

The following step it is based on the selection of a certain number of trust points (at least two) on the test image. This step is necessary because, due to the absence of standard reference point inside lithography, we use them to correctly geometrical transform the acquired test image, with the aim to be the most possible similar to the certificate ones. In this way the final verification result, due by means of threshold correlation methods, will be maximised. These geometrical transformations are necessary, as mentioned above, for taking into account the differences between the certification image acquisition phase and the test image ones, in terms of physical means (different cameras, different lens), environmental situation (different illumination), and acquisition conditions (distance, rotation of the camera respect to the lithography, zoom, acquired area).

We can define the test image I_T and the image presents on the certificate as I_C. For all the different above-listed conditions, the two images are different almost ever. Without a geometrical correction, could be possible that the verifier obtain a false negative result (i.e. false lithography result in case of original one tested). To highly reduce this situation the next step in the proposed procedure is basically the application of image transformations (e.g. affine, polynomial, reflective, etc.), based on the identified set of trust points. The starting point of our analysis was the relative difficulty to correct image roto-translation deformation without having some reference points. The use of image transformation, such as affine or polynomial ones, allows to correctly identifying a translation along *x* and *y* axis, as well as a combined rotation on an angle α of the first image respect to the second one.

As described in [106 – 107], is possible correcting a great amount of errors selecting trust points on the two figures. Trust points are points present in both the two images, which identifying clearly the same real point. The Table 4.2 reports a set of classical transformation with the related minimum numbers of necessary trust points, with the related set of correctable distortions.

Table 4.2 – Type of transformation in relation to distortions [see Ref. 107].

Transformation Type	Min Trust Points	Description
Non Reflective Similarity	2 pairs	Use this transformation when shapes in the input image are unchanged, but the image is distorted by some combination of translation, rotation, and scaling. Straight lines remain straight, and parallel lines are still parallel.
Similarity	3 pairs	Same as “Non Reflective Similarity” with the addition of optional reflection.
Affine	3 pairs	Use this transformation when shapes in the input image exhibit shearing. Straight lines remain straight, and parallel lines remain parallel, but rectangles become parallelograms.
Projective	4 pairs	Use this transformation when the scene appears tilted. Straight lines remain straight, but parallel lines converge toward vanishing points that might or might not fall within the image.
Polynomial	6 pairs (second order) 10 pairs (third order) 15 pairs (fourth order)	Use this transformation when objects in the image are curved. The higher the order of the polynomial, the better the fit, but the result can contain more curves than the base image.
Piecewise Linear	4 pairs	Use this transformation when parts of the image appear distorted differently.
Local Weighted Mean	12 pairs	Use this transformation, when the distortion varies locally and piecewise linear is not sufficient.

In this analysis we have used affine, similarity and polynomial (second order) transformations. The selection of the transformations was based on the number of trusted point inserted by the verifier during verification phase. If the verifier defines only two trust points the proposed system applying a Non reflective Similarity Transformation for correcting only rotation and translation distortions. Otherwise, if are selected a different amount of trust points, a different transformation is applied, for correcting also other distortion. The trust point selection is manually made by operator on the acquired test image, using the electronic version of the certification image as reference for the trust point position. For allowing the verifier to correctly select trust point we have made dedicated verification software, which allow a precise point determination using also area selection and enlargement functions.

Verification software, after having acquired the trust points, automatically applies the correct transformation, which allows obtaining a corrected version of to be used during matching phase.

Due to the presence, in the digital certificate of authenticity, of a high resolution image of the interested zone, the proposed approach is weak at copy attack. In fact it is always possible that a counterfeiter acquires an original lithography, prints at high resolution the certification image and superposes it on the verification area indicated in the paper certificate. In this way a verifier can recognize as original a copy, if the acquired zone is not too much greater than the original portion.

To avoid copy attack, it is possible to encrypt the original high resolution image I_C by asymmetric key algorithm; meanwhile the image present in clear on the paper certificate is a low resolution version of it, used only for indicating the trust points that could be used in verification phase. In this way the data present in the certification media cannot be used for copy attack. Obviously, for verifying the lithography originality, it is necessary decrypt the encoded image, using the associated public key. If this process is made in clear for the verifier, it is always possible acquiring the encoded high resolution image necessary for counterfeiting copied lithography. Exists a lot of possible solution, both hardware and/or software, to overcame this problem. In fact it is possible use encryption microcontrollers [115], which can be used to encrypt all the execution memory. Or it is possible use secure processors in interaction with secure programming [116 – 118]. All this methods allow securing both the verification program and the user data (i.e. original decrypted high resolution image area) during execution. The used program allows a verifier to input the test image, acquired by him/herself using HRes Digital Media (e.g. digital camera) inside the verification software, which run in a secure memory area. After that the program automatically acquires the public key K_{public} present in the certification media and the original encrypted high resolution image I_C^* and, using trusted points, manually inserted by the verifier on test image I_T , applies geometrical correction to this one; then it decrypts in its secure memory space the certificate image I_C^*, obtaining I_C, applies the verification algorithm, destroys the decrypted image from the secure memory space and produces the verification output.

In the following Figure 4.20 the previously described process is shown, for better understanding.

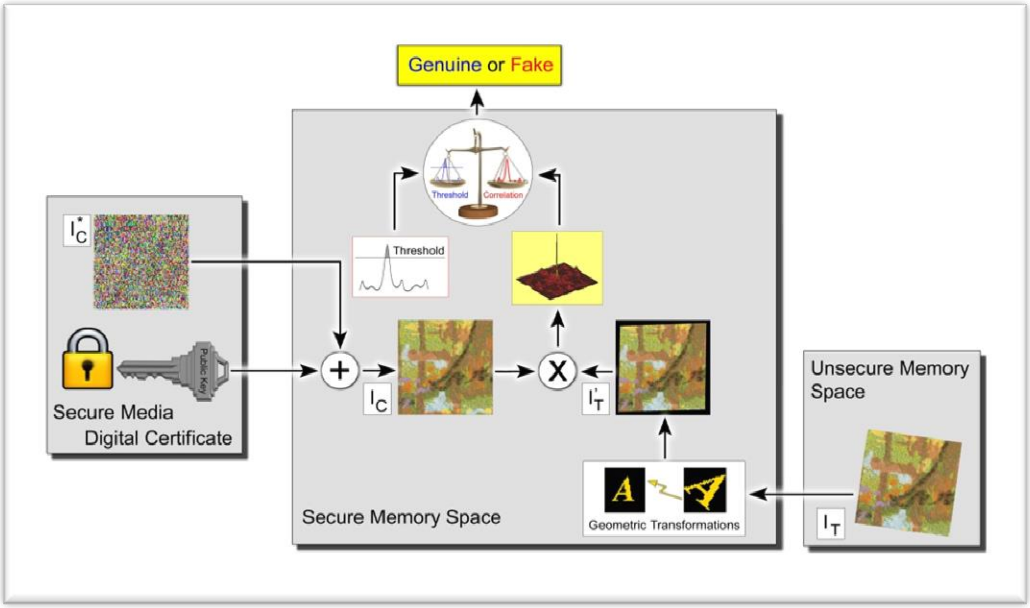


Figure 4.20 – Complete schema showing the lithography verification phase. It is highlighted the execution of verification program in a secure memory space. The data outside secure memory space or secure device are encoded for not allowing copy attack.

The asymmetric cryptography used for encrypt/decrypt certification image I_C could be any available one, for instance RSA or ECC, with a suitable key length (512 or 1024 for RSA, 128 or 256 for ECC). The image can also be encrypted both in a unique step, and pixel by pixel or, for a best trade-off between encrypted image dimension and information security, divided in zones and encrypted zone by zone.

After having aligned the two images, is possible verifying if these are extracted from the same lithography. In fact, the image transformation evaluates only geometrical differences among the two images. If we have two different lithography having the same subject, the two images are at first sight similar, and after correcting geometrical distortions, are pretty the same image. The presence of a Hylemetric characteristic such the colour pattern previously described, having a randomly distribution, different from a lithography to another one, allows using a correlation approach, to determine if the two images are extracted from the same lithography or not. The verification steps are very similar to the previous described one for Oil Painting and, in particular, are based on the same equations, Eqs. (4.1) – (4.2).

For the verification phase execution we have create a dedicated Matlab$^{\copyright}$ program, which allows the verifier to select verification areas among the two images, to input the trust points, having also a help system for selecting the same points on the two images, similar to the one used in Oil Painting case study. This program is also able to add controlled noise on the test image for testing noise strength against different noise parameters. Obviously the software does not implement cryptographic solution, which is out of the scope of our work and the certificate images are provided with trusts points on them, which is a possible enhancement to the previously described procedure.

In Figure 4.21(a) is shown a peace of Cascella's Portofino lithography reported in Figure 4.18, which could be used inside the originality certificate, in paper and electronic format. In Figure 4.21(b) is reported a similar zone, acquired during verification phase, which represents the test image. It can be easily viewed as the manual acquisition of the test image leads to have the introduction, in this case, of rotation and translations respect to the certificate image; in particular the test image is counter clockwise rotated of 6 degrees and also translated. Also in this case the acquisition was made using a commercial Nikon Coolpix 8700 Camera, with embedded Nikkor ED 8.9-71.2 mm objective, staying in front of the interested lithography area at ~10 cm with macro function.

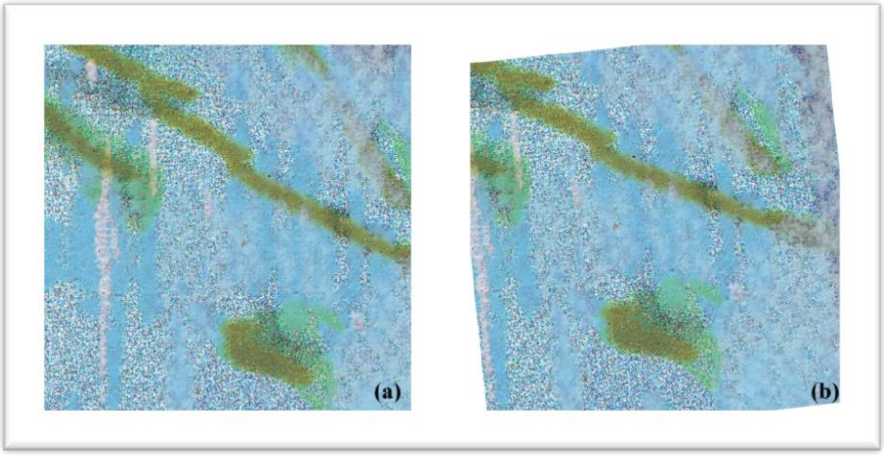


Figure 4.21 – Certificate Image (a) and Test Image (b). It could be noted that test image is a counter clockwise rotated and translated version of (a).

In Figure 4.22 Salt and Pepper noise is added to test image, which degrades the resulting C_α value; in any case the resulting value is still over the threshold T_α. In Figure 4.22 are also drawn C_α function with and without geometrical transformation, to highlight how significantly change it in the two cases.

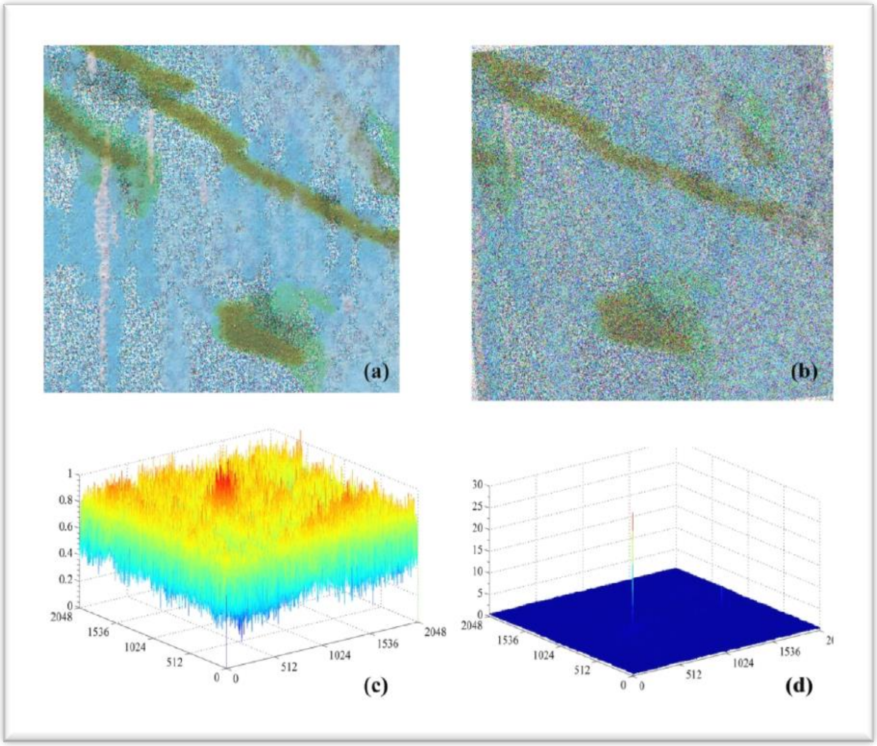


Figure 4.22 – Example of verification result with Salt and Pepper Noise addition. (a) Certificate Image; (b) Roto-traslated Test image with Gaussian Noise Added (0.3 distribution value); (c) Correlation result without Test image geometrical correction; (d) Correlation result after Test image geometrical correction using two trust points.

In Table 4.3 are reported the correlation value C_α for the different added noise and the related necessary parameters. Are also reported the different statistical threshold values for a set of possible thresholds. All the results are made on Cascella's Albero di Arancio lithography, where test image is only translated respect certification image by 480 pixels horizontally and 456 pixels vertically.

Table 4.3 – Correlation values for different added noise, with related noise parameters. It has to be noted that statistical thresholds are constructed using *correlation function mean value* and standard deviation and are not directly connected to any noise function mean values and variances.

Noise Type	**Noise Parameters**	$3\bar{m}_C + \sigma_C$	$3\bar{m}_C$	$3\sigma_C + \bar{m}_C$	$3\sqrt{\sigma_C}$	$3\sqrt{\sigma_C + \bar{m}_C}$	C_α
Gaussian	Mean Value equal to 0.10 Variance equal to 0.10	4.09	3.07	4.09	3.03	4.29	31.04
Gaussian	Mean Value equal to 0.10 Variance equal 0.15	3.99	3.03	3.88	2.93	4.20	28.81
Gaussian	Mean Value equal to 0.15 Variance equal to 0.10	4.10	3.09	4.04	3.00	4.28	30.47
Gaussian	Mean Value equal to 0.15 Variance equal 0.15	4.00	3.07	3.84	2.90	4.20	28.38
Salt & Pepper	Distribution equal 0.1	4.15	3.01	4.42	3.20	3.39	34.81
Salt & Pepper	Distribution equal 0.2	4.01	2.96	4.11	3.06	4.28	31.60
Salt & Pepper	Distribution equal 0.3	3.86	2.92	3.80	2.91	4.15	28.30
Poisson	No parameter to be defined	4.21	3.04	4.52	3.24	4.53	35.90
Speckle	Distribution equal to 1.0	3.53	2.79	3.15	2.58	3.87	22.29
Speckle	Distribution equal to 1.5	3.42	2.75	2.92	2.45	3.78	20.07
Speckle	Distribution equal to 2.0	3.34	2.73	2.73	2.34	3.70	18.42

It could also be noted that the used threshold varies in any experiment. This is due to the fact that we have used an adaptive statistical threshold, based on statistical characteristics of the correlation function. The threshold T_α used in this case study was:

$$T_\alpha = 3 \cdot \overline{m}_C, \tag{4.4}$$

where $\overline{m}_C$ is always the mean value of the correlation function reported in Eq. (4.1). It has to be noted that is possible define alternative statistical thresholds. We have used in our experiments also different thresholds, with similar results, such as three times the mean value plus once standard deviation, three times the standard deviation plus once mean value and so on. Table 4.3 shows also results for these different thresholds. The choice of the threshold in Eq. (4.4) is due to the very low variance of it values among different noises. For avoiding misunderstanding the variance and mean value described in relation to Gaussian Noise are the noise statistical values, not directly related to the mean value and standard deviation present in the heading row, which are, as previously described, statistical values extracted from the correlation function $C_\alpha(\Delta x, \Delta y)$.

For testing not only roto-translation effects, but also scale ones, which are the more common geometrical distortion finding in acquisition phase, due to different acquisition distance between certification and verification phases, we have used a different Cascella's lithography, also reported in Figure 4.18. In Figure 4.23 is reported the certification image extracted from Cascella's Albero di Arancio lithography and a test image I_T with both width and height scaled by 20%, not referred to the image center, and translated horizontally by 478 pixel and vertically by 458. The resulting correlation value after geometrical correction is $C_\alpha = 14.84$ (with a threshold equal to $T_\alpha = 2.53$). It could be noted that the correlation function allow also to determine with an error less than 2% the pixels translation in both dimensions also in this case.

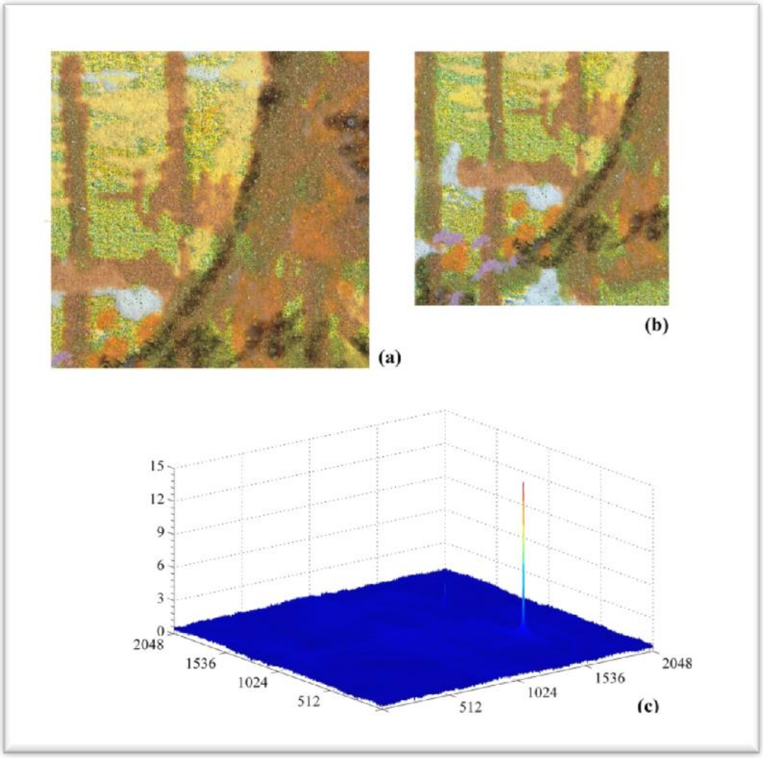


Figure 4.23 – (a) Cascella's Albero di Arancio Certification Image; (b); Test image scaled by 80% in both directions; (c) Resulting equal to 14.84 with geometrical transformation.

In Figure 4.24 is reported the previous case, but with the addition of a 9 degrees clockwise rotation on the test image. In this case correlation values are evaluated both with and without second order polynomial transformation, to highlight the impacts on resulting correlation values. The correlation value C_{α} is equal to 1.28, with a threshold T_{α} equal to 0.86 in case of application of none geometrical transformation and it increases to 20.01 (with T_{α} equal to 3.00) in case of polynomial transformation. Figure 4.24(b) shows $I_{T}^{'}$, the corrected version of I_T , while Figure 4.24(c) and Figure 4.24(d) shows respectively the 2D representations of correlation function $C_\alpha(\Delta x, \Delta y)$ for I_T and $I_T^{'}$.

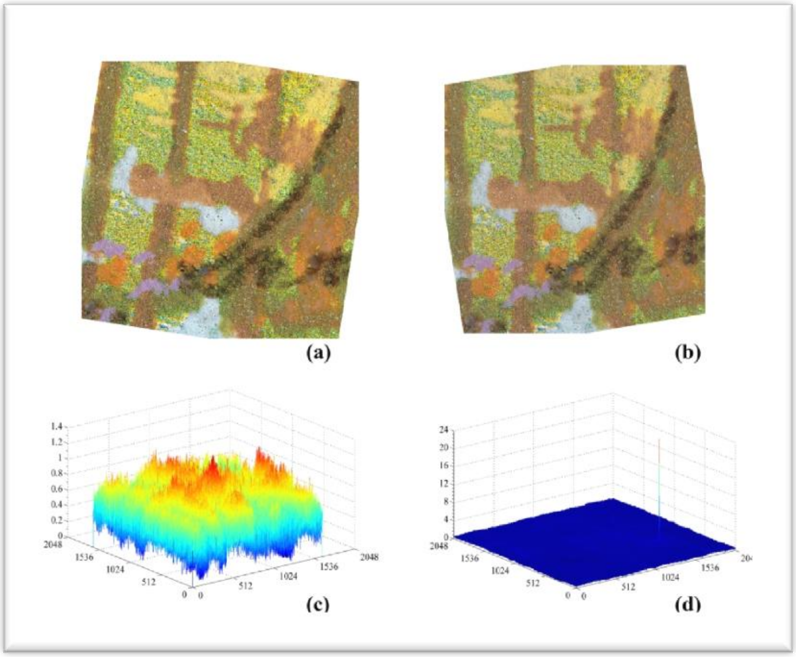


Figure 4.24 – (a) Test image rotate of 9 degree clockwise and scaled by 20% in both directions; (b); Test image after Geometrical Correction; (c) Resulting equal to 1.28 in case of no geometrical transformation; (d) Resulting equal to 24.01 in case of geometrical transformation.

It is interesting noting that, after geometrical transformation, the proposed system is able also to correctly identifying the translation occurred between I_C and I_T . It is possible applying also this correction and recalculating the correlation function obtaining higher values for correlation peak.

4.4 Drug Package authentication

One of the more sensible counterfeiting object categories is pharmaceutics products, and the counterfeiting rate continues to increase. The global pharmaceutical supply chain is at growing risk from counterfeit drugs, which cost companies billions and endanger the health of patients. Currently, parallels markets that claim to offer the same pharmacological product at a lower price than the normal distribution channels are appearing. In many cases, the offered product is only a copy in packaging nearly identical to that of the authentic product. These copies have no real effect (or, in the worst case, have significant side effects). Secure packaging is an important factor in countering fake products. This requirement has led to the enforcement of stringent legislation to ensure that pharmaceutical packaging cannot be easily imitated. Through the usage of new anti-counterfeiting technology, pharmaceutical packaging manufacturers can easily produce secure packaging and fulfil the requirements of government policies. The World Health Organization (WHO) estimates that the global trade in counterfeit drugs is experiencing continuous growth [56], about 1% of prescribed drugs in the developed world and 30% in parts of the developing world can be fakes. The threat is even greater on the internet, where 50% of drugs bought on illegal online pharmacies are thought to be counterfeit.

As the forged trade grows and becomes more profitable, criminals are becoming increasingly sophisticated and capable in the way that they package their products. In addition to manufacturing fake drugs, counterfeiters are seeking to infiltrate the legal supply chain. This approach allows them to steal authentic shipments and redirect them to other markets, reselling them for their own profit. Another emerging threat to the security of the pharmaceutical supply chain is ‘third shift’ packaging production. This process involves contractors or their staff carrying out extra hidden production runs and selling the resulting genuine packaging to counterfeiters. As a result, global regulatory bodies have introduced strict legislation to ensure maximum security of pharmaceutical packaging. The WHO Expert Committee on Specifications for Pharmaceutical Preparations has stressed the importance of implementing a quality assurance program. In the relevant report [57], the committee focuses on the role of packaging in relation to the stability of pharmaceuticals and the potential for counterfeiting. It is specified that the design of the packaging must prevent tampering with or counterfeiting of the enclosed medicinal products. Packaging must also carry the correct information and identification of the product.

The US Food and Drug Administration (FDA) enforces rule 21 CFR Part 211 [58], which specifies current good manufacturing practices for finished pharmaceuticals. Within this framework, the rule mandates that tamper-evident packaging should be used for over-the-counter (OTC) human drug products. According to the regulation, which aims to protect drug packaging against counterfeiting, it should not possible to duplicate the packaging using commonly available materials or processes.

In 2003, in response to the increasing number of counterfeiting incidents, the US FDA formed a Counterfeit Drug Task Force, which has released an annual report related to the global drug counterfeiting situation through 2006 [59]. The task force also aims to create a comprehensive system of modern protective measures against counterfeit drugs. One of the measures is to ensure the security of packaging. Recently, many solutions have been proposed to meet this goal. The best-known such solution is the usage of a barcode containing standard information related to the drugs and package, but tamper-resistant tapes, holograms and colour-shifting inks and dyes are also widely used.

In the following a method using light speckle is analysed, to counter this phenomenon.

4.4.1 White Light Speckle Hylemetry

Starting from the state of the art techniques discussed in the preceding section 2.4, we are proposed a drug package authentication method that can be identified as a covert UV ink approach combined with a biometry-like solution and micro-texting. For understanding the proposed method, first of all we have to introduce White Light Speckle technique.

When a coherent light beam is scattered by a diffuse surface, a random speckle pattern is observed. This random pattern has a particular statistical property. Chiang and Asundi [119] proposed the white-light speckle method as an alternative to the laser speckle method in an effort to alleviate the problem of decorrelation associated with the latter. White-light speckle photography was pioneered by Burch and Forno [120 – 121]. This technique only requires incoherent light illumination and a surface with speckle-like reflectivity, which is produced either naturally or artificially [122 – 123]. In the pioneer work, this reflectivity was applied by spraying the object surface with a retro-reflective paint. White-light speckle can be used to determine the surface deformation by comparing the grey intensity changes of the object surface before and after deformation. Two-dimensional digital image cross-correlation of the light speckle can be used to verify the “similarity” of two speckle fields acquired at different times. Sjödahl has developed an efficient algorithm that relies on digital image cross-correlation [108, 124 – 126] for use on laser speckle patterns.

The Sjödahl algorithm employs the computationally efficient Fast Fourier Transform (FFT) method of correlation. The cross-correlation is calculated in the frequency domain by multiplying the conjugate of one transform by the spectrum of the other. The algorithm compares two images (or sub-images) I_C and I_T. In general, $I_T^{'}$ is a geometrically corrected version of the test image I_T. This function may be expressed as follows:

$$C_\alpha(p,q) = F^{-1}\left[\frac{F^*(I_C)F(I_T')}{\left|F^*(I_C)F(I_T')\right|^\alpha}\right] \tag{4.5}$$

Where $C_\alpha(p,q)$ is the discrete two-dimensional correlation; F and F^{-1} are the forward and backward Fourier transform operators, respectively; and * indicates the complex conjugate. The coefficient α controls the correlation peak width. The optimum values range are the same defined in Section 4.3 for Hylemetry in Artworks verification.

Referring also to the phosphor PUF (see Section 2.4.2.5), it is possible to describe the usage of sprayed UV ink speckles as a purely random and highly secure PUF for drug packaging.

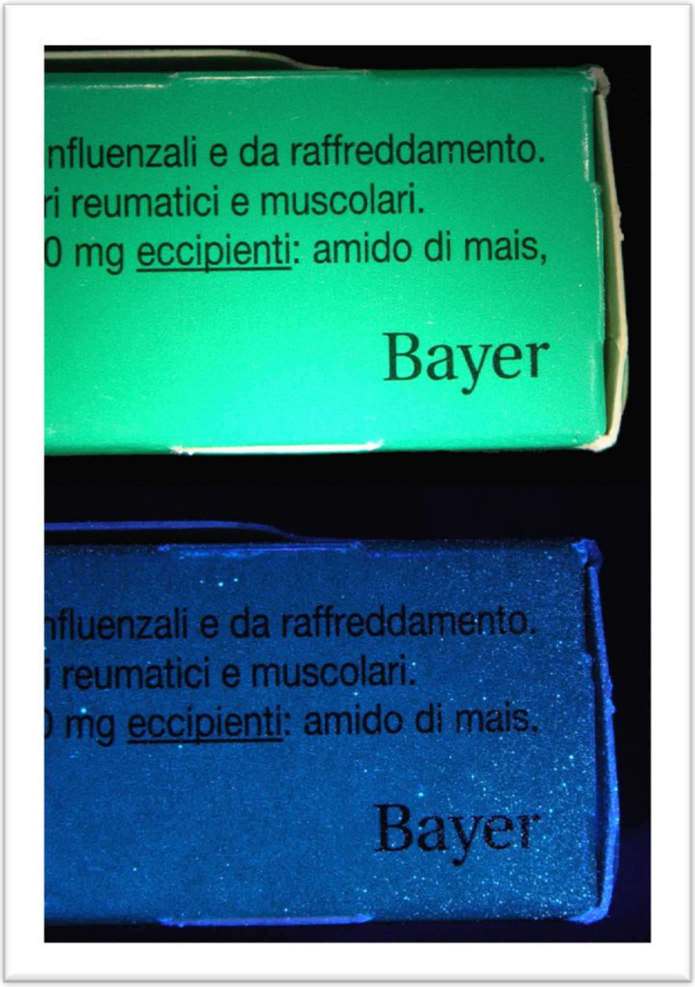

nfluenzali e da raffreddamento.
ri reumatici e muscolari.
0 mg eccipienti: amido di mais,
Bayer
nfluenzali e da raffreddamento.
i reumatici e muscolari.
) mg eccipienti: amido di mais,
Bayer

Figure 4.25 – In (a), Drug package under white light illumination is shown, while in (b) the same package is acquired under UV illumination, showing the speckle pattern.

Sprayed ink produces a random pattern on a surface. Beginning from this assertion, it is possible define an area (reference area) on a drug package (for example, around the producer name, see Figure 4.25), on which UV ink is sprayed. The generated random pattern has the typical aspect and statistics of a laser-scattered speckle field. It also has all of the necessary properties to be identified by its Hylemetric characteristics. In fact, any package has a different speckle field because of the randomness of the pattern generation, as shown in Figure 4.26. This uniqueness grants a low interclass correlation value, so that the speckle field can be acquired at any time without directly interacting with the package itself (i.e., the pattern can be easily acquired by a digital camera under UV illumination). The use of UV ink grants the invariance of package appearance to human sight. After acquisition of the speckle pattern, it is possible to create a dedicated barcode based on the speckle statistic. Because of the large number of speckles present in a small package zone, it is possible to overlay a grid on the acquired speckle image after it is correctly resized to a standard dimension. Thus, speckle sub-fields that retain the speckle pattern characteristics can be obtained. Using a speckle statistic [127], it is possible to create a template for each zone, and these templates can generate a 2D Barcode when combined correctly. In this paper, we use a speckle size distribution (area of a speckle in pixels). This method is chosen because it is necessary to have a robust statistic that allows the unique identification of one speckle sub-field from another.

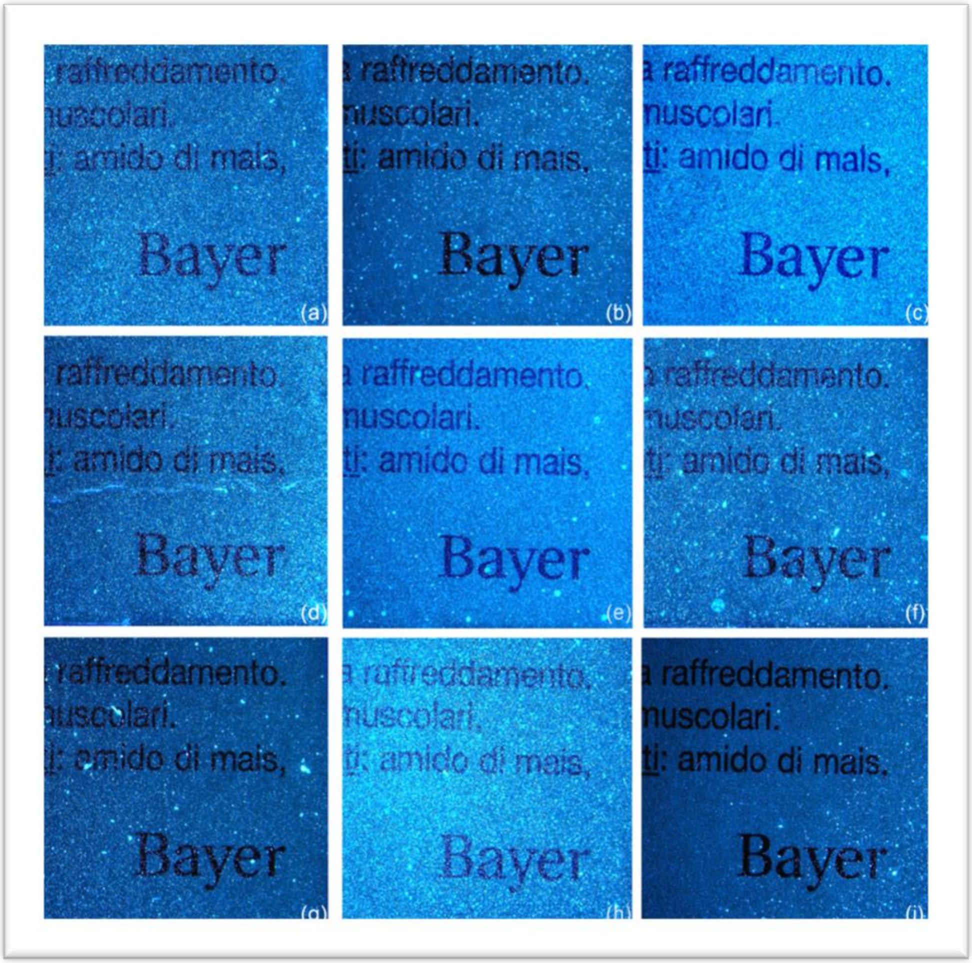


Figure 4.26 – Nine different speckle patterns acquired from nine different drug packages (Bayer® Aspirin©). The speckle patterns are created with the same method, using a UV spray ink from a distance of 10 cm, sprayed for 1 second. The speckle patterns reported in the nine images differ in number, dimension and distribution inside a similar package area.

If any of this template is encrypted by means of a public key infrastructure algorithm (PKI) [128] (for instance, one based on elliptic curve cryptography [129 – 130]), it is also possible to ensure security against a copy attack. In the following chapters, 2D template generation and the results obtained with this method are detailed.

4.4.1.1 UV Speckle PUF Template

Referring to Figure 4.27, the speckle pattern present in the reference area is acquired by a digital camera under UV illumination. Subsequently, with the help of predefined markers or the logo or name of the producer as an area reference, the image of the random pattern is resized to 1024×1024 pixels. The reference area can be defined in a way similar to that of the DataMatrix [71], which allows the acquired area to be easily implemented to the predefined dimensions (i.e., 1024x1024 pixels) using the frequency markers.

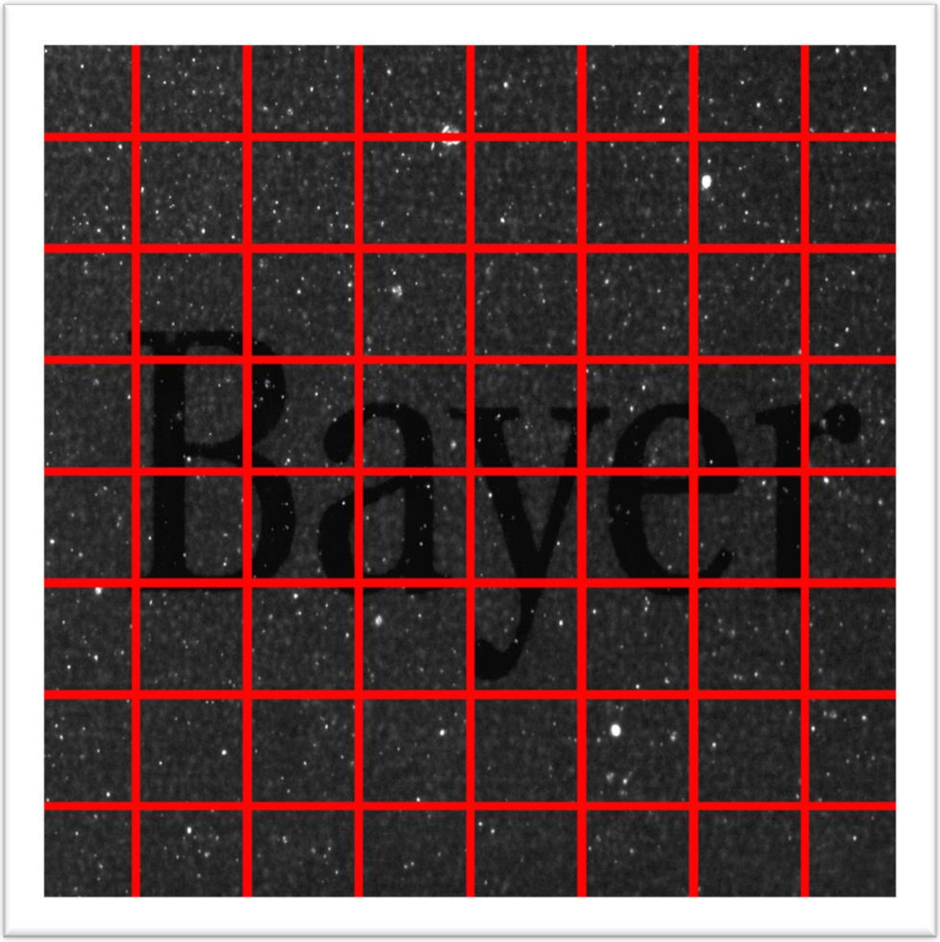


Figure 4.27 – The speckle pattern sample shown in Fig. 2(a) is now subdivided into 64 blocks, using a grid with 128x128 pixels cells.

These markers can also be used as trust points for the necessary geometrical corrections, as described below. In this article, we have passed ten trust points to a third order polynomial transformation. Both approaches are necessary to correct geometrical distortions, as detailed below. Figure 4.28 shows the two possible approaches for area identification and geometrical error correction.

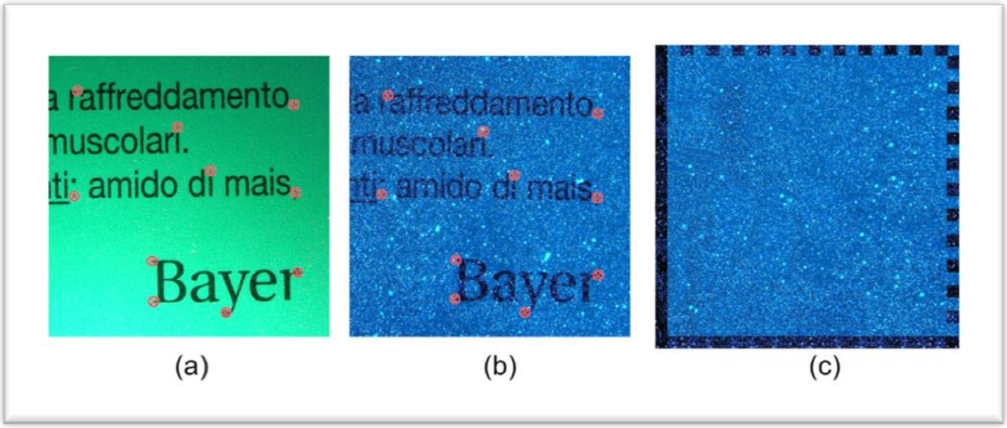


Figure 4.28 – (a) Acquired image with trust points superposition. The usage of ten points allows correction of geometrical distortion using third order polynomial function; (b) same image under UV illumination; (c) acquired image with DataMatrix reference bounding box superposition. The use of the DataMatrix bounding box allows correction of the geometrical distortions when the original standard reference information is known.

The image is subdivided into 64 blocks, each of which has dimensions of 128x128 pixels. A barcode is then created for each block based on the percentage of speckles in the block having the speckle size in the interval defined in Table 4.4.

Table 4.4 – Speckle size interval definition. All speckle insides a speckle field are analyzed and subdivided into 10 intervals in relation to their size, which is expressed in pixels. Then, the intervals identified with 0 and 9 are removed for robustness.

Size Intervals (pixels)	Interval identifier
0< Size ≤5	0
6< Size ≤8	1
9< Size ≤12	2
13< Size ≤17	3

Size Intervals (pixels)	Interval identifier
18< Size ≤23	4
24< Size ≤30	5
31< Size ≤40	6
41< Size ≤50	7
51< Size ≤200	8
Size> 201	9

Note that Table 4.4, does not contain a linear set of intervals. This choice is a more distinctive statistic to be obtained. A set of intervals that represents small speckles with greater density allows a more distinctive statistic to be obtained. The barcode procedure can analyse the speckle field related to a block and count the number of speckles whose size (reported in pixels) falls within one of the proposed intervals. Finally, it is possible to determine a percentage value for each interval related to the number of speckles whose size falls within an interval, with respect to the global number of speckles in the block. The percentage is further converted to a 4-bit binary code according Table 4.5.

Table 4.5 – Percentage conversion. Each percentage related to a speckle size interval is converted to a 4 bit coding following this table.

Percentage Value	4 bit conversion			
0< Sa ≤5	0	0	0	0
5< Sa ≤10	0	0	0	1
10< Sa ≤15	0	0	1	0
15< Sa ≤20	0	0	1	1
20< Sa ≤25	0	1	0	0
25< Sa ≤30	0	1	0	1
30< Sa ≤35	0	1	1	0
35< Sa ≤40	0	1	1	1
40< Sa ≤45	1	0	0	0
45< Sa ≤50	1	0	0	1
50< Sa ≤55	1	0	1	0
55< Sa ≤60	1	0	1	1

Percentage Value	4 bit conversion			
60< Sa ≤65	1	1	0	0
65< Sa ≤70	1	1	0	1
70< Sa ≤75	1	1	1	0
Sa >75	1	1	1	1

Because the majority of speckles have a size under 5 pixels, and very few speckles have a size greater than 200 pixels, these two extreme intervals can be removed from the statistic (consequently, the global speckle number is reduced) to produce a more robust procedure. In fact, during the acquisition phase, some speckles cannot be properly acquired, particularly for very small speckles. The contemporary use of "non-linear" interval range evolution allows a unique statistic to be obtained for each block. Then, each block can be represented by the residual 8 speckle-size intervals, which are converted to a 32-bit string (i.e., 4 bits for each interval, following Table 4.5). Figure 4.29 graphically explains the creation of a 196-bit string, starting from a histogram related to one of the 64 image block. This procedure is repeated for all 64 image blocks. In this way, we can produce a bit stream made up of $64 \times 32 = 2048$ bits. This solution is easily counterfeited by a copy attack. To avoid this problem, any 32-bit string can be encoded using ECC cryptography in a PKI scheme (i.e., the ECDSA approach [131]). In the case of 196-bit public/private keys, which have a security equal to a 2048-bit RSA key, the resulting encoded barcode string comprises $64 \times 196 = 12544$ bits. This string can then be easily converted to a 2D DataMatrix Barcode, which can be printed on the drug package using, for example, infrared ink. The use of infrared ink allows the same package appearance to be maintained, as in the case of the UV ink-speckle pattern.

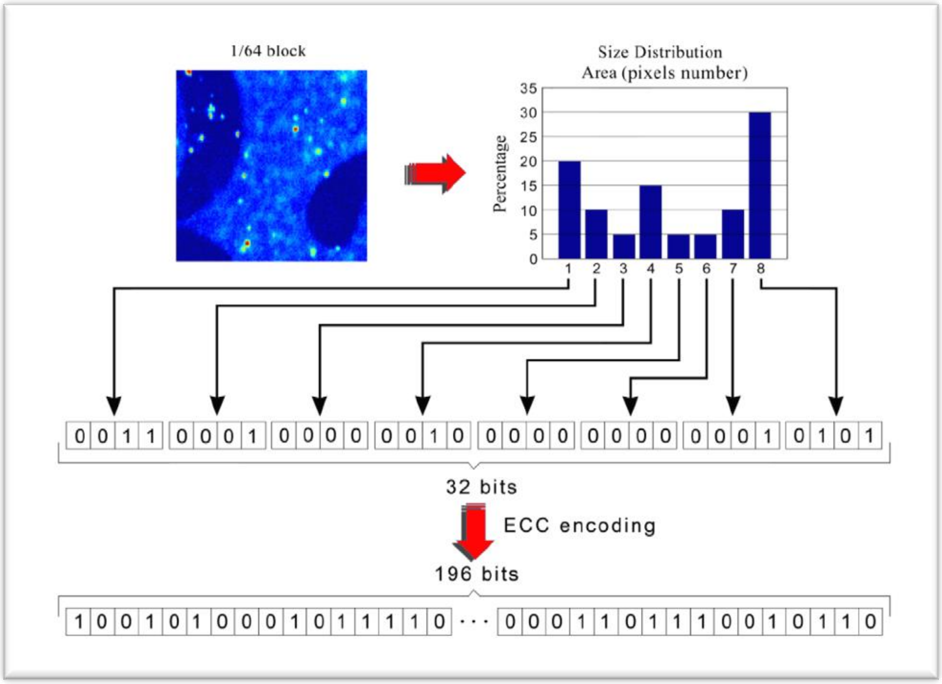


Figure 4.29 – The schema for creating an encoded 196 bit string starting from a block image is reported. Starting from a Speckle Image block, a histogram is created with indication of the percentage for each size interval. Each percentage is converted to a 4 bit string using the conversion in Table 2, creating a 32 bit string related to the single block. After that, the 32 bit string is encoded in a 196 bit string using an ECC private key.

Figure 4.30 shows a histogram related to four different image blocks of the same speckle pattern. Each block provides a different histogram, consequently providing a different barcode string. To emphasize this concept, Figure 4.30(a), (b), (c), and (d) are chosen from four contiguous image blocks.

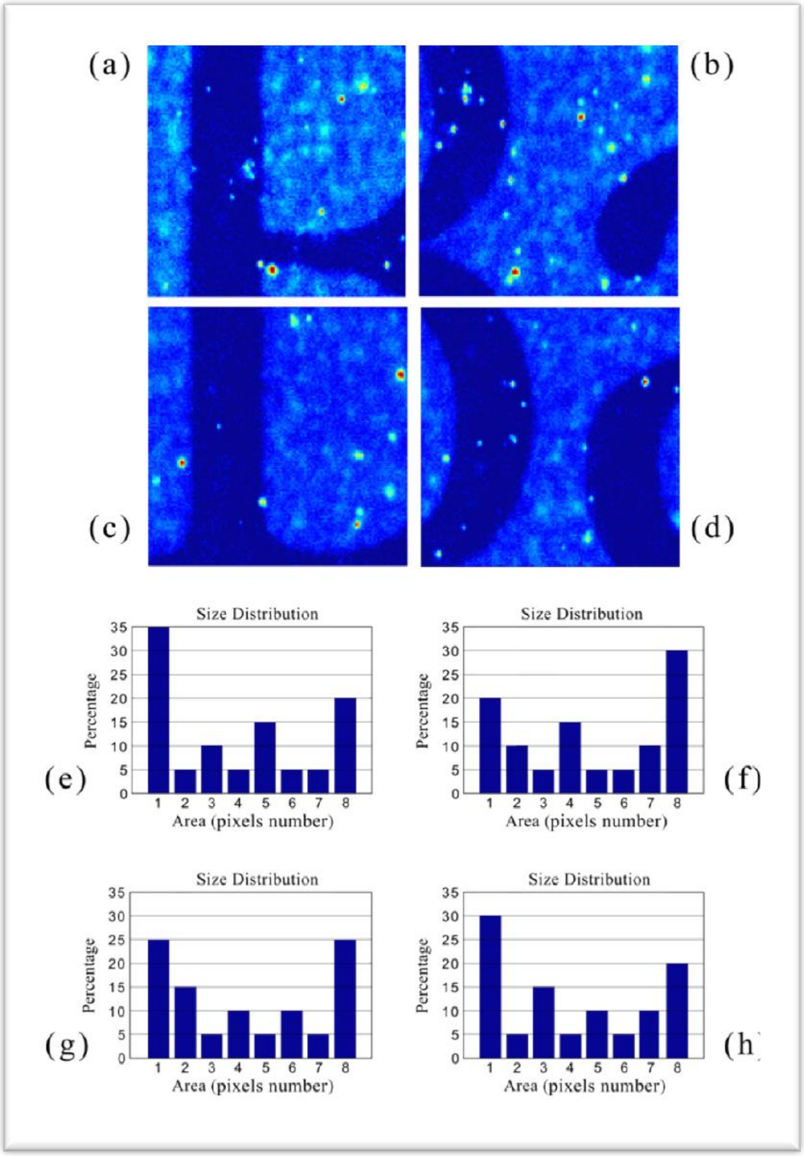


Figure 4.30 – Four different image blocks are shown in (a), (b), (c) and (d) to show that any block represents a different speckle pattern with a different speckle statistic, even between two contiguous blocks. Each statistic, as used in this paper, is reported in (e), (f), (g) and (h) respectively.

4.4.1.2 Verification Phase

During the package verification phase, the same steps required for barcode creation (described in Section 4.4.1.1) must be followed. After the 2048-bit barcode string is recreated, it is possible to extract the original from the 2D barcode using an IR source and the public key related to the private key used during ECC encryption.

Obviously, it is possible that the drug package to be verified has been ruined, or that the acquisition medium introduces geometrical errors such as rotation, translation or scaling. In addition, the under-sampling problem must be considered. To avoid the latter, the acquisition system must have a resolution at least twice that of the original. The use of at least 300 dpi is recommended for acquisition to overcome the under-sampling problem and respect the Nyquist-Shannon Theorem [132]. The geometrical distortion problem can be overcome by using a polynomial transformation. It is possible to find trust points related to a designed bounding box or (as in the case of this paper) the producer name. After four trust points are selected, it is possible to apply a polynomial transformation based on the third degree polynomial function [106] to obtain a correction of the most common acquisition errors.

In the following, some correlation results calculated using Eq.(4.1) are reported. All reported correlations aim to better clarify the similarity or difference among the analysed objects for the sake of clarity; however, these correlations are not part of the proposed verification phase. All verifications are made at Hamming’s distance between the decoded bit streams.

Figure 4.31 shows the normalized 2D correlation between an original speckle image and a distorted version after geometrical correction. The corrected image is identical to the original, as indicated by the normalized correlation peak. In particular, Figure 4.31(b) shows the speckle pattern of Figure 4.31(a) with digitally added geometrical distortions to simulate an incorrect package area acquisition. In Figure 4.31(c), the distorted image is corrected by a polynomial transformation using 10 defined trusted points. Figure 4.31(d) shows the normalized correlation peak between the original package image (Figure 4.31(a)) and the corrected image (Figure 4.31(c)). This result reinforces the importance of the correction. In fact, geometrical distortions introduce so many differences with respect to the original speckle pattern that the extracted bit stream has a high probability to be recognized as non-original, raising the false reject rate (FRR) of the verification system. The geometrical correction using the polynomial transformation minimizes the differences between the generated bit stream and the stream decoded from the 2D barcode. After the acquired image is geometrically corrected, it is possible to extract a verification string for comparison with the original, which must be extracted from the DataMatrix by a public key.

Because the analysed package could be ruined, causing partial loss or modification of the speckle pattern by geometric deformation, we have introduced a Hylemetric threshold to determine the originality of a package. The choice of the correct threshold is based on statistical studies, which aim to determine the typical Hamming's distance between two different speckle patterns and the same value in the case of a ruined package. Obviously, because a polynomial transformation is introduced to correct geometrical distortions, only data loss is considered in this analysis.

A complete analysis of the reported data is conducted in the next section, with emphasis on the false accept ratio (FAR) and false reject ratio modifications caused by threshold selection, acquisition errors and package manipulation.

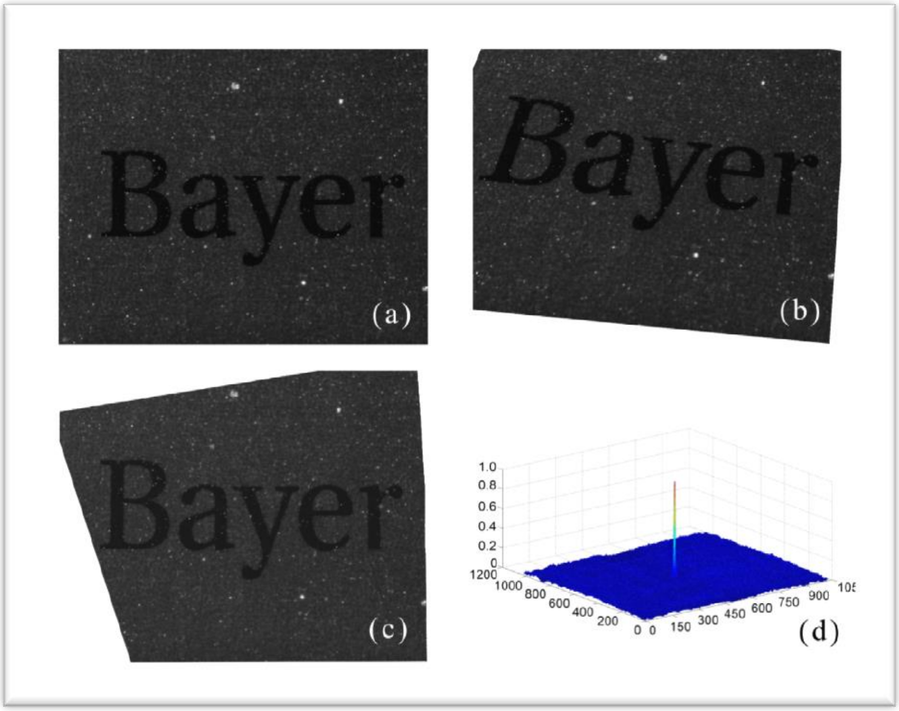


Figure 4.31 – (a) Original speckle pattern; (b) Speckle pattern after geometrical distortion produced by roto-translation and perspective error; (c) Distorted image reported in (b) after automatic geometrical correction by means of third order polynomial transformation; (d) correlation peak between original image (a) and corrected one (c).

4.4.1.3 Analysis and Results

The testing phase uses normalized 2D correlation to graphically emphasize that the verification phase has to be performed made the same steps described in the barcode creation one, well-detailed in the previous paragraphs. In the real application, the correct identification of a package is based on the Hamming's distance under a predefined threshold.

We have tested the application of geometrical correction by a polynomial transformation of an incorrectly acquired package image. After this correction, a Hylemetric correlation is performed to verify the package authenticity. As in any barcode verification method, the geometrical transformation plays a fundamental role. In Figure 4.32, the normalized correlation value C_α between Figure 4.32(a) and Figure 4.32(b) is equal to 0.06 in the case of the image without geometrical correction, and this value increases to 0.68 after geometrical correction. This significant difference is related to a simple prospective error without any other geometric deformation.

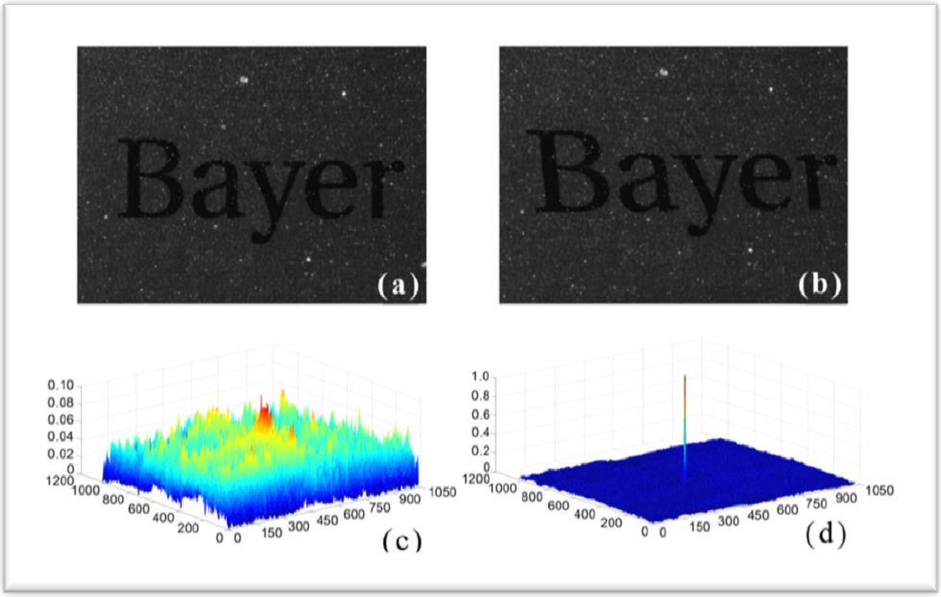


Figure 4.32 – (a) Original speckle pattern image; (b) acquired image with perspective distortion; (c) correlation related to (a) and (b) without geometrical correction. The correlation value is equal to 0.06 related to a statistical threshold of 0.2; (d) correlation related to (a) and (b) with geometrical correction. The correlation value is equal to 0.68 related to a statistical threshold of 0.25.

Another test is performed to demonstrate that any speckle pattern is distinct from another pattern. This distinction is valid for either a complete speckle field or for different sub-images of the same speckle pattern, as shown in Figure 4.33. In particular, three contiguous sub-images, Figure 4.33(a), (b), and (c), are correlated to each other, showing three correlation results that demonstrate that speckle patterns contained are statistically independent between grid cells.

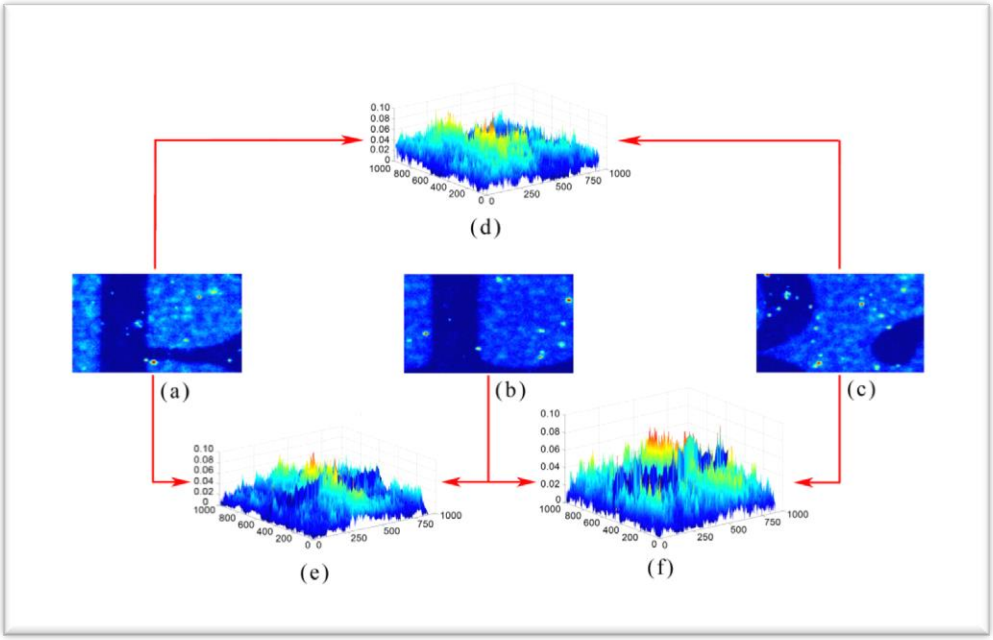


Figure 4.33 – (a), (b) and (c) show three contiguous blocks extracted from speckle pattern reported in Figure 4.26(a). In (d), the correlation between (a) and (c) is reported; the correlation value is equal to 0.009 for a threshold of 0.25. In (e), the correlation between (a) and (b) is reported; the correlation value is equal to 0.008 for a threshold of 0.25. (f) shows the correlation between (b) and (c); the correlation value is equal to 0.008 for a Threshold of 0.25.

The importance of the geometrical correction based on the Digital 2D correlation approach has been shown, and statistical analysis on a set of packaging has been performed.

Table 4.6 shows the Hamming's distances among a set of nine different speckle patterns acquired from nine different drug packages (see Figure 4.26). In this table, we report only the half matrix because the Hamming's distance between bit stream A and bit stream B is equal to the distance between bit stream B and bit stream A, and the results are reported once. The analysis of the Figure 4.26

images indicates that some results have been acquired under rotation transformation, which introduce errors in image comparison; this errors has no impact on the FAR analysis because a rotational translation can only produce a different speckle pattern (as shown by the correlation approach in Figure 4.33).

Table 4.6 – Hamming's distances between the nine speckle patterns reported in Figure 4.26.

Speckle Pattern	**Figure 4.26(a)**	**Figure 4.26(b)**	**Figure 4.26(c)**	**Figure 4.26(d)**	**Figure 4.26(e)**	**Figure 4.26(f)**	**Figure 4.26(g)**	**Figure 4.26(h)**	**Figure 4.26(i)**
Figure 4.26(a)	0	328	378	296	334	276	387	263	383
Figure 4.26(b)		0	320	282	282	344	307	371	313
Figure 4.26(c)			0	382	282	340	277	451	289
Figure 4.26(d)				0	304	298	323	303	369
Figure 4.26(e)					0	334	225	423	249
Figure 4.26(f)						0	351	311	359
Figure 4.26(g)							0	466	214
Figure 4.26(h)								0	474
Figure 4.26(i)									0

Analysing the obtained results simply requires that the necessary threshold to obtain a FAR equal to 0 should be determined so that no package can be recognized as a different one. The evaluation of the correct threshold for use in the system depends on the values of FAR and FRR that could be considered admissible; in fact, the choice of a threshold that leads to a FAR equal to 0% increases the FRR, as demonstrated in the next tests.

In the first analysis, we have chosen a Hylemetric threshold TH_{test} equal to 256. In this way, two packages are considered different if more than 12.5% of the decoded bits in the bit streams are different from the total of 2048. Table 3, shows that to obtain a FAR value equal to 0%, the necessary threshold in our analysis must be equal to 205 (i.e., 10% of bit errors); this threshold is identified in the following as $TH_{FAR=0}$.

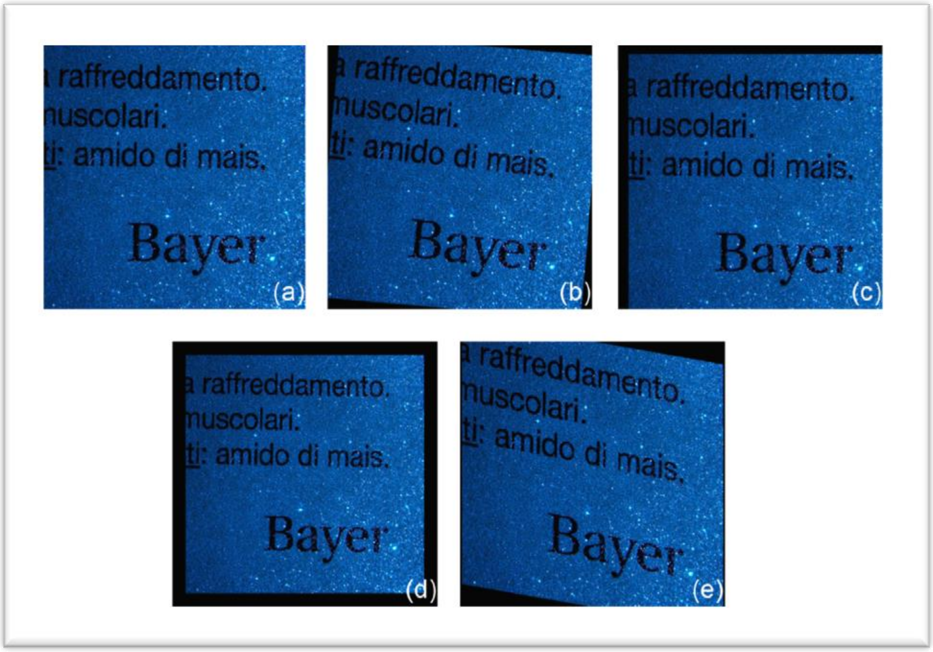


Figure 4.34 – (a) reports the original drug package, as shown in Figure 4.26(i); (b) the same package with a clockwise rotation of 5 degrees; (c) same package with a translation of 20 pixels down and 20 pixels right; (d) same package with reduced scale of 10% in both directions; (e) same package with perspective error of 7 degrees modification on both directions and 8 degrees rotation.

The following tests show the incidence of geometrical error on the Hamming's Distance and the resulting error in FRR evaluation. Because of the application of the polynomial transformation, any further reported values in this section must be considered comparisons between the original image and the geometrical corrected corrupted image. Figure 4.34 shows the speckle pattern related to the package reported in Figure 4.26(i), which was acquired with a geometrical distortion. In particular, 5-degree clockwise rotation (Figure 4.34(b)), a 20 pixel down and 20 pixel left translation (Figure 4.34(c)), a 10% horizontal and vertical scale reduction (Figure 4.34(d)) and a 7-degree perspective horizontal and vertical perspective error with 8 degrees of rotation (Figure 4.34(e)) affect this image.

Table 4.7 shows the Hamming's distance with and without the polynomial transformation for the acquisition of Figure 4.34.

Table 4.7 – Hamming's distances between speckle patterns and their ruined versions. The first column reports the values related to the ruined speckle pattern acquired from the acquisition system The second column reports the same values for the geometrically corrected versions.

Speckle Pattern	Nominal Case	Corrected Case
Rotation	221	201
Translation	235	213
Scale	263	234
Perspective	244	229

The corrected versions clearly lead to reduced Hamming's distances. The values are always non-zero because the test images have been acquired at a different time from the original, so that the two bit streams have some differences. In addition, geometrical corrections do not lead to a perfect copy because scale and rotations introduce interpolation problems with an impact proportional to the inverse of the speckle dimension. Referring to $TH_{FAR=0}$, it is clear that we obtain an FRR equal to 100% in the case of non-geometrically corrected versions, and the FRR for TH_{Test} is equal to 75%. The results differ for the verification values in the second column of Table 4, in which we obtain $FRR(TH_{Test}) = 0\%$ and $FRR(TH_{FAR=0}) = 75\%$. These results clearly show that the use of a threshold that avoids false acceptance leads to high false rejection values.

The next analysis uses damaged versions of some of the packages from Figure 4.26. In this way, it is possible to determine the value of the FRR of the system. As described above, all results are calculated after polynomial transformation allocation. Figure 4.35, some cases of ruined versions of the original packages are reported. In some cases, the ruined version has been acquired several times under different conditions (rotation, translation, scale).

The obtained results show two different situations: the superposition of written artefacts and the loss of speckle information has a minimal impact on the system, leading to a FRR values less than 1% in case of $TH_{FAR=0}$. In fact, in these cases, the Hamming's distances results all exhibit errors below 200 bits. The proposed solution is more sensitive to three dimensional geometric errors. In the same cases, the tested package has been ruined, obtaining not only scale and perspective errors that are corrected by polynomial transformation but also geometrical errors that occur because some points are more distant from the objective than others.

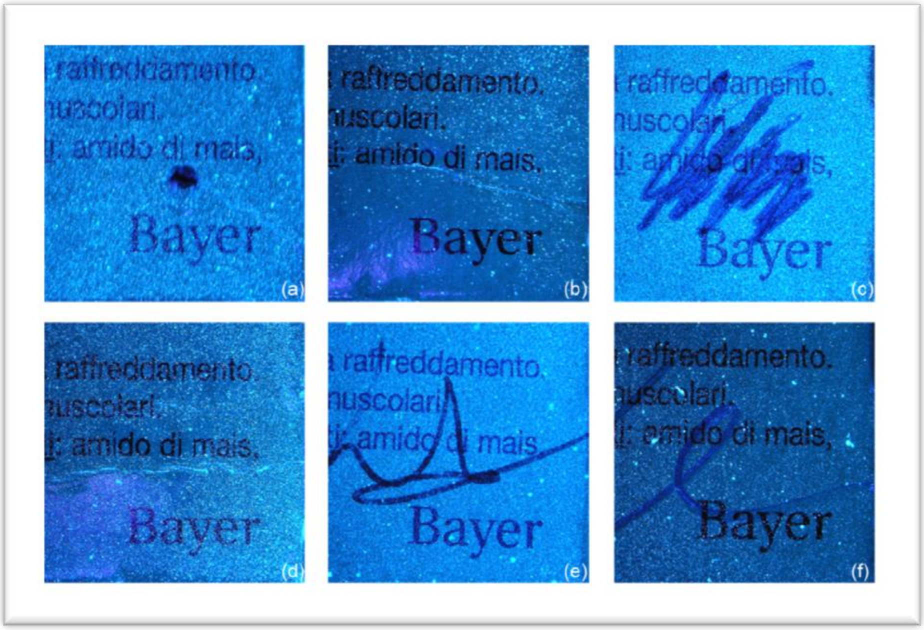


Figure 4.35 – (a) Drug package reported in Figure 4.26(a) with a hole in it; (b) Drug package reported in Figure 4.26(b) with right border folded; (c) Drug package reported in Figure 4.26(c) with massive ink writing; (d) Drug package reported in Figure 4.26(d) folded along horizontal axis in the centre of the package; (e) Drug package reported in Figure 4.26(e) with blue ball pen writing; (f) Drug package reported in Figure 4.26(g) with blue gel pen writing.

This typical case is shown in Figure 4.35(b), in which the right border has been folded. In these cases, the FRR values are approximately 20% in the worst case. A better result can be achieved by using 3D deformation correction algorithms similar to those used in [133] for fingerprint images.

Another tests related to FRR determination has been performed to ensure that a non-ruined package, is still recognized as original by the system after geometrical correction if it is acquired several times under different environment conditions. In relation to Figure 4.26(h), the package has been acquired seven times under different acquisition conditions. The resulting FRR values, which are related to the two thresholds used, are both equal to 0%, even if some values are close to $TH_{FAR=0}$; consequently, it is possible that the final value of FRR could be different from 0% in a more extensive test.

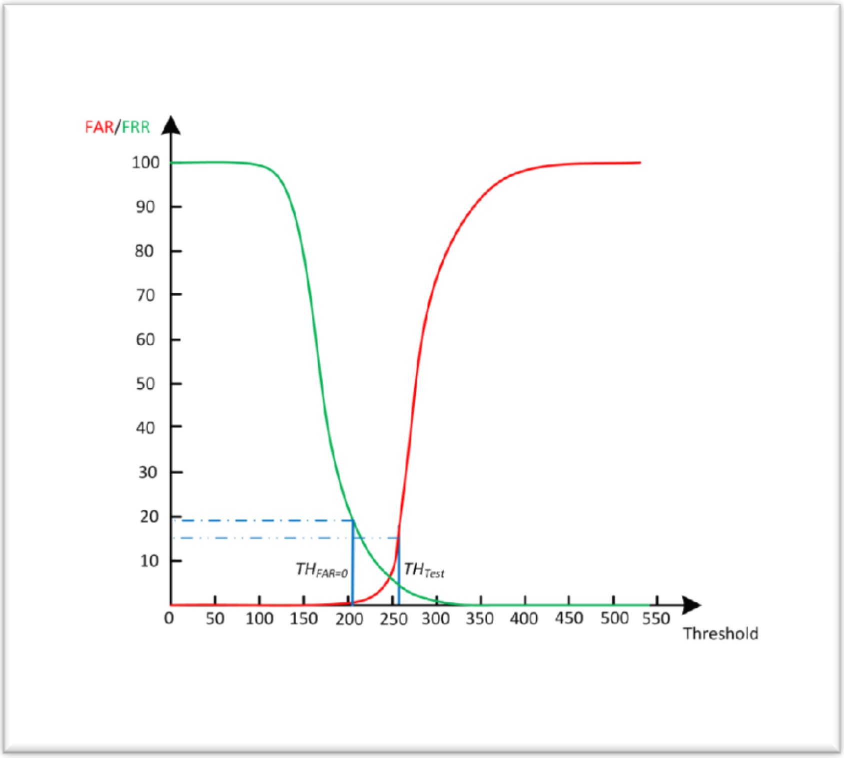


Figure 4.36 – FAR and FRR curves extracted from statistical analysis. The two thresholds used during the article are highlighted.

In conclusion, our statistical analysis shows that there are trade-off between the FAR and FRR due to their overlapping distributions (Figure 4.36). It is possible to select a threshold to decrease the FAR (FRR) in the expense of the FRR (FAR).

For example, selecting the threshold between 0 and 200 bits, the FAR will be 0%; on the other hand, the FAR becomes 100% when the threshold is set to 500 bits or greater.

4.4.2 Holographic Barcode

One of possible enhancement to the previous solution, consists in using a different barcode, more resist to package manipulation. One possibility is the use of a barcode created using the properties of holograms. The synthetic holograms are created using a modified Lee technique, deeply reported in Appendix B. Here the hologram theory is not more reported and only the Holographic Barcode technique is detailed.

The first step is to identify a text to be encoded into the new 2D barcode. In this case the bit stream created by the speckle distribution is used.

The algorithm starts with the generation of a binary image from the initial text message to be encoded. The text is firstly converted in a binary string and successively transformed in characters (symbols), generating a so called Binary Character Image; two bits are coded with a 4×4 pixel character according with Table 4.8. With this procedure we transform the text in a Bitmap image ($\mathbf{I}_T$). The text bitmap image is developed with a number of columns double in comparison with rows. For instance: with a text of 32 Bytes, resultant Bitmap image has dimensions 32x64 bits; with a text of 128 Bytes, resultant Bitmap image has dimensions 64x128 bits; with a text of 512 Bytes, resultant Bitmap image has dimensions 128x256 bits; etc.

Obtained the text bitmap image, the next step consists in the creation of the related Computer Generated Hologram (CGH).

Table 4.8 – Symbols used for transforming a binary string into a Bitmap image

Binary String	Binary Encoded Symbol
$[0\ 0]$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$
$[0\ \ 1]$	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$
$[1\ \ 0]$	$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$
$[1\ 1]$	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$
example: coding of 8 bit string $[0\ 1\ 0\ 0\ 1\ 1\ 1\ 0]$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$

Optical holography [134] is a technique by which both the amplitude and phase of optical field diffracted from an object of interest are recorded as a hologram in the form of interference fringes.

When the optical field from the diffusing object is recorded as hologram, the hologram becomes very similar to a random pattern, because the interference fringes of randomly phase-modulated waves are recorded in the hologram with high density.

A Computer Generated Hologram (CGH) image is a hologram computed by numerically simulating the physical phenomena of light diffraction and interference. The CGH is similar to a random pattern; every zone of a CGH contains all the encoded information.

In the proposed solution, the text Bitmap image is codified in a form of a Fourier-transformed digital hologram. Unfortunately, this type of hologram produces, in reconstruction, the so called twin effect (these copies, superimposing themselves, provoke loss of information). To avoid this problem, we simulate an off-axis hologram by means of the following procedure. First of all, the text image ($\mathbf{I}_T$) is inserted in a black hosting one with dimension, in area, eight times greater (zero padding); e.g. if the text image has dimension 32x64, the black image has dimension equal to 128x128 bits. In this way we obtained the $\mathbf{I}_{TM}$ image.

To make the Fourier-transformed digital hologram, the $\mathbf{I}_{TM}$ image is modulated by a random phase mask $\exp[i\phi(\xi,\eta)]$. The two-dimensional phase $\phi(\xi,\eta)$ is given by random numbers. The $\mathbf{I}_{TM}$ image modulated by the random phase is subsequently numerically Fourier transformed:

$$T(x,y) = \mathbf{FFT}\left\{I_{TM}(\xi,\eta)\exp\left[i\phi(\xi,\eta)\right]\right\}. \tag{4.6}$$

Now, each element (x,y) of the matrix $\mathbf{T}$ is divided in four sub-elements. The first sub-element represents the real and positive part of $T(x,y)$ (0° angle in the corresponding phasor notation); the second one represents the imaginary and positive part of $T(x,y)$ (90° angle in the corresponding phasor notation); the third the real and negative part of $T(x,y)$ (180° angle in the corresponding phasor notation); eventually the last one represents the imaginary and negative part of $T(x,y)$ (270° angle in the corresponding phasor notation).

After this procedure, the resulting matrix has a dimension four time bigger than the original one, due to the fact that each original pixel is now represented by four values. To obtain the CGH with the same dimensions of the zero-padding Image, each set of four values are substituted, with the related average, made by linear interpolation. Subsequently, with a thresholding procedure, the CGH is birarized; we get at this point a CGH represented by a bitmap image ($\mathbf{I}_{CGH}$).

To recover the original text Image ($\mathbf{I}_T$) the procedure is very easy. The IFFT is performed on the $\mathbf{I}_{CGH}$, obtaining two copies of the text image positioned on the four corners of the frame; the left part of the text image is positioned in the corner low-right (and a copy rotated in the corner top-left), while the remaining part is found in low-left (and a copy rotated in the corner top-right).

The text image is reconstructed and, by means of the inverse coding used to generate the text image, converted to the initial text message.

The overall scheme of the CGH construction is reported in Figure 4.37.

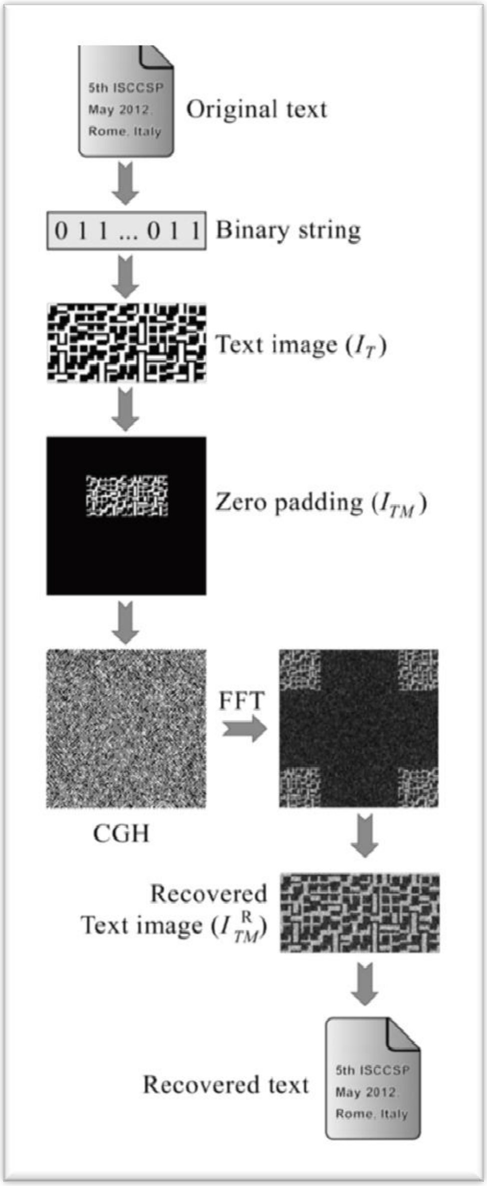


Figure 4.37 – HoloBarcode generation and subsequently string extraction. To implement these tests HoloBarcode has been positioned inside a finder pattern, equal to the one used in the ECC 200 Data Matrix, which is necessary for locating the data area.

4.4.2.1 *Experimental results*

In order to simulate physical damage and dirt marks, some tests have been performed on 2D Data Matrix code and on our HoloBarcode. We are used a simple string, "5th ISCCSP May 2012, Rome, Italy", codified in 32 Bytes, and the same entity of damaging was made on all the Barcodes

Initially, the simulation of damage has been effected on the digital images of the Barcodes.

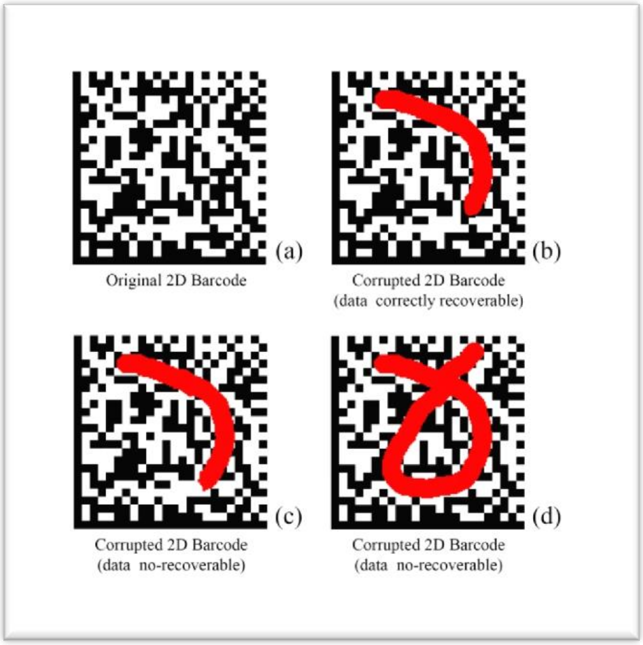


Figure 4.38 – (a) Data Matrix Code without damage, (b) Readable Data Matrix with data loss correction , (c) and (d) not readable Data Matrix code.

Figure 4.38(a) shows a Data Matrix code without data loss, while the Figure 4.38(b), (c) and (d) show different examples of damages by means of overlapping extraneous information.

The code of Figure 4.38(b) is readable. On the contrary, it is not possible to recover the encoded information from Barcode related to the images in Figure 4.38 (c) and (d), never in partial form.

Figure 4.39 shows the HoloBarcode with the same type of loss of data previously effected on the Data Matrix code (see Figure 4.38).

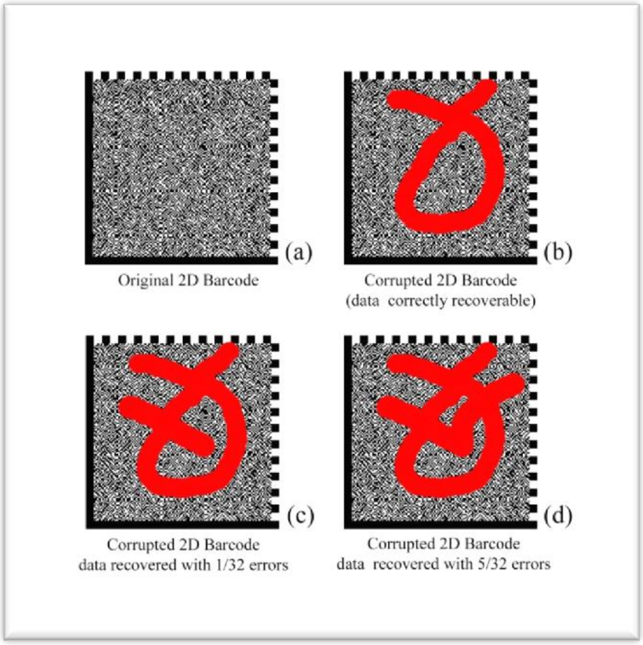
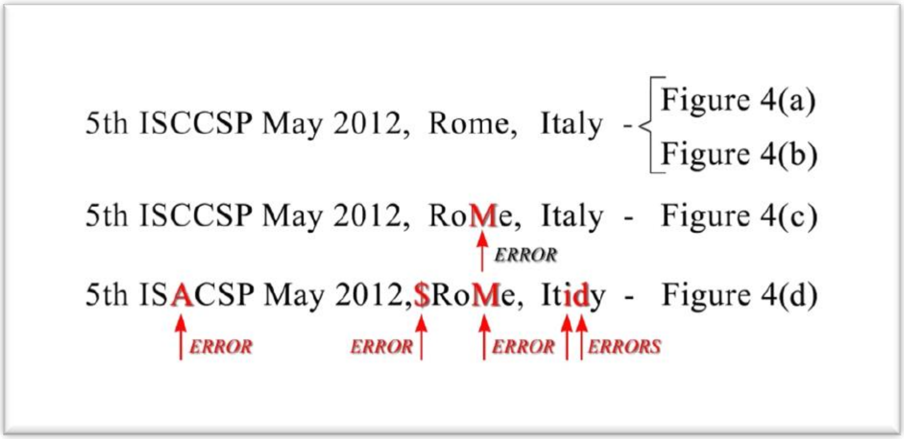


Figure 4.39 – (a) HoloBarcode without damage, (b) HoloBarcode with data loss and data correctly recovered, (c) and (d) HoloBarcode readable, data partially recovered.

Figure 4.39(a) shows the HoloBarcode without data loss. Figure 4.39(b) shows HoloBarcode with data recovered without errors, Figure 4.39(c) and Figure 4.39(d) show two HoloBarcodes where the recovered data have an error and five errors respectively. Figure 4.40 shows the recovered encoded information form Barcode of Figure 4.39.



5th ISCCSP May 2012, Rome, Italy - Figure 4(a) / Figure 4(b)

5th ISCCSP May 2012, RoMe, Italy - Figure 4(c)

5th ISACSP May 2012,$RoMe, Itidy - Figure 4(d)

ERROR
ERROR
ERROR
ERROR
ERRORS

Figure 4.40 – Recovered data from HoloBarcodes of Figure 4.39

This simple first tests indicates two important results:

- Relatively to overlapping extraneous information, HoloBarcode is more robust than the DataMatrix code. The holographic technique, used to develop HoloBarcode, make the system able to provide the embedded information even in presence of data loss also without using algorithms of error checking and correction.
- With HoloBarcode the encoded information are always recoverable, even if in partial form.

In Figure 4.41 and Figure 4.42 we show a second set of tests.

The Data Matrix code and HoloBarcode have been printed with a HP LaserJet 1200 series. Subsequently they have been acquired, at 600 dpi, with a plain scanner.

Figure 4.41 shows the acquired image and a set of a series of simulated damages. The damaged code of Figure 4.41(b) is correctly recovered. Instead, the Data Matrix code of Figure 4.41(c) and Figure 4.41(d) are not readable.

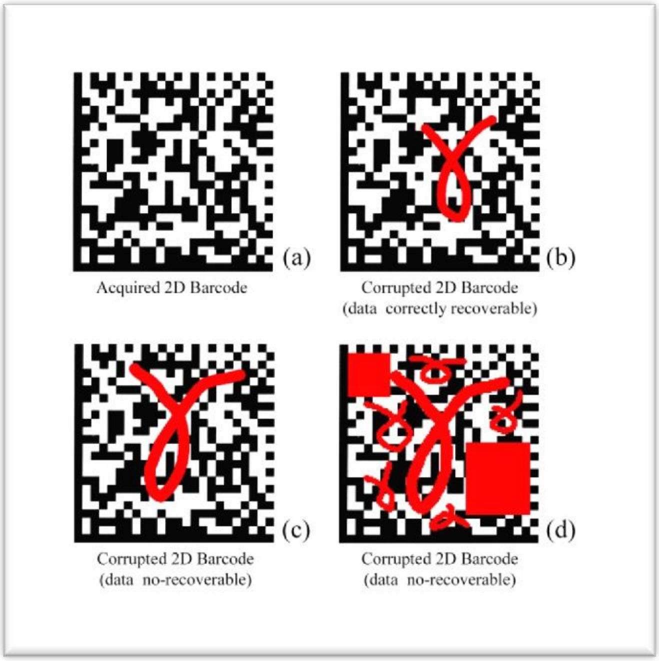


Figure 4.41 – (a) and (b) readable Data Matrix, (c) and (d) encoded information not readable.

Figure 4.42 shows the HoloBarcode with the same type of loss of data previously effected on the Data Matrix code (see Figure 4.41).

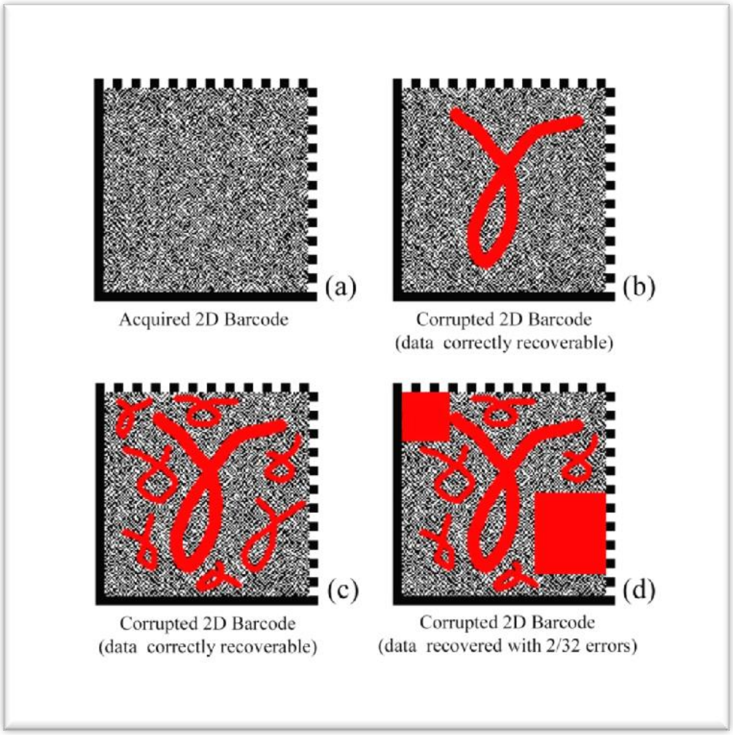


Figure 4.42 – (a) ,(b) and (c) HoloBarcode readable without loss of encoded information, (d) HoloBarcode with information partially recovered.

Also this second set of tests confirms that the HoloBarcode is more robust, with relationship to the code physically damaged, than the DataMatrix code.

The limit of the HoloBarcode resides in the necessity to acquire, with “good” definition the random pattern of the CGH. The HoloBarcode is very robust to possible physical losses of the code. On the other hand, the acquisition of the CGH must have done to high definition; the system of acquisition doesn't have to effect a spatial average of the synthetic hologram.

Chapter 5 Conclusion

5.1 INTRODUCTION 241
5.2 FUTURE PERSPECTIVES 242

5.1 Introduction

In this doctorate work has been presented a solution to verify object authentication applying to non-living matter the biometric paradigm, based on the identification of one or more object characteristics that has a set of properties useful to clearly identify the object among a set of similar ones.

A set of complete experiments has been carried out on different family of object, staring from Euro banknotes, till lithography and drug packages. For each family a complete vision of the state of the art has been presented and the advantage in using the Hylemetric approach has been shown.

In addition, it has been also presented a new possible holographic 2D barcode, which can carry on it the Hylemetric template information useful to automatize and simplify the verification phase.

All the experiments have demonstrate the good perspective of this new approach, and also their intrinsic limitations, trying to reduce or overcame these lasts. In particular on Banknotes and Drug Packages a solution to automatize the creation and verification system both in an intranet connection case or in a stand-alone one, has been described, to cope with all the possible usage situation.

5.2 Future perspectives

In the future works it is possible to try to optimize the holographic barcode solution, which has the intrinsic potentiality to overcame, in particular for drug packages, the standard 2D Barcode limitations.

In relation to the banknote use case, could be interesting verifying also in the real case, using IR inks and adapted printers, the proposed method, which, for the nature of the object under study, could be carried on only in a simulated way. In particular has to be verified the possible interferences between UV and IR inks, when superposed, which constitute the theoretical limit of some of the proposed approaches.

Appendix A Bibliography

[1] **H.T.F. Rhodes**, *Alphonse Bertillon: Father of Scientific Detection*, Abelard-Schuman, New York, (1956).

[2] **F. Galton**, "*Personal identification and description*", Nature, *Vol.* ***38***, pp. 173–177, 201–202, (1888).

[3] **A.K. Jain, P. Flynn, A.A. Ross**, *Handbook of Biometrics*, Springer-Verlag, New York, (2008).

[4] **National Biometric Test Center Collected Works**, 1997-2000, Edited by James L. Wayman, Director, Version 1.3, August, 2000, Prepared under DoD Contract MDA904-97-C-03 and FAA Award DTFA0300P10092, (2000).

[5] **S. Prabhakar, S. Pankanti, and A.K. Jain**, "*Biometric Recognition: Security and Privacy Concerns*", IEEE Security and Privacy Magazine, *Vol.* ***1****(2)*, pp. 33–42, (2003).
http://dx.doi.org/10.1109/MSECP.2003.1193209

[6] **AA.VV.**, *Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni,* CNIPA, (2004).

[7] **A. Martin, G. Doddington, T. Kam, M. Ordowski, and M. Przybocki**, *"The DET Curve in Assessment of Detection Task Performance"* Proceedings of the Fifth European Conference on Speech Communication and Technology, Rhode, Greece, *Vol.* ***4***, pp. 1895–1898, (1997).

[8] **J. Egan**, *Signal Detection Theory and ROC Analysis*, Academic Press, NewYork, (1975).

[9] **D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar**, *Handbook of Fingerprint Recognition 2 ed.*, Springer-Verlag, (2009).

[10] **A. J. Mansfield and J. L. Wayman**, *Best Practices in Testing and Reporting Performance of Biometric Devices*, Version 2.01. Technical Report NPL Report CMSC 14/02, National Physical Laboratory, (2002).

[11] **National Institute of Standards and Technology**, *NIST Biometric Scores Set*.
http://www.itl.nist.gov/iad/894.03/biometricscores.

[12] **G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds**, *"Sheep, Goats, Lambs and Wolves: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation*". In CD-ROM Proceedings of the Fifth International Conference on Spoken Language Processing (ICSLP), Sydney, Australia, (1998).

[13] **J. A. Swets, W. P. Tanner, and T. G. Birdsall**, *"Decision Processes in Perception"*, Psychological Review, *Vol.* ***68****(5)*, pp. 301–340, (1961).
http://dx.doi.org/10.1037/h0040547

[14] **N. Poh and S. Bengio**, *"An Investigation of F-ratio Client-Dependent Normalisation on Biometric Authentication Tasks"*, Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), *Vol.* ***1***, pp. 721–724, Philadelphia, USA, (2005).
http://dx.doi.org/10.1109/ICASSP.2005.1415215

[15] **H. Moon and P. J. Phillips**, *"Computational and Performance Aspects of PCAbased Face Recognition Algorithms"*, Perception, *Vol.* ***30****(5)*, pp. 303–321, (2001).
http://dx.doi.org/10.1068/p2896

[16] **P. Grother and P. J. Phillips**, *"Models of Large Population Recognition Performance"*, Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), *Vol.* ***2***, pp. 68–75, Washington D.C., USA, (2004).
http://dx.doi.org/10.1109/CVPR.2004.1315146

[17] **R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A. Senior**, *"The Relationship Between the ROC Curve and the CMC"*, Proceedings of Fourth

IEEE Workshop on Automatic Identification Advanced Technologies (AutoID), pp. 15–20, Buffalo, USA, (2005).
http://dx.doi.org/10.1109/AUTOID.2005.48

[18] **C. Wilson, A. R. Hicklin, M. Bone, H. Korves, P. Grother, B. Ulery, R. Micheals, M. Zoepfl, S. Otto, and C. Watson**, "*Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report*", NIST Technical Report NISTIR 7123, National Institute of Standards and Technology, (2004).

[19] **S. Z. Li and Anil K. Jain**, *Handbook of Face Recognition*, Springer-Verlag, New York, (2005).

[20] **P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone**, *FRVT2002: Overview and Summary*, (2003).
http://www.frvt.org/FRVT2002

[21] **R. Zunkel**, "*Hand Geometry Based Authentication*", Biometrics: Personal Identification in Networked Society, pp. 87–102, Kluwer Academic Publishers, London, UK, (1999).

[22] **D. Zhang, A. W.-K. Kong, J. You, and M. Wong**, *"Online Palmprint Identification"*, IEEE Transactions on Pattern Analysis and Machine Intelligence, *Vol.**25**(9)*, pp. 1041–1050, (2003).
http://dx.doi.org/10.1109/TPAMI.2003.1227981

[23] **J. Daugman**, *"How Iris Recognition Works?"*, IEEE Transactions on Circuits and Systems for Video Technology, *Vol.**14**(1)*, pp. 21–30, (2004).
http://dx.doi.org/10.1109/TCSVT.2003.818350

[24] **J. Daugman**, "*Recognizing Persons by their Iris Patterns*", Biometrics: Personal Identification in Networked Society, pp. 103–122, Kluwer Academic Publishers, London, UK, (1999).
http://dx.doi.org/10.1016/S1363-4127(98)80016-2

[25] **International Biometric Group**, *Independent Testing of Iris Recognition Technology: Final Report*, (2005).
http://www.biometricgroup.com/reports/public/ITIRT.html

[26] **RAYCO Security**, *"Eyedentify retina biometric reader"*, (1997).

http://www.raycosecurity.com/hirsch/EyeDentify.html

[27] **F. Monrose and A. Rubin**, *"Authentication Via Keystroke Dynamics"*, Proceedings of Fourth ACM Conference on Computer and Communications Security, pp. 48–56, Zurich, Switzerland, (1997). http://doi.acm.org/10.1145/266420.266434

[28] **L. Lee, T. Berger, and E. Aviczer**, *"Reliable On-Line Human Signature Verification Systems"*, IEEE Transactions on Pattern Analysis and Machine Intelligence, *Vol. **18**(6)*, pp. 643–647, (1996). http://dx.doi.org/10.1109/34.506415

[29] **V.S. Nalwa**, *"Automatic On-Line Signature Verification"*, Proceedings of the IEEE, *Vol. **85**(2)*, pp. 215–239, (1997). http://dx.doi.org/10.1109/5.554220

[30] **G. Schirripa Spagnolo, C. Simonetti, L. Cozzella**, *"Superposed strokes analysis by conoscopic holography as an aid for a handwriting expert"*, J. Opt. A: Pure Appl. Opt., *Vol.* ***6***, pp. 869-874, (2004). http://dx.doi.org/10.1088/1464-4258/6/9/009

[31] **J. P. Campbell**, *"Speaker Recognition: a Tutorial"*, Proceedings of the IEEE, *Vol. **85**(9)*, pp. 1437–1462, (1997). http://dx.doi.org/10.1109/5.628714

[32] **M. S. Nixon, J. N. Carter, D. Cunado, P. S. Huang, and S. V. Stevenage**, *Automatic Gait Recognition*, Biometrics: Personal Identification in Networked Society, pp. 231–249, Kluwer Academic Publishers, London, UK, (1999).

[33] **D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman and A. K. Jain**, "*FVC2004: Third Fingerprint Verification Competition"*, Proceedings of International Conference on Biometric Authentication (ICBA), pp. 1–7, HongKong, China, (2004). http://dx.doi.org/10.1007/978-3-540-25948-0_1

[34] **M. Przybocki and A. Martin**, *"NIST Speaker Recognition Evaluation Chronicles"*, Odyssey: The Speaker and Language Recognition Workshop, pp. 12–22, Toledo, Spain, (2004).

http://dx.doi.org/10.1109/ODYSSEY.2006.248120

[35] **P.M. Huby**, "*Review: Matter in Aristotle",* The Classical Review, *Vol.* ***24****(1)*, pp. 44–46, (1974). http://dx.doi.org/10.1017/S0009840X00241711

[36] **W. Clarkson, T. Weyrich; A. Finkelstein, N. Heninger, J.A. Halderman, and E.W. Felten**, "*Fingerprinting Blank Paper Using Commodity Scanners*", 30th IEEE Symposium on Security and Privacy, pp. 301–314 (2009).

[37] **R. Hofer, H. Tschopp, B. Rossi, and R. Ardüser,** "Real fake. A Manual for the Detection of Forgeries", Zurich: SPE – Swiss Police Edition, Zurich Canton Police Forensic Science Department, (2006).

[38] **J.C. Biermann,** Handbook of Pulping and Papermaking (2 ed.), San Diego, California, USA, Academic Press, p. 171, (1996).

[39] Counterfeit Deterrent Features for the Next-Generation Currency Design (Publication Nmab, 472) National Academies Press Washington, D.C. (1993).

[40] **G. DeJean, and D. Kirovski**, "*Can A Physically Secure RFID Be Produced? A Review of RFDNA*", Proceedings of the Fourth European Conference on Antennas and Propagation (CCIB, Barcelona, Spain 12-16 April 2010), (2010).

[41] **G. DeJean, and D. Kirovs.ki**, "*Making RFIDs Unique - Radio Frequency Certificates of Authenticity*", IEEE Antennas and Propagation Society International Symposium, pp. 1039–1042, (2006). http://dx.doi.org/10.1109/APS.2006.1710711

[42] **J.D. Woodward Jr., N.M. Orlans, and P.T. Higgins**, Biometrics, McGraw-Hill/Osdorne, Berkeley, CA, USA (2003).

[43] **J.D.R. Buchanan, R.P. Cowburn, A.V. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, A. Allwood, and M.T. Bryan**, "*Forgery: 'fingerprinting' document and packaging*" Nature, *Vol.* ***436***, p. 475, (2005). http://dx.doi.org 10.1038/436475a

[44] **B. Zhu, J. Wu, and M.S. Kankanhalli**, "*Print signatures for document authentication*," Proc. 10th ACM Conf. on Computer and Communications Security, 2003, pp. 145–154, (2003).
http://doi.acm.org/10.1145/948109.948131

[45] **R. Melen**, "*Record document authentication by microscopic grain structure and method*", European Patent Specification EP0570162B 1999/05.

[46] **W. Clarkson, T. Weyrich; A. Finkelstein, N. Heninger, J.A. Halderman, and E.W. Felten**, "*Fingerprinting Blank Paper Using Commodity Scanners*", 30th IEEE Symposium on Security and Privacy, pp. 301–314, (2009).
http://dx.doi.org/10.1109/SP.2009.7

[47] **D. Bauder**, "*An anti-counterfeiting concept for currency systems*" Technical Report PTK-11990, Sandia National Labs, Albuquerque, NM, (1983).

[48] **T. Haist T, and H.J. Tiziani** , "*Optical detection of random features for high security applications*", Opt. Comm. ***147,*** pp. 173–179, (1998).
http://dx.doi.org/10.1016/S0030-4018(97)00546-4

[49] **R.L. van Renesse**, "*Verifying versus falsifying banknotes*", Conference on Optical Security and Counterfeit Deterrence Techniques II, Poc. SPIE *Vol.**3314***, pp. 71–85, (1998).
http://dx.doi.org/10.1117/12.304710

[50] **H. Matsumoto, and T. Matsumotu**, "*Evaluation Security of a Clone Preventive Technique Using Physical Randomness and Cryptography*", in Optical Security and Counterfeit Deterrence Techniques III, Proc. SPIE *Vol. **3973***, pp. 139–152, (2000).
http://dx.doi.org/10.1117/12.382182

[51] **R.P. Cowburn**, "*Laser surface authentication – reading Nature's own security code*", Contemporary Physics, *Vol. **49**(5)*, pp. 331–342, (2008).
http://dx.doi.org/10.1080/00107510802583948

[52] **G. Schirripa Spagnolo, L. Cozzella, and C. Simonetti**, "*Banknote security using a biometric-like technique: a Hylemetric approach*", Meas. Sci. Technol., *Vol.* ***21***, (2010). http://dx.doi.org/10.1088/0957-0233/21/5/055501

[53] **G. Schirripa Spagnolo, L. Cozzella, and C. Simonetti**, "*Currency Verification by 2D Infrared Barcode*", Meas. Sci. Technol., *Vol.* ***21***, (2010). http://dx.doi.org/10.1088/0957-0233/21/10/107002

[54] **J.H. Merriman,** *"Counterfeit Art"*, Int. J. of Cult. Prop., *Vol.* ***1****(1)*, pp. 27–28, (1992). http://dx.doi.org/10.1017/S0940739192000055

[55] **New York Times**, ART COUNTERFEIT REVEALED, September 24 1922 (1922).

[56] http://www.who.int/medicines/services/counterfeit/impact/ImpactF_S/en/

[57] **WHO Expert Committee on Specifications For Pharmaceutical Preparations**, "*Forty-third Report*", WHO Technical Report Series, pp. 17-20, (2009).

[58] **US Food and Drug Administration**, "*Tamper-evident packaging requirements for over-the-counter (OTC) human drug products*", CFR - Code of Federal Regulations Title 21 Food And Drugs, Part 211 Subpart G, Section 211.132, (2011).

[59] **US Food and Drug Administration**, "*What is the status of electronic track and trace across the drug supply chain?*", FDA Counterfeit Drug Task Force Reports 2006, Section IV, (2006).

[60] **R. Burhouse**, "*How New Packaging Technologies are Helping in the Struggle Against Counterfeit Drugs*", Pharmaceutical Manufacturing Magazine, (2010).

[61] **I. Lancaster**, "*Trends: Holograms and Anti-counterfeiting*", PharmaTech.com, Apr 2, (2008).

[62] **I. Lancaster**, Pharmaceutical Technology, PharmaTech.com, (2008).

[63] **J.H. Han, C.H.L. Ho, and E.T. Rodrigues**, "*Intelligent Packaging*", in: Jung H. Han (Ed.), Innovation in Food Packaging, Academic Press, San Diego, CA, Chap. 9, pp. 138–157, (2009).

[64] **A. Firsov, B. Loechel, A. Schleunitz, A. Svintsov, and Z. Zatisev**, "*Fabrication of Nanoimprint Stamps for Rainbow Holograms using SEM based e-beam lithography*", Proceedings 33rd International Conference on Micro- and Nano- Engineering (MNE 2007), pp. 553–554, (2007).

[65] **C. Lowe**, "*Holography gets smart*", PhysicsWorld.com, February 1, (2008).

[66] **T. Mizuno, T. Goto, M. Goto, K. Matsui, and T. Kubota**, "*Methylene blue sensitized dichromated gelatine holograms: influence of the moisture on their exposure and diffraction efficiency*", Appl. Opt., *Vol.* ***29****(32)*, pp. 4757–4760, (1990). http://dx.doi.org/10.1364/AO.29.004757

[67] **M. Graham**, "*Fake Holograms a 3-D Crime Wave*", Wired Magazine, February 2007, (2007).

[68] **M. Davison**, "Pharmaceutical Anti-Counterfeiting: Combating the Real Danger from Fake Drugs", Wiley-Blackwell, Hoboken, NJ, (2011).

[69] **P.H. Berning, R.W. Phillips**, "*Thin Film Optically Variable Article And Method Having Gold To Green Colour Shift For Currency Authentication*", U.S. Patent n° 4,779,898, (1988).

[70] ISO/IEC 18004:2006 — QR code symbology specification, (2006).

[71] ISO/IEC 16022:2006 — Data Matrix bar code symbology specification, (2006).

[72] FDA 2006 Compliance Policy Guide for the Prescription Drug Marketing Act, (2006).

[73] Pharma Anti-Counterfeiting News, Issue 3, March 2008.

[74] **S. Ghosh**, "*The R.F.I.D Act of 2006 and E-Pedigrees: Tackling the Problem of Counterfeit Drugs in the United States Wholesale Industry*", Mich. Telecomm. & Tech. L. Rev., pp. 577–600, (2006).

[75] **R. Sangoia, C.G. Smithb, M.D. Seymourc, J.N. Venkataramanc, D.M. Clarkd, M.L. Klepere, and B.E. Kahnab**, "*Printing Radio Frequency*

Identification (RFID) Tag Antennas Using Inks Containing Silver Dispersions", Journal of Dispersion Science and Technology, *Vol.* ***25****(4)*, pp. 513-521, (2005). http://dx.doi.org/10.1081/DIS-200025721

[76] **C. Swedberg**, "*Developing RFID-Enabled Phones*", RFID Journal, (2004), http://www.rfidjournal.com/article/articleview/1020/1/1

[77] Nokia Press Release, *Nokia Unveils the world's first NFC product - Nokia NFC shell for Nokia 3220 phone*, (2004).

[78] **R. Melen**, "*Record document authentication by microscopic grain structure and methods*", European patent Specification n° EP 0.570.162 B1, (1999).

[79] **R.L. Jones**, "*Emerging security features for identification documents*", US Patent n° 7.213.757, 2007.

[80] **R.D. Hersch, P. Donzé, and S. Chosson**, "*Colour images visible under UV light*", ACM SIGGRAPH, *Vol.* ***26****(3)*, (2007). http://doi.acm.org/10.1145/1276377.1276471

[81] **R.A. Einhorn**, "*Security Taggents In Adhesive Plastic Film Laminate For Pharmaceutical Packaging*", European Patent Specification n° EP 1.769.485 B1, (2005).

[82] http://www.ingeniatechnology.com/wp-content/uploads/2011/04/

[83] **C.N. Chong, D. Jiang, J. Zhang, and L. Guo**, "*Anti-counterfeiting with a Random Pattern*", Proceedings of SECURWARE 2008, pp. 146–153, (2008). http://dx.doi.org/10.1109/SECURWARE.2008.12

[84] **D. Jiang, and C.N. Chong**, "*Anti-counterfeiting using phosphor PUF*", Proceeding of ASID 2008, pp. 59–62, (2008). http://dx.doi.org/10.1109/IWASID.2008.4688338

[85] **W. Samuel, H.P. Uranus, and M.D. Birowosuto**, "*Recognizing Document's Originality by Laser Surface Authentication*", Proceeding of Second International Conference on Advances in Computing, Control, and Telecommunication Technologies¸ pp. 37–40, (2010). http://dx.doi.org/10.1109/ACT.2010.15

[86] **L. Cozzella, C. Simonetti, and G. Schirripa Spagnolo**, "*It is possible to use biometric techniques as authentication solution for objects? Biometry vs.. Hylemetry*", IEEE Proc. of 5th International Symposium on Communications Control and Signal Processing (ISCCSP), (2012). http://dx.doi.org/10.1109/ISCCSP.2012.6217753

[87] **M.Hirakawa, and J.Iijima**, "*A Study on Digital Watermarking. Usage in the Mobile Marketing Field: Cases in Japan*", in Proceedings of the Secondary International Logistics and Industrial Informatics, pp. 1–6, (2009).

[88] **L. Li, R.L. Wang, and C.C. Chang**, "*A Digital Watermark Algorithm for QR Code*", International Journal of Intelligent Information Processing, *Vol.* ***2****(2),* (2011).

[89] **Jibo Si, and Shuhuai Zhang**, "*Research on embedding and extracting methods for digital watermarks applied to QR Code images*", New Zealand Journal of Agricultural Research, *Vol.****50***, pp. 861–867, (2007). http://dx.doi.org/10.1080/00288230709510361

[90] **A. Albers, and C. Kahl**, "*Design and Implementation of Context-Sensitive Mobile Marketing Platforms*", E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, 10th IEEE Conference, pp. 273–278, (2008). http://dx.doi.org/10.1109/CECandEEE.2008.102

[91] **P.J. Kim, and Y.J. Noh**, "*Mobile Agent System Architecture for supporting Mobile Market Application Service in Mobile Computing Environment*", Geometric Modeling and Graphics International Conference, pp.149–153, (2003). http://dx.doi.org/10.1109/GMAG.2003.1219680

[92] **M.Hirakawa, and J. Iijima**, "*A Study on Data Management Using Mobile Computing with Digital Watermark Technology*", The 6th International Conference on Service Systems and Service management (ICSSSM 2009), pp. 186–191, (2009). http://dx.doi.org/10.1109/ICSSSM.2009.5174880

[93] **Y.P. Wang,** "*Using Barcodes in Documents – Best Practices*", Tampa, FL: Accusoft, (2007).

[94] **A. Longagre Jr., and R. Hussey**, "*Two dimensional data encoding structure and symbology to use with optical reader* " US Patent n° 5.591.956, (1997).

[95] **GS1 barcode technical Comitee**, GS1 DataMatrix - An introduction and technical overview of the most advanced GS1 Application Identifiers compliant symbology, (2009).

[96] **J.H. Merryman**, "*Counterfeit Art*", Int. J. of Cult. Prop., *Vol.* ***1****(1)*, pp. 27–28, (1992).
http://dx.doi.org/10.1017/S0940739192000055

[97] **R.L. van Renesse,** *Optical Document Security*, 2nd ed., London: Artech House, (1997).

[98] **B. Hardwick, W. Jackson, G. Wilson, and A.W.H. Mau**, "*Advanced Materials for Banknote Applications*", Adv. Mater., *Vol.****13***, pp. 980–984, (2001).
http://dx.doi.org/10.1002/1521-4095(200107)13:12/13<980::AID-ADMA980>3.0.CO;2-F

[99] **R.L. Rivest, A. Shamir, and L. Adleman**, "*A method for obtaining digital signatures and public-key cryptosystems*", Communications of the ACM *Vol.* ***21****(2)*, pp. 120–126, (1978).
http://dx.doi.org/10.1145/359340.359342

[100] **L. Nanni L, and A. Lumini,** "*A supervised method to discriminate between impostors and genuine in biometry*", Expert Systems with Applications, *Vol.* ***36***, pp. 10401–10407, (2009).
http://dx.doi.org/10.1016/j.eswa.2009.01.037

[101] **R.A. Mollin**, *RSA and Public-key Cryptography,*London: Chapman and Hall, (2002).

[102] **D. Hankerson, A.J. Menezes, and S. Vanstone**, *Guide to Elliptic Curve Cryptography*, Springer New York: Springer, (2010).

[103] **R.L. Daniel, and D.R.L. Brown**, *Standards for Efficient Cryptography - SEC 1: Elliptic Curve Cryptography*, Mississauga ON Canada: Certicom Research, (2009).

[104] **New York Times**, Art Counterfeit Revealed, September 24, (1922).

[105] Digital Signature Standard (DSS). http://www.itl.nist.gov/fipspubs/fip186.htm

[106] **F.P. Vandome, A.F Mcbrewster, and J. Miller**, *Affine Transformation*, Beau Bassin: Alphascript Publishing, (2010).

[107] **R.C. Gonzales, R.E. Woods, and S.L. Eddins**, *Digital Image Processing using Matlab*, 2nd Edition, Gatesmark Publishing, (2009).

[108] **M. Sjödahl**, "*Digital speckle photography*", in Trends in Optical Non-destructive Testing and Inspection, Amsterdam: Elsevier Publishing, pp. 179–195, (2000).

[109] **A. Senefelder**, *A Complete Course of Lithography with a Preface by Frederic von Schlichtegroll*, London: R. Ackermann, (1819).

[110] **J.R. Groves,** "*Brief Description of Lithography*", Iowa Geological and Water Survey Guidebook Series, *Vol.**28***, pp. 53–56, (2008).

[111] **V. Strauss**, *The Lithographers Manual: A Compendium in Two Volumes*, 20th Anniversary Edition, New York: Waltwin Publishing Company, (1958).

[112] **A.B. Hoen,** "*Discussion of the Requisite Qualities of Lithographic Limestone, with Report on Tests of the Lithographic Stone of Mitchell County*", Iowa Geological Survey Annual Report, pp. 339–352, (1902).

[113] http://www.knottywood-treasures.com/id58.html

[114] http://everything.explained.at/lithography/

[115] Dallas Semiconductor Maxim DS5250 High-speed Secure Microcontroller datasheet rev. 071803

[116] **G.E. Suh, D. Clarke, B. Gassend, M. van Dijk, and S. Devadas**, "*Efficient Memory Integrity Verification and Encryption*", Secure Processors Proceedings of the 36th International Symposium on Microarchitecture, (2003).

http://dx.doi.org/10.1109/MICRO.2003.1253207

[117] **M. Murase, W. Plouffe, K. Shimizu, M. Sakamoto, and V. Zbarsky**, *Cryptographic Secure Programm Overlay*, US patent n° US7886162.

[118] **J. Yang, L. Gao, Y. Zhang**, "*Improving Memory Encryption Performance",* Secure Processors IEEE Transactions on Computers, *Vol.**54***, (2005).
http://dx.doi.org/10.1109/TC.2005.80

[119] **F.P. Chiang, and A. Asundi**, "*White light speckle method of experimental strain analysis*", Appl. Opt. *Vol.**18,*** pp. 409–411, (1979).
http://dx.doi.org/10.1364/AO.18.000409

[120] **L.M. Burch, and C. Forno**, "*A high sensitivity moiré grid technique for studying deformation in large objects*", Opt. Eng., *Vol.**15***, pp. 178–185, (1975).
http://dx.doi.org 10.1117/12.7978755

[121] **C. Forno**, "*White light speckle photography for measuring deformation, strain and shape*", Opt laser Technol., *Vol.**16***, pp. 217–221, (1975).
http://dx.doi.org/10.1016/0030-3992(75)90042-0

[122] **P.J. Rae, S.J.P. Palmer, H.T. Goldrein, A.L. Lewis, and J.E. Field**, "*White-light digital image cross-correlation (DICC) analysis of the deformation of composite materials with random microstructure*", Opt. Lasers Eng. *Vol. **41***, pp. 635–648, (2004).
http://dx.doi.org/10.1016/S0143-8166(02)00179-3

[123] **M. Sjödahl, and L. Larsson**, "*Monitoring microstructural material changes in paper through microscopic speckle correlation rate measurements*", Opt. Lasers Eng. *Vol. **42,*** pp. 193–201, (2004).
http://dx.doi.org/10.1364/OE.17.012309

[124] **M. Sjödahl, and L. Benckert**, "*Electronic speckle photography—analysis of an algorithm giving the displacement with subpixel accuracy*", J Appl Opt *Vol. **32***, pp. 2278–2284, (1993).
http://dx.doi.org/10.1364/AO.32.002278

[125] **M. Sjödahl** "*Electronic speckle photography—increased accuracy by non integral pixel shifting*", J. Appl. Opt. *Vol.* ***33***, pp. 6667–6673, (1994). http://dx.doi.org/10.1364/AO.33.006667

[126] **M. Sjödahl** "*Accuracy in electronic speckle photography*", J. Appl. Opt. *Vol.* ***36,*** pp. 2875–2885, (1997). http://dx.doi.org/10.1364/AO.36.002875

[127] **J.W. Goodman**, "*Statistical properties of laser speckle patterns*", J.C. Dainty (Ed.) Laser Speckle And Related Phenomena, Topics in Applied Physics, Springer-Verlag, Berlin, *Vol.* ***9***, pp. 9–75, (1975). http://dx.doi.org/10.1007/BFb0111436

[128] **R. Housley**, "Public Key Infrastructure (PKI)", H. Bidgoli (Ed), The Internet Encyclopedia, John Wiley & Sons, Inc., Hoboken, New Jersey, pp. 156–165, (2004).

[129] **D. Hankerson**, **A. J. Menezes, and S.Vanstone**, "Guide to Elliptic Curve Cryptography", Springer, New York, (2010).

[130] **R.L. Daniel, and D.R.L. Brown**, "Standards for Efficient Cryptography—SEC 1: Elliptic Curve Cryptography", Mississauga, ON, Canada: Certicom Research, (2009).

[131] FIPS PUBS 186-3 – Digital Signature Standard - ECDSA - Elliptic Curve Digital Signature Algorithm, (2009).

[132] **C. E. Shannon**, "*Communication in the presence of noise (reprinted)*", Proc. Institute of Radio Engineers, *Vol.* ***37****(1)*, pp. 10–21, (1998). http://dx.doi.org/10.1109/PROC.1984.12998

[133] **Y. Wang, D. L. Lau, and L. G. Hassebrook**, "*Fit-Sphere Unwrapping and Performance Analysis of 3D Fingerprints*", Applied Optics, *Vol.* ***49****(4)*, pp. 592–600, (2010). http://dx.doi.org/10.1364/AO.49.000592

[134] **P. Hariaran**, *Optical holography: principles, techniques and applications*, Cambrige University Press, (1996).

[135] **G. Tricoles**, "*Computer generated holograms: an historical review*", Applied Optics, *Vol.* ***26****(20)*, pp. 4351–60, (1987). http://dx.doi.org/10.1364/AO.26.004651

[136] **O. Bryngdahl O., and F. Wyrowski**, "*Digital Holography - Computer-Generated Holograms"*, Progress in Optics, *Vol. **28***, pp. 21–81, North Holland, (1990).
http://dx.doi.org/10.1364/JOSA.52.001123

[137] **E.N. Leith, and J. Upatnieks,** 'Reconstructed Wavefronts and Communication Theory', JOSA, *Vol. **52**(10)*, pp. 1123–1128, (1962). http://dx.doi.org/10.1016/S0079-6638(08)70288-9

[138] **B.R. Brown, and A.W. Lohmann**, "*Complex Spatial Filtering with Binary Masks*", Applied Optics, *Vol.**5**(6)*, pp. 967–969, (1966). http://dx.doi.org/10.1364/AO.5.000967

[139] **W.H**. **Lee**, "*Computer Generated Holograms: techniques and applications*", Progress in Optics, *Vol.16*, pp. 119–232, North Holland, (1978).
http://dx.doi.org/10.1016/S0079-6638(08)70072-6

[140] **W.H. Lee**, "*Sampled Fourier Transform Hologram Generated by Computer*", Applied Optics, *Vol.**9**(3),* pp. 639–643, (1970).
http://dx.doi.org/10.1364/AO.9.000639

Appendix B Synthetic Holograms

With the term ***Computer Generated Hologram*** (CGH) or ***Synthetic Hologram*** (SH) we intend a class of holograms created as graphical output of an algorithm calculated by a Personal Computer [135-136]. Starting from a Wave front mathematical description or a points array representative of an object, it is possible calculating the hologram amplitude and showing the result on a display.

In the optic holography, the wave front registration on the holographic plate is implemented using optical instruments. The CGH is created using only computer simulated algorithms. The CGH represents the wave front diffracted by an object on the hologram plane and it is not necessary that the object really exists; so it is possible creating CGH of impossible and unrealizable objects, using only a mathematical description of the object itself.

Also the object reconstruction is easier for the CGH, instead of a real optic holograms, due to the necessity only of applying mathematical inverse operations, instead of laser illumination.

As for optical holograms, also SH can be classified as Fourier Transform holograms or Fresnel Holograms depends on relations between the object and the complex wave front recorded on the hologram itself. In the first case light from the object is diffracted in the Fraunhofer Zone (far field diffraction), and the relation between complex amplitude on hologram plane and object complex amplitude can be expressed as:

$$F(u,v) = \Im\{f(x,y)\} \tag{B.1}$$

$F(u,v)$ has to be transformed in a real and non-negative function for creating a transmittance able to follow the off-axis optic holography rules. This step is made by encoding algorithms. In fact the main difference between an SH and a conventional hologram is the way in which the complex wave front is recorded.

In the off-axis holography, developed by Leith e Upatnieks in the 1962 [137], the transmittance function is proportional to

$$\begin{aligned} t(x,y) &= \left| R \cdot e^{j2\pi\alpha x} + A(x,y) \cdot e^{j\phi(x,y)} \right|^2 = \\ &= R^2 + A^2(x,y) + 2RA(x,y)\cos\left[2\pi\alpha x - \phi(x,y)\right] \end{aligned} \tag{B.2}$$

where

- $R \cdot e^{j2\pi\alpha x}$ represents the deviated reference wave;
- $A(x,y)e^{j\phi(x,y)}$ represents the object wave; and
- $t(x,y)$ is the resulting interference pattern intensity variance between the two waves.

In the CGH the holograms transmittance function and the object wave front are represented by means of mathematical equations different from the above-reported (B.2), because it is necessary overcame the problem to codify a complex wave front generated by the object in a real and non-negative function.

The complex wave front encoding for creating Synthetic Holograms was demonstrated the first time by Brown and Lohmann in the 1966 with the *Detour Phase Hologram* method [138]. Their holograms have the following three main properties:

- A good hologram transmittance value;
- The CGH could encode both amplitude and phase information for each complex real value of the transmittance function;
- The CGH was implemented without an explicit reference field.

For creating a such digital hologram, the complex function representative wave front, $A(x,y)e^{j\phi(x,y)}$ is firstly sampled, then is divided in equally spaced cells. After that rectangular windows are extracted from each cell. Every window is determined by three parameters:

1. The height h_{nm};
2. The width w_{nm} ;
3. The centre respect with the cell centre c_{nm} .

These parameters are selected has follow:

$$\begin{aligned} h_{nm} &= A_{nm} dy \\ w_{nm} &= w \\ c_{nm} &= \phi_{nm} \frac{dx}{2\pi M} \end{aligned} \tag{B.3}$$

Where A_{nm} and ϕ_{nm} are amplitude and phase of the wave front samples taken at $x = ndx$ and $y = mdy$ with dx and dy are the sampling distances along the two axis. It has to be noted that the maximum value of $\{A_{nm}\}$ has been normalized to 1. Eventually the parameter M is the actual binary hologram frequency.

When this pattern is reported on a holographic plate this creates a pure amplitude transmittance equal to:

$$\begin{aligned} & t_1(x,y) = \sum_n \sum_m \varphi\left[\frac{(x - ndx - c_{nm})}{w}\right] p\left[\frac{(y - mdy)}{h_{nm}}\right] \\ & \textit{where} \\ & p(x) = \begin{cases} 0 & \text{for } |x| \le \dfrac{1}{2} \\ 1 & \text{otherwise} \end{cases} \end{aligned} \tag{B.4}$$

B.1 Lee’s Delayed Sampling Method

In the 1970 Lee proposed a radical change in the off-axis CGH encoding [139 – 140]. The principal behind the so called **Lee Method** directly derives from one of the sampling function properties. In fact Lee noted that if two real functions are sampled at periodic intervals and a sampling delay is present in one of the two functions, could be created a constant phase difference in the same functions Fourier Transformations.

Starting from this point, Lee combines the four real and non-negative functions sampled with delays in phase quadrature, obtaining the Fourier Transform of the complex function on the Fourier transformed plane.

The phase information is now encoded in the position of the samples in the hologram itself. If we think about a function $f_s(x)$, defined as the sampled version of $f(x)$, $f_s(x)$ can be written as:

$$f_s(x) = \sum_n f(nd_x + \varepsilon)\delta(x - nd_x - \varepsilon) \qquad \text{(B.5)}$$

Where $\delta(x)$ is the Dirac Delta function and d_x the sampling interval. The Delta Dirac is a special function, with unitary area, defined as:

$$\delta(x - x_0) = \begin{cases} 1 & \text{for } x = x_0 \\ 0 & \text{otherwise.} \end{cases} \qquad \text{(B.6)}$$

The parameter ε is a little sampling pulse displacement respect with $f(x)$ origin. If $f(x)$ is a bandwidth limited function, it can be recovered using a low-pass filter in front of the sampled function $f_s(x)$. In this case the displacement ε has no effects on the $f(x)$ reconstruction starting from the sampled version $f_s(x)$.

Anyway, if $f_s(x)$ passes through a bad-pass filter with the impulse response equal to:

$$g(x) = \frac{\sin\left(\dfrac{\pi x}{d_x}\right)}{\pi x} \exp\left(\frac{j2\pi x}{d_x}\right) \qquad \text{(B.7)}$$

The exit from this filter will be:

$$\begin{aligned} f_1(x) &= \sum_n f\left(nd_x+\varepsilon\right)\frac{\sin\left(\dfrac{\pi\left(x-d_x-\varepsilon\right)}{d_x}\right)}{\pi\left(x-d_x-\varepsilon\right)}e^{\left(\frac{j2\pi\left(x-nd_x-\varepsilon\right)}{d_x}\right)} \\ &= e^{\left(j2\pi x/d_x\right)}e^{\left(j2\pi\varepsilon/d_x\right)}\sum_n f\left(nd_x+\varepsilon\right)\frac{\sin\left(\dfrac{\pi\left(x-d_x-\varepsilon\right)}{d_x}\right)}{\pi\left(x-d_x-\varepsilon\right)} \end{aligned} \tag{B.8}$$

The summation reported in (B.8) is the $f_s(x)$ low-pass filtering result, so it equals to $f(x)$. So we can rewrite (B.8) as follow:

$$f_1(x) = e^{\left(j2\pi x/d_x\right)}e^{\left(j2\pi\varepsilon/d_x\right)}f(x) \tag{B.9}$$

It can be noted that in the $f_1(x)$ formulation is present a constant phase term, equal to $2\pi\varepsilon/d_x$. This result indicates that it is possible adding a constant phase term to the function before sampling it, with a certain predetermined delay ε and then it is possible filtering it with a bass-pass filter. On the basis of these observations, is obvious that any complex function, represented as $A(x,y)e^{j\phi(x,y)}$ can be decomposed in real, non-negative functions and that the phase information related to each component can be encoded sampling the original function with a predetermined precise phase displacement ε. The so encoded complex value function can now be reconstructed using only a band-pass filter.

One possible way to decompose the complex values function in real and non-negative ones is the following:

$$\begin{aligned} f(x,y) &= A(x,y)e^{j\phi(x,y)} \\ &= \left[f_{r+}(x,y) - f_{r-}(x,y) \right] + j\left[f_{i+}(x,y) - f_{i-}(x,y) \right] f(x,y) \end{aligned} \tag{B.10}$$

Functions at second member of (B.10) are:

- $f_{r+}(x,y)$ positive portion of complex function real part;
- $f_{r-}(x,y)$ negative portion of complex function real part;
- $f_{i+}(x,y)$ positive portion of complex function imaginary part;
- $f_{i-}(x,y)$ negative portion of complex function imaginary part.

The phase information of these four components could be recorded sampling any of them with a different displacement ε, equal to 0, $d_x/4$, $d_x/2$, $3d_x/4$ respectively. In this way the lower ε value is equal to 1/4 of the starting sampling interval, d_x, so the complex function has to be sampled with a rate fourth times the spatial bandwidth along the x coordinate.

For better understanding how implementing a single cell in a Lee Hologram, we have to analyse the following Figure B.1.

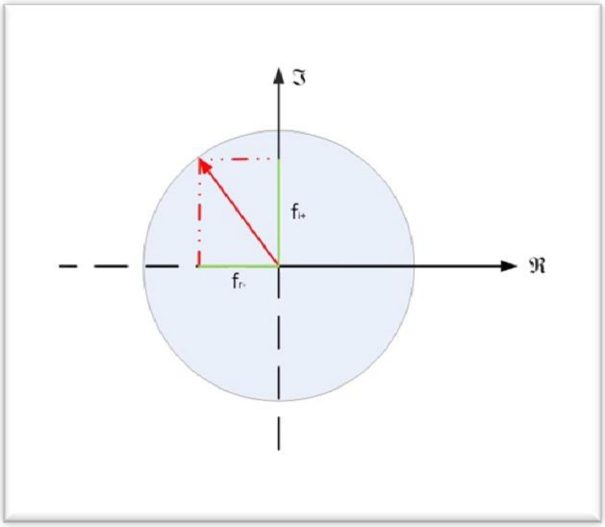


Figure B.1 – Lee Hologram phasor decomposition schema. It shows a real and imaginary components related to a single cell to be transformed.

From the previous Figure B.1 it is possible understanding that any Complex Field component of the Fourier sesies could be decomposed in a real and a immaginary part o the Gauss plane. Following the Lee encoding, it is possible obtaining four hypotetical functions, one for each of the four semi-axes on the Gauss plane. In this way, any given phasor can be decomposed in 2 components, one real and one immaginary, and two of the four functions will be always equal to zero, whereas the other two will be a module proportional to the projections of the phasor on the two related semi-axes.

In the following Figure B.2 is reported the encoding of a Complex Phasor:

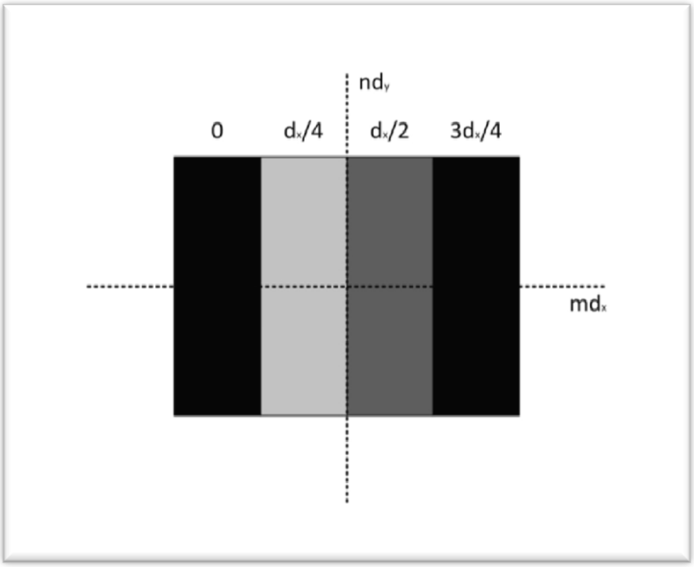


Figure B.2 – Lee Hologram phasor decomposition schema. It shows a real and imaginary components related to a single cell to be transformed.

Starting from these analysis, the hologram transmittance function can be expressed as follow:

$$\begin{aligned} h(x,y) = \sum_n \sum_m f_{r+}\left(md_x, nd_y\right)\delta\left(x-md_x, y-nd_y\right)+ \\ f_{r-}\left(md_x+d_x/2, nd_y\right)\delta\left(x-md_x-d_x/2, y-nd_y\right)+ \\ f_{i+}\left(md_x+d_x/4, nd_y\right)\delta\left(x-md_x-d_x/4, y-nd_y\right)+ \\ f_{i-}\left(md_x+3d_x/4, nd_y\right)\delta\left(x-md_x-3d_x/4, y-nd_y\right) \end{aligned} \quad \text{(B.11)}$$

Due to the fact that the four functions are all real and non-negative, also the four functions $h(x,y)$ reported in (B.11) are real and non-negative and at same way their Fourier Transform:

$$\begin{aligned} &H(u,v) = H^{*}(u,v) \quad \textit{real} \\ &H(u,v) > 0 \quad \textit{non-negative} \\ &\textit{where} \\ &H(u,v) = \Im\{h(x,y)\}. \end{aligned} \tag{B.12}$$

The last step for enhancing the quality of the reconstructed hologram and for reporting the final dimension to a N x N matrix, simpler and faster to manage with a Fast Fourier Hologram, is the substitution of the four sub-cells, with one created as the median value of the four original, for each complex sampled value.