N^o: .....

People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Djillali Liabes University of Sidi Bel Abbes



Thesis

Submitted in fulfillment of the requirements for the degree

of Doctor in Networks and Telecommunications

Faculty : Electrical Engineering
Department : Telecommunications

Author

Mr NOUIOUA Nadhir

Secure Transfer of Medical Images Based on Blind Watermarking Methods and Cryptography Application to Telemedicine

Committee members:

Pr.	BELLOULA Kamel	UDL SBA	President
Pr.	CHOUAKRI Sid Ahmed	UDL SBA	Examiner
Pr.	MERAZKA Fatiha	USTHB ALG	Examiner
Pr.	SEDDIKI Ali	UDL SBA	Supervisor
Dr.	GHAZ Abdelkrim	UDL SBA	Co-Supervisor

"If i have seen further it is by standing on the shoulders of giants"
Sir Isaak Newton

Acknowledgments

First and foremost, praise and thanks to God, the Almighty, for His showers of blessings throughout my research work to complete the research successfully.

I forward my sincere thanks to Prof. Seddiki Ali and Dr. Ghaz Abdelkrim for their valuable help during the work on this thesis. Their suggestions were always there whenever I needed them. As research supervisors, they spared their valuable time for the in-depth discussion on this research work.

Also, I would like to extend my heartfelt thanks to the Department of Telecommunications and the Telecommunication and Digital Signal Processing Laboratory head, Prof. Djebbari Ali, for providing us with laboratory access during this work.

I am extremely grateful to my parents for their love, prayers, care, and sacrifices in educating and preparing me for my future. Also, I express my thanks to my sister and brother for their support and valuable prayers. To my beloved nephew Hamouda, for the countless moments we have shared together and for the joy, he brought into my life.

Finally, I would like to thank all the people who were helpful to me, whether directly or indirectly, in the completion of this research work.

Sidi Bel Abbes, the September 14th, 2022.

Contents

Contents iv

List of Figures vii

List of Tables ix

Nomenclature xii

Abstract xii

0 Introduction 1
- 0.1 Motivation . . . 1
- 0.2 Research Objectives . . . 2
- 0.3 Research Questions . . . 3
- 0.4 Research Outcome . . . 5
- 0.5 Thesis Outline . . . 6

1 Recap on digital image 7
- 1.1 Introduction . . . 8
- 1.2 What is a digital image . . . 9
- 1.3 Binary, grayscale and color images . . . 9
  - 1.3.1 Binary images . . . 9
  - 1.3.2 Gray levels images . . . 9
  - 1.3.3 color images . . . 10
- 1.4 Color spaces . . . 11
  - 1.4.1 RGB color space . . . 11
  - 1.4.2 YCbCr color space . . . 12
  - 1.4.3 CMYK color space . . . 13
  - 1.4.4 HSI color space . . . 14
  - 1.4.5 YIQ color space . . . 16
- 1.5 Biomedical imaging . . . 16
  - 1.5.1 X-ray Radiography . . . 17
  - 1.5.2 Ultrasound . . . 17
  - 1.5.3 Computed tomography . . . 19
  - 1.5.4 Magnetic Resonance Imaging . . . 21
- 1.6 Telemedicine . . . 22

Conclusion . . . 22

2 Digital watermarking & cryptography 24
- 2.1 Introduction . . . 26
- 2.2 ABC's of watermarking . . . 27

2.3 Requirements of digital watermarking . . . 29
2.3.1 Imperceptibility . . . 29
2.3.2 Robustness . . . 30
2.3.3 Data payload . . . 31
2.3.4 Security . . . 32
2.3.5 Computational complexity . . . 32
2.4 Digital watermarking classifications . . . 32
2.4.1 Working domain . . . 32
2.4.2 Type of document . . . 33
2.4.3 Human perception . . . 34
2.4.4 Reversibility . . . 35
2.5 Watermarking Attacks . . . 35
2.5.1 Active attacks . . . 35
2.5.2 Passive attacks . . . 36
2.5.3 Forgery attacks . . . 36
2.5.4 Collusion attacks . . . 37
2.6 Fields of application . . . 37
2.7 Performances metrics . . . 40
2.8 Cryptography . . . 42
2.8.1 Symmetric key encryption . . . 43
2.8.2 Public key encryption . . . 44
2.8.3 Chaos based cryptography . . . 44
Conclusion . . . 45

3 Blind Digital Watermarking Scheme based on DTCWT and NSCT for Telemedicine Application **46**
3.1 Introduction . . . 47
3.2 Related works . . . 48
3.3 Preliminaries . . . 52
3.3.1 Dual Tree Complex Wavelet Transform . . . 52
3.3.2 Non-Subsampled Contourlet Transform . . . 54
3.4 Methodology . . . 55
3.4.1 Watermark embedding procedure . . . 56
3.4.2 Watermark extraction procedure . . . 57
3.5 Results and Discussion . . . 58
3.5.1 High-fidelity evaluation . . . 59
3.5.2 Robustness analysis . . . 60
3.5.3 Computational cost . . . 68
Conclusion . . . 68

4 Medical Image Watermarking Algorithm using Asymmetric crypto-system and Chaotic Map **70**
4.1 Introduction . . . 71
4.2 Related works . . . 72
4.3 Technical Background . . . 72
4.3.1 Discrete Cosine Transform . . . 72
4.3.2 Discrete Wavelet Transform . . . 74
4.3.3 El-Gamal crypto-system . . . 75
4.3.4 Arnold Chaotic Map . . . 76
4.4 Methodology . . . 77

4.4.1 Watermark insertion and image encryption 77
4.4.2 Watermark extraction 78
4.5 Experimental Results 78
4.5.1 Fidelity evaluation 79
4.5.2 Robustness evaluation 82
Conclusion 85

5 conclusions and Perspectives **87**
5.1 Conclusion 88
5.2 Future Scope 90

Bibliography **91**

List of Figures

1.1 Two-dimensional $(m \times n)$ digital image matrix representation [Tomasz, 2021] . . . 8
1.2 Zoom in Lena pixels . . . 9
1.3 Lena binary image . . . 10
1.4 Lena grayscale image . . . 10
1.5 Lena color image . . . 11
1.6 The RGB color cube [Paulsen and Moeslund, 2020] . . . 12
1.7 Peppers RGB image (from left to right: Red (R), Green (G) and Blue (B)) . . . 12
1.8 Peppers image converted from RGB to YCbCr color space (from left to right: Luminance "Y", and chrominance "Cb, Cr") 13
1.9 Peppers image converted from RGB to CMY color space (from left to right: Cyan "C", Magenta "M" and Yellow "Y" . 13
1.10 The HSI color model depiction [Plataniotis and Venetsanopoulos, 2011] . . . 15
1.11 Peppers image converted from RGB to HSI color space (from left to right: Hue (Y), Saturation (S) and Intensity (I)) . . . 15
1.12 The spectrum of diagnostic X-ray is above the spectrum of visible light [] . . . 17
1.13 Thorax X-ray [Med, 2022] . . . 19
1.14 On the right a cardiac ultrasound image, on the left a cardiac ultrasound image with color Doppler flow [de Leeuw et al., 2007] . . . 20
1.15 Computed tomography (CT) scans [Kamalian et al., 2016] . 20
1.16 Magnetic Resonance Imaging (MRI) scans [Wattjes and Fischer, 2013] . . . 21

2.1 The prisoners' problem [Craver, 1997]. . . . 26
2.2 Watermark embedding process . . . 28
2.3 Watermark extraction process . . . 28
2.4 Compromise between imperceptibility, capacity, and robustness [Attari and Shirazi, 2018] . . . 29
2.5 Information security branches and watermarking classifications [Kadian et al., 2021]. . . . 33
2.6 Euro banknotes watermark. . . . 34
2.7 Common removal attacks [Evsutin and Dzhanashia, 2022]. . 36
2.8 Common geometric attacks [Evsutin and Dzhanashia, 2022]. 37
2.9 Digital watermarking applications [Kumar et al., 2017] . . . 38

2.10 Two-party communication using encryption, with a secure channel for key exchange. The decryption key "d" can be efficiently computed from the encryption key "e". [Menezes et al., 1997] . . . 43
2.11 Encryption using public-key techniques. [Menezes et al., 1997] 44

3.1 Digital watermarking applications . . . 53
3.2 Digital watermarking applications . . . 54
3.3 Digital watermarking applications . . . 55
3.4 Digital watermarking applications . . . 56
3.5 Digital watermarking applications . . . 58
3.6 Digital watermarking applications . . . 58
3.7 Digital watermarking applications . . . 59
3.8 (a) original host image, (b) Salt & pepper (density=1%), (c) Salt & pepper (density=5%), (d) Gaussian noise (density =1%), (e) Gaussian noise (density =2%), (f) Speckle noise (density =1%), (g) Speckle noise (density =5%), (h) Dilatation (5,5), (i) Cropping (1:16), (j) Rotation (90◦), (k) Median Filtering (5,5), (l) Median Filtering (3,3), (m) JPEG Compression (40), (n) JPEG Compression (80), (o) JPEG Compression (80) and Salt & Pepper noise (1%), (p) JPEG Compression (80) and Gaussian noise (1%) . . . 61
3.9 (1) Original watermark, (2) Salt & pepper (density=1%), (3) Salt & pepper (density=5%), (4) Gaussian noise (density =1%), (5) Gaussian noise (density =2%), (6) Speckle noise (density =1%), (7) Speckle noise (density =5%), (8) Dilatation (5,5), (9) Cropping (1:16), (10) Rotation (90◦), (11) Median Filtering (5,5), (12) Median Filtering (3,3), (13) JPEG Compression (40), (14) JPEG Compression (80), (15) JPEG Compression (80) and Salt & Pepper noise (1%), (16) JPEG Compression (80) and Gaussian noise (1%) . . . 62
3.10 Digital watermarking applications . . . 65
3.11 Digital watermarking applications . . . 67

4.1 Discrete Cosine Transform Zig-Zag scan . . . 73
4.2 Discrete Wavelet Transform multilevel resolution . . . 74
4.3 Arnold Chaotic Map scrambling result . . . 77
4.4 Medical host images . . . 79
4.5 (a) Original cover images, (b) Watermarked images . . . 81
4.6 (a) Shuffled watermarked images, (b) Recovered watermarked images . . . 82
4.7 Correlation Coefficients of plain brain medical image . . . 83
4.8 Correlation Coefficients of cipher brain medical image . . . 83
4.9 Correlation Coefficients of plain ankle medical image . . . 84
4.10 Correlation Coefficients of cipher ankle medical image . . . 84
4.11 (a) Original brain image histogram, (b) Watermarked brain image histogram . . . 85
4.12 (a) Original ankle image histogram, (b) Watermarked ankle image histogram . . . 85

List of Tables

1.1 Color spaces pros and cons [Ibraheem et al., 2012] 18

2.1 Spatial domain versus Frequency domain 34

3.1 PSNR (dB) results using various quantization steps 59
3.2 Results of the proposed watermarking scheme without attacks 60
3.3 PSNR and MSE values for the watermarked image under attacks 60
3.4 Findings of the extracted watermark under various types of attacks. 63
3.5 Performance comparison of watermarking techniques in terms of NC and BER under different attack types [Nouioua et al., 2020] 66
3.6 Computational cost comparison [Nouioua et al., 2020] . . . 68

4.1 Medical patient records sample 80
4.2 High fidelity experiments results 81
4.3 Imperceptibility values comparison 81
4.4 Correlation Coefficients results 82
4.5 Hamming Distance 83

Nomenclature

ACM Arnold Chaotic Map

ACR American College of Radiology

BCH Bose Chaudhuri Hocquenghem

BER Bit Error Rate

BPNN Back Propagation Neural Network

CMY Cyan, Magenta, and Yellow

CSF Cyber Security Framework

CT Computed Tomography

CT Contourlet Transform

DC Direct Current

DCT Discrete Cosine Transform

DICOM Digital Imaging and Communications in Medicine

DNST Discrete Non-separable Shearlet transform

DTCWT Dual-Tree Complex Wavelet Transform

DWT Discrete Wavelet Transform

ECC Error Correcting Codes

EPR Electronic Patient Records

HMT Hidden Markov Tree

HSI Hue, Saturation, and Intensity

HVS Human Vision System

IDWT Inverse Discrete Wavelet Transform

ITU − R International Telecommunication Union - Radiocommunication sector

JPEG Joint Photographic Experts Group

LSB Least Significant Bit

LWT Lifting Wavelet Transform

*MD*5 Message Digest 5

MDC Multiple Description Coding

ML Maximum Likelihood

MRI Magnetic Resonance Imaging

NC Normalized Correlation

NEMA National Electrical Manufacturers Association

NIST National Institute of Standards and Technology

NMR Nucleic Magnetic Resonance

NSCT Non-subsampled Contourlet Transform

NTSC National Television Standard Committee

PAL Phase Alternating Line

Pixels Picture elements

PSNR Peak Signal to Noise Ratio

PXEM Parameter-Expanded Expectation-Maximization

RDWT Redundant Discrete Wavelet Transforms

RGB Red, Green, and Blue

SECAM Séquentiel de couleur à mémoire

SNN Spiking Neural Network

SPIHT Set Partitioning in Hierarchical Tree

SSIM Structural Similarity Index Metric

SVD Singular Value Decomposition

T Tesla

US Ultrasound

YCbCr Luminance and Chrominance

Abstract

Watermarking and cryptography, as technologies, have become increasingly important in the digital age for the protection of information and intellectual property. Watermarking involves the embedding of a digital signature or identifying mark into a digital image, audio file, or other types of digital content. This mark can be used to verify the authenticity of the content and detect any tampering or unauthorized use. Cryptography, on the other hand, involves the encoding of information to prevent unauthorized access. By combining watermarking and cryptography, it is possible to create a secure and reliable method for protecting digital content and intellectual property.

In the context of medical images, the use of watermarking and cryptography can be particularly important for ensuring the authenticity and integrity of these images, as well as protecting sensitive medical information. With the growing adoption of telemedicine, which involves the remote exchange of medical images through telecommunications technology, this technology has become increasingly popular as a way to improve access to healthcare, particularly in rural and underserved areas. One of the challenges of telemedicine is the transmission of medical images, such as x-rays or MRI scans, from the patient to the healthcare provider. Digital watermarking can help to ensure the authenticity and integrity of these images, allowing healthcare providers to confidently diagnose and treat patients based on the information contained within the images.

In addition to improving the accuracy of telemedicine services, digital watermarking and cryptography can also help protect the intellectual property rights of the image creators and prevent the unauthorized use or distribution of sensitive medical information. This can be especially im-

portant in the context of telemedicine, where images may be transmitted over long distances and through multiple networks, increasing the risk of unauthorized access.

In brief, the use of digital watermarking technology and cryptography in telemedicine has the potential to provide a number of benefits, including improved image authenticity and integrity, enhanced protection of intellectual property rights, and improved patient care. As the field of telemedicine continues to grow and evolve, it is likely that the role of digital watermarking technology in supporting the delivery of remote medical services will increase.

In this thesis, significant contributions were designed for the application of digital watermarking in telemedicine. The foremost contribution is a blind digital watermarking framework based on the *Dual-Tree Complex Wavelet Transform (DTCWT)* and *the Non-Subsampled Contourlet Transform (NSCT)*. This framework intends to offer a secure and reliable method for protecting the authenticity and integrity of medical images in telemedicine. The second contribution is a medical image watermarking scheme in the transform domain based on *ElGamal* asymmetric crypto-system and the *Arnold Chaotic Map*. This scheme aims to improve the robustness and security of the digital watermarking technique by using a combination of cryptographic and chaotic techniques to encrypt and embed the watermark in medical images. Together, these contributions provide a comprehensive approach to digital watermarking in telemedicine that addresses the challenges of protecting medical images and intellectual property rights while improving the accuracy of telemedicine services.

Keywords: Arnold chaotic system, Authenticity, Cryptography, DCT, DTCWT, Digital watermarking, DWT, ElGamal crypto-system, Information hiding, Intellectual property rights, Medical images, NSCT, Telemedicine, Unauthorized copying.

Résumé

Le tatouage numérique et la cryptographie, en tant que technologies, sont devenus de plus en plus importants à l'ère numérique pour la protection des informations et de la propriété intellectuelle. Le filigrane implique l'intégration d'une signature numérique ou d'une marque d'identification dans une image numérique, un fichier audio ou d'autres types de contenu numérique. Cette marque peut être utilisée pour vérifier l'authenticité du contenu et détecter toute altération ou utilisation non autorisée. La cryptographie, quant à elle, implique le codage des informations pour empêcher tout accès non autorisé. En combinant filigranage et cryptographie, il est possible de créer une méthode sécurisée et fiable pour protéger le contenu numérique et la propriété intellectuelle.

Dans le contexte des images médicales, l'utilisation du filigrane et de la cryptographie peut être particulièrement importante pour garantir l'authenticité et l'intégrité de ces images, ainsi que pour protéger les informations médicales sensibles. Avec l'adoption croissante de la télémédecine, qui implique l'échange à distance d'images médicales grâce à la technologie des télécommunications, cette technologie est devenue de plus en plus populaire comme moyen d'améliorer l'accès aux soins de santé, en particulier dans les zones rurales et mal desservies. L'un des défis de la télémédecine est la transmission d'images médicales, telles que des radiographies ou des IRM, du patient au prestataire de soins. Le filigrane numérique peut aider à garantir l'authenticité et l'intégrité de ces images, permettant aux prestataires de soins de santé de diagnostiquer et de traiter les patients en toute confiance sur la base des informations contenues dans les images.

En plus d'améliorer la précision des services de télémédecine, le filigrane numérique et la cryptographie peuvent également aider à protéger les droits de propriété intellectuelle des créateurs d'images et à empêcher l'utilisation ou la distribution non autorisée d'informations médicales sensibles. Cela peut être particulièrement important dans le contexte de la télémédecine, où les images peuvent être transmises sur de longues dis-

tances et via plusieurs réseaux, ce qui augmente le risque d'accès non autorisé.

En bref, l'utilisation de la technologie de filigrane numérique et de la cryptographie dans la télémédecine peut offrir un certain nombre d'avantages, notamment une authenticité et une intégrité améliorées des images, une protection accrue des droits de propriété intellectuelle et une amélioration des soins aux patients. À mesure que le domaine de la télémédecine continue de croître et d'évoluer, il est probable que le rôle de la technologie de tatouage numérique dans le soutien de la prestation de services médicaux à distance augmentera.

Dans cette thèse, des contributions importantes ont été conçues pour l'application du tatouage numérique en télémédecine. La principale contribution est un cadre de tatouage numérique aveugle basé sur la *Transformée en Ondelettes Complexe à Double Arbre (DTCWT)* et la *Transformée de Contourlet Non Sous-échantillonnée (NSCT)*. Ce cadre vise à offrir une méthode sécurisée et fiable pour protéger l'authenticité et l'intégrité des images médicales en télémédecine. La deuxième contribution est un schéma de tatouage d'image médicale dans le domaine de transformation basé sur le cryptosystème asymétrique *ElGamal* et le *Systeme Chaotique d'Arnold*. Ce schéma vise à améliorer la robustesse et la sécurité de la technique de tatouage numérique en utilisant une combinaison de techniques cryptographiques et chaotiques pour chiffrer et intégrer le filigrane dans les images médicales. Ensemble, ces contributions fournissent une approche globale du tatouage numérique en télémédecine qui répond aux défis de la protection des images médicales et des droits de propriété intellectuelle tout en améliorant la précision des services de télémédecine.

Mots clefs : Système chaotique Arnold, Authenticité, Cryptographie, DCT, DTCWT, Filigrane numérique, DWT, Crypto-système ElGamal, Dissimulation d'informations, Droits de propriété intellectuelle, Images médicales, NSCT, Télémédecine, Copie non autorisée.

الملخص

أصبحت العلامات المائية والتشفير ، كتقنيات ، ذات أهمية متزايدة في العصر الرقمي لحماية المعلومات والملكية الفكرية. تتضمن العلامة المائية تضمين توقيع رقمي أو علامة تعريف في صورة رقمية أو ملف صوتي أو أنواع أخرى من المحتوى الرقمي. يمكن استخدام هذه العلامة للتحقق من أصالة المحتوى واكتشاف أي تلاعب أو استخدام غير مصرح به. من ناحية أخرى ، يتضمن التشفير تشفير المعلومات لمنع الوصول غير المصرح به. من خلال الجمع بين العلامات المائية والتشفير ، من الممكن إنشاء طريقة آمنة وموثوقة لحماية المحتوى الرقمي والملكية الفكرية.

في سياق الصور الطبية ، يمكن أن يكون استخدام العلامات المائية والتشفير مهمًا بشكل خاص لضمان صحة وسلامة هذه الصور ، فضلاً عن حماية المعلومات الطبية الحساسة. مع تزايد الاعتماد على الطب عن بعد ، والذي يتضمن التبادل عن بعد للصور الطبية من خلال تكنولوجيا الاتصالات السلكية واللاسلكية ، أصبحت هذه التكنولوجيا ذات شعبية متزايدة كوسيلة لتحسين الوصول إلى الرعاية الصحية ، لا سيما في المناطق الريفية والمناطق المحرومة من الخدمات. تتمثل إحدى تحديات التطبيب عن بُعد في نقل الصور الطبية ، مثل الأشعة السينية أو فحوصات التصوير بالرنين المغناطيسي ، من المريض إلى مقدم الرعاية الصحية. يمكن أن تساعد العلامات المائية الرقمية في ضمان صحة وسلامة هذه الصور ، مما يسمح لمقدمي الرعاية الصحية بتشخيص وعلاج المرضى بثقة بناءً على المعلومات الواردة في الصور.

بالإضافة إلى تحسين دقة خدمات التطبيب عن بعد ، يمكن أن تساعد العلامات المائية الرقمية والتشفير أيضًا في حماية حقوق الملكية الفكرية لمنشئي الصور ومنع الاستخدام غير المصرح به أو توزيع المعلومات الطبية الحساسة. يمكن أن يكون هذا مهمًا بشكل خاص في سياق التطبيب عن بُعد ، حيث يمكن نقل الصور عبر مسافات طويلة وعبر شبكات متعددة ، مما يزيد من خطر الوصول غير المصرح به.

باختصار ، فإن استخدام تقنية العلامات المائية الرقمية والتشفير في الطب عن بعد لديه القدرة على توفير عدد من الفوائد ، بما في ذلك تحسين موثوقية الصورة وسلامتها ، وتعزيز حماية حقوق الملكية الفكرية ، وتحسين رعاية المرضى. مع استمرار نمو مجال الطب عن بعد وتطوره ، من المحتمل أن يزداد دور تقنية العلامات المائية الرقمية في دعم تقديم الخدمات الطبية عن بُعد.

في هذه الأطروحة ، تم تصميم مساهمات كبيرة لتطبيق العلامات المائية الرقمية في الطب عن بعد. المساهمة الرئيسية هي إطار عمل للعلامات المائية الرقمية العمياء يعتمد على *DTCWT* و *NSCT* . يهدف هذا الإطار إلى تقديم طريقة آمنة وموثوقة لحماية أصالة وسلامة الصور الطبية في التطبيب عن بُعد. المساهمة الثانية هي مخطط العلامات المائية للصور الطبية في مجال التحويل بناءً على نظام تشفير غير متماثل ونظام *Arnold* الفوضوي. يهدف هذا المخطط إلى تحسين متانة وأمن تقنية العلامة المائية الرقمية باستخدام مزيج من تقنيات التشفير والفوضى لتشفير العلامة المائية وتضمينها في الصور الطبية. توفر هذه المساهمات معًا نهجًا شاملاً للعلامات المائية الرقمية في الطب عن بُعد والتي تتصدى لتحديات حماية الصور الطبية وحقوق الملكية الفكرية مع تحسين دقة خدمات التطبيب عن بُعد.

الكلمات الدلالية : نظام *Arnold* الفوضوي ، الأصالة ، التشفير ، *DCT* ، *DTCWT* ، العلامات المائية الرقمية ، *DWT* ، نظام التشفير *ElGamal* ، إخفاء المعلومات ، حقوق الملكية الفكرية ، الصور الطبية ، *NSCT* ، التطبيب عن بعد ، النسخ غير المصرح به.

Introduction 0

0.1 Motivation

The widespread use of broadband technologies, particularly the internet, has revolutionized how humans communicate, share knowledge, and make decisions. With more than 3 billion individuals currently connected, the internet has created new opportunities in various fields, including business, education, and health. However, it has also led to the prevalence of cybercrime, where hackers can access sensitive data from unsuspecting users.

This has led to the prevalence of cybercrime, where hackers can abduct sensitive data from unsuspecting users. Information security is a crucial topic that has been addressed by various organizations and agencies. The *National Institute of Standards and Technology (NIST)*, for instance, developed the *Cybersecurity Framework (CSF)* as a way to address this issue. It provides cybersecurity professionals with a set of standards and best practices that can be utilized to protect information and systems from threats. As images and videos become more prevalent, hackers have been able to gain access to sensitive data. This has led to the emergence of digital watermarking technology and cryptography, which were designed to protect images and videos from unauthorized use. Digital watermarking and cryptography are also used by organizations that need to ensure the integrity of their data.

Since medical images are extremely sensitive and can be misused to the detriment of patients, medical organizations have taken steps to protect them. Furthermore, medical images are a valuable asset in telemedicine,

which is a form of telecommunication that uses video conferencing and other technologies to enable patients to connect with doctors or other health professionals remotely. It enables patients who live in remote areas where there are no physicians or hospitals to receive medical care from experts at other locations.

The process of digital watermarking is used by security professionals as a way to add hidden information to an image or video file to track its use and protect it from being copied or altered. On the other hand, cryptography is the practice of securing communication by encoding messages to prevent unauthorized access. It involves the use of mathematical algorithms and protocols to convert plaintext, or unencrypted information, into ciphertext, or encrypted information, and vice versa. This thesis discusses the process of digital watermarking and cryptography, including novel techniques for digital watermarking and cryptography for telemedicine applications.

0.2 Research Objectives

Medical images are very sensitive images that require delicacy in handling since any processing performed on them should not make changes that may adversely affect the usefulness of these images, which may result in dangerous consequences. The safety of these medical photos can be ensured by adding a watermark to them. However, the sensitive nature of these images means that several rules are much stricter than those that apply to images that are not medical. Given the relationship between imperceptibility and insertion capacity, a high degree of imperceptibility reduces the possible insertion capacity, which can also reduce the effectiveness of the tattoo. However, it is necessary to have a high degree of imperceptibility so as not to cause interference between the inserted mark and the important information of the medical image. The issue of imperceptibility has been resolved thanks to the development of reversible watermarking technologies, sometimes referred to as "watermarking without losses." This sort of watermarking makes it possible to discover an identical replica of

the original picture after the mark has been removed from the host image. However, reversible methods have two major drawbacks: the security problem, which occurs because the image loses its protection as soon as the mark is extracted, and the capacity problem, which occurs because reversible methods provide a small insertion capacity, which is even considered to be lower than those of non-reversible methods. Both of these drawbacks make reversible methods less desirable than non-reversible methods. The goal of this study is not to discover a strategy that can solve all of the issues that have been brought up, but rather to make significant and original improvements to methods that have already been developed.

According to the aims, the objective of this thesis is to make use of approaches to overcome the constraints of conventional ways while still satisfying the same demands as the latter. Advocating for the use of approaches for watermarking that are founded on the idea of blind watermarking. These watermarking techniques involve embedding identifying information into an image in a way that is imperceptible to the human eye. This makes it difficult for unauthorized individuals to detect or remove the watermark. Where it is expected that the degree of imperceptibility would be maintained in this scenario, however, the capacity for insertion will no longer be dependent on the degree of imperceptibility. This sort of watermarking approach is particularly beneficial for protecting sensitive photographs, especially medical images. Because of this, it is very useful for protecting medical images.

0.3 Research Questions

- The first question arises, What is digital image watermarking? In simple terms, digital image watermarking is the process of adding a visible or invisible mark to an image to claim ownership or protect copyrights.
- What are the different types of digital image watermarking techniques? Digital watermarking techniques include visible, invisible, robust, fragile, blind, and semi-blind. Visible watermarks are visible

on the image and are often used for copyright protection or branding. Invisible watermarks are not visible to the naked eye but can be detected with specialized software. Robust watermarks are resistant to tampering, while fragile watermarks can be easily detected but are also easily destroyed. Blind watermarks do not require a reference image to be detected, while semi-blind watermarks do.

- Why is there even a need for digital image watermarking? The answer is quite obvious, security enhancement, copyright protection, and covert communication.

- What are the drawbacks of digital image watermarking? The deficiencies of digital image watermarking include increased file size, reduced image quality, susceptibility to attacks, and limited capacity. Watermarking an image typically involves adding additional data, which can increase the file size and potentially degrade the image quality. Watermarked images are also often targeted by attackers who try to remove or alter the watermark, and some watermarking methods have limited capacity for data.

- How can digital image watermarking be implemented? Digital image watermarking can be implemented using methods such as the spatial domain technique, the frequency domain method, or a hybrid scheme. The specific method chosen will depend on the requirements and constraints of the application. These methods involve embedding the watermark directly into the pixel values or frequency coefficients of the image, using non-linear functions, spreading the watermark across a wide frequency range, or a combination of these techniques.

- What is cryptography? Cryptography is the science of keeping information secret and safe. It involves the use of codes and ciphers to protect information from being understood by anyone who is not authorized to access it.

- Is there many types of cryptography? There are many types of cryptography, including symmetric-key cryptography, asymmetric-key

cryptography, hash functions, digital signatures, and steganography. Cryptography is used to protect a wide range of information, including emails, text messages, and financial transactions.

- Why is it crucial to secure medical images? Securing medical images is crucial since they contain sensitive personal and medical information that must be protected from unauthorized access, modification, or disclosure. This is especially important in the context of telemedicine, where medical images are transmitted and stored electronically.

- What is Telemedicine? Telemedicine is the use of electronic communication and information technologies to provide clinical health care from a distance.

0.4 Research Outcome

- Nouioua, N., Seddiki, A., Ghaz, A. (2020). Blind digital watermarking framework based on DTCWT and NSCT for telemedicine application. Traitement du Signal, Vol. 37, No. 6, pp. 955-964. https://doi.org/10.18280/ts.370608.

- N. Nadhir, S. Ali and G. Abdelkrim, "Medical Image Watermarking Scheme in Transform Domain based on Asymmetric crypto-system and Arnold Chaotic Map," 2021 44th IEEE International Conference on Telecommunications and Signal Processing (TSP), 2021, pp. 267-272, https://doi.org/10.1109/TSP52935.2021.9522620.

- Nouioua, N., Seddiki, A., Ghaz, " Joint Watermarking-Encryption Scheme Utilizing Transform Domain and Advanced Encryption Standard," 2022 2nd IEEE International Conference on Electrical, Computer and Energy Technologies (ICECET), 2022, https://doi.org/10.1109/ICECET55527.2022.9873045.

- Nouioua, N., Seddiki, A., Ghaz, "Blind Digital Watermarking Method Based on Quadtree Decomposition and Complex Wavelet Transform

for Medical Application," 2022 2nd IEEE International Conference on Electrical, Computer and Energy Technologies (ICECET), 2022, https://doi.org/10.1109/ICECET55527.2022.9873503.

- A., Ghaz, Seddıkı, A., Nouıoua, N. Comparative study of encryption algorithms applied to the IOT.The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2022, 21, 469-476, https://doi.org/10.55549/epstem.1226679

- A., Ghaz, Nouioua, N., Seddiki, A. (2022). Biometric Fingerprint Security Enhancement Utilizing Watermarking and Cipher Block Chaining. Submitted to Traitement du Signal.

0.5 Thesis Outline

The outline of this thesis is described as follows:

- Chapter 1 describes the detailed theory of digital watermarking, along with basic concepts of cryptography, also it contains a detailed literature review on digital image watermarking algorithms

- Chapter 2 Demonstrate digital watermarking from A to Z, highlighting the key pillars of this technology in terms of requirements, categorization, and application fields.

- Chapter 3 addresses a blind watermarking algorithm for medical images based on dual-tree complex wavelet transform.

- Chapter 4 of this thesis presents an approach for medical image security based on watermarking, asymmetric cryptography and chaotic maps.

- Chapter 5 conclude the thesis and provide future research scopes.

Recap on digital image

1

Contents

1.1 Introduction . . . 8
1.2 What is a digital image . . . 9
1.3 Binary, grayscale and color images . . . 9
1.3.1 Binary images . . . 9
1.3.2 Gray levels images . . . 9
1.3.3 color images . . . 10
1.4 Color spaces . . . 11
1.4.1 RGB color space . . . 11
1.4.2 YCbCr color space . . . 12
1.4.3 CMYK color space . . . 13
1.4.4 HSI color space . . . 14
1.4.5 YIQ color space . . . 16
1.5 Biomedical imaging . . . 16
1.5.1 X-ray Radiography . . . 17
1.5.2 Ultrasound . . . 17
1.5.3 Computed tomography . . . 19
1.5.4 Magnetic Resonance Imaging . . . 21
1.6 Telemedicine . . . 22
Conclusion . . . 22

Through this chapter, a brief overview about digital image, and its segmentation depending on colors was provided. Further, a sight on biomedical imaging, and telemedicine was also behold.

1.1 Introduction

"A picture is worth a thousand words." — Anonymous.

Today, humanity stands in a digital era, where digitalization is as necessary as the rest of the requirements of daily life. Through time, the Pharaonic civilization is a witness to the strength of images in information and history transmission. The migration from analog to digital imaging had led to a colossal advancement in several disciplines [Aubert and Kornprobst, 2006], specifically in medicine, where the image decreased medical errors, and increased medical interventions quality by facilitating diseases diagnosis, which yields prompt efficient treatment processes.

"Image" as a concept is about the materialization of physical objects visualized by the human eye. Moreover, a digital image can be plainly defined as a matrix with specific values organized in rows and columns, as presented in Figure 1.1 [Aber et al., 2019].

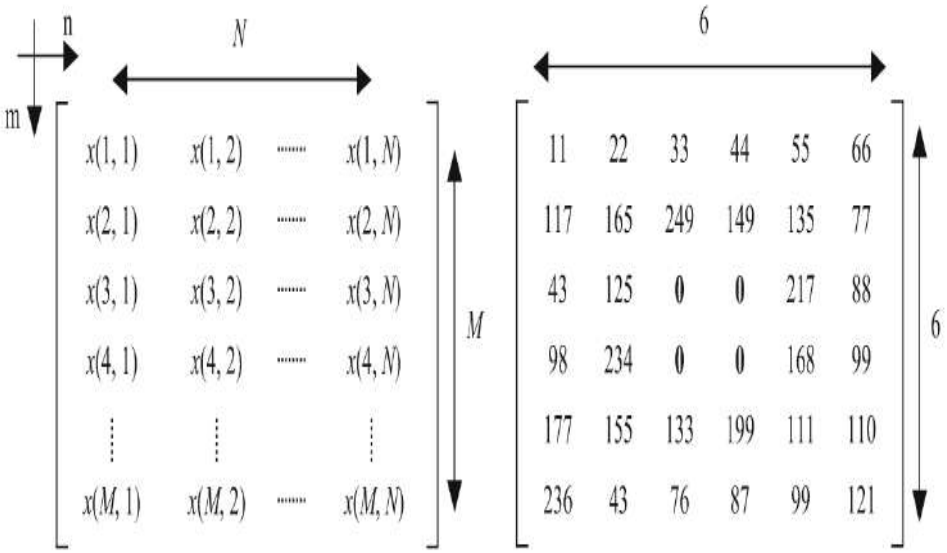


Figure 1.1 – *Two-dimensional* $(m \times n)$ *digital image matrix representation [Tomasz, 2021]*

The structure of this chapter is organized as follows: Sec. 1.2 presents the digital image. Sec. 1.3 elucidates the different digital image classes. Color spaces were examined in Sec. 1.4. Sec. 1.5 has been devoted to imaging in medicine. In this latter section, an overview of telemedicine was noted in Section 1.6.

1.2 What is a digital image

Mathematically, $f(x,y)$, is the determining function of an image, while x and y represent the spatial coordinates. The amplitude at any point on the x,y grid is known as the intensity. Thus, an image is referred to as a "digital image" if the coordinates and intensities are finite and discrete [Gonzalez and Woods, 2008]. *Pixels* or picture elements is the constructing component of the digital image (see Figure 1.2).

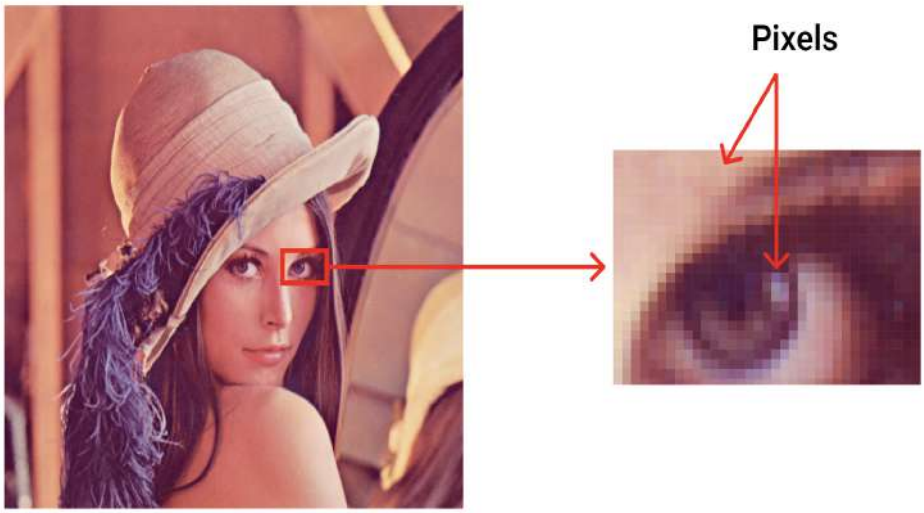


Figure 1.2 – *Zoom in Lena pixels*

1.3 Binary, grayscale and color images

1.3.1 Binary images

If pixels of an image can take only black or white values, represented with 0's and 1's, then the image in your hands is called a "binary image" [Feng et al., 2015] [Feng et al., 2017], further, binary images show extreme sensitivity to noise [Chen et al., 2018]. Figure 1.3 illustrates an example of a binary image.

1.3.2 Gray levels images

Broadly, and as its name indicates, a gray-level image (also known as a grayscale image) is composed of 256 shadows of gray (i.e., 2^8) for an 8-bit system). Thus, if the gray levels were presented on a histogram, the



Figure 1.3 – *Lena binary image*

horizontal axis would be stretched from 0 to 255 [Baidoo, 2018]. Figure 1.4 depicts a grayscale image.



Figure 1.4 – *Lena grayscale image*

1.3.3 color images

Thanks to digital color imaging, nowadays, human eye captures are easily reproduced [Plataniotis and Venetsanopoulos, 2011]. Differently from the previously described gray levels imaging concept where a proper intensity (gray shadow) is attached to each pixel, color images utilize the

trichromatic theory of color, where each pixel is defined by three values, representing the red, green, and blue colors [Paulsen and Moeslund, 2020],



Figure 1.5 – *Lena color image*

1.4 Color spaces

1.4.1 RGB color space

Red, green, and blue represent the forming elements of the RGB color space (i.e., various components are merged together to generate the desired color), represented using a three-dimensional model. It was first introduced in *Maxwell* [1] works [Maxwell, 1857] [Maxwell, 1860]. In a 3D Cartesian coordinate system (see Figure 1.6), the tristimulus values representing the color pixel presented in equation 1.1 can be pictured by a single dot, [Paulsen and Moeslund, 2020]. The RGB color standard matches nicely with the real physical equipment used to generate colors with computers, such as TV displays, which have red, green, and blue phosphors [Ledley et al., 1990].

$$\text{Color pixel} = [\text{ Red, Green, Blue }] = [R, G, B] \tag{1.1}$$

The inconvenience of the RGB color space is the requirement for equal

[1] James Clerk Maxwell (13 June 1831 - 5 November 1879) a Scottish mathematician

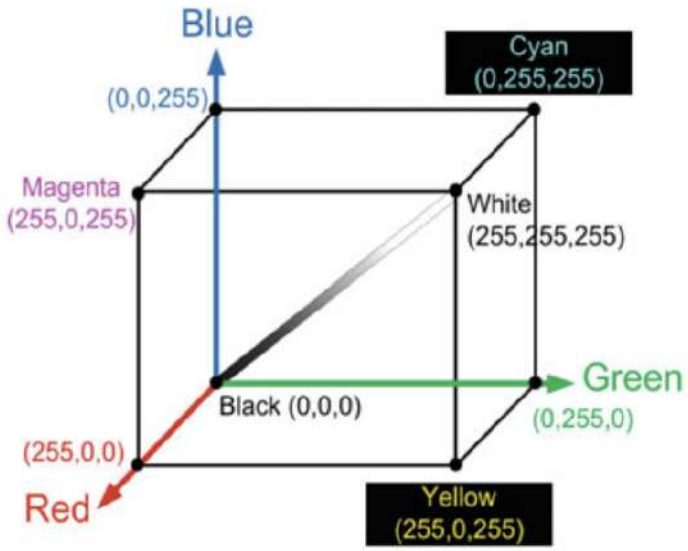


Figure 1.6 – *The RGB color cube [Paulsen and Moeslund, 2020]*

bandwidths to represent the three components, which indicates that each color component has the same pixel depth and display resolution. The human vision system (HVS), on the other hand, is more sensitive to green light and less sensitive to red and blue light [Lukac and Plataniotis, 2007]. Figure 1.7 illustrates divided RGB image components.



Figure 1.7 – *Peppers RGB image (from left to right: Red (R), Green (G) and Blue (B))*

1.4.2 YCbCr color space

In YCbCr color space, or *ITU-R (International Telecommunication Union - Radiocommunication sector) Recommendation BT.601*, abbreviated with *Rec. 601*, which is oriented to encode interlaced analog video signals in digital video [ITU, 2011] (i.e., DVD and blue-ray discs). In this standard, three essential

elements represent colors: luminance, denoted "Y", and chrominance "Cb, Cr" (see Figure 1.8). As extra information, luminance perceived by human vision is superior to chrominance [Alahmadi et al., 2013]. Starting from the nonlinear RGB color space, YCbCr formula 1.2 is determined as follows:

$$\begin{pmatrix} Y \\ Cb \\ Cr \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.177 \\ -0.299 & -0.587 & 0.886 \\ 0.701 & -0.587 & -0.114 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix} + \begin{pmatrix} 16 \\ 128 \\ 128 \end{pmatrix} \quad (1.2)$$

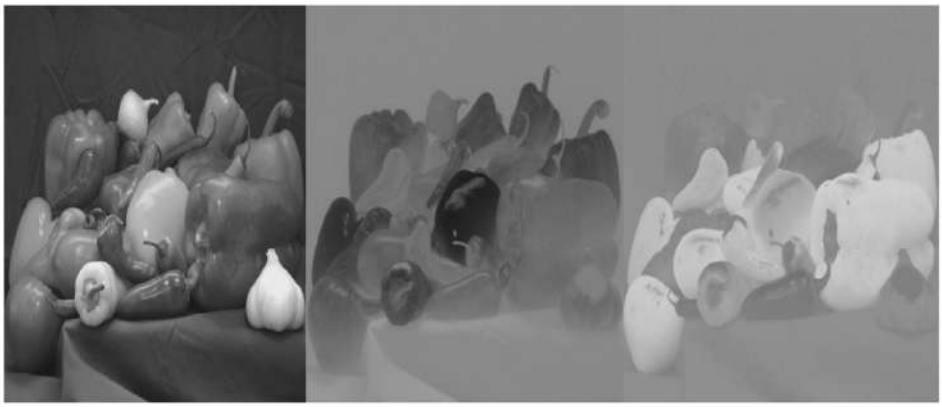


Figure 1.8 – *Peppers image converted from RGB to YCbCr color space (from left to right: Luminance "Y", and chrominance "Cb, Cr")*

1.4.3 CMYK color space



Figure 1.9 – *Peppers image converted from RGB to CMY color space (from left to right: Cyan "C", Magenta "M" and Yellow "Y"*

Cyan, magenta, and yellow are the three elementary pigment colors of the CMY color model (see Figure 1.9) [Gonzalez and Woods, 2008], CMY

model is a ubiquitous system for printing. Printing black by combining cyan, yellow, and magenta pigments, on the other hand, has significant drawbacks. Colored ink is costly, and printing three ink layers might cause the printed paper to become overly moist, and since black is such an essential and popular color in printing, CMYK systems frequently include a fourth ink "K" to have a real black color [Chen, 2012]. The CMY model is mathematically presented by the following equation 1.3:

$$\begin{pmatrix} C \\ M \\ Y \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} R \\ G \\ B \end{pmatrix} \tag{1.3}$$

1.4.4 HSI color space

In the 1970s, *computer graphics* [2] scientists created a new color space to better correlate with how the human eye perceives colors, HSI was the designed model, which is short for hue, saturation, and intensity. As elucidated in Figure 1.10 The hue "H" is determined by the angle around the vertical axis and ranges from 0 to 360 degrees. It is often represented by an angle on a color wheel, with red at 0 degrees, green at 120 degrees, and blue at 240 degrees. The saturation "S" is a ratio that starts at 0 (on the I-axis) and increases radially to a maximum value of 1 on the cone's surface. While, intensity "I" represents the brightness of a color, and how much light is reflected. It is often represented as a value between 0 (black) and 1 (white). Whereas the equations 1.4, 1.5, 1.6, and 1.7 give the mathematical explication of each component, an example of HSI conversion is presented in Figure 1.11. A recapitulation of the mentioned color spaces, plus advantages and disadvantages, is marked in the Table 1.1.

$$H = \begin{cases} \theta & \text{if } B \leq G \\ 360 - \theta & \text{if } B > G \end{cases} \tag{1.4}$$

$$\theta = \cos^{-1}\left\{ \frac{\frac{1}{2}[(R-G)+(R-B)]}{[(R-G)^2+(R-B)(G-B)]^{1/2}} \right\} \tag{1.5}$$

[2] Computer graphics is the process of creating visuals with the use of computers

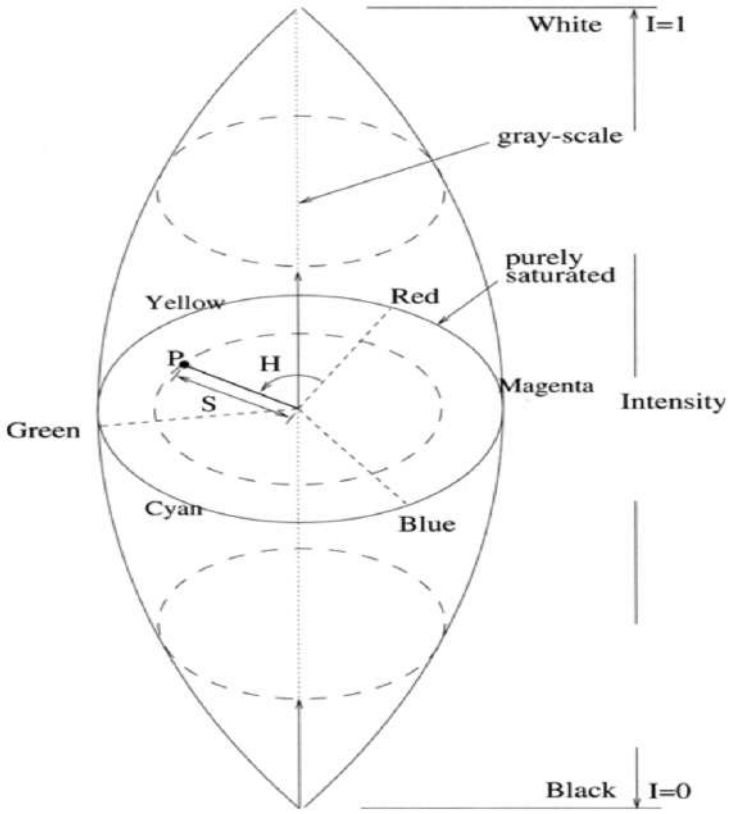


Figure 1.10 – *The HSI color model depiction [Plataniotis and Venetsanopoulos, 2011]*

$$S = 1 - \frac{3}{(R+G+B)}[\min(R,G,B)] \tag{1.6}$$

$$I = \frac{1}{3}(R+G+B) \tag{1.7}$$



Figure 1.11 – *Peppers image converted from RGB to HSI color space (from left to right: Hue (Y), Saturation (S) and Intensity (I))*

1.4.5 YIQ color space

The YIQ color space is a color model used in color television systems. It separates the luminance "Y" component from the chrominance "I and Q" components of a color signal. The "Y" component represents the brightness of a color, while the "I" and "Q" components represent the chromaticity, hue, and saturation.

The mathematical equation 1.8 depicts the conversion process between the RGB and YIQ color spaces as follows:

$$\begin{pmatrix} Y \\ I \\ Q \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.274 & -0.322 \\ 0.211 & -0.523 & 0.312 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix} \tag{1.8}$$

The YIQ color space is used in the national television system committee (NTSC) color television system, which is used in the United States and Japan. It is also used in the phase alternating line (PAL) and SECAM (Séquentiel de couleur à mémoire) [3]), which are used in Europe and other parts of the world.

1.5 Biomedical imaging

The process of creating an understandable visual representation of medical data is known as medical imaging. Patients' diseases are more effectively diagnosed when they are assisted by medical structural images. In a broad sense, medical imaging refers to all methods of storing and processing data. The digital imaging and communications in medicine (DICOM), the fruit of a collaboration between the american college of radiology (ACR) and the national electrical manufacturers association (NEMA) [Best et al., 1992], is a standard developed for the computer handling of biomedical imaging data [Maitine, 2015], for information storage and exchange in the health care sector [Baljon et al., 1996]. Among the structural imaging methods, the most commonly used in medicine are:

- X-ray Radiography

[3] French translation of Color Sequential with Memory Systems

- Ultrasound (US)
- Computed tomography (CT)
- Magnetic Resonance Imaging (MRI)

1.5.1 X-ray Radiography

X-rays are electromagnetic waves with wavelengths that are longer than the visible spectrum. Electromagnetic radiation has wave-like properties, propagating as clusters of energy called photons with a definite wavelength. Discordantly to acoustic waves or other, electromagnetic waves works without the need of any carrier [Toennies, 2012]. With a speed of light and wavelength in the range of 0.01 to 15 nm, as depicted in Figure 1.12, X-rays move in straight paths, avoiding diffraction and reflection outcomes [Szabo, 2014]. The main principle of radiation generation is the deceleration of rapid electrons penetrating a solid metal anode.

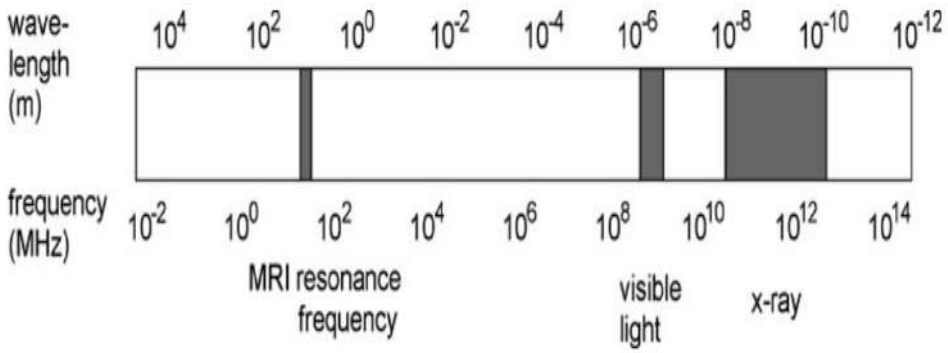


Figure 1.12 – *The spectrum of diagnostic X-ray is above the spectrum of visible light []*

In medicine, body tissues absorb X-rays (a quantity of X-ray energy gets attenuated by the body), providing as a result relevant images used in medical diagnostics (see Figure 1.13).

1.5.2 Ultrasound

Far from X-rays, ultrasound imaging (also known as Sonography), transmits a single wave into the body with a specified direction [Toennies, 2012]. When these propagating longitudinal sound waves are emitted by the transducer and strike a boundary between tissues (e.g., soft tissue

Table 1.1 – *Color spaces pros and cons [Ibraheem et al., 2012]*

Color space	Components	Advantages	Disadvantages
RGB	Red, Green, Blue	(1) Because of its nature, the border is not constrained, and color differences are regular	(1) Highly interpolated causes erroneous. (2) Not suitable for some applications
YCbCr	Y Luminance, (Cb and Cr) are chrominance blue difference, and red difference	(1) Perfect in image compression (2) Used in saving images as a file format for image (3) Y luminance can be use separately for storage in high resolution and the chromaticity components treated separately to improve the performance	(1) The color range is restricted in the color TV images because of the information compression required for the displayed image (2) The displayed color depends on the primaries RGB that displayed the signal
CMY	Cyan, Magenta, yellow	(1) Commonly used for production printer color	(1) Since it is a subtractive model, the components are pigments or inks not colors
HSI	Hue, Saturation, Intensity	(1) Preferable for users view since the components are correlated better with human perception of color (2) The chrominance components (H and S) are associated with the way humans perceive, it became perfect for image processing applications (3) The (Hue) component can be used for performing segmentation process rather than the three components which fasts the algorithm (4) Separate the chromatic from achromatic values	(1) Undefined achromatic hue points are sensitive to value deviations of RGB and instability of hue, because of the angular nature of the feature (2) Does not supply with insight for color manipulation (3) Not uniform



Figure 1.13 – *Thorax X-ray [Med, 2022]*

and bone), the transducer receives back a certain amount of energy as an echo, where it can be translated into an interpretative image [Guzman and Brienza, 2020].

The exploited frequency in ultrasound imaging is typically between 2.5 and 10 MHz, which is much above the range audible to humans and is thus referred to as "ultrasound." Sonography is ubiquitous in medical practice, as it is able to image full body parts (examples of ultrasound imaging are shown in Figure 1.14), except if the organ is covered by a bone, where the projected waves will be totally reflected.

In cardiac diagnosis, ultrasound plays a crucial role through the mechanism termed echocardiography, where the doppler effect allows calculating the velocity within the heart. The foundation of this concept is that the transmitted and received wave frequencies vary as the acoustic source moves closer or further away from the observer [Cikes et al., 2019].

1.5.3 Computed tomography

Computed tomography, where tomography derives from the Greek word *tomein* which means cutting or slicing, represents an essential imaging tool in clinical practice, for the purpose of discriminating tissues and structures. The X-ray scanner is based on *Radon's* [4] theorem (1917), which specifies how to rebuild the two-dimensional geometry of an object from a

[4]Johann Karl August Radon (16 December 1887 – 25 May 1956) an Austrian mathematician

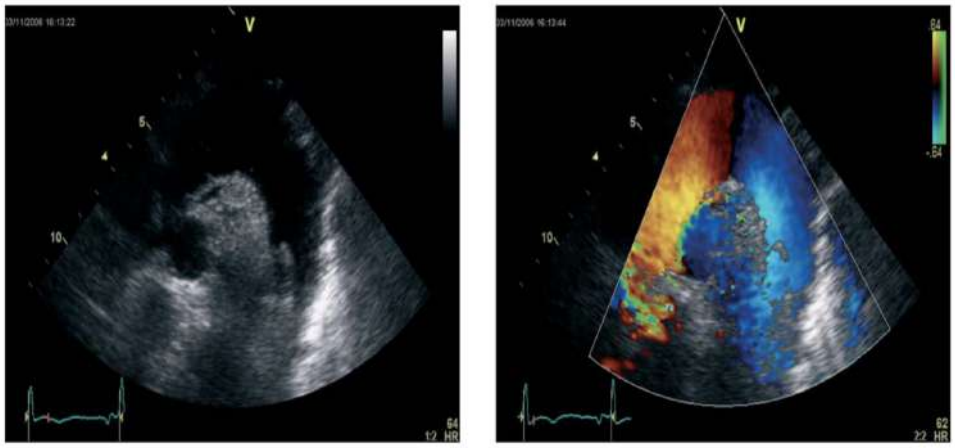


Figure 1.14 – *On the right a cardiac ultrasound image, on the left a cardiac ultrasound image with color Doppler flow [de Leeuw et al., 2007]*

sequence of projections recorded all around it, underpinning the notion of X-ray tomography. This approach could be extended to reconstructing an object's interior tomography based on how rays traveling through it are absorbed according to their angles of penetration, allowing the slicing of the investigated organ. Each pixel in the image is given a gray level value proportionate to the X-ray absorption by the associated body volume [Maitine, 2015].

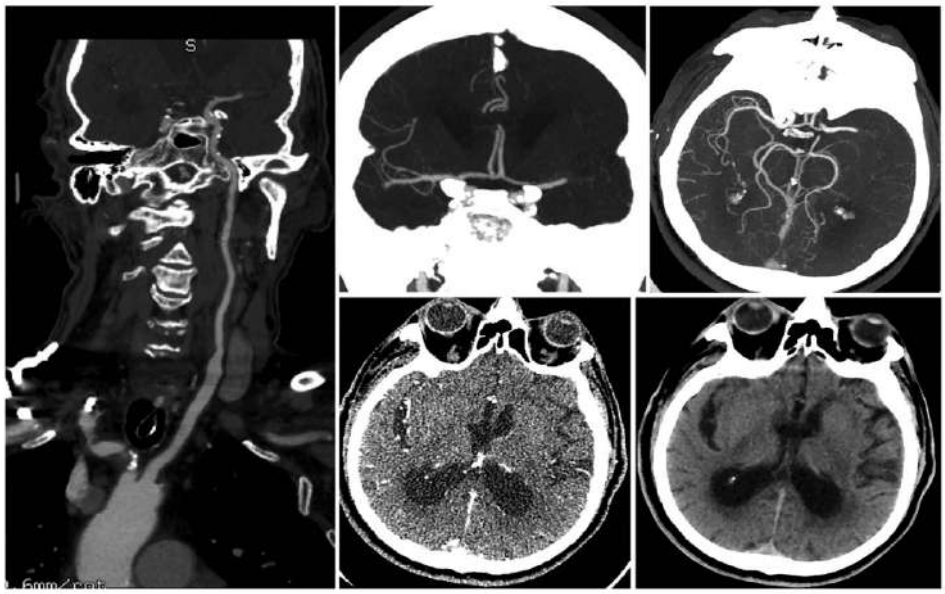


Figure 1.15 – *Computed tomography (CT) scans [Kamalian et al., 2016]*

1.5.4 Magnetic Resonance Imaging

MRI is nucleic magnetic resonance (NMR) based for medical imaging purposes, which states that in the presence of a high magnetic field, hydrogen nuclei receive radio frequency pulses from the resonator and get activated [Dale et al., 2015], based on the magnetic property of hydrogen nuclei, found in water and fats in the body. Thus, if the nucleus is subjected to a static external field, the spin axis of each proton attempts to align with the applied field as a consequence [Symonds, 1992], afterward, a scanner detects the released energy from rotated hydrogen nuclei protons. In order to reconstruct an intelligible image, where typical magnetic field strengths in MRI are 0.08T to 2T, where T (Tesla) represents the measurement unit [Weinreb and Redman, 1987], image resolution and quality can be increased by using higher field strengths [Bangerter et al., 2020]. Currently, MRI medical imaging (see Figure 1.16) is considered the safest imaging method, owing to the fact that it does not utilize radioactive or ionizing radiation, furthermore, no harmful effects on health have been recorded due to its usage.

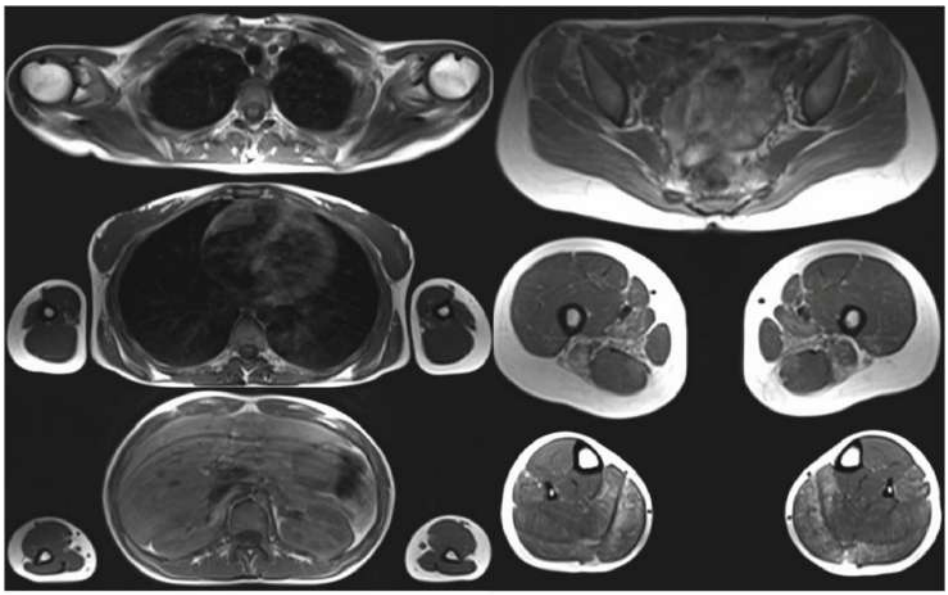


Figure 1.16 – *Magnetic Resonance Imaging (MRI) scans [Wattjes and Fischer, 2013]*

1.6 Telemedicine

Telemedicine [Kirch, 2008], is about the application of telecommunication media such as image, video, and sound for health care services, furthermore, telemedicine is the umbrella term for many modalities like teleradiology, telepathology, teledermatology, and tele-emergency [Gogia, 2020]. In short, telemedicine allows healthcare professionals to provide remote clinical services by using information technologies [Weinstein et al., 2014]. As a solution, telemedicine is particularly beneficial for suburban patients, where it saves time and traveling expenditure [Taylor-Gjevre et al., 2017], as well as in limited capacities urban areas. Due to the tremendous technological achievements, telemedicine is expected to gain more acceptability and usage by individuals [Krusche, 2022], especially after proving its worthiness during the *SARS-CoV2* pandemic by mitigating infection risks [Payán et al., 2022].

Conclusion

With the overwhelming availability of high-tech devices, digital images have paramount importance to humans, where rapid development is experienced with the integration of modern image processing techniques in recent years, where the discipline of image processing enabled more precise and efficient image processing approaches.

In this chapter, an overview of the digital image, which has a vital utility in humans' day-to-day lives, color model classifications were discussed to determine and expose the difference and application field for each model, a zoom on medical imaging techniques and their critical role in diagnosis where digital images are of essential importance vis-à-vis the medical field since imaging mechanisms such as X-rays, CT scans, and MRI scans helped to diagnose and treat a broad spectrum of medical disorders. Furthermore, the adoption of telemedicine has exploded in recent years. This tendency has been intensified by the *COVID-19* epidemic, as more healthcare institutions and individuals resort to telemedicine to deliver and receive medical treatment remotely. Telemedicine enables remote

consultations, monitoring, and diagnostics, which may be particularly advantageous for patients in rural locations or with mobility limitations.

From entertainment and art to medicine and technology, digital images play a vital role in contemporary civilization. With the continuous development of image processing technology and the expanding use of telemedicine, the significance of digital images will only rise in the coming years.

Digital watermarking & cryptography

2

Contents

2.1 Introduction . . . 26
2.2 ABC's of watermarking . . . 27
2.3 Requirements of digital watermarking . . . 29
2.3.1 Imperceptibility . . . 29
2.3.2 Robustness . . . 30
2.3.3 Data payload . . . 31
2.3.4 Security . . . 32
2.3.5 Computational complexity . . . 32
2.4 Digital watermarking classifications . . . 32
2.4.1 Working domain . . . 32
2.4.2 Type of document . . . 33
2.4.3 Human perception . . . 34
2.4.4 Reversibility . . . 35
2.5 Watermarking Attacks . . . 35
2.5.1 Active attacks . . . 35
2.5.2 Passive attacks . . . 36
2.5.3 Forgery attacks . . . 36
2.5.4 Collusion attacks . . . 37
2.6 Fields of application . . . 37
2.7 Performances metrics . . . 40
2.8 Cryptography . . . 42

2.8.1 Symmetric key encryption 43
2.8.2 Public key encryption 44
2.8.3 Chaos based cryptography 44
Conclusion 45

In this chapter, the main branches of digital image watermarking and all the essential elements forming this science were discussed, starting from the outset ending with the current achievements.

2.1 Introduction

Since the dawn of history, security has been a crucial topic for human beings. In the primitive ages, our ancestors used their instinctive behavior to protect their treasures using hand-crafted weapons, and it was the first protection system ever made. Throughout time, human evolution has changed treasured notions and even defense systems.

The 0's and 1's era made academia, and industry researchers above a new challenge of protecting data from piracy, and maleficent use. Due to the illegitimate exploitation of digital information worldwide, resulting from the growth of telecommunications technologies, digital watermarking was adopted as a potential solution to protect copyrights and intellectual property [Rana et al., 2017]. The shared contents via the web can be in the form of multimedia (image, video, audio...), documents, or else. The core idea of digital watermarking is about concealing proprietary information within a support [Abdulla and Navas, 2020], without degrading this last quality (e.g. image), to ensure the prevention of susceptible contents from unauthorized manipulations for security reasons (e.g., copyright, integrity, non-repudiation...).

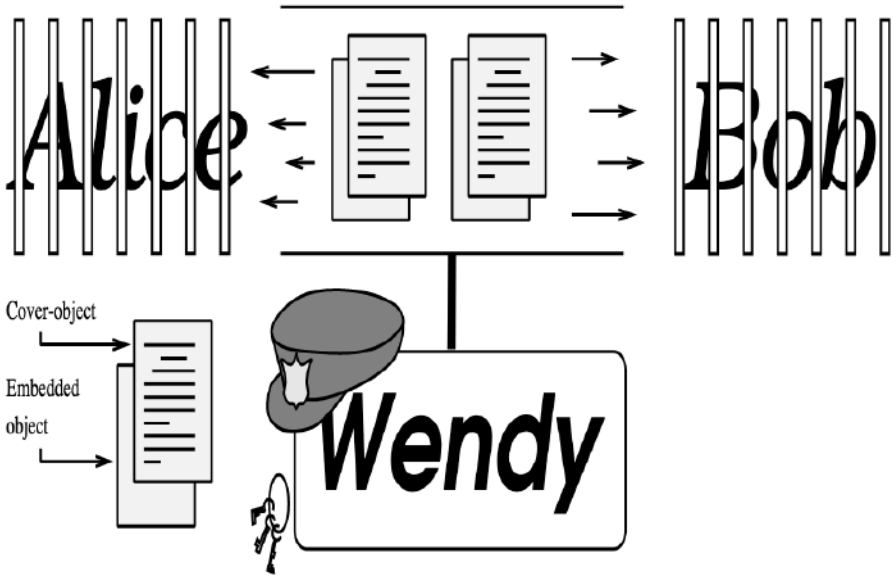


Figure 2.1 – *The prisoners' problem [Craver, 1997].*

The watermarking was derived from steganography [Nouioua et al., 2020]. Linguistically speaking, *stenography* is a Greek term composed of

two parts: *stegano* which means hiding, and *graphy* which means drawing or writing, where this method is the art of camouflaging a secret message within material support.

In 1984, *Simmons* [1] introduced the prisoners' problem, Figure 2.1, that clearly defines the steganography concept, which is about a subliminal channel between prisoners based on the camouflage of secret data [Singh et al., 2017]. In this communication model, prisoners Alice and Bob have to securely correspond without attracting the attention of Wendy, the guardian. On this basis, prisoners agreed on a method that hides a secret message in a cover object.

The rest of the chapter is organized as follows: The basic mechanisms of digital watermarking are provided in Sect. 2.2. Section 2.3 provides the main requirements of digital watermarking. Details about watermarking classification, watermarking attacks, and fields of application are depicted in Sections 2.4, 2.5, and 2.6, respectively. Sec. 2.7 is dedicated to digital watermarking benchmarking metrics. Next, a brief review of cryptography is presented in Section 2.8.

2.2 ABC's of watermarking

As mentioned before, digital watermarking is a method used to implant concealed digital information such as text, images, or audio into digital assets such as photographs and videos. Watermarks are commonly not visible, but they may be detected and extracted by specifically designed software and hardware. The watermarking procedure is based on two essential parts, The embedding phase, which is about incorporating a secret message within the support, where the inserted information must not evoke any degradation in perceptual quality, is followed by the extraction phase, which consists of extrapolating the hiding message from the host medium [Tefas et al., 2009]. The Figure 2.2 and Figure 2.3 depict the elementary steps of watermark embedding and extraction. Mathematically

[1] Gustavus J. Simmons (born 1930) a cryptographer and former manager of the applied mathematics Department and Senior Fellow at Sandia National Laboratories

speaking, the embedding and extraction procedures can be modeled using the formulas 2.1 and 2.2.

Embedding phase

$$I_W = E(I, W) \tag{2.1}$$

In the case of image watermarking, "I_W" is the watermarked image, "I" represents the original image, W denotes the watermark, and "E" the embedding function.

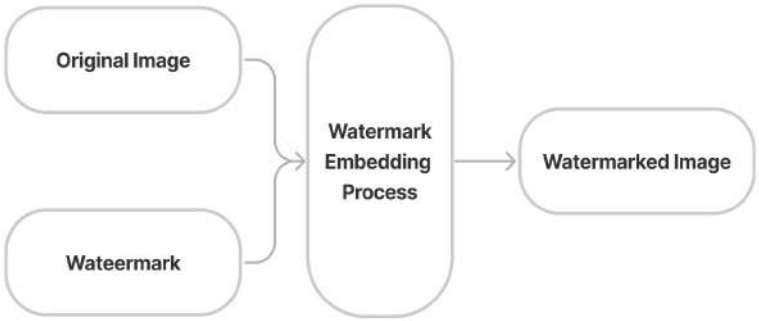


Figure 2.2 – *Watermark embedding process*

Extraction phase

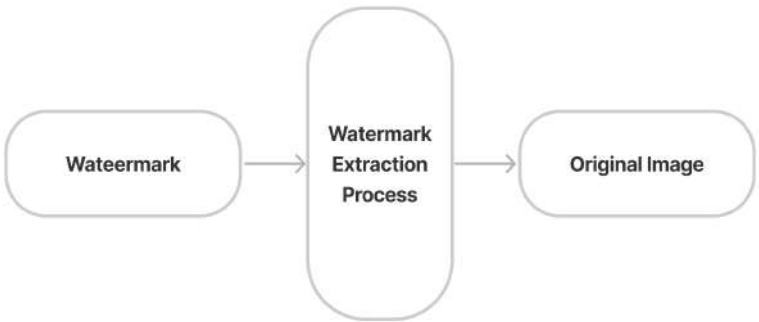


Figure 2.3 – *Watermark extraction process*

$$\widehat{W} = D\left(\widehat{I}_W, I, \right) \tag{2.2}$$

Here, "$\widehat{W}$" is the extracted watermark, "$\widehat{I}_W$" serves as the watermarked image, "I" denotes the original host image, and "D" is the extraction function

2.3 Requirements of digital watermarking

The essential elements of a digital watermarking framework can be summarized in the three pillars depicted in the Figure 2.4, imperceptibility, capacity, and robustness [Sharma et al., 2021]. Moreover, parameters are not limited to the previously listed elements. Additional criteria can be taken into consideration while designing a digital watermarking algorithm to obtain a high-rank mechanism.

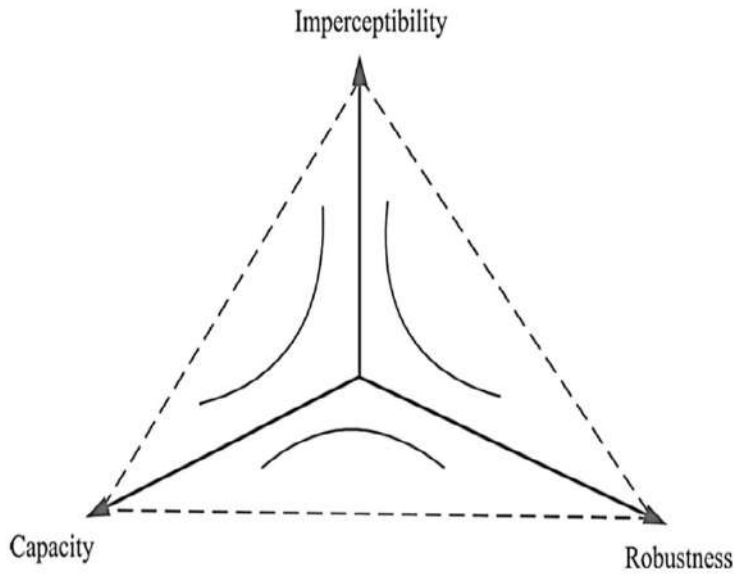


Figure 2.4 – *Compromise between imperceptibility, capacity, and robustness [Attari and Shirazi, 2018]*

2.3.1 Imperceptibility

The quality evaluation of the watermarked image correlated to the original data pertains to imperceptibility, [AlShaikh et al., 2019] since images are extremely sensitive to any sort of distortion in some specific usages (e.g.,

medicine), the watermarking method has to be suitably implemented in a high-fidelity conservative way.

2.3.2 Robustness

Robustness means that the watermarking mechanism should retain the secret data's properties and structure despite several intentional and unintentional manipulations or attacks [Rani et al., 2015]. It might be categorized into the following types:

Robust

Robust watermarking is intended to be resistant to a wide range of attacks and malicious manipulations. Therefore, even if the support is affected, the extracted watermark can be totally or partially recognized. This is typically done to protect against unauthorized use or distribution of the file. The watermark is designed to remain detectable even if the file is altered or processed in some way, such as through cropping, resizing, or applying image editing techniques. Robust watermarking techniques are used in a variety of applications, including copyright protection, authenticity verification, and tamper detection. There are many different methods for robust watermarking, each with its own set of strengths and weaknesses. Some techniques rely on visible watermarks that are embedded directly into the image or audio file, while others use invisible watermarks that are embedded in the underlying data of the file. Regardless of the method used, robust watermarking is an important tool for protecting digital content and ensuring its authenticity.

Semi-fragile

Semi-fragile watermarking techniques are a type of digital watermarking that is designed to be resistant to a certain amount of tampering or manipulation but will be damaged or destroyed if the file is subjected to more severe attacks. This type of watermarking is often used in applications where it is important to detect tampering, but the file does not necessarily need

to be completely protected against all types of attacks. Semi-fragile watermarking can be used in a variety of scenarios, including forensic analysis, content authentication, and intellectual property protection. There are many different methods for implementing semi-fragile watermarking, including both visible and invisible techniques. One common approach is to use a watermark that is embedded in the low-frequency coefficients of a discrete cosine transform (DCT) of the image or audio data. If the file is subjected to certain types of tampering, such as cropping or resizing, the watermark will be damaged or destroyed, indicating that the file has been tampered with. However, if the file is only subjected to mild manipulation, the watermark will remain intact and can still be detected.

Fragile

Fragile watermarking schemes are a type of digital watermarking technique that is designed to be easily detected but easily distorted or destroyed when the original content is modified or tampered with. These types of watermarks are typically used to identify the ownership or authenticity of a digital document or image. However, their fragile nature means that any slight alteration to the original content can result in the watermark being distorted or completely lost, rendering it irrecoverable. This makes fragile watermarking schemes less reliable than other types of watermarking techniques, such as robust watermarking schemes, which are more resistant to tampering and modification. Despite their limitations, fragile watermarking schemes are still used in certain cases where the primary goal is to easily and quickly detect any unauthorized use or tampering with the original content.

2.3.3 Data payload

An efficient digital watermarking scheme should be heedful of the embedding capacity criterion [Shih, 2017] since this is one of the essential requirements in view of the fact that the incorporated watermark may affect the support fidelity and robustness.

2.3.4 Security

Security is the operation of denying unauthorized manipulations, such as the consultation and modification of the incorporated watermark or the embedding of new secret data within the support, to illegitimate persons (e.g., hackers...). Thus, the security concept is about the protection of the watermarked image [Garg and Kishore, 2020].

2.3.5 Computational complexity

Time consumption defines the mandatory period that a watermarking process takes to embed and extract the watermark. Rapid computational digital watermarking algorithms are more eligible for implementation in real-time applications. Furthermore, highly secured schemes are more computationally expensive [Mousavi et al., 2014].

2.4 Digital watermarking classifications

2.4.1 Working domain

Spatial domain

The spatial domain is about replacing or adding watermark bits directly to the host image. This method provides imperceptibility and low time consumption, but on the other hand, it provides low levels of robustness. The least significant bit (LSB) is the most utilized material in the spatial domain for digital watermarking purposes [Kumar, 2019].

Frequency domain

In the transform domain, the watermark is inserted in frequencies obtained from appropriate transforms, which makes it more robust against attacks compared to the spatial domain methods. The most known transforms used in digital watermarking are based on wavelets, mentioning among them: the discrete cosine transform [Ahmadi Mohammad Abadi and Chalechale, 2016], the discrete wavelet transform (DWT) [Joseph and

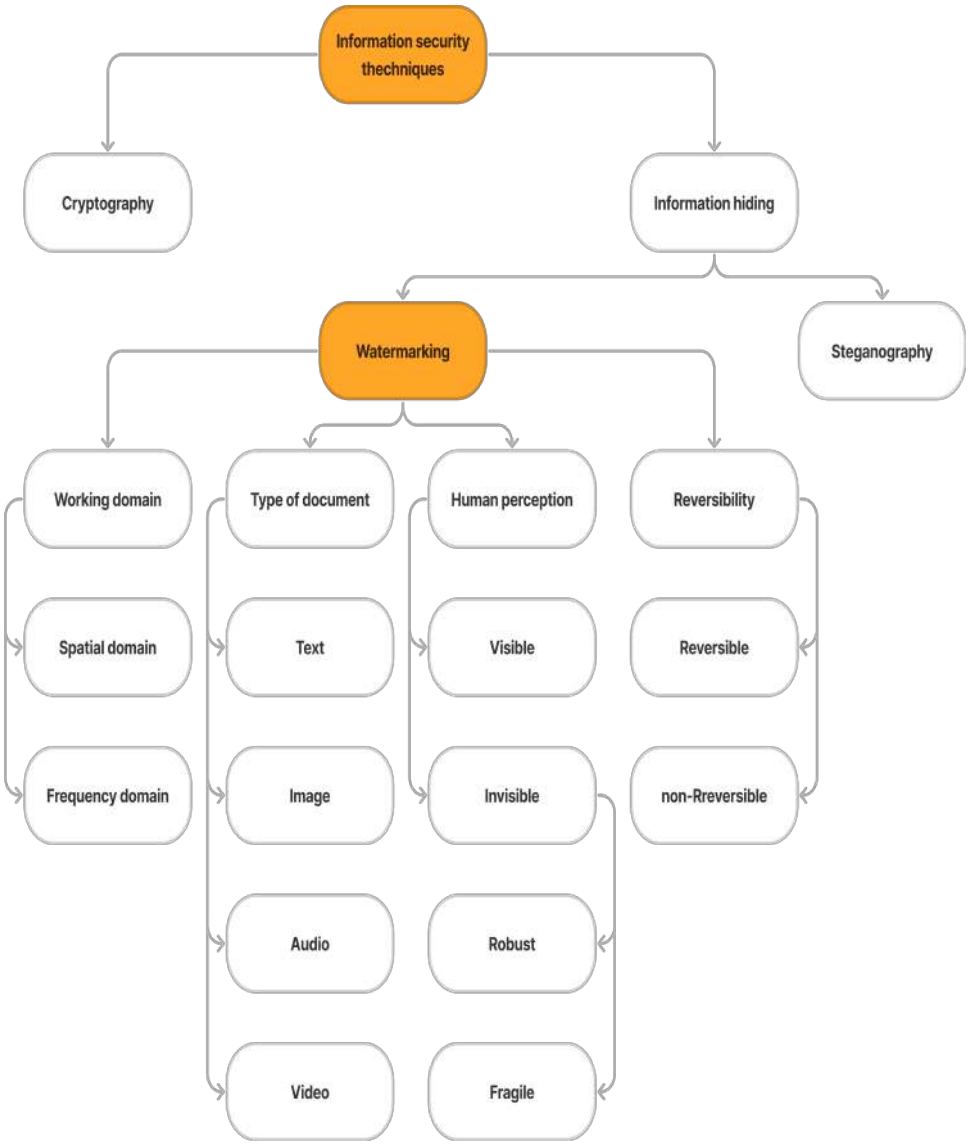


Figure 2.5 – *Information security branches and watermarking classifications [Kadian et al., 2021].*

Rajan, 2020][Al-Gindy and Ghaly, 2019], and the lifting wavelet transform (LWT) [Singh, 2019].

The following Table 2.1 elucidates the main differences between spatial and transform domains.

2.4.2 Type of document

As a matter of fact, the exchanged data via various networks are not outlined in a single type, different categories of media are transmitted daily, such as texts, audio, and videos, however, digital watermarking is more

Table 2.1 – *Spatial domain versus Frequency domain*

	Spatial domain	Frequency domain
Imperceptibility	Percetible/ Imperceptibile	Imperceptibile
Robustness	Fragile/ Semi-fragile	Robust
Capacity	High	Low
Computational cost	Low	High



Figure 2.6 – *Euro banknotes watermark.*

focused on images, since they represent approximately 35% of multimedia contents on the web [Singh and Sharma, 2021].

2.4.3 Human perception

Visible watermarking

Figure 2.6, highlights perfectly the visual watermark, where *Europa* [2], was added to euro banknotes as a translucent security marker against forgery. Visible watermarking is about embedding a signature or a logo to the support perceptually in order of determining the ownership and avoiding maleficent manipulations [Yao et al., 2019]. Additionally, the watermark might be in the form of a pseudo-random sequence [Abraham and Paul, 2012].

[2]Greek mythology portrait

Blind watermarking

This technique is about secretly incorporating a watermark into a cover image so that the watermark is not visible to the public. Furthermore, the detection and extraction of the watermark can be done without the requirement of the original host image [Lin et al., 2001], and vice versa for non-blind watermarking schemes [Benoraira et al., 2015], also the watermark can be legally extracted only by authorized persons who have prior knowledge of the watermarking process.

2.4.4 Reversibility

Reversibility is the operation of recovering the original data after the watermark extraction [Zhou et al., 2021] [Hamadou et al., 2020]. Since, in some fields such as the medical sector, images are sensitive to malformations [Thabit and Khoo, 2014], any minuscule change will lead to misinterpretation by medical experts. On the other hand, the watermarking method is said "irreversible" if the incorporated watermark and the modification exerted on the host image are permanent.

2.5 Watermarking Attacks

In spite of the potentiality provided by digital watermarking for diverse media protection, several sorts of attacks exist, resulting in a partial and global demolition of the embedded watermark [Singh et al., 2014]. The attacks might be categorized as follows:

2.5.1 Active attacks

When the watermark is deleted or hidden by a phisher, the violation type is labeled "active attack," which may provoke a large-quality degradation. Furthermore, it defines a censorious issue for proprietorship [Hosam, 2019]. In this category, the attacker utilizes image enhancement, as illustrated in Figure 2.7, illuminated in light and color branches, to remove the mark. In addition, the geometrical manipulations shown in Figure 2.8, can

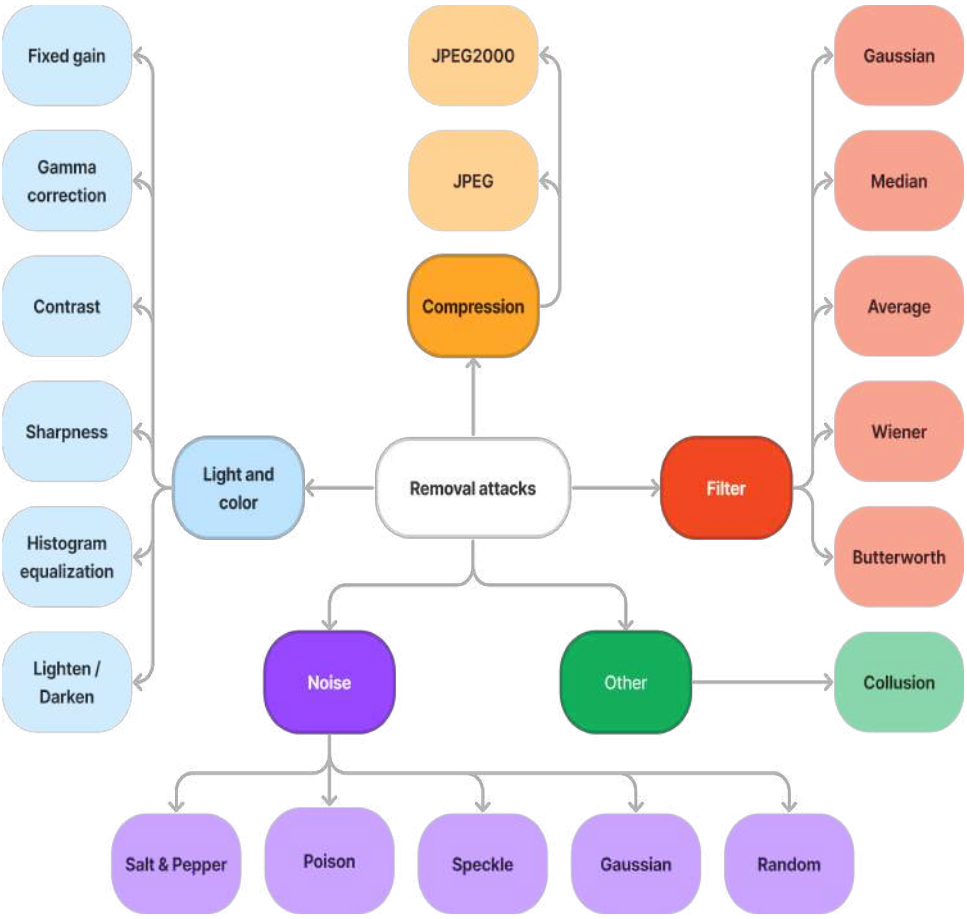


Figure 2.7 – *Common removal attacks [Evsutin and Dzhanashia, 2022].*

be used to abolish the embedded signature, where maneuvers such as rotation, cropping, and resizing can straightly annihilate the watermark [Nin and Ricciardi, 2013].

2.5.2 Passive attacks

If the attacker's target is merely the detection of the watermark's presence, the invasion type is called a "passive attack" [Cox et al., 2000]. Nevertheless, even though the hacker's objective seems harmless, in covert communication, e.g., prisoners problem [Chaum, 1984], the secret mark should be audible and accessible only to authorized parties.

2.5.3 Forgery attacks

At this point, instead of eliminating the watermark, the assailant embeds a new signature, which may result in some earnest issues of integrity and

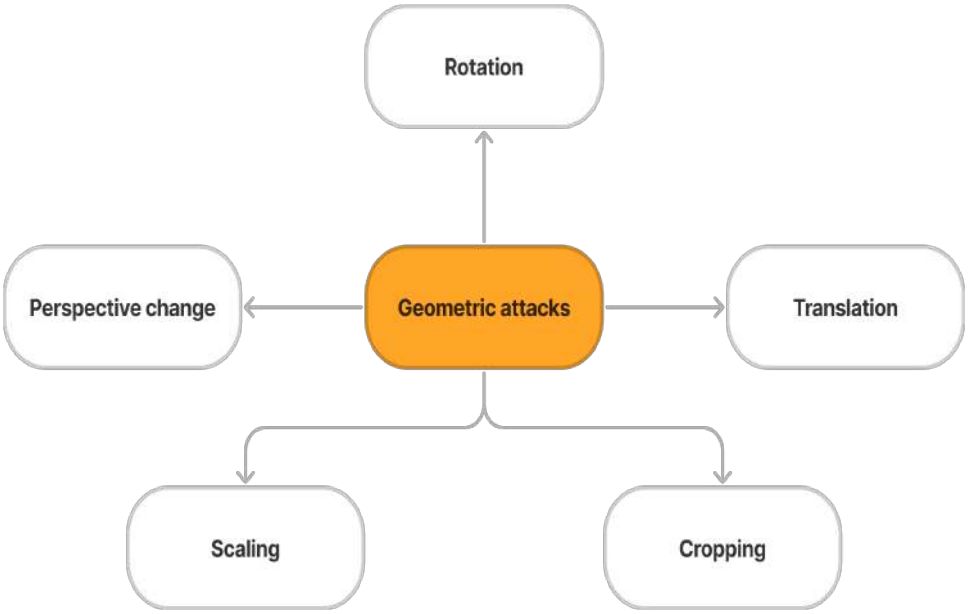


Figure 2.8 – *Common geometric attacks [Evsutin and Dzhanashia, 2022].*

authentication [Jung, 2017]. In forgery attacks, the problem estate in the lack of discrimination between intentional and unintentional attacks [Ekici et al., 2004], as lossy compression or quality degradation results from the transmission.

2.5.4 Collusion attacks

In collusion attacks, the invader collects a set of copies of the watermarked image [Kanocz et al., 2009], which contains the same mark, and attempts to excerpt the watermarking algorithm to get a replica of the unmarked image [Karmakar et al., 2016]. Moreover, the attacker can use watermarked images with various signatures to construct a new unwatermarked version.

2.6 Fields of application

Digital watermarking is considered the shield of numerical data against fraudulent employment. Nowadays, it is adopted by modern society in various domains, i.e., content protection. Figure 2.9 represents the major application fields of this technology. Furthermore, digital watermarking can be exploited for hardware protection [Mohanty et al., 2017]. In the sequel literature, a few major application areas are discussed.

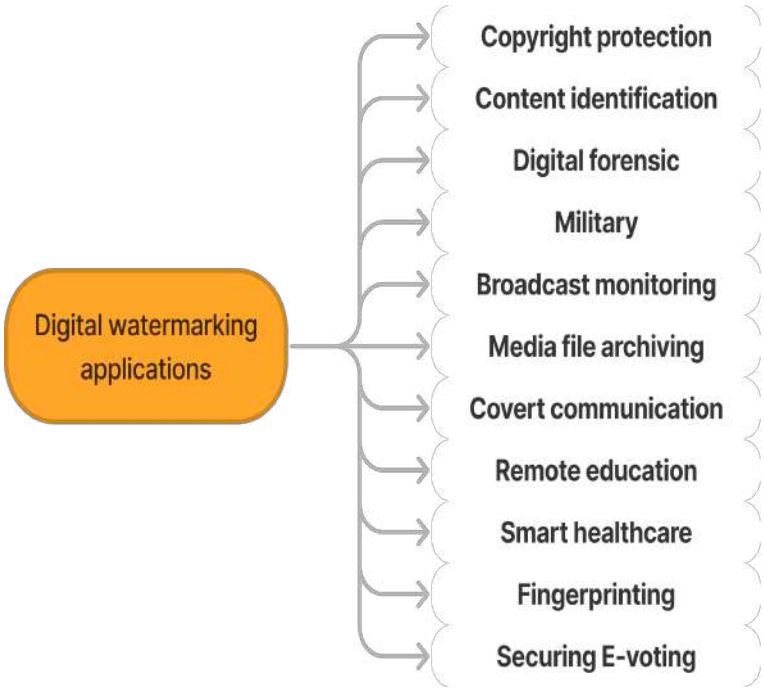


Figure 2.9 – *Digital watermarking applications [Kumar et al., 2017]*

Copyright protection

> *"Each Contracting State undertakes to provide for the adequate and effective, protection of the rights of authors and other copyright proprietors in literary, scientific and artistic works, including writings, musical, dramatic and cinematographic works, and paintings, engravings and sculpture."* [3]

Copyright is used by creators to illustrate the ownership they have over their works (books, photographs, movies, etc.). A watermark is inserted within the support to ensure protection from counterfeiting and illegal redistribution.

Fingerprinting

The authenticity of fingerprints in numerical media assures that the rights holder is notified upon the appearance of an illegal copy [Lian et al., 2008]. Analogically, fingerprints can be represented by material parameters, i.e., fingerprints and iris. Thus, digital fingerprinting is about the suite of pa-

[3] Universal Copyright Convention, Article I, Geneva 1952. [uni, 1952]

rameters that describe the unicity of numerical support where each photocopy has a particular digital watermark [Dymarski et al., 2018].

Authentication and Integrity Verification

Authentication is the detection procedure for modifications exerted on data [Yusof and Khalifa, 2007]. Furthermore, image integrity [Mestiri et al., 2017] means that the image should not be altered in any case, except by the certified community, where fragile or semi-fragile watermarking schemes can be used for the integrity checking process [Chahal and Khurana, 2013].

Broadcast Monitoring

Broadcast monitoring can be depicted as the procedure of finding and tracking all activity on a broadcasting channel to see if it violates any laws or is illegal [Agbaje, 2017]. Therefore, it can be used to track commercials that are being played [Radharani and Valarmathi, 2010], and other types of broadcasting.

Medical Applications

In the medical sector, digital watermarking is utilized essentially for the following reasons: integrity verification and authentication to prove that transferred data is clear of maleficent modification and belongs to the correct patient, where adopted watermarking techniques should be careful to prevent quality degradation since, as already mentioned about medical image sensitivity, the final main reason is data hiding, where generally, information about patients, such as electronic patient records (EPR), is incorporated into the medical image [Allaf and Kbir, 2019].

Fraud detection

Always under the umbrella of copyright protection, fraud detection is about securing the ownership of distributed multimedia from various ways of tampering [Lan and Tewfik, 1999], and ensuring that the received media output is from a trustworthy source [Sunesh, 2011]. Thus, any ma-

nipulations executed on the received image will be considered fraudulent evidence of property infringement.

Id card verification

Id cards and passports images falsification represent an international issue [Thongkor and Amornraksa, 2012], watermarking might solve this problem by assuring the authenticity of the attached image by embedding citizen data (e.g., National Serial Number) within the Id/passport photograph.

2.7 Performances metrics

For the sake of calibrating a watermarking scheme's efficiency, a set of metrics needs to be computed to assure and validate the watermarking framework's adaptability in terms of imperceptibility and robustness.

Mean Square Error

$$MSE = \frac{1}{M \times N} \sum_{0}^{M-1} \sum_{0}^{N-1} (C(i,j) - W(i,j))^2 \tag{2.3}$$

To measure the square error among two matrices (e.g., images), the mean square error (equation 2.3) is calculated. The previous equation elements stand for the next: "M" and "N" denote the row and column numbers. "C" and "W" represent the original and the watermarked image, respectively, moreover, pixel coordination is presented by "i" and "j".

Peak Signal to Noise Ratio (PSNR)

Since high fidelity is essential for watermarking system evaluation [Begum and Uddin, 2020]. PSNR (equation 2.4) computes the difference between the original signal and the corrupted noisy signal to extract the level of damage affected by noise.

$$PSNR = 10 \log \frac{Peak^2}{MSE} \tag{2.4}$$

Peak is the biggest value within image matrices. MSE is performed using the equation 2.3.

Structural Similarity Index Metric (SSIM)

To measure the disparity between the original and the watermarked images [Liu et al., 2021], SSIM is fulfilled using the following equation 2.5:

$$\mathrm{SSIM}(I, \hat{I}) = \frac{(2\mu_I\mu_{\hat{I}} + c_1)\,(2\sigma_{\hat{I}} + c_2)}{\left(\mu_I^2 + \mu_{\hat{I}}^2 + c_1\right)\left(\sigma_I^2 + \sigma_{\hat{I}}^2 + c_2\right)} \tag{2.5}$$

Normalized Correlation (NC)

Since comparing the extracted watermark with the incorporated one is an essential process [Yadav and Sehra, 2018], the normalized correlation serves this role and is defined as follows in the equation 2.6:

$$NCC = \frac{\sum_{i=1}^{x}\sum_{j=1}^{y}\left(W_{or}(i,j) \times W_{ex}(i,j)\right)}{\sum_{i=1}^{x}\sum_{j=1}^{y} W_{or}^2(i,j)} \tag{2.6}$$

Bit Error Rate (BER)

Error rate within a communication system is expressed with BER (equation 2.7), which consists of dividing accumulated errors on entire transmitted bits [Abdulla and Navas, 2020].

$$BER = \frac{\text{Errors}}{\text{Number of bits}} \tag{2.7}$$

Correlation Coefficients

Correlation coefficients metric (equation 2.8) is conducted to extrapolate similitude between original and watermarked/ciphered and original/plain digital documents [Fatima and Tuptewar, 2016].

$$CC = \frac{\sum_M \sum_N (A(M,N) - \bar{A})(B(M,N) - \bar{B})}{\sqrt{\sum_M \sum_N \left(A(M,N) - \bar{A}^2\right) \sum_M \sum_N \left((B(M,N) - \bar{B})^2\right)}} \tag{2.8}$$

Hamming Distance

Hamming distance is a metric used in cryptography to measure the number of positions at which two strings of equal length differ. It is often used to detect and correct errors in transmitted data as well as to compare the similarity of two different strings. In cryptography, the Hamming distance is used to evaluate the security of a cryptographic system as well as to detect and correct errors in encrypted messages.

2.8 Cryptography

> *"If you think technology can solve your security problems, then you don't understand the problems and you don't understand technology."*
> *— Bruce Schneier*

At this moment, and while you are reading this thesis, there are plenty of hackers who try to attack crypto-systems to reach the personal information of internet users around the globe. Cryptography can simply be defined as the mathematical studies applied to guarantee adequate solutions for a couple of security dilemmas: privacy and authentication [Diffie and Hellman, 1976].

"*Cryptology* is defined as the science or art of secret writings; the main goal is to protect and defend the secrecy and confidentiality of the information with the help of cryptographic algorithms." [Mihailescu and Nita, 2021] [Mihailescu and Nita, 2020]

"*Cryptography* represents the defensive side of cryptology; the main objective is to create and design the cryptographic systems and their rules." When we are dealing with cryptography, we can observe a special kind of art: an art that is based on protecting the information by transforming it into an unreadable format called "ciphertext." [Mihailescu and Nita, 2021] [Mihailescu and Nita, 2020]

Inferred from the above definitions, it could be stated that cryptography is the art of preventing data from spying and detecting heinous exertions, by rendering it from clear into illegible content. In the next subsections, the elementary derivatives of cryptography are elucidated.

2.8.1 Symmetric key encryption

Symmetric cryptography, also known as "classic ciphers", is essentially based on the operation of encryption using the same key for all the communicating entities. the leading controversy of this technique is the key distribution safety [Menezes et al., 1997], where this issue is denoted as the "key distribution problem" [Diamanti et al., 2016].

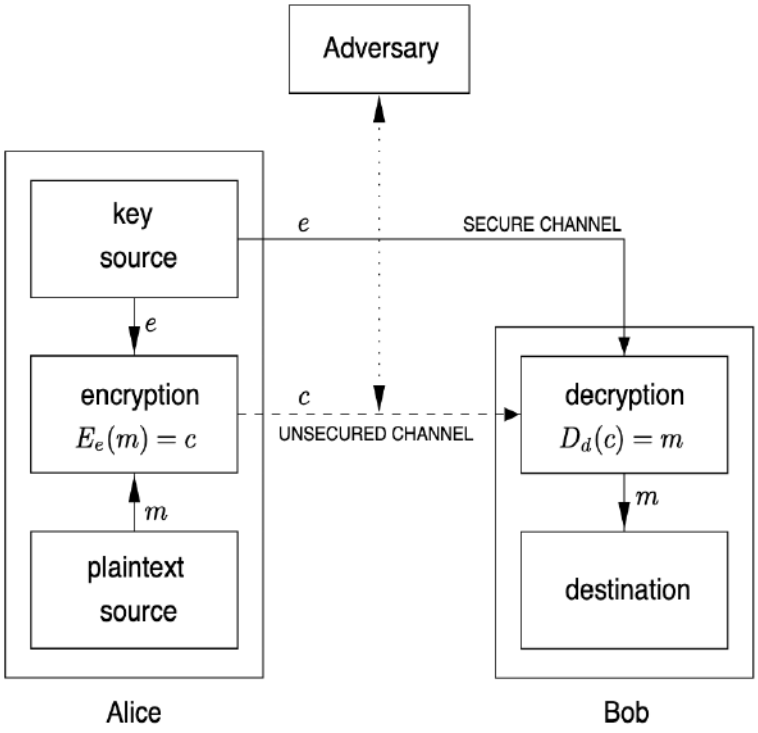


Figure 2.10 – *Two-party communication using encryption, with a secure channel for key exchange. The decryption key "d" can be efficiently computed from the encryption key "e". [Menezes et al., 1997]*

Intending to clear the symmetric key encryption, Figure 2.10 interprets the operating mechanism. On account of the fact that the exchanging parties have an anterior familiarity with the encryption and decryption schemes, obviously, the key "e" should be secretly transferred, since the decryption key "d" can be extrapolated starting from the encryption key "e" [Menezes et al., 1997]. Moreover, symmetric algorithms could be cleft into two classes: block and stream ciphers, where the first cipher serves a set of bytes and the last works on a single byte of data [Amador and Green, 2005].

2.8.2 Public key encryption

Diametrically opposed to the symmetric encryption, asymmetric cryptosystems exploit public and private keys [Xu and Ge, 2009]. The scope of the public key is the encryption of the plain text, and as its name indicates, it is publicly accessible. The private key is exerted for the ciphertext decryption and is known only to its holder.

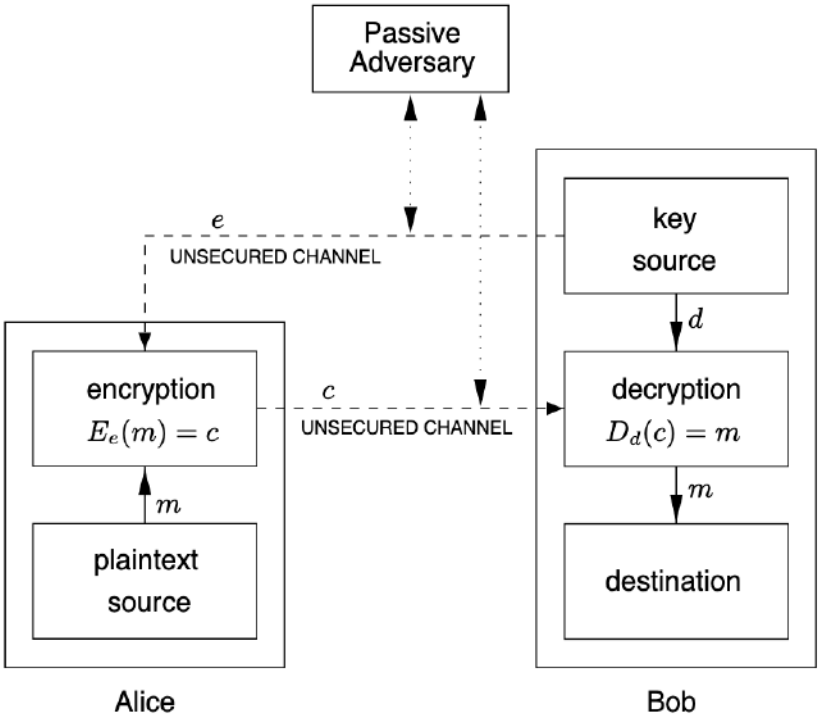


Figure 2.11 – *Encryption using public-key techniques. [Menezes et al., 1997]*

2.8.3 Chaos based cryptography

The chaos system for cryptography was introduced by *Robert Matthews* [4] in [Matthews, 1989], randomness, complexity, and ergodicity parameters are well delivered by chaotic systems due to the chaos system's sensitivity for initial conditions [AlMutairi and Bonny, 2020]. From mathematicians' point of view, it is solid to determine chaos, however, it is obvious to note it when it appears [Biswas et al., 2020]. Recently, chaotic systems are widely exploited in several fields, especially in image encryption [Girdhar et al., 2021][Ye et al., 2018]. A narrow transition in the input image will lead to

[4] Robert A.J. Matthews (born 23 September 1959), is a British physicist and scientist

a tremendous variation in the output, where the result will be similar to noise due to the non-linearity, determinism, and dynamic nature of chaos systems [Mohamed, 2020]. Moreover, the most outstanding chaotic system utilized in image encryption is the Arnold map which will be explained in the sequel.

Conclusion

To recap what has been said before, this chapter delved into the topic of digital watermarking, a technology that allows the embedding of hidden messages within digital data in order to protect proprietary rights and deter copyright violations. The chapter covered the two main domains of digital watermarking, spatial and transform, and highlighted the benefits of each. Additionally, the main branches of an effective watermarking scheme were discussed, including robustness, imperceptibility, and capacity.

The chapter also provided an overview of cryptography, which plays an important role in digital watermarking. Cryptography is used to protect the hidden message from unauthorized access and ensure that it can only be extracted by authorized parties. Additionally, the chapter discussed a collection of performance metrics that can be used to evaluate the efficiency of different digital watermarking schemes. These metrics help to determine the effectiveness of a given scheme in terms of its robustness, imperceptibility, and capacity.

Finally, it was mentioned that recent technological advancements have enabled internet users to exchange confidential data more securely. Digital watermarking is now possible and widely used to protect the rights of owners. Digital watermarking is a powerful tool that can help to protect the rights of creators, authors, and owners in the digital age, and it is likely to become increasingly important in the future.

3 Blind Digital Watermarking Scheme based on DTCWT and NSCT for Telemedicine Application

Contents

3.1 Introduction . . . 47
3.2 Related works . . . 48
3.3 Preliminaries . . . 52
3.3.1 Dual Tree Complex Wavelet Transform . . . 52
3.3.2 Non-Subsampled Contourlet Transform . . . 54
3.4 Methodology . . . 55
3.4.1 Watermark embedding procedure . . . 56
3.4.2 Watermark extraction procedure . . . 57
3.5 Results and Discussion . . . 58
3.5.1 High-fidelity evaluation . . . 59
3.5.2 Robustness analysis . . . 60
3.5.3 Computational cost . . . 68
Conclusion . . . 68

Motivated by the previous chapters, a digital image watermarking scheme for medical application based on frequency domain is presented in this chapter

3.1 Introduction

Numerous pandemics, wars, and natural disasters have struck humanity since the beginning of historical records. Telemedicine provides enormous advantages to humanity, and the strength of this technology was demonstrated by the most recent pandemic, which was caused by the novel coronavirus *COVID-19*. Many medical services, such as remote exams and consultations, were all part of these perks. Medical images, like any other type of data, require a certain level of security and protection against malicious use, which places experts under a strong ethical obligation to safeguard this information from unauthorized use. Private information about a patient's health, also known as electronic patient records, is included in medical images and must be kept secure and unaltered at all times.

Based on the blind digital watermarking principle, which consists of extracting incorporated data without the necessity of the original embedded data's presence, the literature describes a dual-tree complex wavelet transform (DTCWT) and a non-subsampled contourlet transform (NSCT). The approach involves decomposing the host picture using the DTCWT and then applying the NSCT to the low-frequency sub-band obtained with the DTCWT. From the data of the NSCT, an appropriate sub-band is chosen to incorporate a binary watermark, where the employed color space is YIQ and the chrominance component "Q" is the component chosen for watermark embedding. Applying the same decompositions as the embedding procedure will bring the recipient to the watermark even if they are unaware of the concealed mark.

This chapter is organized as follows: Sec. 3.2 presents a literature review on some potential image watermarking methods. The technical background of the research is reported in Sec. 3.3. Sec. 3.4 describes the methodology used in the study, and the discussion of the results is provided in Section 3.5.

3.2 Related works

In [Mittal et al., 2020], Mittal et al. presented a digital image watermarking method based on curvelets. To extract the edge surface of a host image, the approach employs Gaussian filters and a first-order partial differential matrix. Since human eyes' sensitivity for smooth and edged areas is not equal, this study has an impact on the edge surface curvelet coefficients. Edge surface, coarse levels of curvelet transform, and strength parameters were utilized to retain the quality of the artwork while also increasing its resistance to assaults. Furthermore, the host coefficients were chosen to fit the human visual system.

Wang et al. [Wang et al., 2020], introduced a technique for digital image watermarking utilizing Singular Value Decomposition, and a Gaussian-cauchy mixture based vector hidden markov tree (HMT) in the Discrete Non-separable shearlet transform (DNST) domain. This scheme is about running DNST on the host image and then applying SVD to the high-entropy DNST domain blocks. Next, the robust singular values were changed to integrate the digital watermark into the DNST high-entropy blocks. The blind image watermark decoder was made by merging HMT and maximum likelihood (ML) decisions at the receiver. The Gaussian-cauchy mixture marginal distribution and other strong dependencies of DNST domain singular values are included in the first step of modeling resilient DNST domain singular values using a Gaussian-cauchy mixture-based vector. Then, using the parameter-expanded expectation-maximization (PXEM) technique, the statistical model parameters of HMT are calculated.

A watermarking system based on Spiking Neural Network (SNN) was introduced by Malik and Rama [Malik and Rama Kishore, 2020a]. The current research provides a novel and substantial SNN-based image watermarking approach with the goals of resilience and security while requiring less time. The extraction technique is treated as an optimization issue in this approach, and it is handled by using spiking neural networks. The proposed SNN uses spiking neural networks to achieve greater re-

silience against various assaults while requiring less computational complexity. Furthermore, the suggested SNN method's security is achieved by utilizing chaotic-based scrambling on the watermark.

Singh in [Singh, 2019], reported a robust method for medical image watermarking based on LWT and DCT. The watermark and patient report characters are hidden in the host medical image in order to prove authenticity. Before even being embedded into the host picture, the signature is encrypted through message digest (MD5), and the EPR is encoded with bose chaudhuri hocquenghem (BCH), an error-correcting code. Experiments show that the approach is sufficiently strong and secure against a variety of assaults without causing considerable distortion.

A lifting wavelet transform and firefly-based robust digital image watermarking algorithm was presented by Kazemivash et al. [Kazemivash and Moghaddam, 2016a], the technique's main idea was about dissociating the host image into four sub-bands utilizing the LWT, with the first sub-band being divided into non-overlapping blocks. Following that, blocks are ordered in descending order depending on their standard derivation. Due to the link between imperceptibility and robustness, selecting acceptable blocks for the specific embedding procedure appears to be an optimization challenge. The firefly algorithm, which was employed to handle this trade-off while choosing main blocks, results in high resilience and low imperceptibility, and vice versa. Jumbled image bits resulted from Arnold transform exertion on the watermark, which was then employed as a condition for the embedding procedure.

In [Zear et al., 2016], Zear et al. proposed a multiple digital watermarking method for medical utilization based on DWT, DCT, and SVD. The suggested technique employs three watermarks for identity authentication: a medical lump image watermark, a doctor's signature, and the patient's records watermarks. back propagation neural network (BPNN) is used with the extracted image watermark to decrease noise effects on the watermarked image in order to improve the image watermark's resilience performance. The watermark's security is additionally improved by utilizing Arnold transform before embedding it into the host. Lossless arith-

metic compression technique and Hamming error-correcting code are also used to encode the symptom and signature text watermarks, respectively. The patient records are then integrated into the cover image, compressed, and encoded.

Kalra et al. [Kalra et al., 2013] suggested a digital image watermarking technique in the transform domain for copyright protection based on error correcting codes (ECC) and encryption technologies. The mechanism of this system exploits Hamming codes as an error-correcting tool to safeguard the copyright watermark. To improve susceptibility, a watermark was incorporated in the frequency domain using discrete cosine and discrete wavelet transformations. Medium-frequency signals are only targeted using a combination of two strategies. Before embedding, the watermark's randomness is also formed. Rather than embedding in the same position in each block, it is inserted dynamically based on the rows or columns of that block.

A digital watermarking approach proposed by Ariatmanto et al. [Ariatmanto and Ernawan, 2020] based on various embedding strengths. The logic of this method was as follows: image pixels are segregated into non-overlapping blocks. For each image block, the variance pixel value was calculated. The embedding areas were chosen from image blocks with the greatest variance value. Obtained from the DCT, the coefficients at the middle frequency were chosen, and the average of selected DCT blocks was computed to provide varied embedding strengths. The watermark bits were implanted using an embedding function based on the various embedding strengths provided. Before the insertion, the watermark was shuffled using Arnold transform for further protection.

The work of Zebbiche et al. in [Zebbiche et al., 2018], was a robust additive digital image watermarking technique based on the dual-tree complex wavelet transform (DTCWT) and perceptual masking. The watermark is decomposed with DTCWT, and the resultant high-frequency coefficients are then embedded in the high-frequency coefficients of the DTCWT-transformed image via an additive technique. To overcome the additive rule's constraint on regulating the amplitude of the incorporated

watermark, perceptual masking is used. To authenticate the presence of the signature, the watermark detector is given the high-frequency coefficients of the DTCWT-converted candidate watermark as well as the high-frequency DTCWT coefficients of the watermarked picture during the detection phase. Leung et al. [Leung et al., 2012] introduced a technique based on wave atoms for digital image watermarking. The principle of this method is that rather than the lowest or highest sub-bands, the scale band was chosen to be integrated into this research. To embed data, a multiplicative-based technique is used. Multiple description coding (MDC), initially decomposes the original image into sub-image descriptions to incorporate the watermark, only by gathering all of these details can the watermark be retrieved. The suggested method's core idea is to alter the energy of particular squares inside the wave atom tiling for various descriptions based on the watermark bit value. A comparison between energy variations will lead to the encoded watermark recovery.

Kumar et al. [Kumar et al., 2018], suggested a multiple image watermarking scheme based on hybridization of redundant discrete wavelet transforms (RDWT), set partitioning in hierarchical tree (SPIHT), non-subsampled contourlet transform (NSCT), and Singular Value Decomposition (SVD). The core idea is about invisibly including dual watermarks, a logo, and a signature in selected sub-bands of a cover image. The entropy of each section of the host image is determined using the sub-sampling approach, which divides the image into sub-images. Then, the NSCT is executed on the sub-image with the highest entropy. In addition, RDWT is applied to a sub-band of the NSCT image. In the latter case, SVD was performed on the cover image's RDWT coefficients, which delivered the singular vector. Both watermarks go through the same procedure. The NSCT sub-band of the signature watermark, on the other hand, is first encrypted using Arnold encryption to enforce the suggested scheme security and then deconstructed using RDWT. Furthermore, RDWT and NSCT selection choices were made due to their shift-invariant nature. The suggested approach provides high PSNR, NC, and SSIM values, according to the findings and analyses.

Su and Chen [Su and Chen, 2017] suggested a watermarking algorithm to answer the problem of copyright protection, this work introduces a new blind watermarking technique that embeds the binary watermark into the blue channel of an RGB image in the spatial domain. The generating concept and distribution properties of the direct current (DC) coefficient are utilized to directly affect pixel values in the spatial domain for embedding watermarks and then separated sub-watermarks are embedded into various portions of the host image. While constructing the watermark, the sub-watermark is extracted using a blind approach based on the DC coefficients of the watermarked image and the key-based quantization step, and then the statistical rule and method of "first picked, second combined" are recommended to create the final watermark. As a result, the suggested technique is implemented in the spatial domain rather than the frequency domain, due to its advantages.

3.3 Preliminaries

3.3.1 Dual Tree Complex Wavelet Transform

An advanced version of the DWT known as the Dual-Tree Complicated Wavelet Transform (or simply Dual-Tree CWT) was developed by Kingsbury [Yadav and Sehra, 2018]. The DWT and CWT (Complex Wavelet Transform) criteria are integrated into one in the DTCWT [Zebbiche et al., 2018]. The key advantages of this transformation include translation invariance and strong directional selectivity [Liu et al., 2019]. Figure 3.1 illustrates both the structure of the DTCWT as well as the orientations of the coefficients. Mathematically speaking, the DTCWT finds the real and imaginary sections by concurrently applying two parallel DWTs, one for each branch [Alkhathami et al., 2013]. This results in both the real and imaginary sections being found. It is conceivable that the shift insensibility that is provided by the DTCWT could be used to create a watermarking system that is resistant to geometric assaults. This is made possible by the fact that the DTCWT uses the DTCWT. In addition, the DTCWT must evaluate both the real and imaginary sections, and the findings of this assessment will

show how phase information may be obtained. The major differentiation between the real and imaginary components is shown by the creation of the filter bank. This distinction is shown by the fact that if the filters are the same across all of the branches, then there will be no forward movement. Additionally, it is highly challenging to construct filter banks, and while they are being calculated, they take up more memory than normal. The DTCWT functions 3.1, 3.2, and 3.3 are described as follows:

$$\varphi(x,y) = \varphi_o(x)\varphi_o(y) - \varphi_b(x)\varphi_b(y) + J\left[\varphi_o(x)\varphi_b(y) + \varphi_b(x)\varphi_o(y)\right] \quad (3.1)$$

$$\text{Real}\{\varphi(x,y)\} = \varphi_o(x)\varphi_o(y) - \varphi_b(x)\varphi_b(y) \quad (3.2)$$

$$\text{Imaginary}\{\varphi(x,y)\} = \varphi_o(x)\varphi_b(y) - \varphi_b(x)\varphi_o(y) \quad (3.3)$$

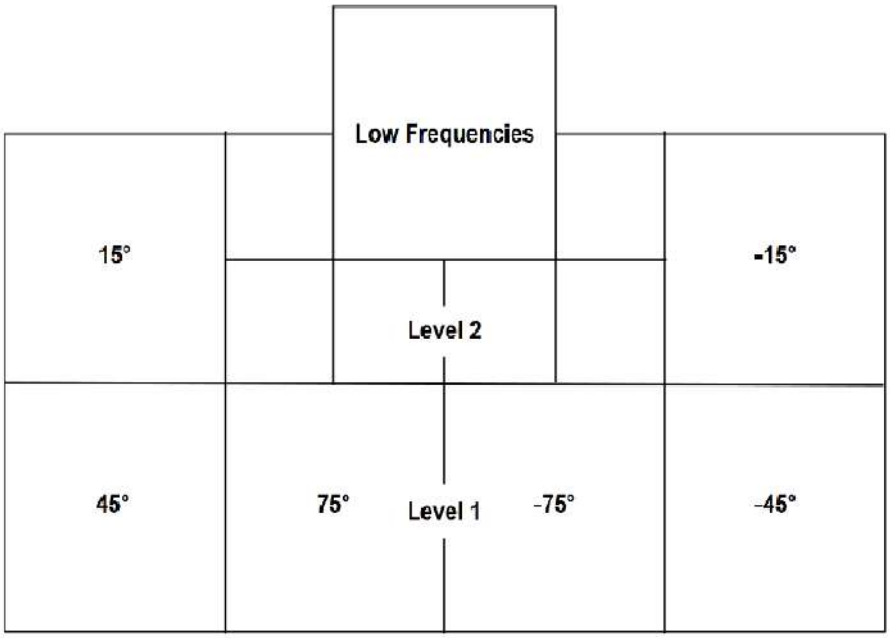


Figure 3.1 – *Digital watermarking applications*

The symbols o and b, stand for orthogonal real wavelets and biorthogonal real wavelets, respectively. To condense a lengthy explanation, the DTCWT principle entails applying filters to image rows and columns to

generate low-pass sub-bands (approximation) and high-pass sub-bands (details) [Wang et al., 2019a]. This is done to produce low-pass and high-pass sub-bands. 15 degrees, 45 degrees, and 75 degrees are the various details of sub-band directionalities that are provided by the DTCWT [Kumar and Rajendra Naik, 2019]. [Note: The directionality characteristic that is guaranteed by the DTCWT renders pictures insensitive to the coefficient fluctuations that cause artifacts, which in turn will result in high-fidelity watermarks that can be recovered from the image.

3.3.2 Non-Subsampled Contourlet Transform

Non-subsampled contourlet transform is used to depict contours more effectively [Ghaz et al., 2014]. The contourlet transform (CT) is a multi-resolution and multidirectional transform that was initially reported by Do and Vetteli [Do and Vetterli, 2005]. It was developed by these two researchers.

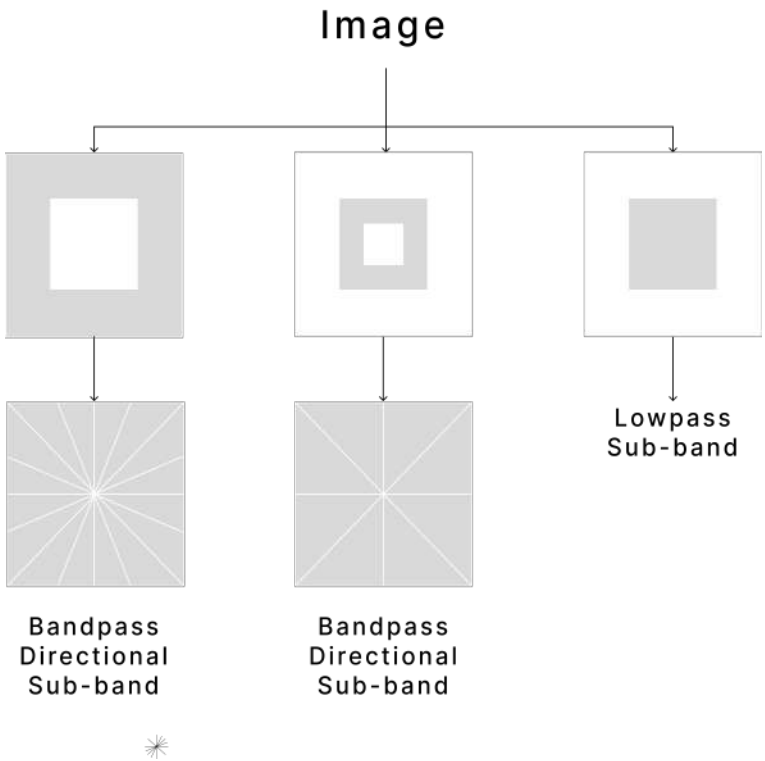


Figure 3.2 – *Digital watermarking applications*

The shift-invariant model of CT was developed by Da Cunha and colleagues [Da Cunha et al., 2006], and their model is referred to as NSCT

[Nam et al., 2020]. During the process of picture breakdown and reconstruction [Wang et al., 2019b], the NSCT is also responsible for eliminating down and up samples, as seen in Figure 3.2.

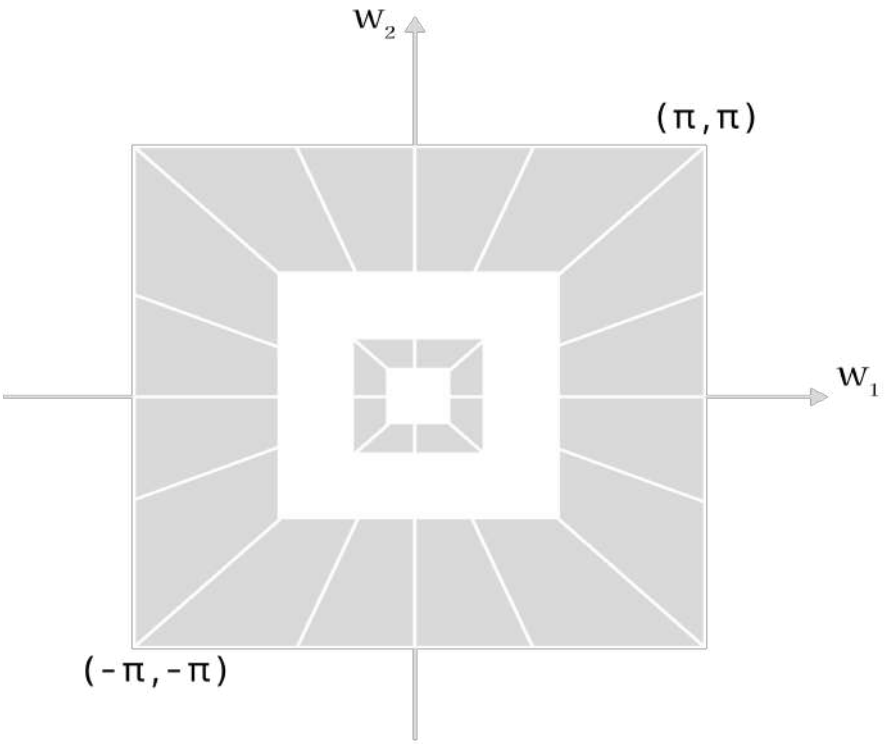


Figure 3.3 – *Digital watermarking applications*

The non-subsampled pyramid, also known as the NSP, is applied to the picture to achieve multi-scale decomposition. Both low frequencies and high frequencies will be produced as a consequence of this process. After that, the non-subsampled directional filter bank, also known as the NSDFB, is applied to the high frequencies of each scale to get multi-directional decomposition (see Figure 3.3) [Wang et al., 2019b]. Low-pass coefficients are denoted by the abbreviation KLP, while directional high-pass coefficients are denoted by the abbreviation Ks,dHP, where s stands for scale and d refers to direction index.

3.4 Methodology

This approach proposes a way to use blind digital watermarking as a means of ensuring authentication and protecting copyright. As was alluded to in passing in the preamble, the foundation of this method is the

DTCWT-NSCT color transformation performed in the YIQ color space. The integration of these transformations leads to enhanced directionality and translation invariance, which are both valuable advantages. A graphical representation of the embedding and the extraction processes is shown in Figure 3.4.

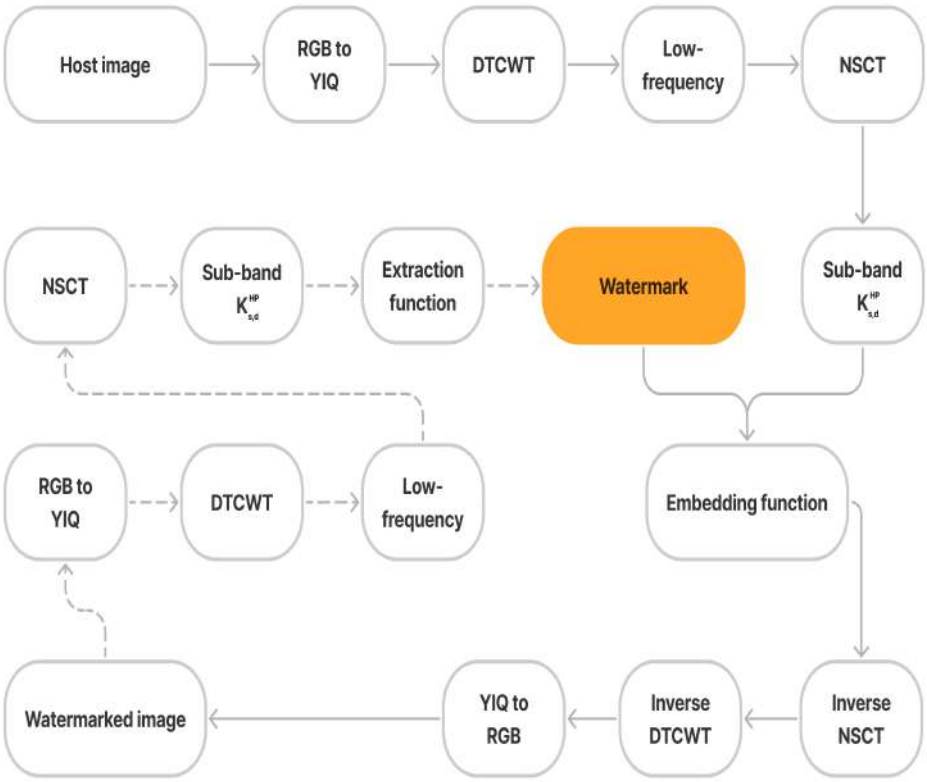


Figure 3.4 – *Digital watermarking applications*

3.4.1 Watermark embedding procedure

The embedding method involves adding the binary watermark to a colored cover image. To obtain the watermarked image, the cover image is first transformed into YIQ color space, then the DTCWT is applied to the Q component, the low-frequency sub-band is decomposed using NSCT, and finally, a high-frequency sub-band is assigned for the watermark embedding using a quantization embedding mechanism. The algorithm 1 illustrates the transforms cascading and the embedding mechanism.

Algorithm 1 Watermark embedding

Input: cover image, watermark
Output: watermarked image
Begin

- Load the host and watermark images
- Cover image color space conversion from RGB to YIQ
- Apply the dual-tree complex wavelet transform on the chrominance component denoted "Q"
- Execute the NSCT to the low pass sub-band determined in the previous step with three levels (0,2,3) and "pkva" filters
- Use the following formula 3.4 to quantify the high-pass sub-band "K1,3HP" acquired from the NSCT:

$$Q(i,j) = \text{mod}\left(\left(\text{round}\left(\frac{K_{1,3}^{HP}}{\nabla}\right)\right), 2\right) \tag{3.4}$$

- Insert the watermark using the following equations 3.5 and 3.6:

$$C(i,j) = K_{1,3}^{HP} \quad \text{if} \quad Q(i,j) = W(i,j) \tag{3.5}$$

$$C(i,j) = \begin{cases} K_{1,3}^{HP} - \nabla & \text{if} \quad K_{1,3}^{HP} \geq 0 \\ K_{1,3}^{HP} + \nabla & \text{else} \quad K_{1,3}^{HP} < 0 \end{cases} \tag{3.6}$$

  Where i and j are coordinates, C is the embedding matrix. Consideration should be given to its value, since increasing it will result in high robustness and reduced imperceptibility

- Inverse NSCT
- Inverse DTCWT
- YIQ TO RGB conversion

End

3.4.2 Watermark extraction procedure

In this phase, the watermarked image is the only element required for the watermark recovery, where the same transform combination employed in the incorporation phase is utilized for the retrieving operation. The algorithm 2 is a rundown of the stages involved in the watermark extraction process.

Algorithm 2 Watermark extraction

Input: watermarked image
Output: watermark
Begin

- Read the watermarked image
- Repeat steps 2, 3 and 4 from the embedding algorithm
- Apply the following formula 3.7 to retrieve the embedded watermark:

$$W_{\text{extracted}} = \begin{cases} 1 \text{ if } \mod\left(\left(\text{round}\left(\frac{Kw_{1,3}(i,j)}{\nabla}\right)\right), 2\right) = 1 \\ 0 \text{ elsewhere} \end{cases} \tag{3.7}$$

End

3.5 Results and Discussion

The simulation was run on hardware that included an Intel® i5-4200U 1.6GHz CPU and 6GB of RAM, where experiments were carried out using the MATLAB R2019a program. As host, a collection of medical images was employed [Med, 2022], which are shown in Figure 3.5. Figure 3.6 illustrates the watermark that was put to use. The dimensions of the host picture are 512×512 pixels, while the watermark's dimensions are 32×32 pixels. The suggested approach was tested using different types of attacks with different parameters. The technique's robustness was compared to the robustness of previous works mentioned in the related works.

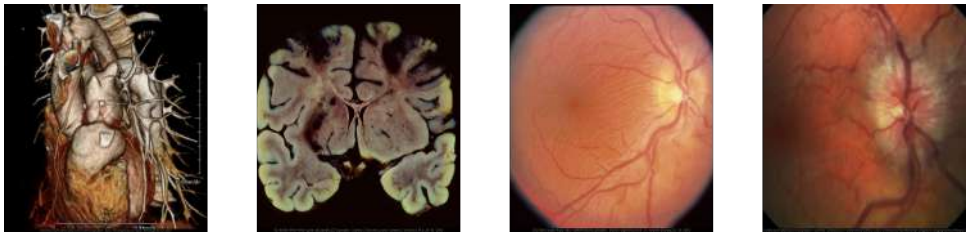


Figure 3.5 – *Digital watermarking applications*



Figure 3.6 – *Digital watermarking applications*

3.5.1 High-fidelity evaluation

The results of the PSNR measurements are shown in Table 3.1 for a variety of quantization factors. Experiments were carried out in order to determine which practical quantization step was the most efficient. $\nabla = 0.4$ is the value of the coefficient that was chosen for this procedure, which ensures satisfactory results in terms of imperceptibility and robustness. The decision was made not just based on the high imperceptibility of the approach but also on the basis of its robustness.

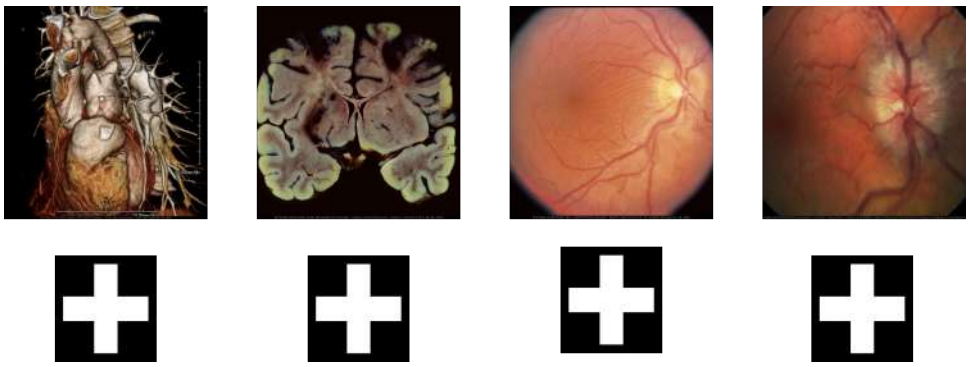


Figure 3.7 – *Digital watermarking applications*

As displayed in Figure 3.7, the watermarked images resulting from the suggested scheme show that the incorporated watermark is invisible, which implies high visual quality. According to Table 3.2, the average PSNR delivered using the embedding step $\nabla = 0.4$ is 38,2 dB, which automatically implies low MSE levels. Moreover, relevant results were provided in terms of structural similarity and normalized correlation, and very low bit error rate values were obtained, which can be easily confirmed by observing the extracted watermarks where no alternation was reported.

Table 3.1 – *PSNR (dB) results using various quantization steps*

Step (∇)	Lena	Pepper	Heart	Brain	Retinitis 1	Retinitis 2
0.1	50.1236	46.1090	49.3278	48.2367	49.0729	49.8012
0.15	46.9143	43.3693	46.6859	45.9393	46.0144	46.7493
0.2	44.5781	41.3380	44.4242	44.0048	43.7813	44.3972
0.25	42.6303	39.7855	42.4947	42.5041	42.0543	42.4289
0.3	41.0747	38.6808	40.9109	41.1629	40.5529	40.8459
0.35	39.7382	37.6197	39.5798	39.8461	39.3006	39.4849
0.4	38.5812	36.7948	38.4307	38.7095	38.1899	38.3257

Table 3.2 – *Results of the proposed watermarking scheme without attacks*

Metric	Lena	Pepper	Heart	Brain	Retinitis 1	Retinitis 2
PSNR	38.5812	36.7948	38.4307	38.7095	38.1899	38.3257
MSE	1.39×10^{-4}	2×10^{-4}	10^{-4}	10^{-4}	10^{-4}	10^{-4}
SSIM	1	1	1	1	1	1
NC	1	0.9905	0.9968	0.9904	1	1
BER	0	0.0029	0	0	0	0

3.5.2 Robustness analysis

Employing the PSNR and MSE as objective measures, the proposed technique's resistance was tested by executing repeated manipulations illustrated by noise, geometrical, filtering, and compression attacks. The Table 3.3 depicts that the suggested method delivers high robustness against several attacks, where the visual quality is adequately maintained as shown in Figure 3.8.

Table 3.3 – *PSNR and MSE values for the watermarked image under attacks*

Metric	PSNR	MSE
Salt & Pepper (density=1%)	24.8276	0.00329
Salt & Pepper (density =5)	18.1044	0.0155
Gaussian noise (mean=0; density =1)	20.1769	0.0096
Gaussian noise (mean=0; density =2)	17.3515	0.0184
Speckle noise (density =1)	25.3927	0.00289
Speckle noise (variance =5)	18.9520	0.0127
Dilatation (5,5)	22.9343	0.00509
Cropping (1:16)	17.1590	0.0192
Rotation (90◦)	17.7789	0.0167
Median Filtering (5,5)	35.0752	0.000311
Median Filtering (3,3)	35.1687	0.000304
JPEG Compression (40)	35.4549	0.000285
JPEG Compression (80)	37.4132	0.000181
JPEG Compression (80) and Salt & Pepper (1)	27.9466	0.00160
JPEG Compression (80) and Gaussian noise (1)	22.6457	0.00544

In general, the aim of a watermarking technique is to make it as difficult as possible for attackers to remove or alter the watermark while still maintaining the visibility and quality of the original content. This condition was satisfied by the suggested method as depicted in Figure 3.9, where the extracted watermarks from several attacks are still recognizable after various attacks, which affirms that the used watermarking technique is rel-

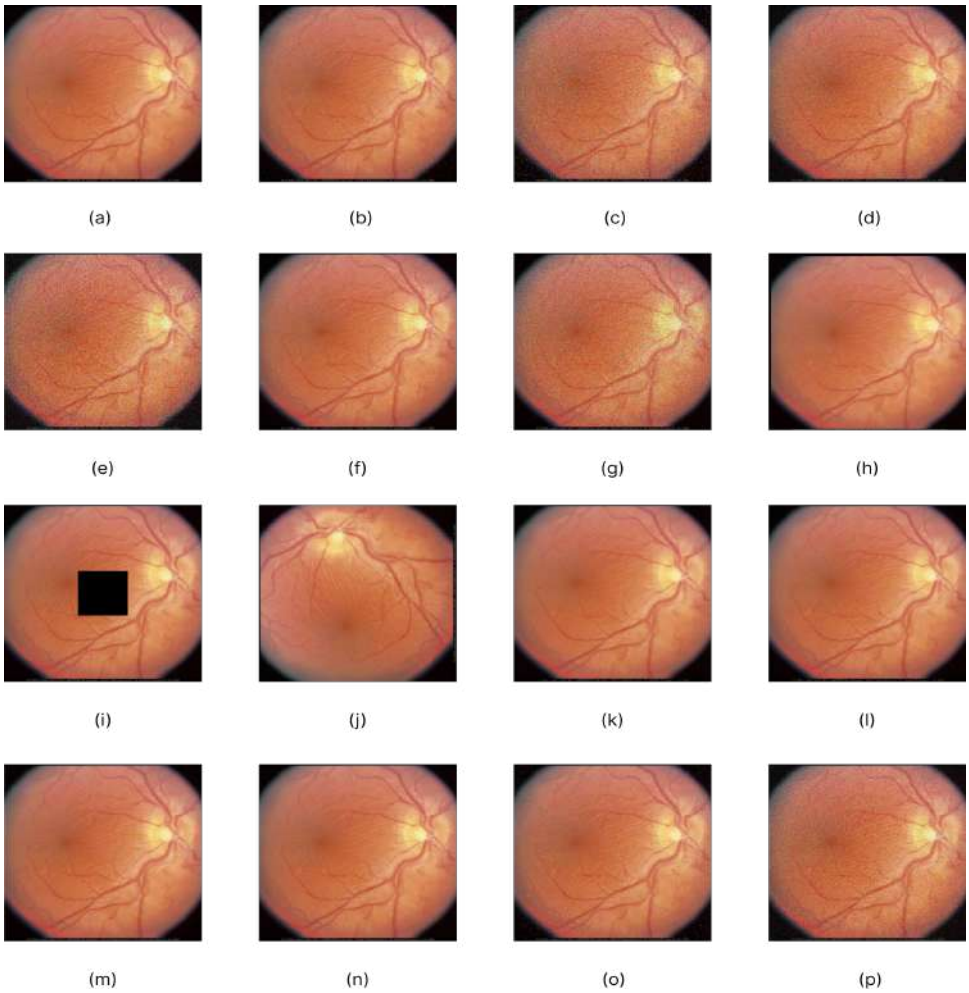


Figure 3.8 – *(a) original host image, (b) Salt & pepper (density=1%), (c) Salt & pepper (density=5%), (d) Gaussian noise (density =1%), (e) Gaussian noise (density =2%), (f) Speckle noise (density =1%), (g) Speckle noise (density =5%), (h) Dilatation (5,5), (i) Cropping (1:16), (j) Rotation (90○), (k) Median Filtering (5,5), (l) Median Filtering (3,3), (m) JPEG Compression (40), (n) JPEG Compression (80), (o) JPEG Compression (80) and Salt & Pepper noise (1%), (p) JPEG Compression (80) and Gaussian noise (1%)*

atively robust and resistant to tampering. Moreover, Table 3.4 depicts the normalized correlation and bit-error rate values supplied as a consequence of many attacks to conclude the usefulness of the current approach, where high NC and low BER values were reported, indicating that extracted watermarks withstand attacks.

Figure 3.10 and Figure 3.11 depict the resilience of the proposed technique when challenged with increasing concentrations of various noises and JPEG compression factors. Under salt & pepper noise, the NC values at 10% and 5% densities are 0.7158 and 0.9149, respectively, which are sufficient to identify the extracted watermark. For speckle noise, ele-

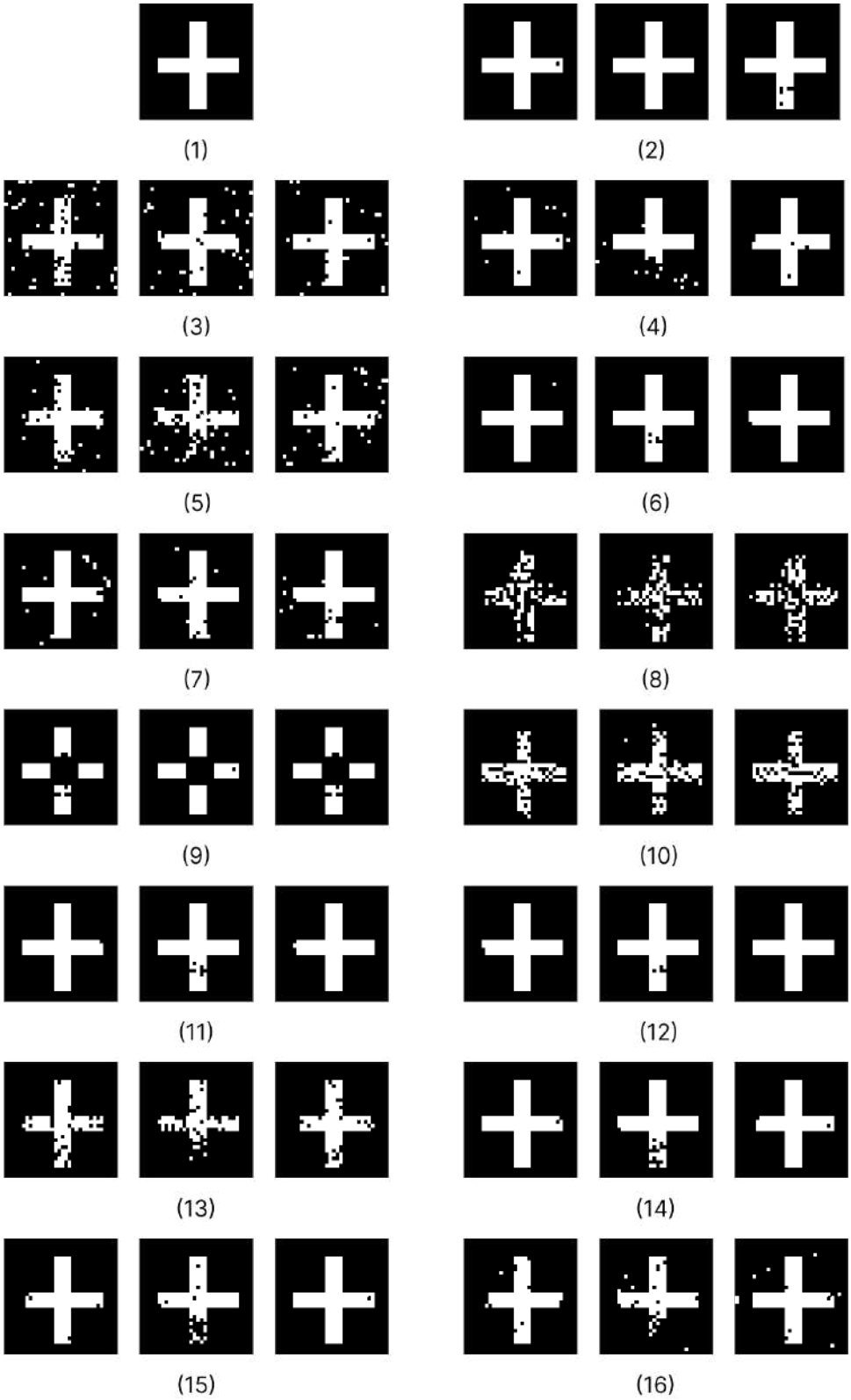


Figure 3.9 – *(1) Original watermark, (2) Salt & pepper (density=1%), (3) Salt & pepper (density=5%), (4) Gaussian noise (density =1%), (5) Gaussian noise (density =2%), (6) Speckle noise (density =1%), (7) Speckle noise (density =5%), (8) Dilatation (5,5), (9) Cropping (1:16), (10) Rotation (90◦), (11) Median Filtering (5,5), (12) Median Filtering (3,3), (13) JPEG Compression (40), (14) JPEG Compression (80), (15) JPEG Compression (80) and Salt & Pepper noise (1%), (16) JPEG Compression (80) and Gaussian noise (1%)*

Table 3.4 – *Findings of the extracted watermark under various types of attacks.*

Attacks	Image	NC	BER
Salt & pepper (density=1%)	Heart	1	0
	Brain	0,9839	0.0049
	Retinitis 1	1	0
Salt & pepper (density =5%)	Heart	0.8811	0.0381
	Brain	0.8182	0.0566
	Retinitis 1	0.9284	0.0225
Gaussian noise (mean=0; density =1%)	Heart	0.9710	0.0088
	Brain	0.8648	0.0400
	Retinitis 1	0.9685	0.0098
Gaussian noise (mean=0; density =2%)	Heart	0.8958	0.0313
	Brain	0.7412	0.0762
	Retinitis 1	0.8949	0.0332
Speckle noise (density =1%)	Heart	0.9968	0.0010
	Brain	0.9839	0.0049
	Retinitis 1	0,9968	0.0010
Speckle noise (variance =5%)	Heart	0.9646	0.0107
	Brain	0.9456	0.0166
	Retinitis 1	0.9506	0.0156
Dilatation (5,5)	Heart	0.4200	0.1533
	Brain	0.4809	0.1377
	Retinitis 1	0.5027	0.1338
Cropping (1:16)	Heart	0.8043	0.0576
	Brain	0.8043	0.0576
	Retinitis 1	0.8250	0.0518
Rotation (90°)	Heart	0.7011	0.0850
	Brain	0.6897	0.0879
	Retinitis 1	0.7053	0.0840
Median Filtering (5,5)	Heart	0.9904	0.0029
	Brain	0.9775	0.0010
	Retinitis 1	0.9968	0
Median Filtering (3,3)	Heart	0.9936	0.0020
	Brain	0.9872	0.0039
	Retinitis 1	1	0
JPEG Compression (40)	Heart	0.8892	0.0332
	Brain	0.7762	0.0654
	Retinitis 1	0.8958	0.0313
JPEG Compression (80)	Heart	0.9807	0.0146
	Brain	0.9516	0.0020
	Retinitis 1	0.9936	0.0020
JPEG Compression (80) and Salt & Pepper (1%)	Heart	0.9743	0.0078
	Brain	0.9057	0.0283
	Retinitis 1	0.9968	0.0010
JPEG Compression (80) and Gaussian noise (1%)	Heart	0.9450	0.0166
	Brain	0.8512	0.0439
	Retinitis 1	0.9617	0.0117

vated results were obtained with an average of 0.97 in terms of the normalized correlation and bit-error rate being approximately null. The suggested technique provided acceptable results for a Gaussian noise attack with an NC average of 0.84 and BER average value of 0.06. In addition to its robustness against noise, the proposed method also showed strong performance when tested against a range of JPEG compression factors. The results demonstrated that the method was able to maintain a high level of performance even at high compression levels. For example, at a compression factor of 30, the normalized correlation value was 0.7548, while at a factor of 40, the NC value was 0.8958, and 0.99 for the rest of the compression factor. This indicates that the method was able to effectively resist JPEG compression and maintain the integrity of the watermarked image even at higher levels of degradation. In general, the method showed low bit error rates across all compression factors, suggesting that it is highly resistant to image degradation. These results confirm that the proposed method has the potential to be used in a variety of real-world applications where image degradation may be a concern.

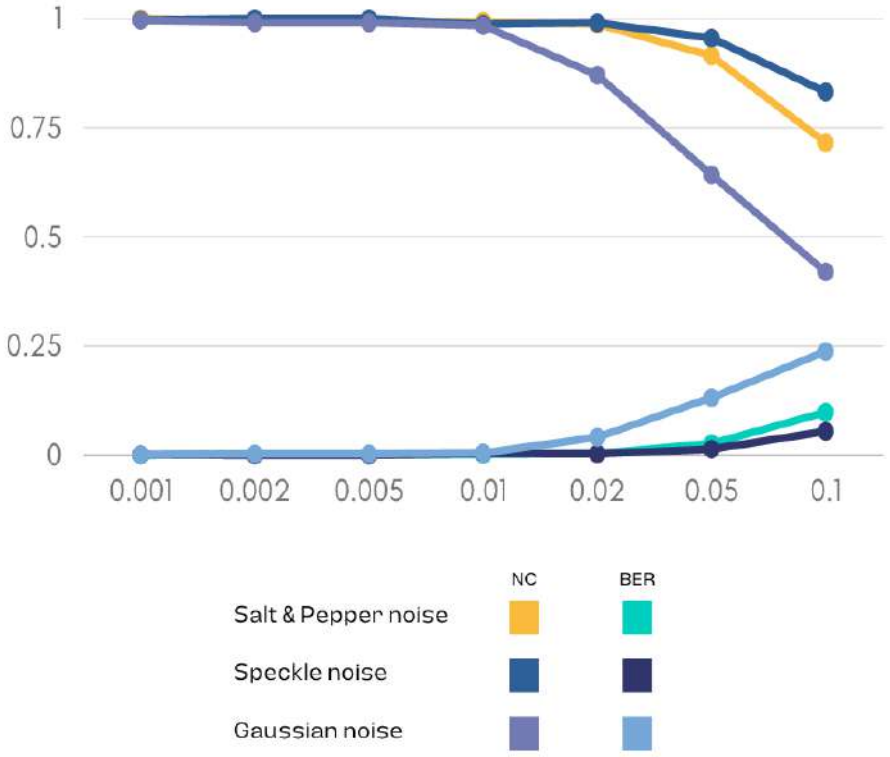


Figure 3.10 – *Digital watermarking applications*

Table 3.5 – *Performance comparison of watermarking techniques in terms of NC and BER under different attack types [Nouioua et al., 2020]*

Attacks	[Singh, 2019]		[Kazemivash and Moghaddam, 2016b]		[Zear et al., 2016]		[Kalra et al., 2013]		[Ariatmanto and Ernawan, 2020]		Proposed method	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
Salt & Pepper noise (1%)	0.80	0	0.96	0.0156	0.7569	0	1	0	0.93	0.0684	1	0
Gaussian noise (1%)	0.61	0.0400	-	-	-	-	0.95	0.081	-	-	0.99	0.0010
Gaussian noise (0.5%)	-	-	0.91	0.0322	-	-	-	-	-	-	1	0
Gaussian noise (0.1%)	-	-	-	-	-	-	-	-	0.99	0.0098	1	0
Speckle noise (1%)	0.88	0	-	-	0.9024	0.1119	1	0	-	-	1	0
Speckle noise (0.5%)	-	-	0.99	0.0010	0.9860	0	-	-	-	-	1	0
Rotation (5°)	0.03	0.4970	-	-	-	-	-	-	0.49	0.5098	0.53	0.1250
Rotation (90°)	-	-	0.10	0.5205	-	-	-	-	-	-	0.71	0.0830
Median filter (3*3)	-	-	0.90	0.0391	0.0025	0	0.77	0.3590	0.99	0.0020	1	0
JPEG (60)	0.95	0	-	-	0.9679	0	0.79	0.3350	1	0	1	0
JPEG (80)	0.98	0	1	0	0.9812	0	1	0	1	0	1	0
JPEG (80) and Salt & Pepper noise (1%)	0.80	0.0057	-	-	-	-	-	-	-	-	1	0
JPEG (80) and Salt & Pepper noise (0.2%)	-	-	-	-	0.9074	0	-	-	-	-	1	0
JPEG (80) and Gaussian noise (1%)	0.89	0	-	-	-	-	-	-	0.99	0.0020	0.99	0.0020
JPEG (80) and Gaussian noise (0.2%)	-	-	-	-	0.8135	0	-	-	-	-	1	0
Salt & Pepper noise (0.3%) and Median filter (3,3)	-	-	-	-	-	-	-	-	0.99	0.0020	1	0

Table 3.5 presents a comparison between the NC and BER findings obtained by the proposed work and those obtained by other methods, including those presented in [Singh, 2019, Kazemivash and Moghaddam, 2016a, Zear et al., 2016, Kalra et al., 2013, Ariatmanto and Ernawan, 2020]. The cover image that was analyzed and compared was of Lena, who served as the standard host for all of the other methods.

This result is identical to the one obtained by the technique [Kalra et al., 2013], which means that it can be noted that the suggested approach has the highest possible resilience to Slat & Pepper noise when the density is set to 1%.

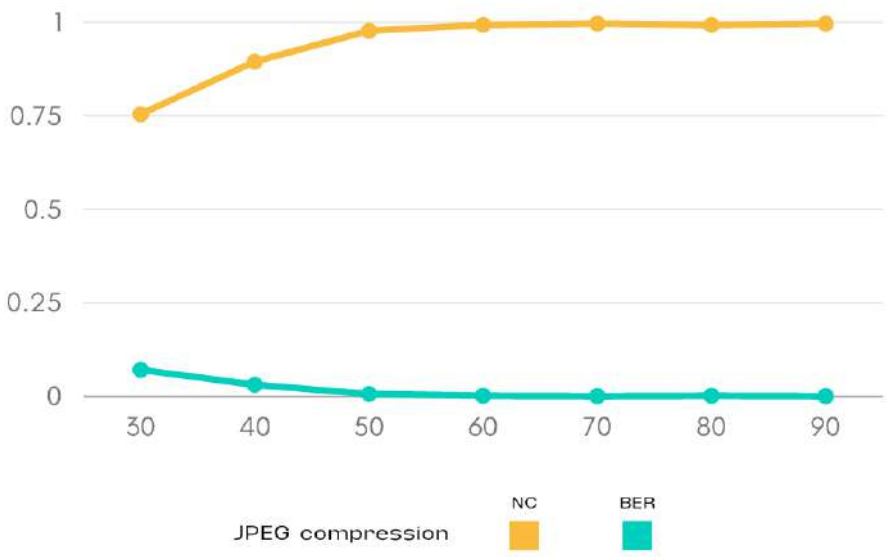


Figure 3.11 – *Digital watermarking applications*

NC values obtained from various Gaussian noise densities are 0.61 and 0.95 for 1% density for the schemes [Singh, 2019, Kazemivash and Moghaddam, 2016a, Zear et al., 2016, Kalra et al., 2013], 0.91 for 0.5% density for the method [Kazemivash and Moghaddam, 2016a], and 0.99 for 0.1% density for the technique [Ariatmanto and Ernawan, 2020]. However, the method at hand offers higher robustness than other techniques that have been previously reported. Compared to other methods, this one gave the most accurate NC results for both ninety-degree rotation angles that were tested.

The experimental findings presented in this section demonstrate that the proposed scheme is capable of withstanding common signal process-

ing operations as well as geometrical attacks. The suggested system has improved resilience, payload capacity, and imperceptibility in comparison to previous comparable watermarking schemes, and as a result, it is particularly well suited for copyright protection due to its acceptable payload capacity. Additionally, the watermark may be recovered from the medical image that has been watermarked without making use of the original cover image, which demonstrates the blind feature of the proposed approach.

3.5.3 Computational cost

Table 3.6 depicts the execution time for embedding and extraction operations of other methods and the proposed structure. In general, it is feasible to demonstrate that the proposed method obtains a high processing speed while simultaneously preserving imperceptibility and durability. The algorithm's usefulness against diverse assaults is shown by its higher performance in comparison to other strategies. Table 6 also displays the speedy computational cost, where the embedding procedure took 0.2244s versus 0.1046s for the retrieval process. The offered data enable to conclude that the suggested methodology represents the most effective, and hence, the proposed technique is applicable to real-world circumstances.

Table 3.6 – *Computational cost comparison [Nouioua et al., 2020]*

Technnique	Embedding	Extraction
[Leung et al., 2012]	2.43	0.92
[Su and Chen, 2017]	0.1948	5.8023
[Malik and Rama Kishore, 2020b]	1.26	3.38
[Zebbiche et al., 2018]	1.6766	0.0269
[Mittal et al., 2020]	0.4071	0.2076
[Ariatmanto and Ernawan, 2020]	0.2188	0.1250
Suggested method	0.2224	0.1046

Conclusion

The research aimed to develop a blind watermarking method for use in medical images that utilizes the dual-tree complex wavelet transform (DTCWT) and the non-subsampled contourlet transform (NSCT). The proposed technique uses binary logos as watermarks and color photographs

of medical conditions as the host images. The proposed method was evaluated in terms of its robustness, imperceptibility, and processing time.

The proposed algorithm was found to be highly resistant to various types of signal processing alterations, such as image cropping, rotation, and noise, thus making it suitable for use in a wide range of applications. The algorithm also demonstrated strong performance when it came to JPEG compression, which is an important consideration when working with medical images. Additionally, the algorithm maintained favorable visual quality, making it suitable for use in clinical contexts. Furthermore, the algorithm was found to have an extremely quick processing time, making it suitable for real-time applications.

In the future, the security of the proposed algorithm will be enhanced by incorporating a strong crypto-system to protect the watermark. This will make the proposed method even more efficient and secure. Overall, the proposed algorithm offers a balance between robustness and imperceptibility, making it suitable for use in a wide range of applications, particularly in the field of medical imaging.

4 Medical Image Watermarking Algorithm using Asymmetric crypto-system and Chaotic Map

Contents

4.1 Introduction . . . 71
4.2 Related works . . . 72
4.3 Technical Background . . . 72
4.3.1 Discrete Cosine Transform . . . 72
4.3.2 Discrete Wavelet Transform . . . 74
4.3.3 El-Gamal crypto-system . . . 75
4.3.4 Arnold Chaotic Map . . . 76
4.4 Methodology . . . 77
4.4.1 Watermark insertion and image encryption . . . 77
4.4.2 Watermark extraction . . . 78
4.5 Experimental Results . . . 78
4.5.1 Fidelity evaluation . . . 79
4.5.2 Robustness evaluation . . . 82
Conclusion . . . 85

This chapter presents a joint encryption-watermarking system for medical image applications based on transform domain and ciphering.

4.1 Introduction

The lightning-fast pace of technological advancement in the medical field, especially in the branch of medical imaging, makes it imperative that the privacy of patients' information be protected. As previously seen in chapter 2, telemedicine is a technique that allows patients to dispatch digital data to professionals through networks [Farncombe and Iniewski, 2017], and it has brought a variety of development benefits to the medical industry. Since each damaged pixel may be mistakenly judged by experts, the sensitivity of medical images may be a substantial limitation during transmission. As a consequence of this, the accuracy of medical images must be maintained at a high level to protect the privacy of patient information while it is being sent across communications channels.

In this study, a transform-domain approach using El-Gamal cryptography and Arnold chaotic mapping for watermarking medical images was provided. This research's major contribution is to present an effective method for securing patient data through Crypto-Watermarking, a hybridization of cryptography and watermarking that yields a secure scheme in which a crypto-system is implemented to ensure property protection while communicating via a watermarking technique. The El-Gamal public key encryption process begins with the DWT deconstruction of the cover picture (medical image), followed by the selection of the approximate sub-band for data integration and the application of the DCT to that sub-band. After inserting the EPR, the unpredictable Arnold map is added. The photo is watermarked using the Inverse Discrete Wavelet Transform (IDWT). And last, to add even more complexity and unpredictability to the process, Arnold's map was applied to the collected watermarked image.

This chapter is organized as follows: Sec. 4.2 describes the related works. Sec. 4.3 highlights the employed transforms and crypto-systems. The approach algorithms are discussed in Sec. 4.4, while Sec. 4.5 reveals the method's findings.

4.2 Related works

Arya et al. came up with a method based on the cascade of lifting wavelet transform and singular value decomposition, which is explained in [Arya et al., 2011]. In this scheme, the watermark is inserted after exerting both LWT second level and SVD on the host image and the watermark in question, respectively. This technique was reported for validation purposes, and the choice of the transformations was due to their ability to reach high robustness levels without affecting image quality. The method's outcomes in terms of high fidelity and attack resilience confirm its strength. A discrete wavelet transform-based technique for image watermarking was reported in [Choudhary and Parmar, 2016]. The core idea is about embedding a low-frequency sub-band of a watermark into the low-frequency sub-band of the cover image delivered by the DWT decomposition, correspondingly employing a visibility factor (embedding factor). As a result, this method provided acceptable imperceptibility results.

4.3 Technical Background

The following is an explanation of the procedures that will be used in the suggested scheme, which are briefly investigated in this section.

4.3.1 Discrete Cosine Transform

In order to transform a signal from spatial to the frequency domain, the DCT serves this operation [Dubolia et al., 2011] [Yang and Jin, 2009], utilizing the cosine waveform, which was first introduced by Ahmed et al. in [Ahmed et al., 1974]. The discrete cosine transform is normally used to process two-dimensional data (e.g., images), where it is often used to generate an image's rectangular array of pixels, which represent the real signal only [Parker, 2017].

DCT is popularly exploited in image compression since it ensures high subjective quality and the image is reconstructed by a minimal number of coefficients [Gupta et al., 2014].

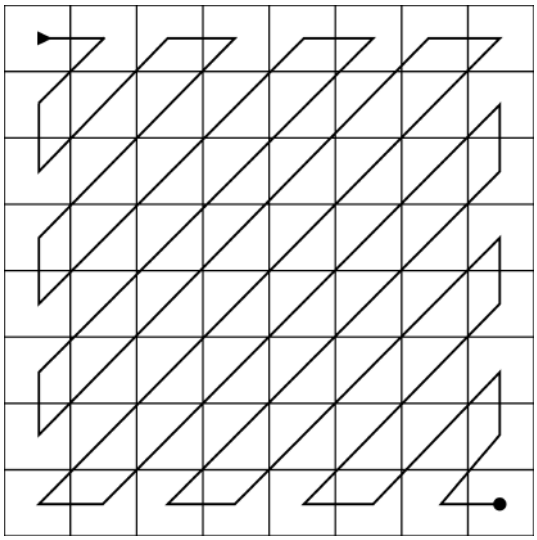


Figure 4.1 – *Discrete Cosine Transform Zig-Zag scan*

$$D(s,r) = \frac{2}{\sqrt{SR}}\alpha(s)\alpha(r)\sum_{p=0}^{s-1}\sum_{q=0}^{R-1} g(p,q) \times \cos\frac{(2p+1)s\pi}{2S} \times \cos\frac{(2q+1)r\pi}{2R} \tag{4.1}$$

$$G(p,q) = \frac{2}{\sqrt{SR}}\sum_{s=0}^{S-1}\sum_{r=0}^{R-1} \alpha(s)\alpha(r)D(p,q) \times \cos\frac{(2p+1)s\pi}{2S} \times \cos\frac{(2q+1)r\pi}{2R} \tag{4.2}$$

$$\alpha(s)\alpha(r) = \begin{cases} 1/\sqrt{2}, & \text{if } s,r = 0 \\ 1, & \text{else} \end{cases} \tag{4.3}$$

The DCT technique could be utilized to perform the transformation on the complete image or non-overlapping portions of a specified size. After a DCT has been conducted, the frequency coefficients of a block may be split into low, middle, and high-frequency sub-bands [Roy and Pal, 2017] by employing a zigzag scan as shown in Figure 4.1. Changing the coefficients in the high-frequency sub-band will not significantly degrade the image quality. In contrast, the low-frequency sub-band is responsible for the bulk of the image, and any modifications to this sub-band would significantly degrade the image quality. When it comes to adding watermark bits, middle-frequency sub-band coefficients are your best chance for producing a high-quality, trustworthy watermarked image [Ko et al., 2020].

4.3.2 Discrete Wavelet Transform

In the frequency domain, there is a transform known as the discrete wavelet transform (DWT), where wavelets with changeable transform frequencies are at the core of their operational idea, and the transform itself may be reversed if necessary. The fact that the discrete wavelet transform is able to deconstruct signals at several scales is the key to its utility, the scales that are employed are selected in line with the specific goals that are being sought [Tang and Zhou, 2022]. The signal is split up into four different sub-bands by the DWT denoted as LL (approximation details), HL (horizontal details), LH (vertical details), and HH (diagonal details), where L and H refer to low and high respectively [Abdullad et al., 2021]. Among the perks of using a multiresolution representation is that it provides an intuitive hierarchical framework for analyzing visual data (see Figure 4.2). At different resolutions, the physical structures of an image are often distinguished by a wide variety of visual characteristics [Mallat, 1989].

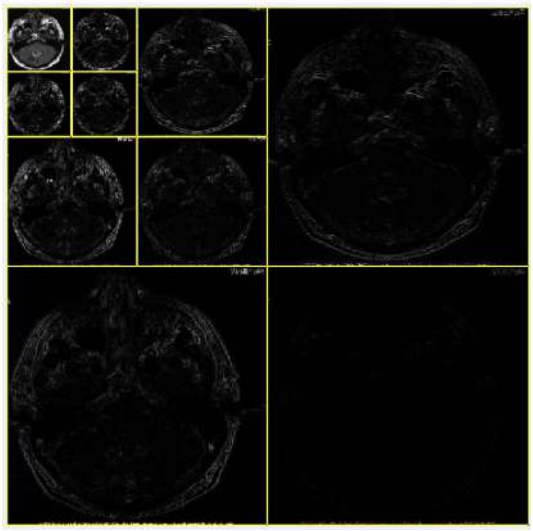


Figure 4.2 – *Discrete Wavelet Transform multilevel resolution*

Moreover, in digital watermarking, the discrete wavelet transform is advantageous due to the psycho-visual masks delivered by the multi-level resolution delivered by this decomposition, which helps in watermarking operations [Fares et al., 2021]. The discrete wavelet transform is given by the following equation 4.4:

$$W(x,y) = (f(t), \psi(x,y)) \tag{4.4}$$

x and y represent scaling and translation factors, respectively, $f(t)$ is the individual signal, whereas (x,y) is the wavelet function. The wavelet transform produces $W(x,y)$.

The sub-band coefficients can be extrapolated using the following equations: 4.5, 4.6, 4.7, and 4.8, where multi-resolution levels could be achieved by reapplying the formulas to each obtained sub-band.

$$LL(x,y) = \frac{p(x,y) + p(x,y+1) + p(x+1,y) + p(x+1,y+1)}{2} \tag{4.5}$$

$$LH(x,y) = \frac{p(x,y) + p(x,y+1) - p(x+1,y) - p(x+1,y+1)}{2} \tag{4.6}$$

$$HL(x,y) = \frac{p(x,y) - p(x,y+1) + p(x+1,y) - p(x+1,y+1)}{2} \tag{4.7}$$

$$HH(x,y) = \frac{p(x,y) - p(x,y+1) + p(x+1,y) - p(x+1,y+1)}{2} \tag{4.8}$$

4.3.3 El-Gamal crypto-system

El-Gamal in 1985 [ElGamal, 1985], based on the works of Diffie and Hellman in [Diffie and Hellman, 1976] presented a probabilistic asymmetric crypto-system that depends on the challenging nature of effectively responding to the discrete logarithm problem [Hwang et al., 2019].

El-Gamal's crypto-system depends on the fact that it is hard to compute the discrete logarithm modulus of large prime numbers. The discrete logarithm issue is one of the most difficult mathematical problems due to its reliance on conjunction to discover all possible answers.

As a consequence, decrypting this encryption system is either almost impossible or requires an astronomically long period [Yousif et al., 2020]. The asymmetric encryption method necessitates that the encryption and decryption keys must be distinct in order to solve key distribution issues related to symmetric crypto-systems [Luo et al., 2019].

The essential phases of the El-Gamal crypto-system: key generation,

encryption, and decryption are described in the following Algorithm algorithm 3.

Algorithm 3 El-Gamal crypto-system

Begin

1. **Key Generation**

- Select a large prime number P to produce a prime order group Z_p
- Pick g a primitive element $g \in Z_P$ and x as a secret key
- Compute the following formula 4.9:

$$y = g^x (\mathrm{mod}\, P) \tag{4.9}$$

- Distribute P, g, y publicly
- Maintain the private key x

2. **Encryption**

- Segment the plain text into blocks $m_1, m_2 \ldots$ where $m \in (0, P)$
- Randomly choose a number r
- Perform the encryption utilizing the equations 4.10 and 4.11

$$C_1 = g^r (\mathrm{mod}\, P) \tag{4.10}$$

$$C_2 = m * y^r (\mathrm{mod}\, P) \tag{4.11}$$

3. **Decryption**

- Recover the plain text by performing the following operation 4.12:

$$m = C_2 * (C_1^{-x}) \bmod P \tag{4.12}$$

End

4.3.4 Arnold Chaotic Map

In [Arnold and Avez, 1968], a pixel shuffling method known as the Arnold chaotic map (ACM) was reported, which consists of pixels' locations changing repeatedly (see Figure 4.3), where original placements can be restored over a certain number of changeovers [Pradhan et al., 2014].

Initial condition sensitivity is the quality of this function, as the results of this dynamical system are dramatically varied depending on even the

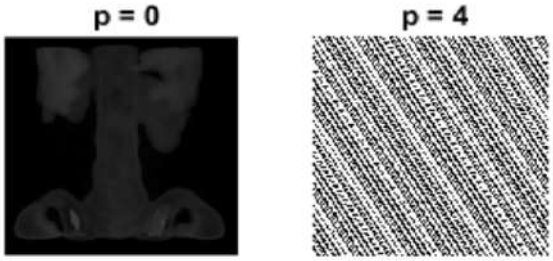


Figure 4.3 – *Arnold Chaotic Map scrambling result*

tiniest initial conditions. The following equations 4.13 and 4.14 represent the Arnold chaotic map mechanisms:

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \quad \begin{bmatrix} i \\ j \end{bmatrix} \bmod N, \text{ where } i', j' \\ i, j = \{0 \dots N-1\} \tag{4.13}$$

To calculate the corresponding inverse of the Arnold chaotic map, the following formula is thus applied:

$$\begin{bmatrix} i \\ j \end{bmatrix} = \left(\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} i' \\ j' \end{bmatrix} + \begin{bmatrix} N \\ N \end{bmatrix} \right) \bmod N \tag{4.14}$$

While i' and j' represent the final locations of the chaotic map pixels permuted coordination, the pixel coordinates of the original image are represented by i and j , and N is the image size.

4.4 Methodology

4.4.1 Watermark insertion and image encryption

Throughout this process (see algorithm 4), the questioned image is a medical image. A DWT of the third level is applied to the image, and then, the DCT is used on the sub-bands acquired following decomposition. In this instance, the patient records are secured using the El-Gamal cryptosystem, the cipher text was shifted using the Arnold chaotic map, and after the cipher text embedding on the DCT result, the Arnold chaotic map was applied to the watermarked image yet again to improve the approach's resilience.

Algorithm 4 Watermark extraction and image decryption

Input: Medical image, text
Output: Encrypted watermarked image
Begin

- Load the medical image and EPR (text)
- Discrete wavelet transform 3^{rd} level application on the host image
- Discrete cosine transform exertion on the sub-band "LL3" obtained from the previous step
- Ciphering the EPR using El-Gamal crypto-system
- Scrambling the cipher EPR denoted "ENC_{EPR}" utilizing Arnold chaotic map
- Cipher text incorporation into low-frequencies of the block named "$DCTLL3$" obtained from the step 3 employing the following formula 4.15:

$$W_{\text{image}} = DCT_{LL3} + \left(10^{-8} \times ENC_{EPR}\right) \tag{4.15}$$

- Applying DCT and DWT inverses respectively to outcome the watermarked image
- Exerting Arnold chaotic map on the watermarked image

End

4.4.2 Watermark extraction

Within this stage, upon applying DCT to the sub-band acquired from the DWT decomposition, the Arnold cat map inverse is conducted on the obtained randomized watermarked image. Then, when the encrypted text is retrieved, an inverse of the Arnold map is used, and then El-Gamal decryption is employed to recover the plain text. More details are revealed in the algorithm 5.

4.5 Experimental Results

A detailed performance analysis of the suggested approach is offered in this section, where the tests demonstrated were employed to illustrate the effectiveness of the suggested watermarking method. The utilized host image shown in Figure 4.4 dimensions of 512 × 512, and the patient records

Algorithm 5 Watermark extraction and decryption

Input: Encrypted image, DCT_{LL3}
Output: EPR
Begin

- Exert inverse Arnold chaotic map on the encrypted image in order to recover the watermarked image
- Discrete wavelet transform 3^{rd} level application on the watermarked image
- Discrete cosine transform exertion on the sub-band "$LL3_{wm}$" obtained from the previous step, the outcome of this step is denoted "DCT_{LL3wm}"
- Encrypted patient records are extracted utilizing the following equation 4.16:

$$\text{Cipher}_{EPR} = (DCT_{LL3wm} - DCT_{LL3}) \times 10^8 \tag{4.16}$$

- The Arnold chaotic map inverse application on the recovered ciphered EPR
- Deciphering the EPR utilizing El-Gamal decryption algorithm

End

are represented with 4387 ASCII characters. A general sample of medical records is depicted in Table 4.1.

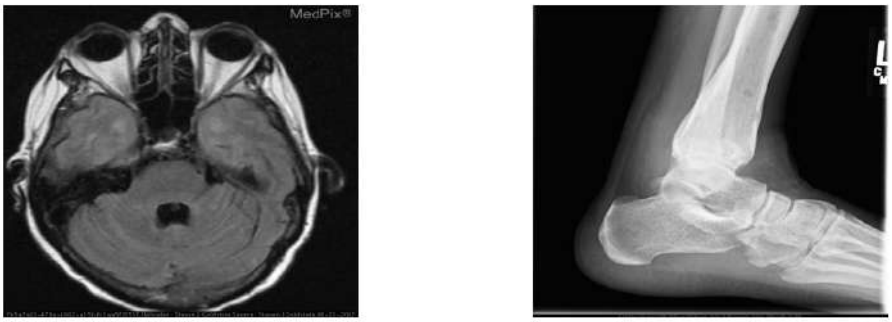


Figure 4.4 – *Medical host images*

4.5.1 Fidelity evaluation

The results of the experiments presented in Table 4.2 demonstrate that the proposed method is successful in achieving high perceptual quality, where, due to the revealed numbers in terms of peak signal-to-noise ratio

Table 4.1 – *Medical patient records sample*

body system	examples of contents
General	Overall feelings of wellness, weight gain or loss, fever, chills, night sweats, fatigue, weakness
Skin	Changes in color, dryness, hair loss, rashes, pruritis, bruising, bleeding
Head	Headaches, trauma, syncope
Eyes	Change in vision (blurry vision, double vision, floaters), trauma, use of corrective lenses
Ears	Change in hearing, tinnitus, vertigo, pain
Nose	Discharge, stuffiness, epistaxis
Mouth	Soreness, gum bleeding, issues with teeth
Throat	Difficulty swallowing, painful swallowing, change in voice
Neck	Pain, stiffness, swelling, lumps
Respiratory system	Shortness of breath, dyspnea, wheezing, cough (dry vs. productive), orthopnea, hemoptysis
Cardiovascular system	Chest pain, palpitations
Gastrointestinal system	Nausea, vomiting, constipation, diarrhea, abdominal pain, hematemesis, melena, hematochezia, jaundice
Genitourinary system	Urinary frequency, urgency, hesitancy, dysuria, hematuria, incontinence, pain Females: Vaginal discharge, discomfort, itching, character of menstrual periods, contraceptive method Males: Erectile dysfunction, lesions, contraceptive method
Nervous system	Seizures, tremors, weakness, altered sensations, difficulties in speech, incoordination
Musculoskeletal system	Pain, trauma, tenderness, swelling, decreased range of motion
Neuropsychiatric system	Changes in mood (anxiety, depression), changes in memory, difficulty sleeping, difficulty concentrating
Endocrine system	Polyuria, polydipsia, polyphagia, intolerance to heat or cold
Peripheral vascular system	Varicose veins, leg cramping, edema

and mean square error, the watermarked image is identical to the original host image (see Figure 4.5), which proves that the suggested technique protects the medical image from any slight impurity that can be misdi-

agnosed by experts in the medical sector. Further, in terms of structural similarity and normalized correlation, the method in hand provided maximal values, which confirms its efficiency, and the results explain that no alteration occurred during the communication process.

Table 4.2 – *High fidelity experiments results*

metrics		PSNR	MSE	SSIM	NC
images	Ankle	inf	0	1	1
	Brain	inf	0	1	1

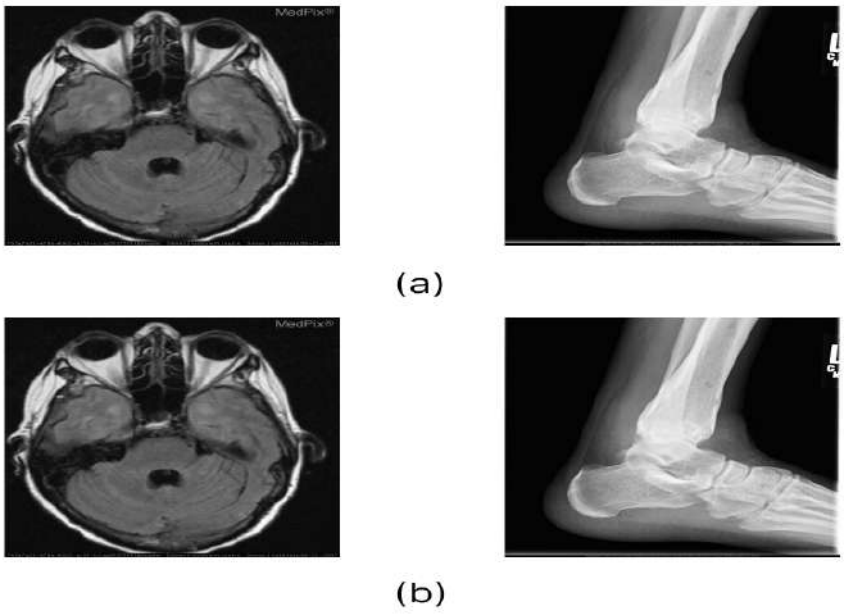


Figure 4.5 – *(a) Original cover images, (b) Watermarked images*

Table 4.3 – *Imperceptibility values comparison*

Technique	PSNR	NC
[Arya et al., 2011]	38	-
[Choudhary and Parmar, 2016]	37.5052	0.9848
Proposed scheme	inf	1

Based on Table 4.3, it is logical to deduce that the suggested scheme reports superior imperceptibility results compared to other technique, which approves the combination of the used transforms DCT-DWT.

4.5.2 Robustness evaluation

According to Table 4.4, the proposed technique reduced prediction and the independence of neighboring pixels, which gives further resilience to analysis-based attacks.

As seen in Figure 4.6, the suggested procedure converts the watermarked medical image into an ambiguous texture that cannot be interpreted by the human visual system. From Figure 4.7, and Figure 4.9, it is comprehensible that there is a high correlation between adjacent pixels of the plain images, where high linearity can be observed, in contrast to the results in Figure 4.8, and Figure 4.10 where the neighboring pixels are less correlated, which gives the cipher image inferior levels of predictability due to the crypto-system and the chaotic map employment.

Table 4.4 – *Correlation Coefficients results*

Correlation Coefficients		Horizontal	Vertical	Diagonal
Ankle	Plain image	0.9974	0.9975	0.9948
	Cipher image	0.1379	-0.3988	-0.2429
Brain	Plain image	0.9899	0.9920	0.9819
	Cipher image	0.1149	-0.0339	0.0514

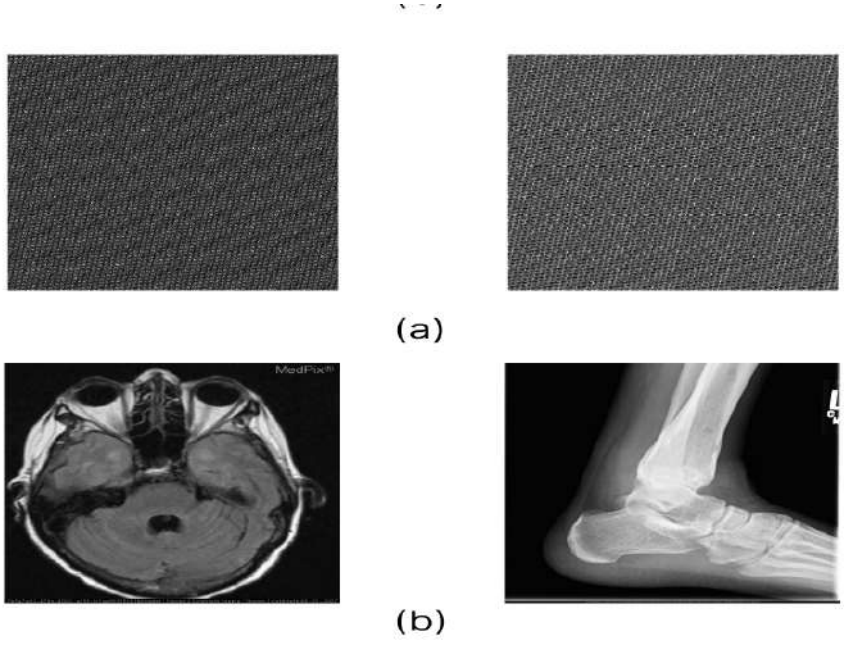


Figure 4.6 – *(a) Shuffled watermarked images, (b) Recovered watermarked images*

Based on Table 4.5, it is pretty fair to assume that the application of the Arnold chaotic map has rendered the incorporated medical records less

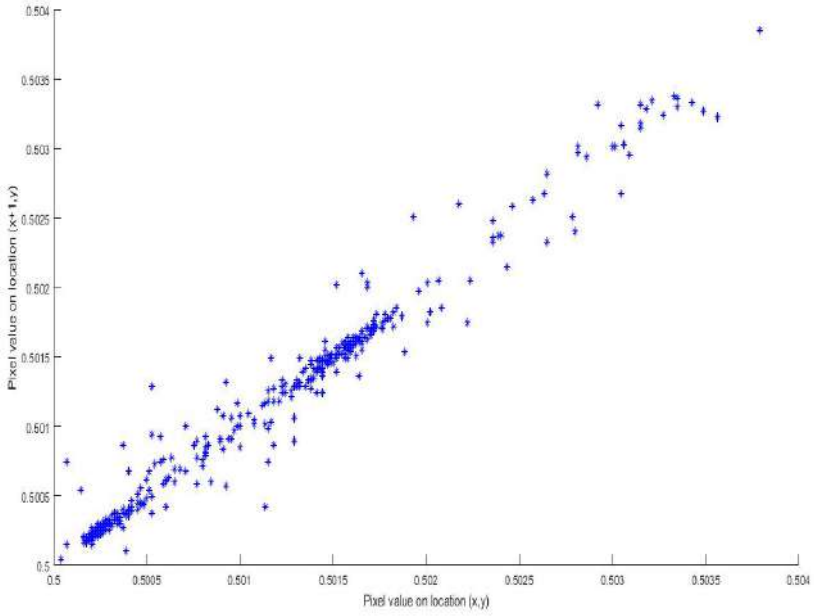


Figure 4.7 – *Correlation Coefficients of plain brain medical image*

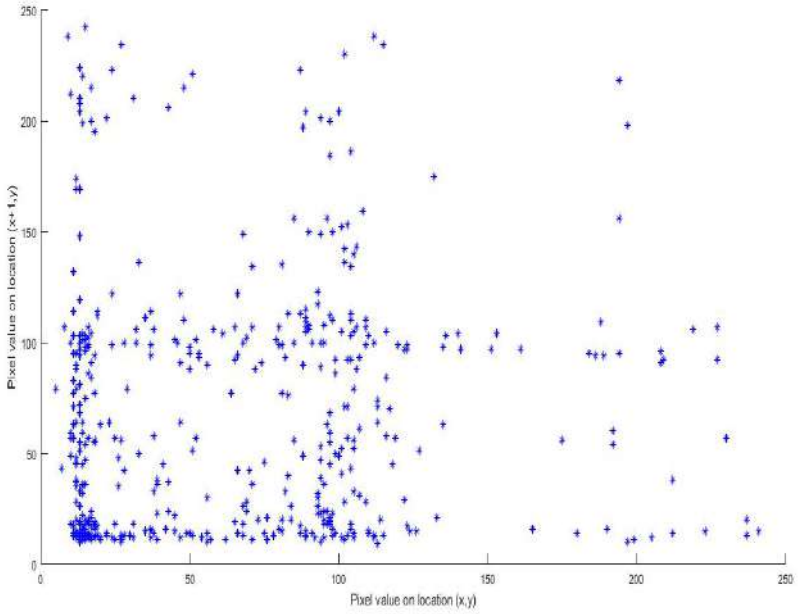


Figure 4.8 – *Correlation Coefficients of cipher brain medical image*

anticipated because of the tremendous scrambling levels that occurred on the cipher text.

Table 4.5 – *Hamming Distance*

ACM Period	16	50	163
Hamming Distance	4.95	4.99	4.98

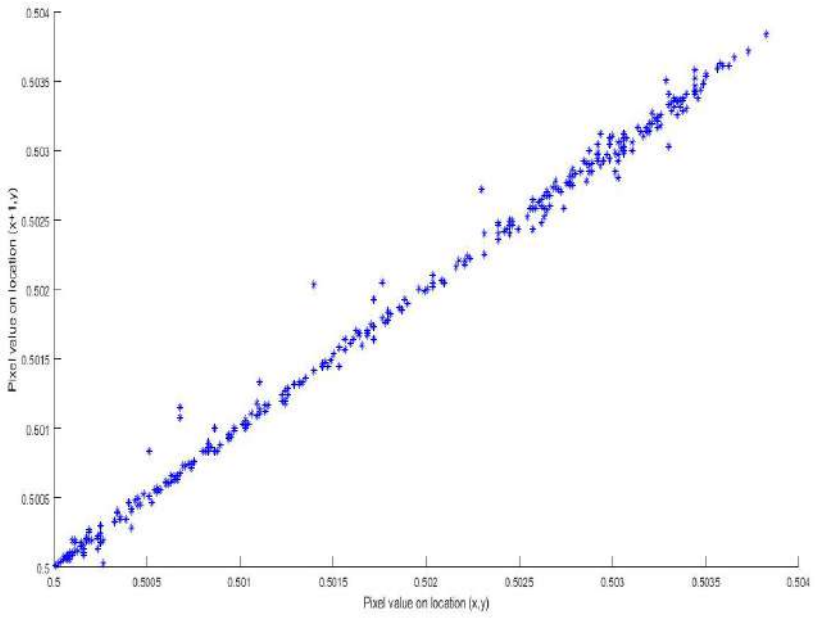


Figure 4.9 – *Correlation Coefficients of plain ankle medical image*

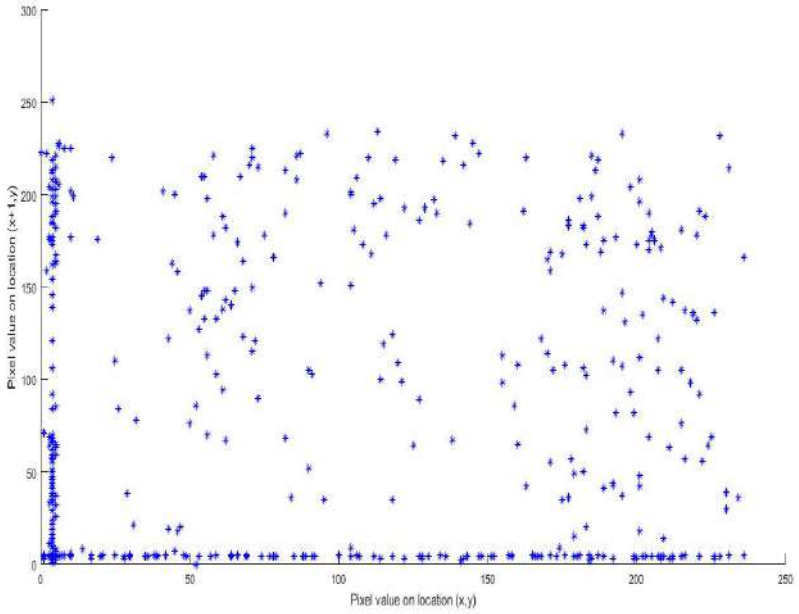


Figure 4.10 – *Correlation Coefficients of cipher ankle medical image*

Observers might certainly mention the resemblance between the watermarked image and the original host image histograms depicted in Figure 4.11, and Figure 4.12 since this demonstrates the soundness of the suggested technique vis-à-vis the analytical tools. The similarity of the histograms validates the algorithm's resilience to different prediction ap-

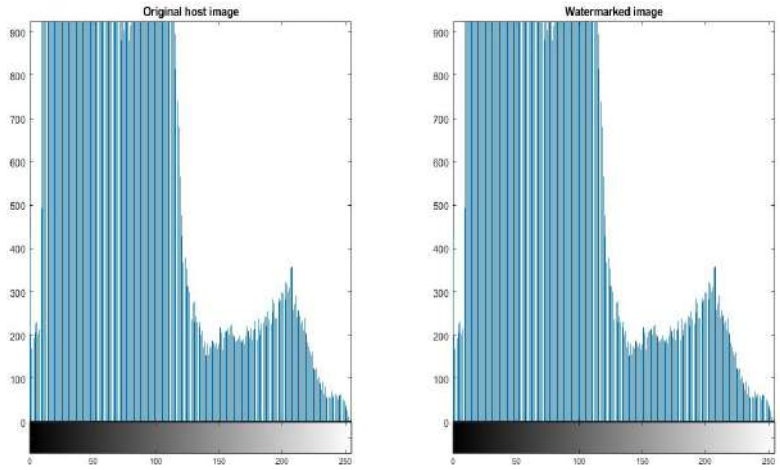


Figure 4.11 – *(a) Original brain image histogram, (b) Watermarked brain image histogram*

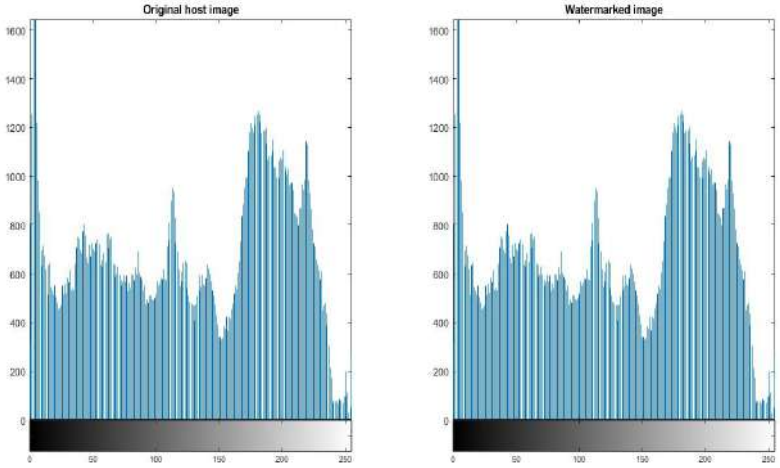


Figure 4.12 – *(a) Original ankle image histogram, (b) Watermarked ankle image histogram*

proaches. Due to this, locating the hidden text is a challenging task. As a brief recap, the proposed mechanism achieved results that affirm the high performances in terms of high fidelity and robustness.

Conclusion

The proposed approach for watermarking medical images in this chapter focuses on the use of transform domain techniques, asymmetric cryptosystems, and Arnold's chaotic map to embed an electronic patient record (EPR) into a medical host image. The process begins by conducting a dis-

crete wavelet transform (DWT) on the medical host image to acquire the approximation sub-band, which is then used to generate a discrete cosine transform (DCT) result. The EPR is then embedded into this DCT result. To further increase security, the El-Gamal crypto-system is used to encrypt the EPR before embedding it in the DCT result. The Arnold cat map is also used to shuffle the watermarked image to increase unpredictability.

The results of this approach demonstrate the effectiveness of the method in terms of imperceptibility and robustness. However, future research may consider incorporating other, more robust cryptographic algorithms in order to provide faster encryption and decryption processes, as well as decreased power and memory consumption and fewer computational resource needs.

In summary, the proposed solution for watermarking medical images combines the use of transform domain techniques, asymmetric crypto-systems, and Arnold's chaotic map to ensure the security and robustness of the electronic patient record. Future research may aim to improve the method by incorporating other, more efficient cryptographic algorithms.

5 Conclusions and Perspectives

Contents

5.1 Conclusion 88
5.2 Future Scope 90

This chapter provides a summary of the main conclusions that can be drawn from the research presented in this thesis. The novelty and limitations of this research are also summarized, along with suggestions for potential future studies.

5.1 Conclusion

This thesis has examined the use of the dual-tree complex wavelet transform (DTCWT) for medical image watermarking, with a focus on protecting the integrity and security of patient data. The DTCWT was chosen for its ability to decompose medical images into frequency sub-bands, allowing for the application of a watermark that is both robust and imperceptible to the human eye. The results of the research demonstrated that the proposed watermarking technique is effective at protecting medical images against various types of attacks while maintaining a high level of visual quality.

Additionally, the potential for hybridization with cryptography was explored as a way to enhance the security of medical images in telemedicine applications. By combining watermarking and cryptography, it is possible to create systems that provide even greater levels of protection for sensitive medical information. This is especially important in the current environment, where the importance of data security and privacy in the healthcare industry is increasingly being recognized. The methods presented in this thesis have the potential to make a significant contribution to the development of secure systems for the protection of medical images and data and may help to increase trust in telemedicine by safeguarding the privacy of patients.

Overall, potential digital image watermarking applications exist in the realm of telemedicine, such as the protection of patient confidentiality, which is crucial to guarantee that sensitive personal information included inside medical images is not tampered with during transmission. This may aid in enhancing the telemedicine field by safeguarding the privacy of patients, which will lead to more system trust in return.

There are several potential benefits to using watermarking in telemedicine:

- Copyright protection: Watermarking can be used to protect the copyright of medical images and prevent unauthorized use or distribution.

- Authenticity and integrity: Watermarking can help to ensure the authenticity and integrity of medical images, which is important for maintaining the accuracy and reliability of diagnoses and treatments.
- Privacy and security: Watermarking can be used to protect the privacy of patient information and to ensure that medical images are not tampered with or altered during transmission.

Additionally, there are also some potential drawbacks to using watermarking in telemedicine:

- Complexity: Implementing watermarking can be complex and may require the use of specialized software or hardware.
- Cost: There may be costs associated with implementing watermarking, including the cost of purchasing software or hardware and the cost of training staff to use it.
- Impact on image quality: Some watermarking techniques may have a negative impact on the quality of the images, which could potentially affect the accuracy of diagnoses and treatments.

In conclusion, this thesis has presented a comprehensive study on the use of blind watermarking methods and cryptography for the secure transfer of medical images in telemedicine applications. Through the development and evaluation of multiple watermarking techniques, it has been demonstrated that these methods can effectively protect medical images against various types of attacks. As well as the technical contributions of this work, the research presented in this thesis has also highlighted the importance of data security and privacy in the healthcare industry and the potential for watermarking and cryptography to play a role in safeguarding sensitive medical information. This is particularly relevant in the current climate, where the use of telemedicine is rapidly expanding and the need for secure systems is more pressing than ever.

In addition, this thesis has made a significant contribution to the field of medical image watermarking and cryptography and has provided a foundation for future research in this area. It is hoped that the findings of this

work will be useful in the development of secure systems for the transfer of medical images in telemedicine and will contribute to the enhancement of trust in this important and rapidly growing field.

5.2 Future Scope

There are several potential directions for future research and development in the area of watermarking for telemedicine applications. One important area of investigation is the development of more robust and secure watermarking techniques that are resistant to a wide range of attacks. These techniques could potentially be used to protect the privacy and security of medical images in telemedicine, and to ensure the authenticity and integrity of the images. Another potential area of research is the optimization of watermarking techniques to minimize the impact on image quality. This could involve finding ways to reduce the visual impact of the watermark or to minimize any degradation of the image quality caused by the watermarking process. Finally, there may be opportunities to investigate new methods for protecting the privacy and security of medical images in telemedicine, such as the use of encryption or other security measures. Overall, further research and development in these areas could help to improve the effectiveness of watermarking in telemedicine and ensure the privacy, security, and integrity of medical images in this context.

Bibliography

(1952). Universal copyright convention. https://portal.unesco.org.

(2011). Recommendation bt.601. https://www.itu.int/rec/R-REC-BT.601.

(2022). U.s. national library of medicine. https://medpix.nlm.nih.gov.

Abdulla, N. T. B. and Navas, K. A. (2020). Robust video watermarking resilient to inadvertent attacks. In *2020 International Conference on Power Electronics and Renewable Energy Applications (PEREA)*, pages 1–5.

Abdullad, M. J., Ismail, A. R., and Abubakar, A. (2021). Analysis of watermarking techniques with wavelet and cosine transform for imperceptibility on image. *2021 18th International Multi-Conference on Systems, Signals amp; Devices (SSD)*.

Aber, J. S., Marzolff, I., Ries, J. B., and Aber, S. E. (2019). Digital image processing and analysis. *Small-Format Aerial Photography and UAS Imagery*, page 191–221.

Abraham, J. and Paul, V. (2012). Imperceptible image indexing using digital watermarking. *Communications in Computer and Information Science*, page 110–116.

Agbaje, M. (2017). *Broadcast monitoring using digital watermarking*.

Ahmadi Mohammad Abadi, A. and Chalechale, A. (2016). Parallelization of a color dct watermarking algorithm using a cuda-based approach. *2016 6th International Conference on Computer and Knowledge Engineering (ICCKE)*.

Ahmed, N., Natarajan, T., and Rao, K. (1974). Discrete cosine transform. *IEEE Transactions on Computers*, C-23(1):90–93.

Al-Gindy, A. and Ghaly, G. (2019). Three levels dwt watermarking technique for color images and watermarks. *International Journal of Recent Technology and Engineering*, 8(3):564–569.

Alahmadi, A. A., Hussain, M., Aboalsamh, H., Muhammad, G., and Bebis, G. (2013). Splicing image forgery detection based on dct and local binary pattern. *2013 IEEE Global Conference on Signal and Information Processing*.

Alkhathami, M., Han, F., and Van Schyndel, R. (2013). Fingerprint image watermarking approach using dtcwt without corrupting minutiae. *2013 6th International Congress on Image and Signal Processing (CISP)*.

Allaf, A. H. and Kbir, M. A. (2019). A review of digital watermarking applications for medical image exchange security. *Innovations in Smart Cities Applications Edition 2*, page 472–480.

AlMutairi, F. and Bonny, T. (2020). Image encryption based on chua chaotic oscillator. In *2020 3rd International Conference on Signal Processing and Information Security (ICSPIS)*, pages 1–4.

AlShaikh, M., Laouamer, L., Laouid, A., Bounceur, A., and Hammoudeh, M. (2019). Robust and imperceptible medical image watermarking based on dijkstra algorithm. *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*.

Amador, J. J. and Green, R. W. (2005). Symmetric-key block cipher for image and text cryptography. *International Journal of Imaging Systems and Technology*, 15(3):178–188.

Ariatmanto, D. and Ernawan, F. (2020). An improved robust image watermarking by using different embedding strengths. *Multimedia Tools and Applications*, 79(17-18):12041–12067.

Arnold, V. I. and Avez, A. (1968). *Ergodic problems of classical mechanics*, volume 9. Benjamin.

Arya, M. S., Siddavatam, R., and Ghrera, S. P. (2011). A hybrid semi-blind digital image watermarking technique using lifting wavelet transform — singular value decomposition. *2011 IEEE INTERNATIONAL CONFERENCE ON ELECTRO/INFORMATION TECHNOLOGY*.

Attari, A. A. and Shirazi, A. A. (2018). Robust audio watermarking algorithm based on dwt using fibonacci numbers. *Multimedia Tools and Applications*, 77(19):25607–25627.

Aubert, G. and Kornprobst, P. (2006). Image processing: Mathematics. *Encyclopedia of Mathematical Physics*, page 1–10.

Baidoo, E. (2018). Implementation of gray level image transformation techniques. *International Journal of Modern Education and Computer Science*, 10(5):44–53.

Baljon, M., Gerritsen, M., Van Rappard, F., Dijk, W., and Van Der Putten, N. (1996). Dicom application profiler for modelling and checking dicom datasets. *Computers in Cardiology 1996*.

Bangerter, N. K., Morrell, G., and Grech-Sollars, M. (2020). Magnetic resonance imaging. *Bioengineering Innovative Solutions for Cancer*, page 163–194.

Begum, M. and Uddin, M. S. (2020). Digital image watermarking techniques: A review. *Information*, 11(2):110.

Benoraira, A., Benmahammed, K., and Boucenna, N. (2015). Blind image watermarking technique based on differential embedding in dwt and dct domains. *EURASIP Journal on Advances in Signal Processing*, 2015(1).

Best, D. E., Horii, S. C., Bennett, W., Thomson, B., and Snavely, D. (1992). Review of the american college of radiology-national electrical manufacturers' association standards activity. *Computer Methods and Programs in Biomedicine*, 37(4):305–309.

Biswas, H. R., Hasan, M., and Bala, S. K. (2020). Chaos theory and its applications in our real life.

Chahal, J. S. and Khurana, S. (2013). A review on digital image watermarking. *International Journal of Emerging Technology and Advanced Engineering*, 3(12):p482–484.

Chaum, D. (1984). *Advances in Cryptology*. Springer, 1 edition.

Chen, J. (2012). *Handbook of Visual Display Technology*. Springer.

Chen, J., Lu, W., Fang, Y., Liu, X., Yeung, Y., and Xue, Y. (2018). Binary image steganalysis based on local texture pattern. *Journal of Visual Communication and Image Representation*, 55:149–156.

Choudhary, R. and Parmar, G. (2016). A robust image watermarking technique using 2-level discrete wavelet transform (dwt). *2016 2nd International Conference on Communication Control and Intelligent Systems (CCIS)*.

Cikes, M., D'hooge, J., and Solomon, S. D. (2019). Physical principles of ultrasound and generation of images. *Essential Echocardiography*.

Cox, I., Miller, M., and Bloom, J. (2000). Watermarking applications and their properties. *Proceedings International Conference on Information Technology: Coding and Computing*.

Craver, S. (1997). *On public-key steganography in the presence of an active warden*. IBM T.J. Watson Research Center.

Da Cunha, A., Zhou, J., and Do, M. (2006). The nonsubsampled contourlet transform: Theory, design, and applications. *IEEE Transactions on Image Processing*, 15(10):3089–3101.

Dale, B. M., Brown, M. A., Semelka, R. C., and Brown, M. A. (2015). *MRI: Basic principles and applications*. John Wiley amp; Sons, Ltd, 5 edition.

de Leeuw, J. G., Wardeh, A., Sramek, A., and van der Wall, E. E. (2007). Pseudo-aortic dissection after primary pci. *Netherlands Heart Journal*, 15(8):265–266.

Diamanti, E., Lo, H.-K., Qi, B., and Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Information*, 2(1).

Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654.

Do, M. and Vetterli, M. (2005). The contourlet transform: An efficient directional multiresolution image representation. *IEEE Transactions on Image Processing*, 14(12):2091–2106.

Dubolia, R., Singh, R., Bhadoria, S. S., and Gupta, R. (2011). Digital image watermarking by using discrete wavelet transform and discrete cosine transform and comparison based on psnr. *2011 International Conference on Communication Systems and Network Technologies*.

Dymarski, P., Lee, H., and Jo, Y. (2018). Audio files protection using logo watermarking, fingerprinting and encryption. *2018 25th International Conference on Systems, Signals and Image Processing (IWSSIP)*.

Ekici, O., Sankur, B., Coskun, B., Naci, U., and Akcay, M. (2004). Comparative evaluation of semifragile watermarking algorithms. *Journal of Electronic Imaging*, 13(1):209.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472.

Evsutin, O. and Dzhanashia, K. (2022). Watermarking schemes for digital images: Robustness overview. *Signal Processing: Image Communication*, 100:116523.

Fares, K., Khaldi, A., Redouane, K., and Salah, E. (2021). Dct amp; dwt based watermarking scheme for medical information security. *Biomedical Signal Processing and Control*, 66:102403.

Farncombe, T. . and Iniewski, K. . (2017). *Medical Imaging: Technology and Applications*. CRC Press/Taylor amp; Francis Group.

Fatima, N. and Tuptewar, D. J. (2016). Comparison of hybrid watermarking technique on different color spaces. *2016 Conference on Advances in Signal Processing (CASP)*.

Feng, B., Lu, W., and Sun, W. (2015). Secure binary image steganography based on minimizing the distortion on the texture. *IEEE Transactions on Information Forensics and Security*, 10(2):243–255.

Feng, B., Weng, J., Lu, W., and Pei, B. (2017). Steganalysis of content-adaptive binary image data hiding. *Journal of Visual Communication and Image Representation*, 46:119–127.

Garg, P. and Kishore, R. R. (2020). Performance comparison of various watermarking techniques. *Multimedia Tools and Applications*, 79(35-36):25921–25967.

Ghaz, A., Kpalma, K., and Bounoua, A. (2014). Nsct edge enhancement for sift key points extraction. *IOSR journal of VLSI and Signal Processing*, 4(2):84–90.

Girdhar, A., Kapur, H., and Kumar, V. (2021). A novel grayscale image encryption approach based on chaotic maps and image blocks. *Applied Physics B*, 127(3).

Gogia, S. (2020). *Fundamentals of telemedicine and telehealth*. Elsevier/Academic Press.

Gonzalez, R. C. and Woods, R. E. (2008). *Digital Image Processing*. Prentice Hall, 3ed edition.

Gupta, A., Walia, E., and Vaidya, M. (2014). feature level fusion of palm print and fingerprint modalities using discrete cosine transform;. *2014 International Conference on Advances in Engineering amp; Technology Research (ICAETR - 2014)*.

Guzman, S. and Brienza, D. (2020). Ultrasound and magnetic resonance imaging methods for determining pressure injury risk. *Innovations and Emerging Technologies in Wound Care*, page 21–39.

Hamadou, A., Camara, L., Issaka Hassane, A. A., and Naroua, H. (2020). Reversible fragile watermarking scheme for relational database based on prediction-error expansion. *Mathematical Problems in Engineering*, 2020:1–9.

Hosam, O. (2019). Attacking image watermarking and steganography a survey. *International Journal of Information Technology and Computer Science*, 11(3):23–37.

Hwang, M.-S., Lee, C.-C., and Hsu, S.-T. (2019). An elgamal-like secure channel free public key encryption with keyword search scheme. *International Journal of Foundations of Computer Science*, 30(02):255–273.

Ibraheem, N. A., Hasan, M. M., Khan, R. Z., and Mishra, P. K. (2012). Understanding color models: A review.

Joseph, H. and Rajan, B. K. (2020). Image security enhancement using dct amp; dwt watermarking technique. *2020 International Conference on Communication and Signal Processing (ICCSP)*.

Jung, K.-H. (2017). Authenticable reversible data hiding scheme with less distortion in dual stego-images. *Multimedia Tools and Applications*, 77(5):6225–6241.

Kadian, P., Arora, S. M., and Arora, N. (2021). Robust digital watermarking techniques for copyright protection of digital data: A survey. *Wireless Personal Communications*, 118(4):3225–3249.

Kalra, G., Talwar, R., and Sadawarti, H. (2013). Digital image watermarking in frequency domain using ecc and dual encryption technique. *Research Journal of Applied Sciences, Engineering and Technology*, 6(18):3365–3371.

Kamalian, S., Lev, M. H., and Gupta, R. (2016). Computed tomography imaging and angiography – principles. *Handbook of Clinical Neurology*, page 3–20.

Kanocz, T., Tokar, T., and Levicky, D. (2009). Robust frame by frame video watermarking resistant against collusion attacks. *2009 19th International Conference Radioelektronika*.

Karmakar, A., Phadikar, A., Phadikar, B. S., and Maity, G. K. (2016). A blind video watermarking scheme resistant to rotation and collusion attacks. *Journal of King Saud University - Computer and Information Sciences*, 28(2):199–210.

Kazemivash, B. and Moghaddam, M. E. (2016a). A robust digital image watermarking technique using lifting wavelet transform and firefly algorithm. *Multimedia Tools and Applications*, 76(20):20499–20524.

Kazemivash, B. and Moghaddam, M. E. (2016b). A robust digital image watermarking technique using lifting wavelet transform and firefly algorithm. *Multimedia Tools and Applications*, 76(20):20499–20524.

Kirch, W., editor (2008). *Telemedicine*, pages 1384–1385. Springer Netherlands, Dordrecht.

Ko, H.-J., Huang, C.-T., Horng, G., and WANG, S.-J. (2020). Robust and blind image watermarking in dct domain using inter-block coefficient correlation. *Information Sciences*, 517:128–147.

Krusche, M. (2022). Telemedicine: A solution for everyone? *Nature Reviews Rheumatology*.

Kumar, A. (2019). A review on implementation of digital image watermarking techniques using lsb and dwt. *Information and Communication Technology for Sustainable Development*, page 595–602.

Kumar, C., Singh, A., Kumar, P., Singh, R., and Singh, S. (2018). Spiht-based multiple image watermarking in nsct domain. *Concurrency and Computation: Practice and Experience*, 32(1).

Kumar, C., Singh, A. K., and Kumar, P. (2017). A recent survey on image watermarking techniques and its application in e-governance. *Multimedia Tools and Applications*, 77(3):3597–3622.

Kumar, C. A. and Rajendra Naik, B. (2019). A new encrypted image watermarking based on dtcwt and random pixel exchange. *2019 5th International Conference on Advanced Computing amp; Communication Systems (ICACCS)*.

Lan, T.-H. and Tewfik, A. H. (1999). Fraud detection and self embedding. *Proceedings of the seventh ACM international conference on Multimedia (Part 2) - MULTIMEDIA '99*.

Ledley, R., Buas, M., and Golab, T. (1990). Fundamentals of true-color image processing.

Leung, H. Y., Cheng, L. M., and Liu, F. (2012). Robust digital image watermarking scheme using wave atoms with multiple description coding. *EURASIP Journal on Advances in Signal Processing*, 2012(1).

Lian, S., Liu, Z., Dong, Y., and Wang, H. (2008). On the joint audio fingerprinting and decryption scheme. *2008 IEEE International Conference on Multimedia and Expo*.

Lin, C.-Y., Wu, M., Bloom, J., Cox, I., Miller, M., and Lui, Y. (2001). Rotation, scale, and translation resilient watermarking for images. *IEEE Transactions on Image Processing*, 10(5):767–782.

Liu, D., Su, Q., Yuan, Z., and Zhang, X. (2021). A blind color digital image watermarking method based on image correction and eigenvalue decomposition. *Signal Processing: Image Communication*, 95:116292.

Liu, J., Li, J., Ma, J., Sadiq, N., Bhatti, U., and Ai, Y. (2019). A robust multi-watermarking algorithm for medical images based on dtcwt-dct and henon map. *Applied Sciences*, 9(4):700.

Lukac, R. and Plataniotis, K. N. (2007). *Color image processing: Methods and applications*. CRC/Taylor amp; Francis.

Luo, Y., Ouyang, X., Liu, J., and Cao, L. (2019). An image encryption method based on elliptic curve elgamal encryption and chaotic systems. *IEEE Access*, 7:38507–38522.

Maitine, B. (2015). *Introduction au traitement mathematique des images - methodes deterministes*. Springer.

Malik, S. and Rama Kishore, R. (2020a). Spiking neural network based scrambled watermark hiding in low-frequency region of digital image. *Journal of Information and Optimization Sciences*, 41(2):437–459.

Malik, S. and Rama Kishore, R. (2020b). Spiking neural network based scrambled watermark hiding in low-frequency region of digital image. *Journal of Information and Optimization Sciences*, 41(2):437–459.

Mallat, S. (1989). A theory for multiresolution signal decomposition: The wavelet representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 11(7):674–693.

Matthews, R. (1989). On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, 13(1):29–42.

Maxwell, J. C. (1857). 1. experiments on colour as perceived by the eye, with remarks on colour-blindness. *Proceedings of the Royal Society of Edinburgh*, 3:299–301.

Maxwell, J. C. (1860). Iv. on the theory of compound colours, and the relations of the colours of the spectrum. *Philosophical Transactions of the Royal Society of London*, 150:57–84.

Menezes, A. J., Vanstone, S. A., and C., V. O. P. (1997). *Handbook of Applied Cryptology*. CRC.

Mestiri, A., Kricha, A., Sakly, A., and Mtibaa, A. (2017). Watermarking for integrity, authentication and security of medical imaging. *2017 14th International Multi-Conference on Systems, Signals Devices (SSD)*.

Mihailescu, M. and Nita, S. L. (2020). *Pro Cryptography and Cryptanalysis: Creating Advanced Algorithms with C and .NET*. Apress, 1 edition.

Mihailescu, M. I. and Nita, S. L. (2021). *Cryptography and Cryptanalysis in MATLAB*. Apress, 1 edition.

Mittal, M., Kaushik, R., Verma, A., Kaur, I., Goyal, L. M., Roy, S., and Kim, T.-h. (2020). Image watermarking in curvelet domain using edge surface blocks. *Symmetry*, 12(5):822.

Mohamed, K. S. (2020). *New frontiers in cryptography: Quantum, blockchain, lightweight, chaotic and DNA*. Springer.

Mohanty, S. P., Sengupta, A., Guturu, P., and Kougianos, E. (2017). Everything you want to know about watermarking: From paper marks to hardware protection: From paper marks to hardware protection. *IEEE Consumer Electronics Magazine*, 6(3):83–91.

Mousavi, S. M., Naghsh, A., and Abu-Bakar, S. A. (2014). Watermarking techniques used in medical images: A survey. *Journal of Digital Imaging*, 27(6):714–729.

Nam, S.-H., Mun, S.-M., Ahn, W., Kim, D., Yu, I.-J., Kim, W.-H., and Lee, H.-K. (2020). Nsct-based robust and perceptual watermarking for dibr 3d images. *IEEE Access*, 8:93760–93781.

Nin, J. and Ricciardi, S. (2013). Digital watermarking techniques and security issues in the information and communication society. *2013 27th International Conference on Advanced Information Networking and Applications Workshops*.

Nouioua, N., Seddiki, A., and Ghaz, A. (2020). Blind digital watermarking framework based on dtcwt and nsct for telemedicine application. *Traitement du Signal*, 37(6):955–964.

Parker, M. (2017). Dct, entropy, predictive coding, and quantization. *Digital Signal Processing 101*, page 311–327.

Paulsen, R. R. and Moeslund, T. B. (2020). *Introduction to medical image analysis*. Springer Nature, 1st edition.

Payán, D. D., Frehn, J. L., Garcia, L., Tierney, A. A., and Rodriguez, H. P. (2022). Telemedicine implementation and use in community health centers during covid-19: Clinic personnel and patient perspectives. *SSM - Qualitative Research in Health*, 2:100054.

Plataniotis, K. N. and Venetsanopoulos, A. N. (2011). *Color image processing and applications*. Springer.

Pradhan, C., Saha, B. J., Kabi, K. K., Arun, and Bisoi, A. K. (2014). Blind watermarking techniques using dct and arnold 2d cat map for color images. *2014 International Conference on Communication and Signal Processing*.

Radharani, S. and Valarmathi, M. (2010). A study on watermarking schemes for image authentication. *International Journal of Computer Applications*, 2(4):24–32.

Rana, R., Thangjam, S., and Singh, S. (2017). Performance analysis of video watermarking in transform domain using differential embedding. *Information and Communication Technology for Intelligent Systems (ICTIS 2017) - Volume 1 Smart Innovation, Systems and Technologies*, page 566–574.

Rani, B. U., Praveena, B., and Ramanjaneyulu, K. (2015). Literature review on digital image watermarking. *Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering amp; Technology (ICARCSET 2015) - ICARCSET '15*.

Roy, S. and Pal, A. K. (2017). A blind dct based color watermarking algorithm for embedding multiple watermarks. *AEU - International Journal of Electronics and Communications*, 72:149–161.

Sharma, G., Kumar, V., and Chaudhary, K. (2021). Authentication of digital media using reversible watermarking. *Lecture Notes on Data Engineering and Communications Technologies*, page 53–64.

Shih, F. Y. (2017). *Digital Watermarking and steganography: Fundamentals and techniques*. CRC Press.

Singh, A. K. (2019). Robust and distortion control dual watermarking in lwt domain using dct and error correction code for color medical image. *Multimedia Tools and Applications*, 78(21):30523–30533.

Singh, A. K., Dave, M., and Mohan, A. (2014). Wavelet based image watermarking: Futuristic concepts in information security. *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences*, 84(3):345–359.

Singh, A. K., Kumar, B., Singh, G., and Mohan, A. (2017). *Medical image watermarking: techniques and applications*. Springer.

Singh, B. and Sharma, M. (2021). Tamper detection technique for document images using zero watermarking in wavelet domain. *Computers Electrical Engineering*, 89:106925.

Su, Q. and Chen, B. (2017). Robust color image watermarking technique in the spatial domain. *Soft Computing*, 22(1):91–106.

Sunesh, H. K. (2011). Watermark attacks and applications in watermarking. In *National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC)*. Citeseer.

Symonds, E. M. (1992). *Magnetic Resonance Imaging in Obstetrics and Gynaecology*. Butterworth-Heinemann.

Szabo, T. L. (2014). *Diagnostic Ultrasound Imaging: Inside out*. Elsevier/AP, Academic Press is an imprint of Elsevier.

Tang, M. and Zhou, F. (2022). A robust and secure watermarking algorithm based on dwt and svd in the fractional order fourier transform domain. *Array*, 15:100230.

Taylor-Gjevre, R., Nair, B., Bath, B., Okpalauwaekwe, U., Sharma, M., Penz, E., Trask, C., and Stewart, S. A. (2017). Addressing rural and remote access disparities for patients with inflammatory arthritis through video-conferencing and innovative inter-professional care models. *Musculoskeletal Care*, 16(1):90–95.

Tefas, A., Nikolaidis, N., and Pitas, I. (2009). Image watermarking. *The Essential Guide to Image Processing*, page 597–648.

Thabit, R. and Khoo, B. E. (2014). Robust reversible watermarking scheme using slantlet transform matrix. *Journal of Systems and Software*, 88:74–86.

Thongkor, K. and Amornraksa, T. (2012). Digital image watermarking for photo authentication in thai national id card. *2012 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*.

Toennies, K. D. (2012). *Guide to medical image analysis methods and algorithms*. Springer London.

Tomasz, Z. (2021). *Starting digital signal processing in Telecommunication Engineering: A laboratory-based course*. Springer.

Wang, W., Ning, Y., Hu, Y., and Yang, Y. (2019a). Research on a digital watermarking algorithm for color image based on dual-tree complex

wavelet transform (dtcwt). *2019 2nd World Conference on Mechanical Engineering and Intelligent Manufacturing (WCMEIM)*.

Wang, X.-y., Wen, T.-t., Shen, X., Niu, P.-p., and Yang, H.-y. (2020). A new watermark decoder in dnst domain using singular values and gaussian-cauchy mixture-based vector hmt. *Information Sciences*, 535:81–106.

Wang, X.-y., Zhang, S.-y., Wen, T.-t., Yang, H.-y., and Niu, P.-p. (2019b). Coefficient difference based watermark detector in nonsubsampled contourlet transform domain. *Information Sciences*, 503:274–290.

Wattjes, M. P. and Fischer, D. (2013). *Neuromuscular imaging*. Springer.

Weinreb, J. C. and Redman, H. C. (1987). *Magnetic Resonance Imaging*. Saunders.

Weinstein, R. S., Lopez, A. M., Joseph, B. A., Erps, K. A., Holcomb, M., Barker, G. P., and Krupinski, E. A. (2014). Telemedicine, telehealth, and mobile health applications that work: Opportunities and barriers. *The American Journal of Medicine*, 127(3):183–187.

Xu, C. and Ge, Y. (2009). The public key encryption to improve the security on wireless sensor networks. *2009 Second International Conference on Information and Computing Science*.

Yadav, J. and Sehra, K. (2018). Large scale dual tree complex wavelet transform based robust features in pca and svd subspace for digital image watermarking. *Procedia Computer Science*, 132:863–872.

Yang, W.-M. and Jin, Z. (2009). A watermarking algorithm based on wavelet and cosine transform for color image. *2009 First International Workshop on Education Technology and Computer Science*.

Yao, Y., Zhang, W., Wang, H., Zhou, H., and Yu, N. (2019). Content-adaptive reversible visible watermarking in encrypted images. *Signal Processing*, 164:386–401.

Ye, G., Pan, C., Huang, X., and Mei, Q. (2018). An efficient pixel-level chaotic image encryption algorithm. *Nonlinear Dynamics*, 94(1):745–756.

Yousif, S. F., Abboud, A. J., and Radhi, H. Y. (2020). Robust image encryption with scanning technology, the el-gamal algorithm and chaos theory. *IEEE Access*, 8:155184–155209.

Yusof, Y. and Khalifa, O. O. (2007). Digital watermarking for digital images using wavelet transform. *2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*.

Zear, A., Singh, A. K., and Kumar, P. (2016). A proposed secure multiple watermarking technique based on dwt, dct and svd for application in medicine. *Multimedia Tools and Applications*, 77(4):4863–4882.

Zebbiche, K., Khelifi, F., and Loukhaoukha, K. (2018). Robust additive watermarking in the dtcwt domain based on perceptual masking. *Multimedia Tools and Applications*, 77(16):21281–21304.

Zhou, X., Ma, Y., Zhang, Q., Mohammed, M. A., and Damasevicius, R. (2021). A reversible watermarking system for medical color images: Balancing capacity, imperceptibility, and robustness. *Electronics*, 10(9):1024.

Abstract

In the digital era, watermarking and encryption have become more vital for the security of information and intellectual property. The process of watermarking includes the incorporation of a digital signature or identifying mark into a digital image, audio file, or other forms of digital material. This symbol may be employed to authenticate the content's validity and identify any unlawful misuse. In contrast, cryptography involves encrypting information to prevent unauthorized access. Significant advancements regarding the application of digital watermarking in telemedicine were developed in this thesis. The most significant contribution is a system for blind digital watermarking based on the Dual-Tree Complex Wavelet Transform (DTCWT) and the Non-Subsampled Contourlet Transform (NSCT). This framework aims to provide a secure and trustworthy way for safeguarding the validity and integrity of medical images in telemedicine. The second contribution is a transform-domain medical image watermarking strategy based on the ElGamal asymmetric cryptosystem and the Arnold chaotic map. This strategy attempts to increase the resilience and security of the digital watermarking technology by encrypting and embedding the watermark in medical images using a combination of cryptographic and chaotic techniques. These contributions provide an integrated method for digital watermarking in telemedicine that addresses the issues of protecting medical images and intellectual property rights while enhancing the accuracy of telemedicine services.

Keywords: Arnold chaotic system, Authenticity, Cryptography, DCT, DTCWT, Digital watermarking, DWT, ElGamal crypto-system, Information hiding, Intellectual property rights, Medical images, NSCT, Telemedicine, Unauthorized copying.

Résumé

À l'ère numérique, le filigrane et le cryptage sont devenus plus vitaux pour la sécurité des informations et de la propriété intellectuelle. Le processus de filigrane comprend l'incorporation d'une signature numérique ou d'une marque d'identification dans une image numérique, un fichier audio ou d'autres formes de matériel numérique. Ce symbole peut être utilisé pour authentifier la validité du contenu et identifier tout abus illégal. En revanche, la cryptographie implique le cryptage des informations pour empêcher tout accès non autorisé. Des avancées significatives concernant l'application du tatouage numérique en télémédecine ont été développées dans cette thèse. La contribution la plus importante est un système de filigrane numérique aveugle basé sur la transformée en ondelettes complexe à double arbre (DTCWT) et la transformée de contourlet non sous-échantillonnée (NSCT). Ce cadre vise à fournir un moyen sûr et fiable pour sauvegarder la validité et l'intégrité des images médicales en télémédecine. La deuxième contribution est une stratégie de tatouage d'images médicales à domaine transformé basée sur le cryptosystème asymétrique ElGamal et la carte chaotique d'Arnold. Cette stratégie tente d'augmenter la résilience et la sécurité de la technologie de filigrane numérique en cryptant et en incorporant le filigrane dans les images médicales à l'aide d'une combinaison de techniques cryptographiques et chaotiques. Ces contributions fournissent une méthode intégrée pour le tatouage numérique en télémédecine qui répond aux problèmes de protection des images médicales et des droits de propriété intellectuelle tout en améliorant la précision des services de télémédecine.

Mots clefs : Système chaotique Arnold, Authenticité, Cryptographie, DCT, DTCWT, Filigrane numérique, DWT, Crypto-système ElGamal, Dissimulation d'informations, Droits de propriété intellectuelle, Images médicales, NSCT, Télémédecine, Copie non autorisée.

الملخص

في العصر الرقمي ، أصبحت العلامات المائية والتشفير أكثر أهمية لأمن المعلومات والملكية الفكرية. تتضمن عملية العلامة المائية دمج توقيع رقمي أو علامة تعريف في صورة رقمية أو ملف صوتي أو أشكال أخرى من المواد الرقمية. يمكن استخدام هذا الرمز للمصادقة على صلاحية المحتوى وتحديد أي إساءة استخدام غير قانونية. في المقابل ، يتضمن التشفير تشفير المعلومات لمنع الوصول غير المصرح به. تم تطوير تطورات كبيرة فيما يتعلق بتطبيق العلامات المائية الرقمية في الطب عن بعد في هذه الأطروحة. أهم مساهمة هي نظام للعلامة المائية الرقمية العمياء على أساس التحويل المويج المركب ثنائي الشجرة (*DTCWT*) وتحويل كونتورليت غير المكون من عينات فرعية (*NSCT*). يهدف هذا الإطار إلى توفير طريقة آمنة وجديرة بالثقة لحماية صحة وسلامة الصور الطبية في التطبيب عن بعد. المساهمة الثانية هي إستراتيجية العلامة المائية للصور الطبية في مجال التحويل بناءً على نظام التشفير غير المتماثل *ElGamal* وخريطة *Arnold* الفوضوية. تحاول هذه الإستراتيجية زيادة مرونة وأمان تقنية العلامات المائية الرقمية عن طريق تشفير العلامة المائية وتضمينها في الصور الطبية باستخدام مزيج من تقنيات التشفير والفوضى. توفر هذه المساهمات طريقة متكاملة للعلامات المائية الرقمية في الطب عن بعد والتي تتناول قضايا حماية الصور الطبية وحقوق الملكية الفكرية مع تعزيز دقة خدمات التطبيب عن بعد.

الكلمات الدلالية: نظام *Arnold* الفوضوي ، الأصالة ، التشفير ، *DCT* ، *DTCWT* ، العلامات المائية الرقمية ، *DWT* ، نظام التشفير *ElGamal* ، إخفاء المعلومات ، حقوق الملكية الفكرية ، الصور الطبية ، *NSCT* ، التطبيب عن بعد ، النسخ غير المصرح به.