REPUBLIC OF TURKEY

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Information Technologies

INCORPORATING A WATERMARKING WITH AN IRIS CODE TO ENSURE THE COPYRIGHT PROTECTION OF THE IMAGE

Dhuha Tawfeeq MUSTAFA

Master of Science

Supervisor

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Istanbul, 2022

INCORPORATING A WATERMARKING WITH AN IRIS CODE TO ENSURE THE COPYRIGHT PROTECTION OF THE IMAGE

Dhuha Tawfeeq MUSTAFA

Information Technologies

Master of Science

ALTINBAŞ UNIVERSITY

2022

The thesis titled (INCORPORATING A WATERMARKING WITH AN IRIS CODE TO ENSURE THE COPYRIGHT PROTECTION OF IMAGE) prepared by DHUHA TAWFEEQ MUSTAFA and submitted on (4/2/2022) has been **accepted unanimously of votes** for the degree of Master of Science in Information Technologies.

_______________________________ _______________________________

Asst. Prof. DR.Abdullahi Abdu IBRAHIM

Supervisor

Thesis Defense Jury Members:

Asst. Prof. DR.Abdullahi Abdu IBRAHIM	Faculty of Engineering and Architecture, Altinbas University	________________
Asst. Prof. Dr. Muhammad ILYAS	Faculty of Engineering and Architecture, Altinbas University	________________
Asst. Prof. Dr. Amjed Razzaq AlABBAS	Department of Computer Engineering, Alsalam University Collage, Baghdad- Iraq	________________

I hereby declare that this thesis meets all format and submission requirements of a Master‘s thesis.

Approval Date of Institute of Graduate Studies: ____/____/____

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Dhuha Tawfeeq MUSTAFA

Signature

DEDICATION

I dedicate my dissertation work to myself, my family, and many friends. I would like to dedicate to my supervisor Asst. Prof. Dr. Abdullahi Abdu Ibrahim which help me in all stages of the thesis.

PREFACE

First of all, I would like to thank the advisors of Asst .prof. Dr. Abdullahi Abdu Ibrahin for guiding me in writing this thesis, which is a requirement for a master’s degree in Information Technology/Computer Science, as he has always helped me in solving problems that I came across while working on the thesis and I discussed with him my ideas and information I needed in my thesis.

I would also like to thank everyone who provided me with assistance and assistance throughout the study period and everyone who gave me valuable guidance in completing this research.

I thank the staff of Altinbas University for providing the study environment during the two academic years on campus.

ABSTRACT

INCORPORATING A WATERMARKING WITH AN IRIS CODE TO ENSURE THE COPYRIGHT PROTECTION OF THE IMAGE

MUSTAFA Dhuha Tawfeeq

M.Sc., Information Technologies, Altınbaş University,

Supervisor: Asst.Prof.Dr. Abdullahi Abdu IBRAHIM

Co-Supervisor: Asst. Prof. Kanar MUSTAFA

Date: February /2022

Pages: 83

The last decade witnessed a great development in the fields of communications and multimedia techniques, which has led to the need of using techniques for protecting copyright and reducing of illegal copying. The human iris biometric as a watermark embedded within one of the types of multimedia is considered as an emerging and effective technique for copyright protection. An algorithm based on human iris as a watermark embedded within a digital image in order to protect its copyright, has been designed and implemented in this research. The proposed algorithm consists of two main parts: the first extracts iris code, while the second embeds the extracted iris code as watermark in a digital image to protect its ownership. The iris segmentation and iris feature extraction phases are considered the most important phases of the first part. In the iris segmentation phase, the two circles the (internal (pupil) and external (Iris) of the iris area) are detected by using Daugman Integro-Differential Operator after the approximate center of the iris center has been detected. At the same phase, the upper and lower eyelids are determined by using the Linear Hough Transform. While during the iris feature extraction phase, the (1D-Log Gabor Filter) is used to extract iris code. In the second part, the extracted iris code is embedded as a watermark on a set of images to protect their ownership by using (LSB) algorithm based on (XOR) method. The experimental results of the first and second parts proved the effectiveness and accuracy of the proposed algorithm. The results of iris segmentation were accurate and the proposed algorithm (LSB) has shown its effectiveness in hiding the code by: firstly, computing and analyzing the metrics Mean Square Error (MSE), Peak-Signal-to-Noise-Ratio(PSNR), Normalized Correlation(NC), and secondly, comparing the original iris code with the extracted one by using (Hamming Distance), and finally by observing that there is no large massive distortion in the cover image after embedding the iris code in it.

Keywords: Biometric, Iris Recognition, LSB, Watermarking, Feature Extraction.

ÖZET

GÖRÜNTÜYÜN TELİF HAKKI KORUNMASINI SAĞLAMAK İÇİN İRİS KODU İLE BİR FİLİGİN DAHİL EDİLMESİ

MUSTAFA, Dhuha Tawfeeq

Yüksek Lisans, Bilgi Teknolojileri, Altınbaş Üniversitesi,

Danışman: Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Yardımcı Danışman: Asst. Prof. Kanar MUSTAFA

Tarih: Şubat /2022

Sayfalar: 83

Son on yılda, iletişim ve multimedya teknikleri alanlarında, telif haklarının korunması ve yasadışı kopyalamanın azaltılması için tekniklerin kullanılması ihtiyacını doğuran büyük bir gelişme yaşandı. Multimedya türlerinden birinin içine yerleştirilmiş bir filigran olarak insan irisi biyometrisi, telif hakkı koruması için gelişmekte olan ve etkili bir teknik olarak kabul edilmektedir. Bu araştırmada, telif hakkını korumak için dijital bir görüntünün içine yerleştirilmiş bir filigran olarak insan irisine dayalı bir algoritma tasarlanmış ve uygulanmıştır. Önerilen algoritma iki ana bölümden oluşur: ilki iris kodunu çıkarır, ikincisi ise sahipliğini korumak için çıkarılan iris kodunu dijital bir görüntüye filigran olarak gömer. İris bölütleme ve iris öznitelik çıkarma aşamaları, ilk bölümün en önemli aşamaları olarak kabul edilir. İris bölütleme aşamasında, iris merkezinin yaklaşık merkezi tespit edildikten sonra iki daire (iris alanının iç (gözbebeği) ve dış (İris)) Daugman Integro-Diferansiyel Operatörü kullanılarak tespit edilir. Aynı aşamada Linear Hough Transform kullanılarak üst ve alt göz kapakları belirlenir. İris özelliği çıkarma aşaması sırasında, iris kodunu çıkarmak için (1D-Log Gabor Filtresi) kullanılır. İkinci bölümde, çıkarılan

iris kodu, (XOR) yöntemine dayalı (LSB) algoritması kullanılarak sahipliklerini korumak için bir dizi görüntü üzerine filigran olarak gömülür. Birinci ve ikinci bölümlerin deneysel sonuçları, önerilen algoritmanın etkinliğini ve doğruluğunu kanıtladı. İris segmentasyonunun sonuçları doğruydu ve önerilen algoritma (LSB) kodu gizlemedeki etkinliğini şu şekilde gösterdi: ilk olarak, Mean Square Error (MSE), Peak-Signal-to-Noise-Ratio (PSNR) metriklerini hesaplayarak ve analiz ederek , Normalleştirilmiş Korelasyon (NC) ve ikinci olarak (Hamming Distance) kullanarak orijinal iris kodunu çıkarılan kodla karşılaştırarak ve son olarak iris kodunu içine gömdükten sonra kapak görüntüsünde büyük bir büyük bozulma olmadığını gözlemleyerek.
Anahtar Kelimeler: Biyometrik, İris Tanıma, LSB, Filigranlama, Özellik Çıkarma.

TABLE OF CONTENTS

Pages

ABSTRACT.. .... **vii**

ÖZET .... **viii**

LIST OF FIGURES .... **xv**

ABBREVIATIONS .... **xvii**

LIST OF SYMBOLS .... **xviii**

1.INTRODUCTION **1**

1.1 PROPERTY PROTECTION OVERVIEW 1

1.2 MOTIVATION 2

1.3 PROBLEM STATEMENT 3

1.4 CONTRIBUTION 3

1.5 AIM AND OBJECTIVE 3

1.6 THESIE ORGANIZATION 4

2.LITERATURE REVIEW **5**

2.1 PROTECTION OF PROPERTY RIGHTS FOR IMAGES USING BIOMETRICS 5

2.2 INFORMATION HIDING 5

2.2.1 Steganography 7

2.3 WATERMARKING 7

2.4 THE DIFFERENCES BETWEEN WATERMARKING TECHNOLOGY AND STEGANOGRAPHY METHODS 8

2.5 PROPERTY AUTHENTICATION 8

2.5.1 Authentication Method 10

2.5.2 Authentication Technology 10

2.6 BIOMETRIC SYSTEM 11
2.6.1 Biometrics History 12
2.6.2 Biometrics Merits 12
2.6.3 Classified Of Biometrics 13
2.6.4 Biometrics Types 14
2.6.5 Benefits Of Using Biometrics 16
2.6.6 Disadvantages Of Using Biometrics 17
2.7 PROTECTION OF PROPERTY RIGHT FOR IMAGE USING BIOMETRICS……..….18
2.8 WATERMARKING TECHNOLOGY 20
2.8.1 History Of Watermarking 20
2.8.2 Watermarking Properties 20
2.8.3 Watermarking Classification 21
2.8.3.4 classification of a watermarking based on the type system of perception 24
2.8.4 Blind And Non-Blind Watermarking Technologies 26
2.8.5 Requirement And Application Of Digital Watermarking 26
2.8.6 Copyright Protection 28
2.8.7 Biometric Watermarking 29
2.9 HUMAN IRIS STRUCTURE 29
2.9.1 Advantage Of The IRIS 30
2.9.2 Characteristic Of The IRIS 31
2.9.3 Iris Recognition 31
2.9.4 Iris Recognition Application 32
2.9.5.Dependence On IRIS Property Protecion 32
2.10 LITERATURE SURVEY 33
3.METHODOLOGY 35
3.1 THE PROPOSED SYSTEM FORPROTECTINGTHE COPYRIGHT OF IMAGES 35
3.1.1 Iris Code Extraction 35

3.1.2 Apply The Hide Algorithem Using Least Significant Bits Algorithem (LSB) 40
3.1.3 Watermarking 44
3.1.4 Matching………………………………………………………………………45
4.RESULT ANALYSIS.. 46
4.1 CASIA IRIS IMAGE DATA BASE 46
4.2 RESULTS OF THE PROPOSED SYSTEM.. 46
4.2.1 Segmentation Results... 46
4.3 INSERT THE IRIS CODE IN THE COVER IMAGE 47
4.4 QUALITY MEASURMENT TECHNIQUE 49
4.4.1 Result analyses... 50
4.4.2 Analysis of the Attack... 51
4.5 HAMMING DISTANCE 56
5.CONCLUSIONS……………………………………………………………………60
5.1RECOMMENDATIONS AND FUTURE WORKS 57
REFERENCES 58

LIST OF TABLES

Pages

Table 2.1: shows the difference between the watermark technology and the coverage system.…..8

Table 2.2: shows the advantages and disadvantages of authentication techniques……….……....11

Table 2.3: shows the discrepancy between the different biometric technologies with the factors affecting the biometric system………………………………………………………………….….13

Table 2.4: Clarifies requirements of design and applications of the corresponding their……..…27

Table 4.1: Application of metrics (MSE, PSNR, NC) before the attack………………………....52

Table 4.2: Application of metrics (MSE, PSNR, NC) after the attack for the salt and pepper noise value = 0.01……………………………………………..…………..……………………...55

Table 4.3: Scales Application Post-attack for Salt and Pepper Noise Value = 0.03………………56

LIST OF FIGURES

Page

Figure 2.1: Classification of Information Security Technologies[22]……………………….………..6

Figure 2.2: Examples of Conceptual authentication[28]..9

Figuer 2.3: Illustrates Biometric categories[42]……………………………………….……….14

Figuer 2.4: Types of biometrics [1]-[5]: (a) DNA, (b) ear, (c) face, (d) face gram, (e) fingerprint, (f) walking, (g) hand geometry , (h) Eris, (i)Retina, (j) signature, (k) sound, (l) keystroke, (m) ECG, (n) EEG, (o) finger vein, (p) palmar vein[49]………………………………………….....16

Figure 2.5: Benefits of using biometrics[39]…………………………………..………..……..17

Figure 2.6: Disadvantages of using biometrics[39]……………………………………………18

Figure 2.7: Concepts of algorithms used in biometric systems.(a)Verification of the individual. (b) Identification of the person. (c) Assessment and classification. (d) Quality assessment evaluation. (e) Feature extraction. (f) PAD[54]………………………………………………………..19

Figure 2.8: watermarking Classification………………………………………………………..22

Figure 2.9: shows the applications related to watermarking digital images[25]……. ….………..27

Figure 2.10: shows a diagram of the requirements and applications of watermarking[66]……….28

Figure 2.11: shows the anatomy of the human eye[73]……………………………………… ..30

Figure 2.12: Different iris shapes[77]…………………………………………………...…31

Figure 2.13: Box diagram of the iris recognition system…………………………….………….32

Figure 3.1: Iris code Extraction……………………………………………………….…...…37

Figure 3.2: Iris segmentation for different images from Casia…………...………..……..…...….38

Figure 3.3: Daugman Rubber sheet model [101]...…………………………..…………..…..……40

Figure 3.4: The cover image before and after hiding the watermark (iris code)……………..……42

Figure 3.5: Flowchart showing the steps for hiding the watermark (iris code)…………….……..44

Figure 3.6: Flowchart showing the algorithm retrieval steps……………………..…….….….45

Figure 4.1: Segmentation results for different CASIA images………………………...….…48

Figure 4.2: The stages of extracting the iris code……………………………………….......48

Figure 4.3: Embedding the iris code of a number of CASIA1 images in several images whose ownership is to be protected ……………………………………………...………………..…...51

Figure 4.4: Adding salt and pepper noises to the hood image after embedding the iris code in it.52

Figure 4.5: Scheme representing pre- and post-attack PNSR values……………….……………53

Figure 4.6: The difference between PSNR values for two attack values.……………………..…55

ABBREVIATIONS

PIN : Personal Identification Number

PNN : Probabilistic Neural Network

LSB : Least Significant Bits

XOR : Exclusive OR

CASIA : Chinese Academy of Sciences–Institute of Automation

LHT : Linear Hough Transform

MSE : Mean Square Error

PSNR : Peak-Signal-to-Noise-Ratio

NC : Normalized Correlation

HD : Hamming Distains

BW : Black and White

PBFO : Parallel Bacterial Foraging Optimization

DNA : Deoyribonucleic Acid

SVD : Single Value Analysis

DWT : Discrete Wavelet Transform

DCT : Discrete Cosine Transform

LIST OF SYMBOLS

¯,r : The coordinates of Normalized Polar

σ : Bandwidth of the filter

f0 : The center frequency

M, N : The image dimensions

1. INTRODUCTION

1.1 PROPERTY PROTECTION OVERVIEW

In the modern period, with the development of technology, modern devices, and computer systems, there are security risks that threaten computer networks. And the development of technology in Internet dissemination threatens that data will be vulnerable to attacks through a pervasive technological environment in which it is easy to copy, store and exchange data and knowledge without losing quality through digital media. Study of information security and coverage system to preserve data.The science of data steganography is used in two different fields, the frequency domain, and the spatial domain, and there are two technologies to provide security for transmitted information and maintain its confidentiality, the first: encryption and the second: Steganography, as the main obstacle to encryption, is the presence of data in an unhidden way. Although it cannot be read, it is still there, so if there is enough time for someone, they can finally unlock the code of the data, so data security had to be developed and new technologies created[1][2][3]. That is why biometrics is considered one of the best behavioral characteristics in authentication systems[4]. And that biometric techniques provide reliable methods of identification, the use of biometric techniques is very important in our time to determine the identity of a person based on his biophysical characteristics. Face recognition and iris recognition systems have been adopted and have proven their success in security systems and the difficulty of cheating because The biometric features of each person are unique and life-long and have been widely used in applications such as time attendance control, customs verification, monitoring, and access to information [5]. Biometrics include the face, voice, signature, and iris are widely used in authentication systems, and since the information is recorded in a central database, it is at risk of theft, and therefore data must be protected using encryption [6]. In general, hiding of data is a broad field that mainly identifies any system in what medium with data contained within other data It is also known as data embedding and has two types, encryption , and watermark[7]. The term "watermark" is derived from the German term "wassermarke". The watermark mechanism is used applied to physical objects such as clothing labels, product packaging, invoices and papers, and there are two types of watermark: the digital watermark and it is considered a completely invisible identification code or is visible, and the watermark is a secret message that is included in a specific medium called the cover [8].

Watermark technology is used to protect the copyright of the data[9] , As a consequence, the art of encrypting data using a watermark is a constructive way to protect the copyright of multimedia such as audio, video, and image, and to protect its inherent features[10], And to avoid the problems of unauthorized and unsafe manipulation of illegal intruders in how to obtain data, this technology was used, and the watermark technology does not reveal the distinctive image visually, and extracting the information contained in it is only authorized for authorized persons[11]. They are used in two domains, transform domain such as discrete Fourier transform, discrete cosine transform, and spatial domain[12]. Putting a watermark on the image is to hide confidential data or information inside an image called the cover image, and the data must be included inefficient and imperceptible ways because it is difficult to penetrate[13].In this research, we used one of the vital human traits to form a series of numbers known as characteristics that are used to identify him electronically. The feature used from biometrics is the iris which is unique and immutable, and after extraction, the iris code is included in the image as a watermark. It is an effective way to protect and preserve images. It is considered a reliable and safe authentication system for copyright and protection of the user from impersonation by attackers, and the application of this system in research is to protect the user and the system and their data, and this protection is done by using some of his physical or behavioral characteristics in order to form several Layers of defenses against attackers so that only the person with the real identity can break through these defenses. The idea of the research is to prove the ownership of a person using the iris of the eye, Iris based watermarking for property protection.

1.2 MOTIVATION

The main objective of this research is to establish the property rights of the person and achieve reliability based on the use of biometrics. The iris pattern recognition system is the most accurate and reliable standard determination system, where the property rights of an image or any other medium can be guaranteed by hiding the iris code inside an image and it is an effective way to protect the rights of the owner of that code and preserve it from piracy Reliability systems based on the use of biometrics have spread widely compared to traditional reliability systems due to their accuracy and ability to easily distinguish between the real personality of the user and impersonators due to their dependence on personal characteristics in identifying the user, in addition to that these systems are widely accepted among users because they do not need to memorize Many passwords are vulnerable to being stolen or forgotten. It enables this extraction of individual characteristics to deal with people quickly and with high accuracy, this proposal deals with the proof of copyright or ensure the authentication of a person, through the watermark that adopts the use of biometrics

1.3 PROBLEM STATEMENT

The presence of many facilities in the new lifestyle with the advancement of technology has given renewed opportunities for people with subversive and espionage interests, such as pirates and counterfeit people, to access some information and infringe on the privacy of users, steal their information and impersonate their personalities. For it, and in order to stop these sabotage acts, the need arose to provide methods aimed at protecting the security of systems and their users, and to secure protection for communication channels and transmitted information

1.4 CONTRIBUTION

This research aims to apply multiple algorithms for the purpose of proving property rights for a specific medium image, by using the least significant bit method to embed iris data inside an image as a watermark after extracting the iris code and performing treatments on it. The LSB algorithm used in the spatial domain is one of the best algorithms in Preserving the original information of the image, because it is used to hide the less important bits, specifically the first and second bits. The changes are very minor and do not affect the iris code, meaning the code remains reliable. It also aims to study the efficiency of the method used based on the results obtained later. The iris has been used for its uniqueness and stability, which prevents subversive, unreal or unauthorized persons from accessing the data to be protected. Therefore, the aim of the research is to increase the confidentiality of information and choose methods that are difficult to penetrate in addition to choosing information that is difficult to obtain.

The system was implemented using Matlab, because it provides facilities and advanced mathematical and software functions in dealing with images, matrices, filters, and in particular, it provides the possibility of dealing with matrices of no specific size or type.

1.5 AIM AND OBJECTIVE

The research aims to reduce the thefts that occur in biometric information used in various areas of life because it contains behavioral characteristics, and one of the most important of these characteristics is the authentication of the identity of people, which is one of the biometrics techniques. The use of human biometric fingerprints is very important for automatic authentication to identify a person in logging in to a computer or as a key or password for a safe, or entrances to homes or various important institutions such as museums, secure electronic banking services, passport control, building access control, credit cards, airport, Crossing borders, and bank ATMs, and the iris fingerprint was used as a vital sign in this research because it has high reliability, so it works on the inability of fake people to access computer systems or any personal information and attribute it to them, and thus loss of property rights of the real person.

1.6 THESIE ORGANIZATION

The general structure of the research consists of five chapters:

The second chapter included an introduction to concealment of information, verification of ownership, methods of reliability, the system of biometrics, as well as the chapter dealing with the benefits and disadvantages of using biometrics, its varieties and types, as well as the watermark and its classification, protection of property rights, the watermark of biometrics, the structure of the iris and its advantages, and discrimination Persons adopting iris, iris recognition applications, and, relying on iris to establish property rights.

The third chapter includes the proposed system and the steps for obtaining the iris code and embedding it as a watermark inside the images. While the fourth chapter included a presentation of the results that were reached through the application of the system. Finally, the fifth chapter included conclusions, future actions and recommendations.

2. LITERATURE REVIEW

2.1 PROTECTION OF PROPERTY RIGHTS FOR IMAGES USING BIOMETRICS

Nowadays, the reliability systems based on the use of biometrics have become more widespread compared to the traditional reliability systems due to their accuracy and ability to easily distinguish between the real personality of the user and impersonators due to their reliance on personal characteristics in identifying the user, in addition to that these systems are widely accepted among users for not Their need to memorize many passwords that are prone to being stolen or forgotten. It enables this extraction of individual characteristics to deal with people quickly and with high accuracy. This chapter deals with the proof of ownership rights copyright or ensuring the authentication of a person, through the watermark that adopts the use of biometrics, Digital Watermarking Techniques can be described as the process of embedding a distinctive mark in various types of digital media such as text files, images, audio and video files without causing any distortion in the host cover and that the purpose of using watermark is to impede the process of data theft and prevent others Who claims ownership of that digital media[14][15][16].

2.2 INFORMATION HIDING

Information of hiding is defined as the process of embedding confidential data in various forms of digital multimedia such as text files, video files, audio files, and images, and with the rapid growth of communication and networking technologies, hiding information technologies are widely used to achieve multiple purposes, including protection Copyright and ownership confirmation and the realization of communication in a confidential manner, meaning that it has become an important method for maintaining information security. Concealment of information has been studied very extensively by researchers and they proposed and applied the method of inclusion in two fields, namely, the frequency domain and the spatial domain[17][18].A type of methods that do not depend on encryption has been developed, and this type of method is to protect the user and the system and their data by protecting the user from impersonation of the attackers, this protection is done by using some of his physical or behavioral characteristics in order to form several layers of defenses against the attackers so that Only the person who holds the real identity can penetrate these defenses, and these systems are known as biometric systems, which are electronic systems that take models of the vital human features to form strings of numbers known as properties that are used to identify him electronically, as well as through which we can seamlessly identify on the physical or behavioral characteristics of an individual[19][20].The sciences of hiding information steganography and Cryptography are used, with their differences in confirming and documenting data, and in encryption, anyone can discover that there are two people communicating in an encrypted way, while hiding information originally hides the existence of communication so that no one can notice the presence of two people exchanging messages through Communication channels and this made the science of steganography appropriate in some tasks such as hiding copyright marks, as it is easy to remove encrypted copyright information, but when this data is included with the contents of the file itself, it is difficult to detect or remove it [21][22]And Figure 2.1 Shows the Classification of Information Security Technologies[22].

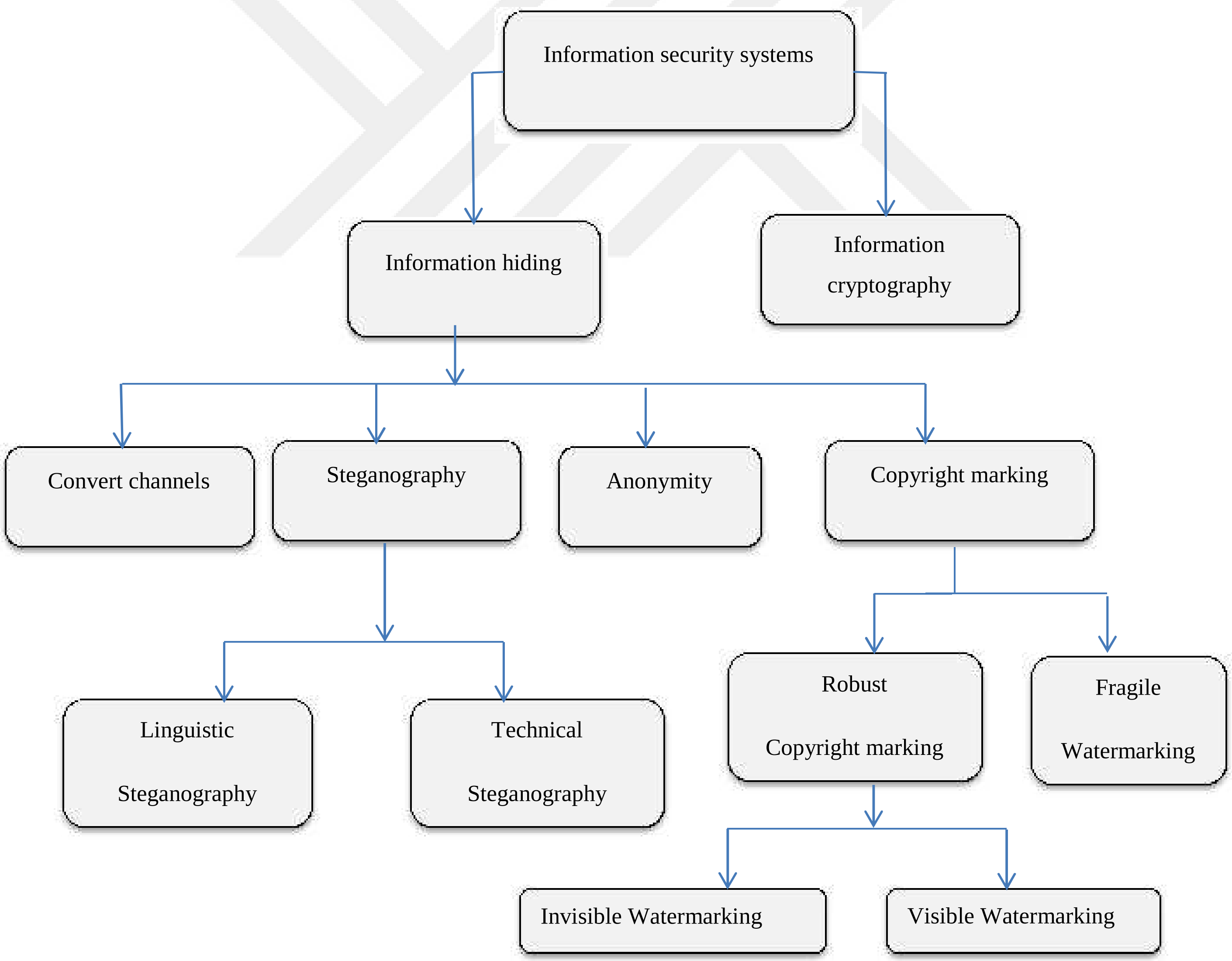


Figure 2.1: Classification of Information Security Technologies[22].

2.2.1 Steganography

The word steganography is known as “covered writing,” and the word steganography is derived from the two Greek words “stegos,” which means cover, and “grafia,” which means writing[10].Also, steganography is the process of covering sensitive information in any medium to transmit it securely over a communications network, and it is the science and art of writing hidden messages in such a way that no one, except the sender and receiver, suspects the existence of a message within the carrier medium, which can be a digital image or a text file or file. Audio or video, and the transmission medium after including the secret message inside it are called (Stego_Media). Stego_Key can be used to control the hiding process or limit the discovery of hidden data[11]. The main goal of using steganography is to cover and hidden communication and secret communication was very important in wars and diplomacy, and from here multiple methods of secret communication were invented, and it has been used in Greek history since about 400 BC invisible inks, symbols, wooden discs and zeros since thousands of years and the oldest ages In order to maintain the confidentiality of the information and its authenticity to the person requested in complete secrecy, and now that we live in the modern and digital era, effective methods are needed to protect the information security, copyright protection, and ownership of ideas and authorship. Steganography is the art and science of hidden, through which it is possible to communicate a message in complete secrecy, by hiding it in the cover file in ways and techniques so that the abusers cannot discover the hidden message[12**].**

2.3 WATERMARKING

Watermarking is used to prove intellectual property protection or authentication, as the watermark obstructs the reproduction process, but it does not prevent illegal reproduction, and it is possible to put a sign embedded with the watermark to disable the reproduction of this product in the event of a request for its reproduction from one side. External, today we see the rapid proliferation of multimedia systems that raise the question of copyright protection, monitoring of takedown signals, and the development of algorithms and real-time applications that may prevent illegal copying and prevent redistribution of stolen copies. One solution to this issue lies in data watermarks. (data watermarking) which is added to multimedia contents in a fixed and unaware way, and then the users have the ability to prove the ownership of the files. Watermarking technology has been developed in the beginning for digital images and videos and access to audio technologies[23][24][25].

2.4 THE DIFFERENCES BETWEEN WATERMARKING TECHNOLOGY AND STEGANOGRAPHY METHODS

The watermarking system combines with the coverage system because they are two methods of one technology, which is information hiding, but there are some differences that distinguish one from the other[26] [7], as shown in Table (2-1).

Table 2.1: Shows the difference between the watermark technology and the coverage system[26] [7].

Watermarking	Steganography
Digital watermarks add some information that takes into account the properties or characteristics of the cover such as copyright, that is, the information included is related to the carrier cover.	The cover system hides the message that is the purpose of the correspondence or communication, meaning that the included information has nothing to do with the carrier cover.
The determinants of the durability of watermarks are concerned with the effort to remove them by (the thief).	The determinants of the robustness of the steganography system focus mainly on revealing the hidden message.
Watermarks introduce less information into the transmitted medium.	The coverage system hides relatively large packets of information.
It is not necessary and sometimes important in the watermark to encrypt the message.	In steganography, it is very important to encrypt the message.
Communication (messaging) in a watermark system is often point-to-many.	Communication in a coverage system is usually point-to-point.

2.5 PROPERTY AUTHENTICATION

The main objective of authentication is to protect the system from unauthorized use, and this feature also enables to withhold some capabilities from some users and thus we can reduce the capabilities of each user according to his job and rank, the different methods of reliability centered on three basic axes in achieving Authentication Aspects[27], as shown in the figure [28].

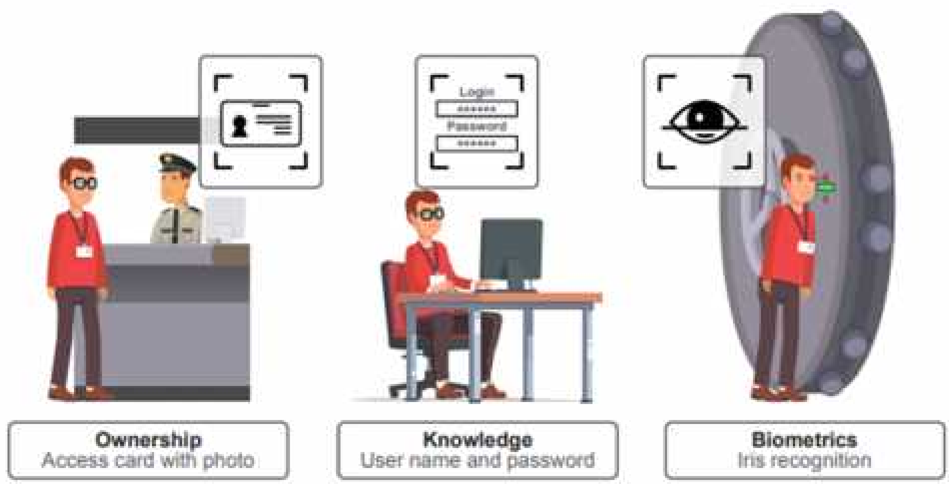


Figure 2.2: Examples of Conceptual authentication[28].

These main themes are:

a. Possession Reliability: is achieved by relying on this axis through the authorized person's possession or possession of some trusted things, which know or confirm his identity. Examples of these things are optical cards and smart cards , and the problem in using these methods is the possibility of stealing these things. things or even share them with others, and if these things are stolen, the reliability of these things will return to their new owner who may misuse them[27][28].

b. Knowledge Reliability: is achieved by relying on this axis through information or knowledge of the authorized person, as only the concerned person knows or can infer that information, as that knowledge allows him to access what he is authorized to access, such as a password, a card. Passport, Personal Identification Number (PIN). But the problem with using these methods is that this knowledge can be forgotten or shared with others[28][29].

c. Human Characteristics: Reliability is achieved by relying on this axis through the human characteristics that distinguish each individual from his peers[29] .The systems based on this axis are among the best systems used to verify the user's personality, because they give a high degree of security compared to other methods. To verify the character, as it cannot be forgotten, stolen or lost, as in the previous axes[30][28].

2.5.1 Authentication Method

a. Verification: In which it is determined whether the person concerned is the real person (the target person Claimed Identity) or is just an impersonator, the problem of verifying the identity of the person can be described as one-to-one (), as the model whose identity is to be confirmed is matched with only one template It is the template of the target person, and if the matching result is positive, this indicates that the person is an authorized person, but if the matching result is negative, this indicates that the person is a fake or an impersonator[31][32].

b. Identification: In it, the identity of the person whose data is entered is identified from among the total number of persons registered in the system's data base. The problem of identifying a person can be described as one-to-many, in which the template to be identified is matched to all stored templates. In the system until the model matches one of the templates, and thus the process of identifying the person has been completed, and in the event that the model does not match any of the stored templates, then the person will be considered an unauthorized person[31][32].

2.5.2 Authentication Technology

The authentication of biometrics is the best compared to traditional techniques, and in some cases, it can be used with traditional to add high reliability, because biometrics determine the unique behavior of a person and thus work to verify the person, that is, every person has a distinctive character and to be permanently nonexistent. These features can be altered or falsified, and these features must be easy to collect and capture, and most importantly, this technology does not violate the user's privacy. Biometric techniques such as iris recognition, facial recognition, DNA, signature, and fingerprint are considered a person's identification system or as a verification system[33][34].This table shows the advantages and disadvantages of authentication techniques[33].

Table 2.2: The advantages and disadvantages of authentication techniques[33].

Technique	Biometrics	Techniques depend token	Techniques depend on Knowledge
Description of technique	-Depends on the individual's uniqueness, behavioral traits and physiological traits. - It works to identify and verify the identity of a person.	-It is very easy and portable for use. -Uses two-factor authentication such as user ID and PIN.	- The user is the one who creates his own password consisting of his combination of alphanumeric characters and numbers. - It is based on a subset of numerical values, which are known as PIN numbers.
Advantages	-No need to memorize difficult and complex passwords. -Flexible and easy to use. -Difficult to fake.	-User can be carried it physically. -We can very easily replace a correct way	-It is a common and traditional way to use authentication. -Economical and simple
disadvantages	-sometimes expensive. -Changes in physical or behavioral characteristics that lead to giving false information and data.	- Lost and stolen. -It can be shared with anyone. -Any typo that blocks the card and locks it.	- Passwords are complex, lengthy, and difficult to memorize. - The attacker can guess the pin code or passwords if they are simple and commonly used. - Can be shared with multiple people.
Examples	Iris recognition, facial recognition, digital signature, voice recognition, cornea, palm of the hand.	smart cards, passport	PIN numbers, passwords

2.6 BIOMETRIC SYSTEM

Biometrics is computer systems that are used to identify people based on their behavioral and physiological traits. These systems are used to verify the identity of the people using the system and are used instead of traditional methods such as passwords and ID cards that can be cracked or simply forged and impersonated, Biometric systems are based on extracting characteristics from biometrics, these characteristics are strings of numbers that represent the attribute

Individually. These properties are then used either to build a pattern-recognition system that identifies users by comparing the entered attribute with attributes previously stored in the database, or to build random secret keys that the user cannot deny their use [35]. Around the world, biometric authentication methods and technologies for multimedia have been proposed, especially based on fingerprints and fingerprints, which are widely used in order to identify as many people as possible and obtain their information. A master central database, and this data is used to issue some documents that cannot be forged (eg passports) and is also used to reissue documents. In the event of his loss[36][37].

2.6.1 Biometrics History

The word biometrics or biometrics consists of two Greek syllables, the first (bio) which means "life" and the second syllable (metrics) which means "measure." This word means the science and technology of analyzing and measuring vital statistics, and this term refers to technologies including identification Individuals by biological and biological characteristics present in the body or behavior (such as fingerprint, iris, retina, voice, signature to distinguish someone from the rest of the people)[38]. The first appearance of biometrics was 29,000 BC, where cavemen used drawings and their fingerprints to sign. These were the most important pieces of evidence on that stick, and then the Babylonians used biometrics and applied them to clay tablets to sign their trade transactions. Biometrics has a long and extensive history since antiquity. Nowadays, the use of biometrics has increased in various ways and has multiple functions, including acceptance, universality, performance, and uniqueness, and each has its own characteristics and advantages, so fingerprints are important in criminal cases, and irises are distinguished by their accuracy and uniqueness. It can be argued that despite the high level of biometric methods, algorithms and techniques must be added to achieve the best results to protect the information to be protected using biometrics[39].

2.6.2 Biometrics Merits

There are many advantages of biometrics, the most important of which are the following[40][39][41].

a. Universality: means that all human beings possess these qualities.
b. Uniqueness: It means that no two individuals have the same biological trait, but rather it is unique and distinct for each individual from the other that no one shares or equals with.
c. Stability: It means that these traits are fixed and permanent in a person throughout his life

and do not disappear from him.

d. Collect ability: The process of obtaining this feature should be easy, and it does not require a lot of time and cost.

e. Performance: the speed, accuracy and durability of performance.

f. Acceptability: It indicates the acceptability of a biometric-based system for users in their daily lives.

g. Circumvention: The sobriety of a system reflects how easily a system can be derailed or compromised by intruders. Table (2-2) shows the variation of different biometric technologies with the factors affecting the biometric system [42].

Table 2.3: Shows the discrepancy between the different biometric technologies with the factors affecting the biometric system[42].

Biometric	Distinctiveness	Permanence	Uniqueness	Acceptability	Circumvention	Collectability	Performance
IRIS	High	High	High	Medium	Low	High	High
Face	High	Medium	Medium	High	High	High	Low
DNA	High	High	High	Low	Low	Low	High
finger print	Medium	High	High	Medium	Medium	Medium	Low
digital signature	Low	Low	Low	High	Low	High	Low
Voice recognition	Low	Medium	Low	High	High	High	Low
Hand Geometry	Medium	Low	High	Medium	Medium	High	Low

2.6.3 Classified Of Biometrics

a. Physiological Biometrics**:** These scales include the characteristics of a person that are directly related to his body and the shape and characteristics of some of his organs such as (fingerprint, face, DNA, palm print, hand topography, iris, and ear shape)[39].

b. Behavioral Biometrics: Each person has behavioral characteristics that he is accustomed to distinguishing him from others, and this type of biometrics is less stable than the first type, as the behavioral characteristics of the individual may be affected by the influence of several factors, including stress, weakness, disease or age, and these characteristics are also characterized by being less safe Examples include Signature, Key Stroke, Voice[43] .Figure 2.3 illustrates Biometric categories[42].

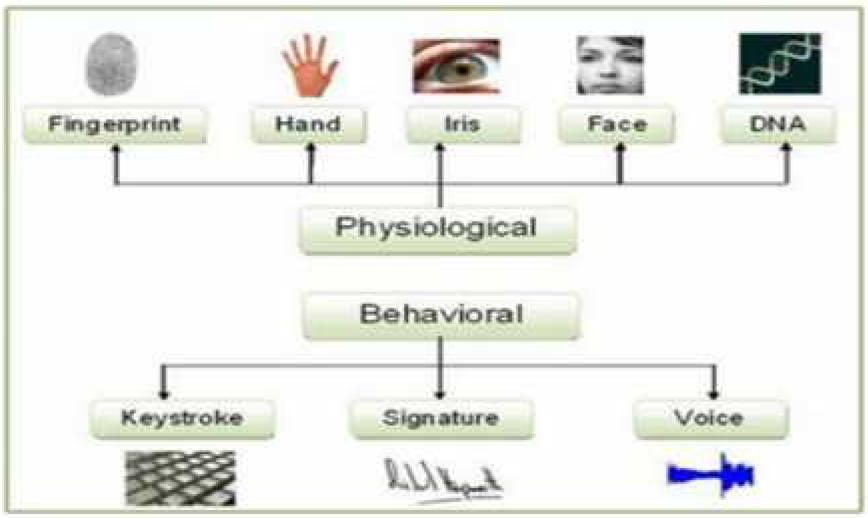


Figure 2.3: Illustrates Biometric categories[42].

2.6.4 Biometrics Types

There are many types of biometrics, including:

a. Fingerprint : The fingerprint is one of the most famous and most widely used vital features in the field of identity verification, because it is easy to obtain and because it is a fixed feature that is formed in the human being before his birth, and is often used as conclusive evidence in which the accused is guilty of the crime The person scanning[44].

b. Geometry Hand : The identity of the person is determined from the hand geometry by analyzing the shape of the hand and taking various measurements with the special scanner, such as the length of the fingers, thickness, depth and surface area of the hand of the individual the work [44].

c. Iris : The colored part surrounding the pupil of the eye (the pupil is the black circle in the center of the eye) consists of structures and tissues that differ from one person to another, even among twins, and also differ from one person’s eye to the other eye, and based on that, it has a high accuracy that exceeds genetic fingerprinting and the systems are counted The mechanism for recognizing the iris of the eye is one of the most accurate systems at the moment, as it can compare six million images in just one second [39].

d. Voice :This type of biometrics combines the physiological and behavioral characteristics of the individual, as the audio characteristics of a speaker's speech are matched with the pre-recorded audio characteristics and are used in cases of entering computer systems or opening doors. The audio fingerprint is based on the first two principles: that each person has a unique audio device. No one is like him, the second: that each person has a unique nervous system that controls the audio system. Noise and psychological state are among the factors that affect the speaker's voice and result in inaccurate voice signature, and anyone can fake the voice using modern digital recordings and use them to enter the system[45].

e. Signature Electronic : signature recognition systems depend not only on the shape of the signature but also on the pen stroke, speed and the point at which the pen is lifted from the paper. Normal differences give different forms of signatures, and people may be tempted to accept a person's signature as proof of their identity[46].

f. Deoxyribonucleic Acid DNA: DNA is a type of biometrics that uses physiological characteristics for identification, and one of its advantages is that it is the most accurate biometric , as every cell in the human body, including those found in saliva, hair, skin and other cells, carries the genetic characteristics that are unique to that person. About the rest of the people.[39].

g. Face : It is one of the oldest and most common methods used in people recognition technologies, and it depends on some facial features such as (eyes, eyebrows, nose, mouth, chin and the relative relationships between them)[47][48]. Figure 2.4 shows the different types of biometrics[49].

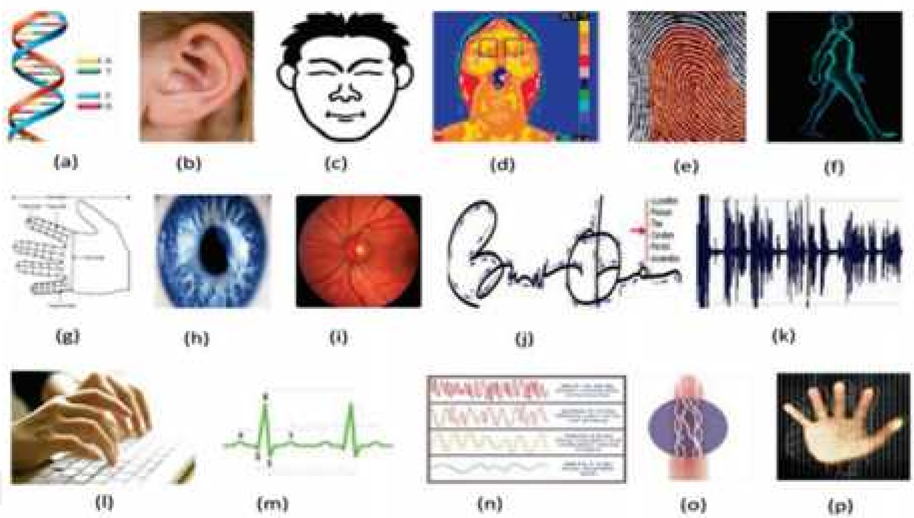


Figure 2.4: Types of biometrics [1]-[5]: (a) DNA, (b) ear, (c) face, (d) face gram, (e) fingerprint, (f) walking, (g) hand geometry , (h) Eris, (i)Retina, (j) signature, (k) sound, (l) keystroke, (m) ECG, (n) EEG, (o) finger vein, (p) palmar vein[49].

2.6.5 Benefits Of Using Biometrics

During the past decade, several reasons have emerged that led to the growing use of biometrics, including[39][50][51]:

a. It provides the appropriate reliability and is easy to use as nothing can be lost or forgotten.

b. Its suitability for organizations and factories, so many public organizations have resorted at the present time to the use of these technologies. Biometric features are used in recording the time of attendance and departure in institutions, that is, they are used in this work time management system as a simple example of several uses for it.

c. Speed in verifying the person, because most of the biometrics are done automatically, so the verification process is usually very fast, and in most cases it takes only a few seconds.

d. Difficult to falsify and not be able to guess, as it is usually difficult to falsify biometrics, and it is characterized by not being able to be guessed or predicted.

e. They are accurate, inexpensive, and difficult to lose or duplicate. Figure 2.5 shows the benefits of using biometrics.

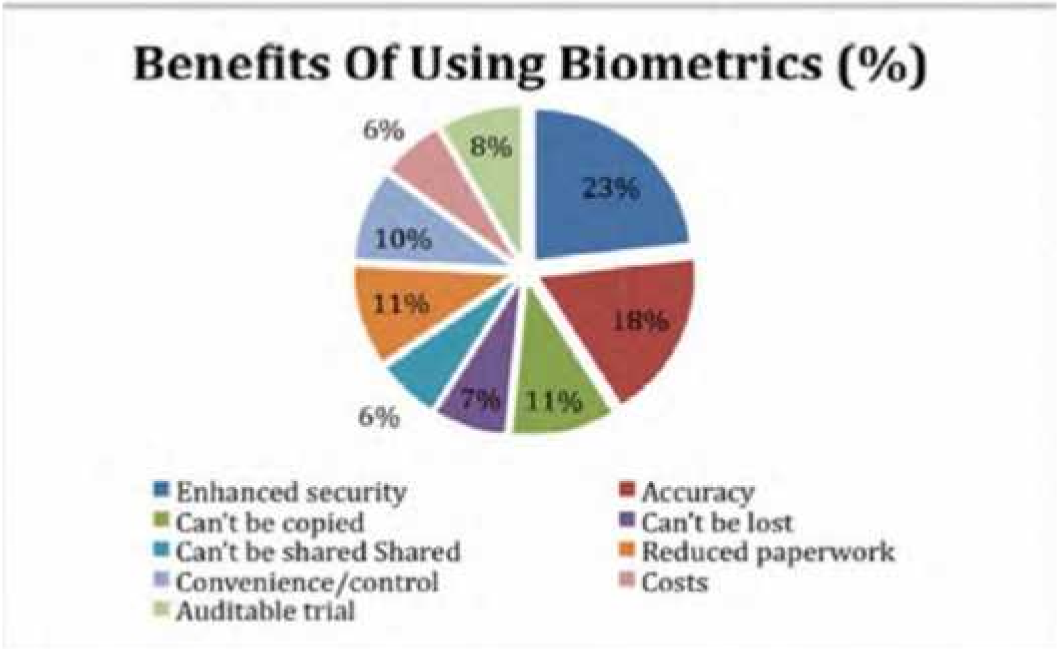


Figure 2.5: Benefits of using biometrics[39].

2.6.6 Disadvantages Of Using Biometrics

The use of biometric systems has advantages and advantages, as there may be some disadvantages and disadvantages in the use of biometrics, as follows[39][50][52]:

a. Possibility of errors during biometric registration or during matching.

b. The need to educate and train users on the algorithms and systems used.

c. People's resistance to this type of technology and not accepting its application.

d. Loss of stored information obtained from biometrics, and protection must be provided for it.

e. Loss of body parts or deformation as may happen to the finger or hand.

f. Misuse of the data obtained using biometrics for purposes other than those for which it was registered, as shown in Figure 2.6.

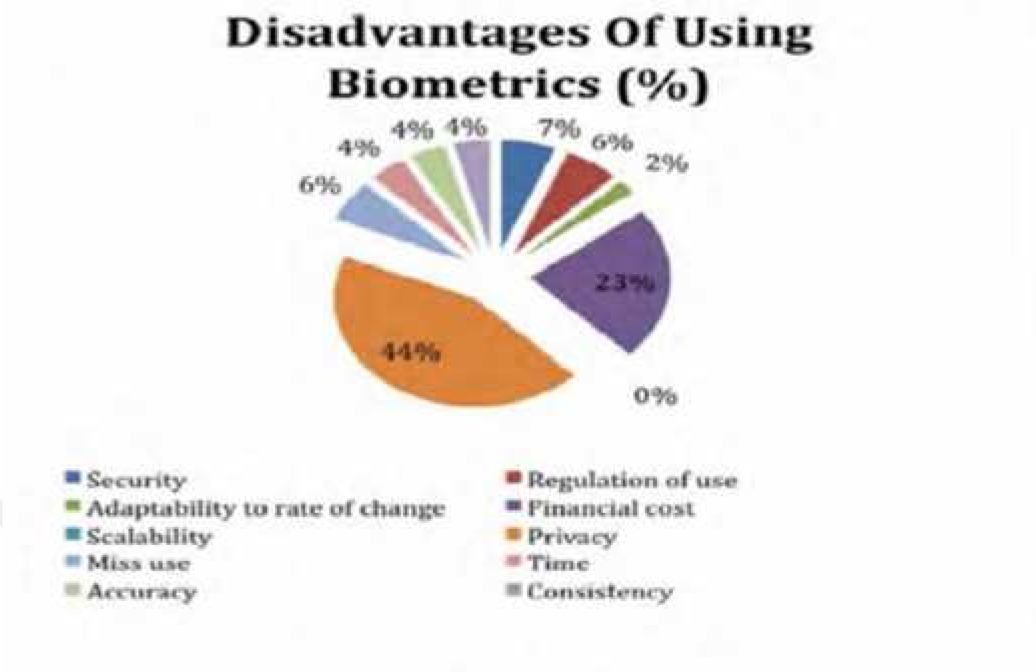


Figure 2.6: Disadvantages of using biometrics[39].

2.7 PROTECTION OF PROPERTY RIGHT FOR IMAGE USING BIOMETRICS

Nowadays, the reliability systems based on the use of biometrics have become more widespread compared to the traditional reliability systems due to their accuracy and ability to easily distinguish between the real personality of the user and impersonators due to their reliance on personal characteristics in identifying the user, in addition to that these systems are widely accepted among users for not Their need to memorize many passwords that are prone to be stolen or forgotten. It enables this extraction of individual characteristics to deal with people quickly and with high accuracy, where the proof of ownership rights (copyright) or the authentication of a person, with techniques and algorithms that adopt the use of biometrics[53][54]. In this figure 2.7, the most important concepts and algorithms used in biometrics are illustrated[54].

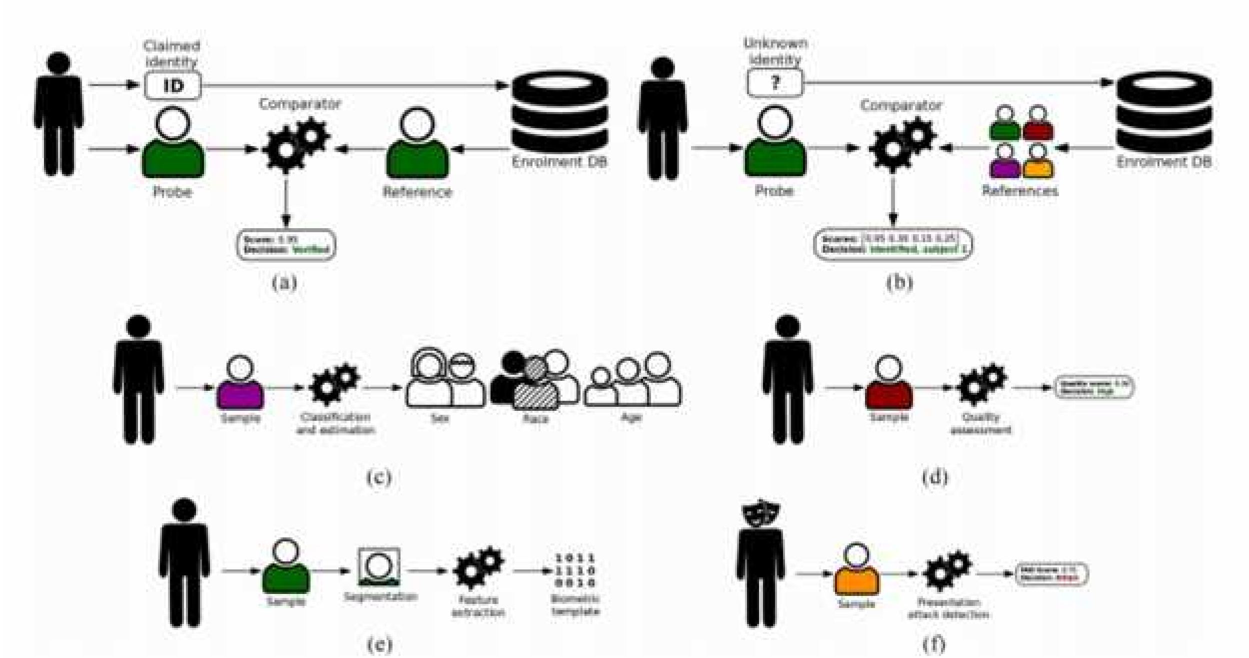


Figure 2.7: Concepts of algorithms used in biometric systems.(a)Verification of the individual. (b)Identification of the person. (c) Assessment and classification. (d) Quality assessment evaluation. (e)Feature extraction. (f) PAD[54].

The process of comparing the distinctive and unique features of the biometric samples in order to prove similarity that these systems seek to:

a. Verification: means that the person is the one concerned and cannot be compared to anyone, (individual comparison)[55][54].

b. Identification: It means searching for a person and identifying him through a large database. Identification requires two methods. The first is verification: It refers to a process that includes confirmation of a biometric claim by conducting a biometric comparison, and the second is identification: It refers to the process of searching for one individual within identifiers. It is located in the biometric registration database, Identification is considered the most prevalent within the use of biometrics [54].

c. Classification and Estimation: These are biometric labels that are referred to the process to assign them before the classification or recognition process, the system must obtain a sample of the used bioassays, which are pre-processed[56].

d. Quality assessment: describes the process of quantification of the quality of the biometric sample obtained[57][54].

e. Extract features: It is a process during which stages are carried out to obtain the most important part of the biometric used, in which all the characteristics of that trait are determined and extracted[58].

f. Attack Detection (PAD) Screen: Explains "Automatic display attack recognition"[54].

2.8 WATERMARKING TECHNOLOGY

It is a copyright protection technology used to protect digital products, and many watermarking algorithms have been developed in recent years. A watermark is a digital code embedded within an image and used in the inline transmission of binary data. The watermark is so easy to handle in multimedia products that it makes unauthorized duplication and redistribution, thus protecting copyright. The watermark is either visible or invisible, and the visible watermark technologies are static, that is, the watermark is stored in both the data segment and the code segment. And the invisible are dynamic (dynamic), that is, the watermark is stored during program execution through the program code, and the watermark is used to hide proprietary information in digital multimedia in order to protect copyright and copyright and ensure the reliability of confidential data and communications[59][60].

2.8.1 History Of Watermarking

The history of the watermark goes back more than 700 years, and the first to use the paper watermark was in Fabriano in Italy, where it referred to the paper watermark that it produced and spread very quickly in Italy and Europe and was used for the paper brand and considered it an indicator of paper quality, shape and strength, as well as used for authentication and the date of paper In the eighteenth century, it was widely and widely used in measures of paper currency and not counterfeiting it through the watermark, and its use spread in measures on other documents and money. Komatsu and Tominaga were the first to use digital watermarking in 1988[61].

2.8.2 Watermarking Properties

When using the watermark in any system, certain characteristics must be available, including[61][62]:

a. Effectiveness : It is considered the most important feature of the watermark that you must possess in order for the watermark to be strong and effective, meaning that it achieves the purpose of its use with high accuracy and efficiency. This is the most important characteristic of a watermark that it possesses.

b. Transparency: Transparency is also an important feature in placing the watermark, and transparency generally means the inclusion of data or information without any change or impact on the original content. That is, it does not cause a significant and noticeable change.

c. Host signal quality: The watermark must be embedded in the host's tag (video, text, image, etc.) and may affect the host, and changes must be unnoticeable on the host especially when the watermark is not visible.

d. Safety: The watermark is used for confidentiality and security and to prove property and copyright rights, as it makes the included data not be destroyed, removed or falsified.

e. Capacity: It represents the amount of data that can be included in the watermark, meaning that it is not in a large size, but rather in a minimum size that does not affect the host.

f. Durability: It is an important feature and the watermark must be strong and resist exposure to attacks by hackers, that is, it resists the accidents it goes through and withstands threats and attacks, and the value of the data does not change during transmission, it keeps its properties.

2.8.3 Watermarking Classification

Watermark technologies are generally classified according to one of the parameters (perception, applications, field, multimedia) as shown in Figure 2.8.

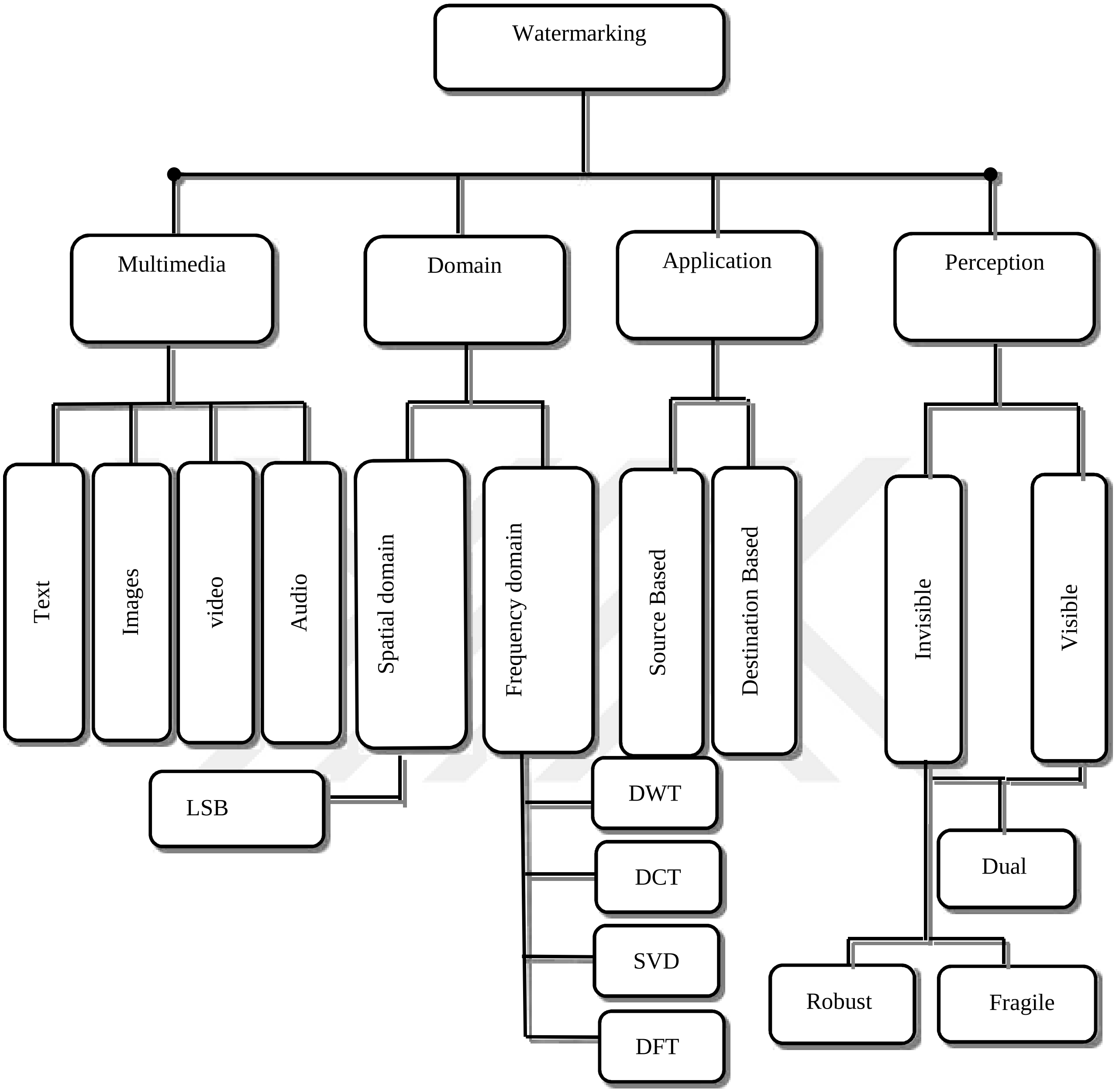


Figure 2.8: watermarking Classification.

Watermarking technologies are categorized into four categories depending on the type of cover:

2.8.3.1 Multimedia

On the type of cover used watermarking techniques can be classified into four types, as shown[63]:

a. Text:- Add watermark to text files (PDF, DOC).

b. Image:- Add watermark to image components.

c. Videos:- Add watermark to video files to control those applications.

d. Drawings: - Adding watermark to drawings with two or three dimensions.

2.8.3.2 Domain

of watermark technologies based on the domain used in the embedding process:

i. Spatial Domain Technique

In spatial domain technologies, the data is guaranteed by direct change of the pixel value of the cover image, as this technique inserts the watermark depending on the data, information, or logo provided by the owner to maintain reliability. The Least Significant Bit (LSB) algorithm is used with the spatial domain ,where the images are modified using the least important bits so that there is no direct and large change to the image, that is, it is without effect and remains preserved in the original, as it represents the lowest bit level of the pixels known and specified in a gray image or a color image and depends on the intensity of the pixel and the resulting watermark is Invisible or visible watermark, the reason for the use of the spatial field by researchers is the optimal balance between ability, durability, and lack of awareness, and these qualities are considered the most important requirements for the success of the technology, and represent the quality of the image of the watermark. These methods are good and work well if the image is not exposed to any external noise, attack, or human modification[25][64].

- Least Significant Bit (LSB) algorithm :

The (LSB) algorithm is the most common and used in the spatial field as a watermark, and the changes that occur to it do not have a significant or noticeable effect on the image, where the change by modifying the least significant bits that work does not affect the image quality or change it directly and significantly. It is an easy to implement and smooth algorithm. The host image is processed by several techniques, where the less significant bits carry less relevant information, and in this way, the quality of the host image is not affected, as this algorithm allows high management and transparency, while observing few and minimal effects on the host[25].

One of the most important advantages of the LSB algorithm: it is easy to understand, implement and simple, It is highly transparent and perceptual, Image quality is preserved and changes are minimal,be very imperceptible, is not computationally complicated and fast program execution and the time it takes is very little and is always applied in the spatial domain, where the watermark in the spatial domain is considered the fastest computing and easiest to implement[65].

ii. Frequency Domain Technique

In the frequency domain techniques, the data is embedded after the conversion operations are performed on the image. This technique hides the data in the signal conversion space in short time and in an efficient manner, and this technique transforms the image using different and predefined transformations that can represent the image with the frequency domain, where the mark ensures Watercolor by using different transformations by changing the transformation field factor of the original image, and these transformations include Fourier transform (DFT),single value analysis (SVD),discrete wavelet transform (DWT),discrete cosine transform (DCT) Hadamard transform, PHT, Fresnel, FFT, CAT, and to get the watermark, any process of extracting it is by using the inverse transformation until the original signal is restored and by applying the phase shift information, the frequency components are collected. This technique is characterized by durability, efficiency, unawareness and safety against attacks, noise, pressure and rotation[25][66].

2.8.3.3 Applaction

Depending on the type of application of the watermark, the watermark can be classified[67]:

i. Source-Based: It is used to determine ownership or prove reliability by adding a watermark to all copies of the relevant digital media that will be distributed.

ii. Destination-Based: Every distributed copy of the digital media contains a watermark in order to identify the relevant buyer and can be used to track the buyer in the event of illegal resale.

2.8.3.4 classification of a watermarking based on the type system of perception

Here the watermark is categorized into two types, the visible watermarking and the invisible watermarking:

i. Visible watermarking

The visual watermarking is one of the types of digital watermarking, where the data (watermarking) is embedded in the cover in a visible way that can be perceived by the human eye, and the resulting cover after the embedding process is completely different from the original cover, and this technology is the most important and common For the purpose of protecting the property of digital multimedia files (images and video) that are published for specific purposes and preventing illegal copying of these digital media[63].

The watermark is embedding in digital contents in general, in which this data is not perceivable, that is, it is hidden and invisible in the original content and only the authorized person can reveal it so that the method of embedding is using different algorithms that can be perceived or observed and can be retrieved with appropriate decoding mechanisms[63].

ii. Invisible watwermarkink

There are also three types of marking the invisible waters are as follows:

a. Robust Watermarking

The use of invisible hard watermarks generally for copyright protection, broadcast monitoring, proof of ownership, fingerprinting and copy control, and high hardness is the basis of hard watermark technologies as they protect against noisy attacks and resist all image manipulations that attempt to remove Embedded mark or destroyed, and the strong invisible watermark refers to the charts with high security and these charts contain the data and thus it is very difficult to remove the watermark, it is mainly used in the protection of copyrights and authorship, as it has high durability as a watermark used by the owner and is embedded with high accuracy It cannot be removed, and to assess the strength of the watermark, we use the application of different types of attacks on it, and then the watermark is extracted and the difference between the extracted watermark and the embedded watermark is evaluated[66].

b. Fragile Watermarking

Technologies for this type of watermark have a specific strength and are very sensitive to all types of distortion, because they are used for the purpose of establishing reliability and security for media and not to prove ownership. The purpose of designing this type of technology is to detect illegal tampering as small changes or tampering with the carrier cover It results in a change or damage to the data of the mark. The fragile watermark is considered the weakest, which exposes the data contained in it to the ease of removal. Any manipulation of the media works to destroy the watermarking[63][66].

c. Dual Watermarking

In this type the invisible watermarking is used as a support for the visible watermark, it is a combination of both types[63].

2.8.4 Blind And Non-Blind Watermarking Technologies

Depending on the need for the parent cover image to detect and extract the watermark, technologies can be divided watermarking to[68]:

a. Non-Blind: This technology needs the image of the original cover to discover and extract the watermark. Some watermark technologies of this type are called “private” indicating the secret key used in the embedding and extraction processes[68].

b. Blind: As for this type of technology, it does not need an image - the original cover, and the technologies of this type are sometimes called “Public” denoting the key used to embed and extract the watermarking[68].

2.8.5 Requirement And Application Of Digital Watermarking

Watermarking applications for digital images are a highly focused area of use in multimedia applications such as copyright protection, data authentication, privacy control, forensics, monitoring device as well as medical reports, where the most important modern applications are described in the following figure 2.9 [25].

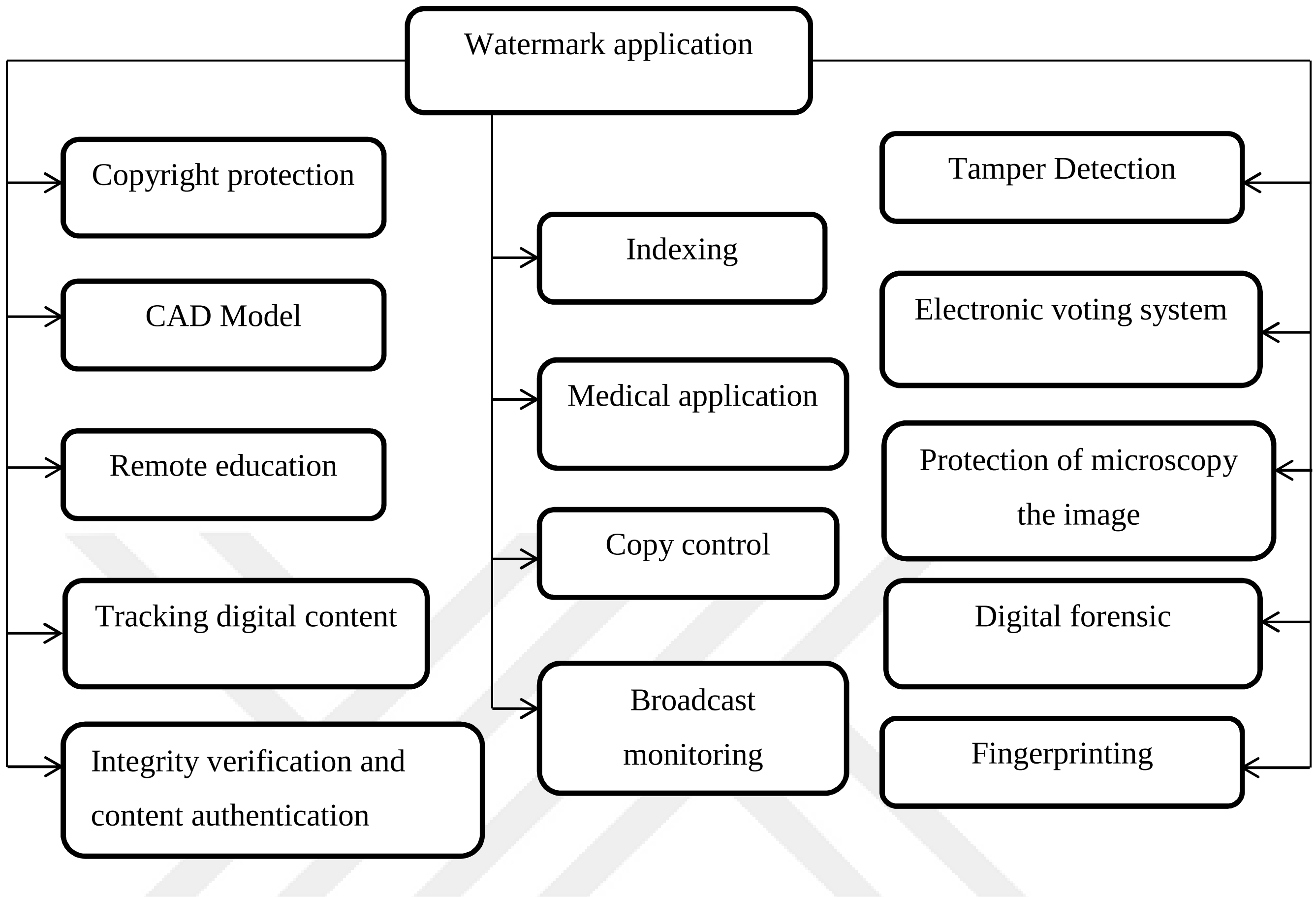


Figure 2.9: The applications related to watermarking digital images[25].

The table (2.4) has shown below explains the specific implementations that the design requires[25].

Table 2.4: Clarifies requirements of design and applications of the corresponding their[25].

Requirements	Application
Security	data authentication, Copyright protection, medical applications, indexing, and telemedicine data exchange, fingerprinting, and tracking to digital content..
Imperceptibility	Copyright protection and fingerprinting.
Reversibility	Medical applications.
keys of Watermarking	copyright protection.
False-positive	Ownership and copy control.

Capacity	Integrity and tamper detection of images of medical.
Robustness	Integrity verification, copyright protection and control authentication.
Cost of computational	Protection of the microscopy image
Resistance of tamper	copyright integrity and authentication.

From all this, we conclude the most important requirements of the watermark are authentication, availability, confidentiality, and integrity the figure shows a graph of the requirements of watermarks and the fields that can be applied to them[66].

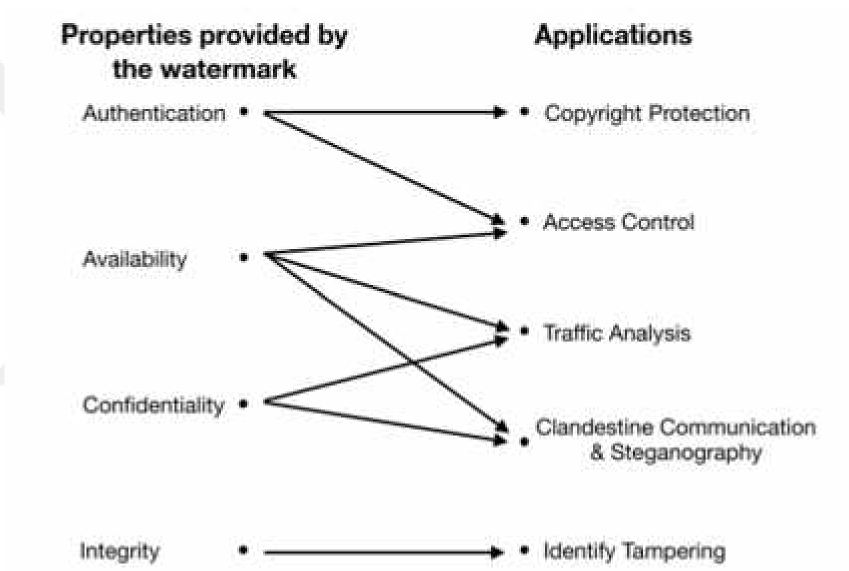


Figure 2.10: shows a diagram of the requirements and applications of watermarking[66].

2.8.6 Copyright Protection

It is one of the applications of watermarking to identify and protect the ownership of copyright and prevent others from claiming ownership of that digital media. I am the owner and the controversy raised about it. It is not possible to simply extract the included information and easily determine who is the owner of the original product. When the watermark is visible, it is not necessary to extract the data because it is visible, and the invisible watermark is used to preserve precious images in the field of art and photography by placing embedded data as a watermark to preserve the ownership of the images, as it includes the ownership information of the mark in the digital contents, in a way that is characterized by high hardness and confidentiality to resist attacks, and discover the manipulation that occurs on the data, and it is possible to discover fake images from real images[16][66][69][70].

2.8.7 Biometric Watermarking

It is a technology that establishes an association between a physiological trait of a human being by embedding information into a digital subject, and that the biometric watermark is increasingly important today and is used for authentication systems, protects the property rights of the owner, and prevents anyone from claiming to be the owner through the reliability that this provides The advantage , and the method of identifying an individual's personality from his identity is called Personal Authentication[14][71] .

2.9 HUMAN IRIS STRUCTURE

The iris is a circular contractile membrane of the eye between the pupil and the sclera, which is the central part of the uveal membrane that covers the eye and is covered by the cornea. The iris contains an inner circle, the pupil, which is usually dark. The structure of the iris tissue (Iris texture) is determined randomly at the stage of development of the eye of the fetus. It is worth noting that the randomness in the structures of the iris is so strong that no two people in the world have the same iris even in the case of identical twins. Rather, the iris differs between the right and left eye in the same person , The formation of the iris begins in the fetus in the third month of pregnancy and the patterns (patterns) and structures that give the iris its individual characteristics are formed in the fetus in the eighth month, although the accumulation of pigments (pigments) in the iris may continue in the first year of the child’s life. The iris then contains many complex patterns and parameters that are unique. For example, Furrows, Arching Ligaments, Ridges, Crypts and we discover through the details of tissues arising from sutures, crypts, radial grooves, pigment and actuate ligaments the uniqueness of iris patterns,

The randomness of iris patterns enables reliable and reliable discrimination decisions to be made and supports fast, reliable, and comprehensive database searches[72][73][74]. The following figure 2.11 represents the anatomy of the human eye in complete parts[73].

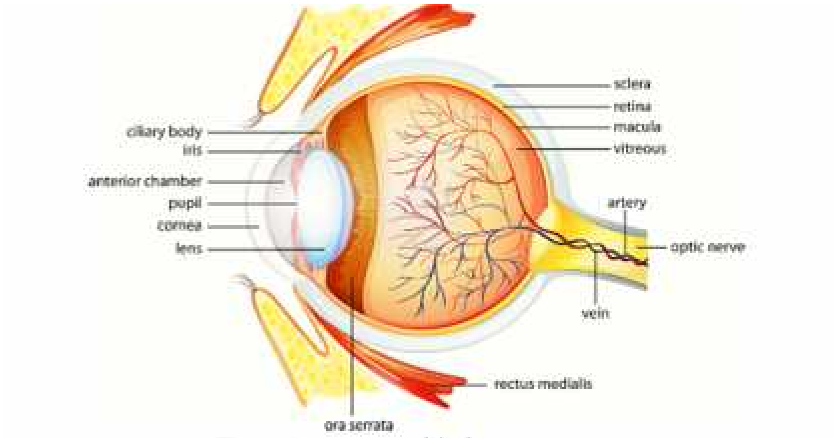


Figure 2.11: The anatomy of the human eye[73].

2.9.1 Advantage Of The IRIS

There are many biometric features that can be used in biometric systems such as face, fingerprint, palm print, iris, ear etc., but among the available features, some are superior to others considering that the greatest focus in biometric systems is to find patterns in biometrics. The chosen attribute is unique so that it helps to uniquely identify the user, and the chosen attribute must not be easily changed by natural causes such as temperature, climate, age, disease , as the iris has a complex and detailed structure, as well as being stable over time, making it the ideal solution for biometric applications[75][76].Figure 2.12 shows different and random patterns of iris tissue[77].

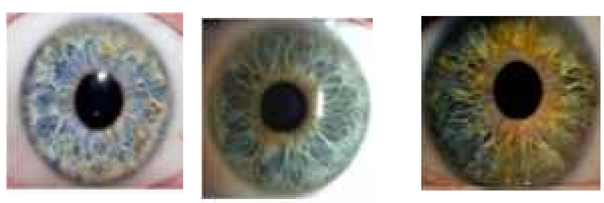


Figure 2.12: Different iris shapes[77].

Another advantage of using the iris in biometric systems is that glasses and contact lenses do not affect the work of these systems, and that only a few complex surgeries can affect their installation, and in this case the user must re-register in the system only once in order to continue working normally It is worth noting that blind people can use iris-based biometric systems as long as they have an iris that can be read by the sensor, and they are recognized and their identity on a regular basis [77][78][72].

In addition to the above, the human iris has other characteristics that enhance its suitability and suitability for use in the automatic identification of people[75][79]:

a. The iris has protection from external factors and from the environment, the protection is the eyelids, eyelashes, and the cornea.

b. It is almost impossible to surgically change it without the risk of affecting or losing vision, and scanning the iris of a dead person is never identical to a living person.

c. It is easy to take pictures of the iris with the sensor even from a distance (up to three meters).

2.9.2 Characteristic Of The IRIS

The IRIS of the human eye contains two essential qualities that are among the greatest characteristic that can be obtained in any biometric system: Uniqueness and Stability[9].

a. Uniqueness Property :The human iris is unique because the iris of no two people in the world is similar, even in the case of identical twins, and its difference even between the right and left eyes of the same person. The iris contains a set of properties, a parameter, or a distinctive property called degrees of freedom, which are used after converting them to numbers. Features in order to identify people[75][80].

b. Stability PropertyMost human traits vary over time. As for the iris, its shape does not change over time, regardless of some slight waviness in color that occurs in early childhood stages. The color of the iris does not affect biometric systems, because these systems use non-colored images in their operations. Its permanent color in the first months after birth is usually completed before the ninth month. One of the strengths of the iris is its stability throughout the human lifespan. This property, as well as the speed of comparing the iris with others, makes iris-based biometric systems a very suitable technology for comparisons and identification [73][81].

2.9.3 Iris Recognition

Since 1993, Daugman has introduced the iris recognition system[82], and this system is considered the basis to this day and is used in this field. The basis of the system is based on the data of the iris used using a video camera and determines the inner pupil and the solid outer borders, and the iris areas are covered by eyelids and eyelashes, which are Processed to extract the iris[79].Through this, we conclude that the term Iris Recognition refers to a system consisting of several stages that aims to identify an unknown iris in an image that includes a human eye using Computational Algorithms,the iris recognition system includes the following stages, Eye aquire, Iris Segmentation, Iris Normalization, Feature Extraction, and Iris Matching. The iris recognition system consists of several stages, as shown in the figure 2.13[83].

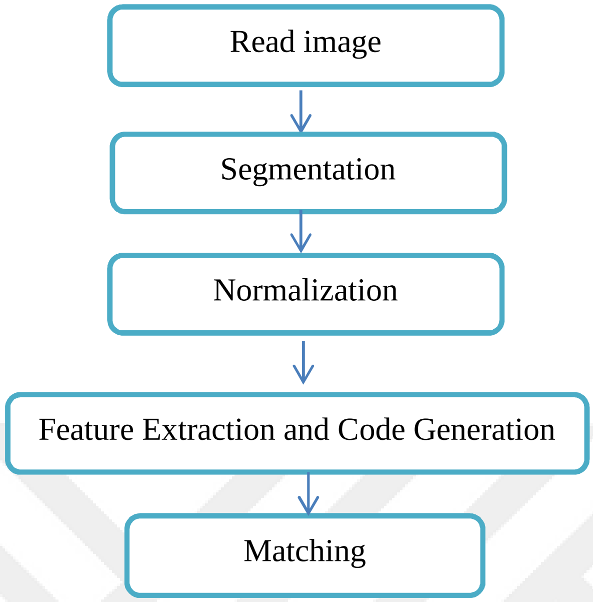


Figure 2.13: Box diagram of the iris recognition system.

2.9.4 Iris Recognition Application

The iris recognition system has a wide range of uses, especially when dealing with security applications, such as protecting personal computers and controlling physical access to them, identifying people in real time and ensuring their authentication, sorting and monitoring criminals, and many other uses. After picking it up from the sensor and converting it to a digital form and properties, it will be used to provide a mathematical representation for each person so that he or she can be identified and his identity in an absolute and unmistakable way. This system, as well as many other countries, considered it a definitional platform for the authentication of persons.India has adopted a unique identification system (UIDAI) Adhar card, which is iris data in a complete database through which people are identified and identified, so it is difficult to deceive the government with fraud or deception by concealing the identity of the unauthorized person[84].

2.9.5. Dependence On IRIS Property Protecion

The property rights of a picture or any specific medium can be guaranteed by hiding the iris code inside the image, which is an effective way to protect the rights of the owner of that image, as it guarantees his full rights to own that image and preserve it from piracy. LSB that uses the XOR method[84][85].

2.10 LITERATURE SURVEY

To protect the reliability of data and the identification of people, biometric traits have been widely used in the field as an example is the use of the iris, they suggested.

Chirchi et al [86] a person identification system to confirm authentication. Depending on the iris, they used the CASIA iris database with the UBIRIS Iris database, which contains a long-range image taken of people from long distances with an effective methodology for detecting the iris of the eye, although the images contain visual noise, different levels of lighting and obstacles.

The cloaking watermark algorithm has been used in many types of biometric-based research, including iris discrimination.

In his research, Lu et al [87] used the watermark algorithm to identify the iris and the coding algorithm (DCT) using the BCH error control coding, where the image was divided into four parts and the BCH code was hidden in each of the four parts of the image, and the image processing was performed by processing Presets, normalizations, CD, FR, and FA scales were used and tests were performed on them.

The diversity in the selection of the cover image has increased. After iris data was included in different images of landscapes, the embedding became within the vital body data.

The researchers, Lalithamani and Sabrigiriraj[88] included the eye data in the image of the hand veins, and the watermarking algorithm was used to hide after performing processing operations. Initialization of the two source and cover images and extracting their properties, and then embedding and comparisons were made. To know the accuracy of the results, FAR and FRR were used as accuracy measures.

Researcher Vyas et al [79] explained iris discrimination using (2-D Garbor filter, DCT, XOR and SUM operation). Acquisition, segmentation, normalization operations were performed on the image. After the treatments, Feature extraction was performed. Finally, matching operations were performed to start the discrimination processes.

In the same year, Kumar et al [89] distinguished and extracted the properties of the iris using the same algorithms mentioned above (2 D and DCT). Some preliminary operations were performed on the image, namely (acquisition, preprocessing), and then extracting properties and matching. The process of Normalization by Daugman rubber sheet model for matching (Hamming Distance), the accuracy of the results was measured using the (Distance matric and false acceptance rate).

In this paper, the researcher explained Jie et al [90]the use of the fingerprint as a cover image to hide the data by applying the LSB Bit replacement algorithm to the image after performing the matching and feature extraction operations, and the results were tested using the FAR scale.

While Pandey and Patil [91] hid the iris information inside the ear, where initial processing operations were performed on the images represented in image optimization and feature extraction, then localization and then image normalization in order for the resulting images to be ready for encoding. Watermarking and Scramble were used to mask, As for the accuracy measures, FAR and FRR were used.

Whereas Dwivedi et al [92] explained the concept of human confidential data using Zero bit watermarking in the image of the iris and used DWT and SVD to strengthen Zero bit watermarking and make it more stable and solid if it was attacked. The efficiency of the algorithm, and the results have also proven its reliability because each image has a secret key that is a fingerprint and is unique, so it is preferable to use the system methodology provided in the security of biometrics for images and a good way for applications that need security such as verification, sharing and checking for violations.

While the researcher Singhe et al [93] in this research used the iris as a host image and the palm as a watermark image, and to strengthen and activate the algorithm, the three techniques were used, namely Parallel bacterial foraging optimization (PBFO) and the second Discrete cosine Transform (DCT) as well as use Discrete wavelet transform (DWT) where the palm print is included within the iris data, the union between the palm and the iris is complementary to reliability, and the aim of this research is to understand the concept of reliability and improve the confidentiality of the user's means of communication, and the researcher found that the palm is useful and effective To document the iris fingerprint in this research.

3. METHODOLOGY

This chapter deals with the steps of the proposed system for protecting property rights for images using the biometric watermark, the human iris. In our time with technological developments, it has become important to use biometrics as the best solution to authenticate and verify a person through behavioral or physiological features, as the biometric system works to reduce intellectual theft, protect the property of the person and guarantee his rights. In this research, we included the iris code and considered it a sign Invisibly watermarked a group of images, and thus we managed to not attract the attention of hackers and subversive attackers, and we used color images, which are considered highly efficient compared to images that adopt the traditional gray-scale watermark. The watermark is a modern and approved technology that aims to provide reliable information It is very and not falsifiable, meaning that it is considered the most appropriate way to protect images or authenticate copyright protection.

3.1 THE PROPOSED SYSTEM FORPROTECTINGTHE COPYRIGHT OF IMAGES

The research proposes a system to protect images from piracy and forgery that is widespread on the Internet and to prove the ownership rights of the owner of these images, and the system extracts the iris code and includes it as a watermark inside the image, the system consists of two basic stages, the first is for obtaining the iris code, and it takes place in the second stage Adding the iris code as a watermark to the image to be protected using the LSB algorithm, which adopts the (XOR) method to include the iris code and hide it in the image to be protected.

3.1.1 Iris Code Extraction

Iris code extraction stage consists of several steps, as shown 3.1. In the beginning the image of the eye is read, and then the primary processing for the eye is done, after that the iris is extracted, then the image is transformed into a rectangular shape, the characteristics are extracted and the iris code is generated.

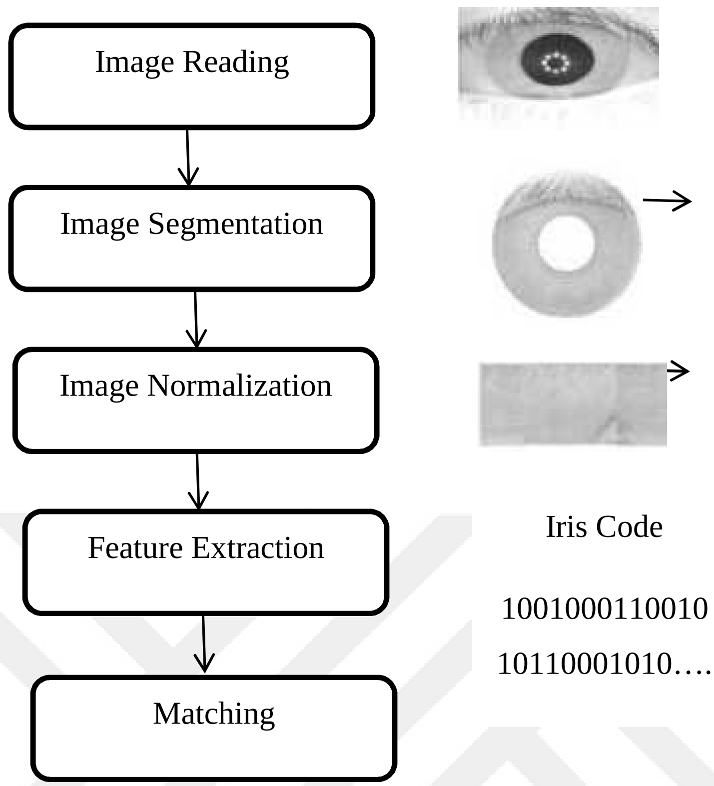


Figure 3.1: Iris code Extraction

3.1.1.1 Iris Image Preprocessing

At this stage, primary processing is done on the eye image with the aim of improving the image and preparing it for next processing, Image preprocessing aims is to remove noise in images of the iris, data simplify and enhance information [94]. That's why Gaussian Filter is used to improve the image characteristics, which is known as the next equation [95]:

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{\frac{x^2+y^2}{2\sigma^2}} \tag{3.1}$$

Since x represents the distance from the original point to the horizontal axis, and y represents the distance from the original point to the vertical axis, and σ represents the standard deviation of Gaussian distributions.

3.1.1.2 Iris segmentation

At this stage, the sever iris region is extracted from the eye image, by specifying two inner circles around the black area of the eye (the pupil) and external around the coloured area of the eye (the iris). For this purpose Daugman's Integro - differential Operator was used, and at this stage, the upper and lower eyelids are also isolated in a line using Hough Transform (HT) [96]. As in Figure 3.2.

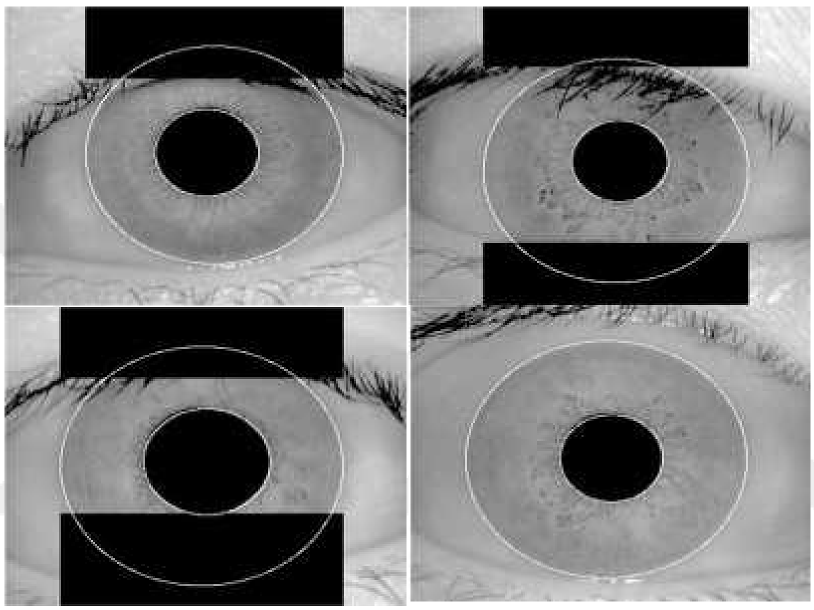


Figure 3.2: Iris Segmentation For Different Images From Casia.

A. Finding the approximate location of the iris center

as mentioned previously, Daugmam's Integro - differential process was approved to locate the inner and outer circles of the iris of the eye. In order to implement this process, at first, the process (Binarization) is performed and the image is transformed from gray to the Binary on the path of (Thresholding), it is takes rid of the weak edges under a low threshold which is converting the image to Black and White (BW) [97] , since all points above the threshold equal 1 and all points below the threshold equal 0, and then comes the Morphological Operator stage , Morphology is a wide set of processing of image operations that process images based the shapes. which is a set of image processing operations related to the shape and the process is done to scan the noise and these processes include reduction and stretching used to ensure the boundaries of the object without changing the area of each of them, and we used the Dilation process to clear the pixel which is unwanted, that is to make the image slim [98], then after that an approximate location of the iris center should be determined . For this purpose, the center of mass of pupil is determined by the calculation of all X and all Y points, and then finding the average for each of them.

B. Determine the inner and outer circles of the iris periphery

Daugman's Integro-Differential Operator is an efficient method for discovering circuits in an image. This process has been used to discover both the periphery of the iris (the outer circle) and the periphery of the pupil (the inner circle). The Daugman's Integro-differential Operator operation is known as the following equation:

$$\max_{r,x_0,y_0}\left|G_{\pm}(r) * \frac{\partial}{\partial_r}\oint_{r,x_0,y_0}\frac{I(x,y)}{2®r}ds\right| \qquad (3.2)$$

Since (x, y) are the coordinates of the eye image, and r is the radius, used to search for a function $G_{\pm}(r)$ which is a Gaussian smoothing function, and s represents the circumference of a circle whose points are(x0, y0) and. r This process is applied multiple times with the Smoothing process for precision [96].

C. Eylids detection

After determining the inner and outer circles of the iris, the (upper eyelid) and (lower eyelid) are discovered and separated using the Hough Transform method. It is used to find the radius of the circle and the coordinates of the pupil and iris area according to the following equation [99]:

$$x_c^2 + y_c^2 - r^2 = 0 \qquad (3.3\ )$$

D. Eyelashs removed

There are two types of eyelashes (separate, multiple) that clump together to overlap the image of the eye, and the eyelashes are separated using a (thresholding) limit, and based on the observation that the color of the eyelashes is usually black and dark, an experimental value is determined for the threshold limit used to separate the eyelashes [100].

3.1.1.3 Normalization

After the iris is deducted from the image of the eye, the second stage takes place, which is the Normalization stage, which aims to convert the iris into fixed dimensions suitable for the stage of extracting the iris code. The Daugman Rubber sheet model is adopted, and the homogeneous Rubber sheet model is used for the Normalization process. Each point within the iris region is represented by a pair of coordinates (x, y), and (r) representing the radius, and an angle *(¯)* and is confined between the period *[0. 2®]* as in Figure (3-3) illustrating the Rubber sheet model [101].

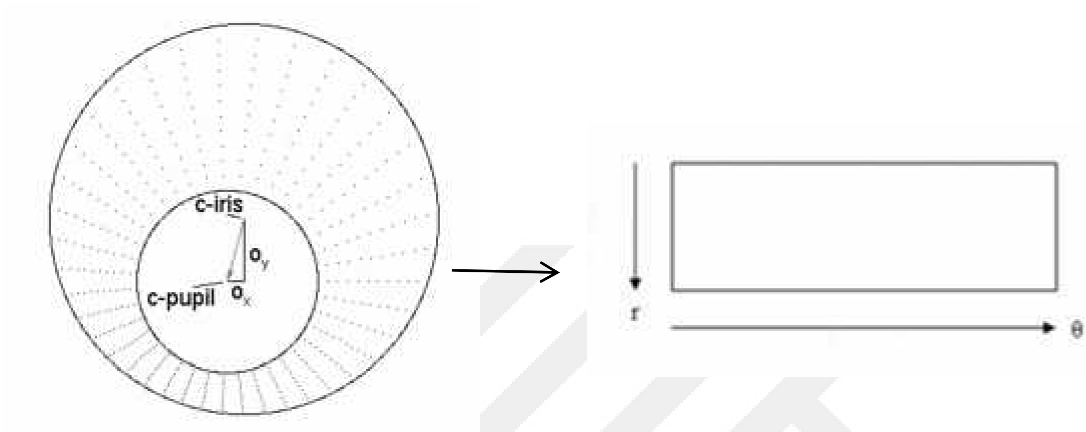


Figure 3.3: Daugman Rubber sheet model [101]**.**

The following equations represent the non-concentric (x, y) coordinates:

$$I(x(r,¯),\ y(r,¯)) \rightarrow I(r,¯) \tag{3.4}$$

and

$$x(r,¯) = (1 - r)\,x_p(¯) + r x_s(¯) \tag{3.5}$$

$$y(r,¯) = (1 - r)\,y_p(¯) + r y_s(¯) \tag{3.6}$$

Since (x, y) represents the original coordinates of the iris region in the image, (r, ¯) represents thecoordinates of Normalized Polar, and x_p, y_p and x_s, y_s represent the pupil and iris coordinates towards the angle [101] .

3.1.1.4 Feature etraction and encoding

The stage of extracting the iris code One of the most important stages in systems that depend on the iris, as the accuracy of these applications depends greatly on the results of this stage. For this purpose, one of the types of Gabor Filter has been adopted in this research, which is the 1D Log Gabor Filter , filters of log-Gabor are more broadly used for natural coding photographs [7]. Filters of log-Gabor are more widely used for coding photographs of natural The Gabor filters can prepare the best wave and display it in the spatial space and the frequency spectrum, and the Gabor filter of a Sine wave and a Cosine is combined with a Gaussian signal, For signal analysis, a quadruple pair of Gabor Filters are used, as the real part is assigned by a Modulation Cosine with a Gaussian signal, and the imaginary part is assigned by a Modulation Sine with a Gaussian signal .To avoid the disadvantages of Gabor filters, It was adopted 1D Log Gabor Filter Which is known by the following equation[102]:

$$G(f) = \exp\left(\frac{-(\log(f / f_0))^2}{2(\log(\pm / f_0))^2} \right) \tag{3.7}$$

Since f0 represents the center frequency. and σ represent (Bandwidth) of the filter.

3.1.2 Apply The Hide Algorithem Using Least Significant Bits Algorithem (LSB)

The second stage of the proposed system is the apply hide algorithm iris code inside image. And for this, Least Significant Bits Algorithm (LSB) method was used to obtain the watermark that represents the iris code, as the iris code is hidden in the far right bit (Bit0) by using the (XOR) method between the image data and the iris code within the binary sentence consisting of 8 bits that represent Gray values for the image. This bit has been chosen exclusively, because any change in its value represents a very small difference in color, for pure black color, for example, carries the value (00000000), and the black color with the value (00000001) also represents a black color, and the difference between it and the previous color is difficult the human eye should distinguish it. Figure (3-4) shows the image whose ownership is to be protected (Cover Image) before hiding the watermark (iris code) and after obtaining a Watermarking Image.

(a) Cover image

(b) Watermarking image

Figure 3.4: The cover image before and after hiding the watermarking (iris code).

In general, the algorithm for hiding the watermark (Code of iris) by adopting the LSB method includes the following steps:

The first step: Read the image (the cover image) in which you want to hide the iris code. The second step: Make sure that the length or size of (Iris Code) is smaller than the size of the cover image, and then transfer the image data to the binary system.

The third step: For each bit of the Iris Code, a specific byte of the Cover Image, the following steps are taken:

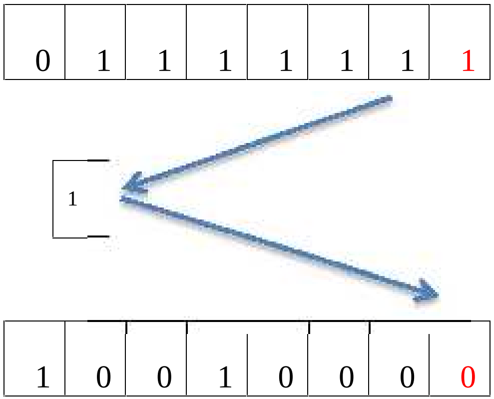
1- First byte of original data from the Cover Image :

0	1	1	1	1	1	1	1

2- First bit of the data to be hidden :

1

3- XOR between code and second bit of image :



4- save result in first bit of image.

Fourth step: Repeat the third step to hide every bit of the iris code.

Figure (3.5) is shown below and represents the steps of the previous hiding algorithm:

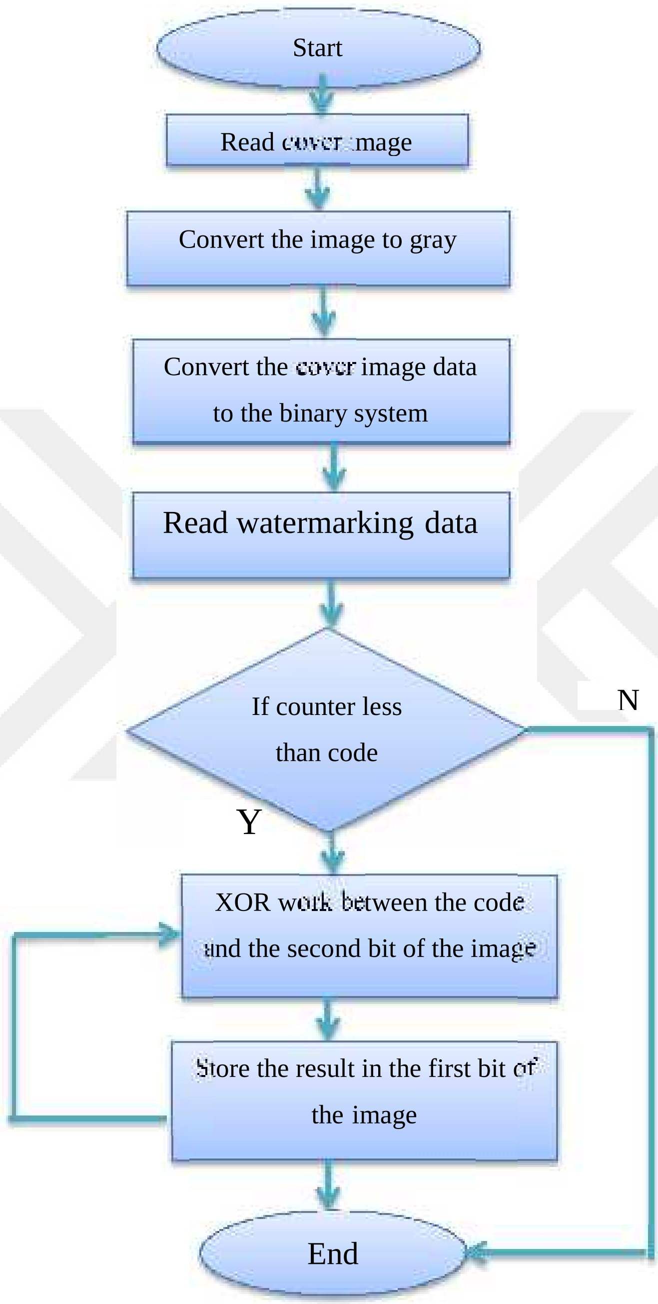


Figure 3.5: The steps for hiding the watermark (iris code).

3.1.3 Watermarking

The process of obtaining the watermark in order to verify the ownership of a particular image consists of the following steps: the difference from the concealment steps, making the XOR between the first bit and the second bit of the image values and storing the result with a variable, then converting the variable's value to the decimal system and writing the result in a file named Result and recovering the original message Figure (3-6) below shows the steps for retrieval.

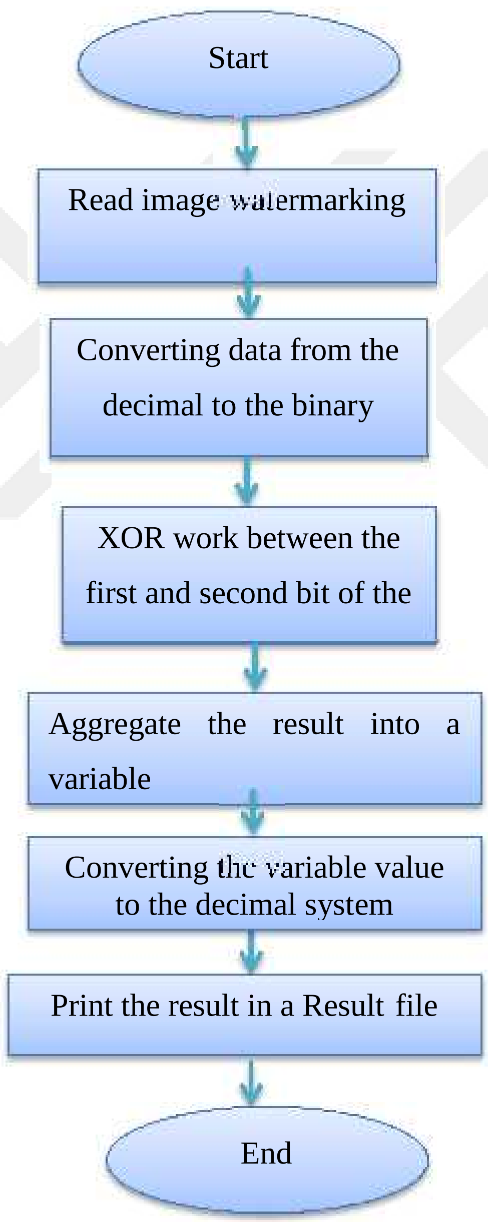


Figure 3.6: Flowchart showing the algorithm retrieval steps**.**

3.1.4 Matching

Hamming Distance ,It gives a measurement of how many bits are the same between two models, and uses Hamming Distance for two models, and the decision can be taken for the two models generated from different irises or from the same iris and the significant distance is represented by the following equation: [103].

$$HD = \frac{1}{N}\sum_{j=1}^{N} X_j \oplus Y_j \qquad (3.8)$$

By implementing the proposed system we used the Hamming distance for matching that Daughman used and includes noise masking so that only significant bits are used between the two iris models when calculating the Hamming distance between them[100].

4. RESULT ANALYSIS

This chapter details the results obtained through the application of the proposed system of property protection for images using the iris-based watermark, It also deals with the analysis of the results obtained by shedding some noise on the images resulting from the application of the system, and the iris code before and after the addition is also compared as a watermarking.

4.1 CASIA IRIS IMAGE DATA BASE

The CASIA database, (Chinese Academy of Sciences – Institute of Automation) is one of the most widely used iris image databases for selecting applications, that adopt iris The first edition of the CASIA Image Database includes (756) images of the iris from (180) eyes, and (108) items for each eye, and 7 samples of images were taken in two sessions, three samples in the first session and four samples in the second session[104]. The iris code of 25 images for 1CASIA database (bmp) and size (320 * 280) was extracted in this paper.

4.2 RESULTS OF THE PROPOSED SYSTEM

As mentioned previously, the proposed system includes two basic parts, the first for obtaining the iris code, and the second for adding the iris code for a watermark in the cover image.

4.2.1 Segmentation Results

The iris recognition system is based on the efficiency and precision of the iris segmentation
As the extraction iris from the pupil, sclera, eyelashes, eyebrows, the skin around the eye is known as iris segmentation [105].The first part includes a stage to subtract the iris of the eye, as in the first step of this stage the approximate location of the iris center is obtained, And in the next step, the inner circumference (the circumference of the pupil) and the outer circumference (the circumference of the iris) were determined using Daugman's Integro-differential Operator and in Figure (4-1) the results of the excision phase of the iris in the proposed system for several images from GASIA.

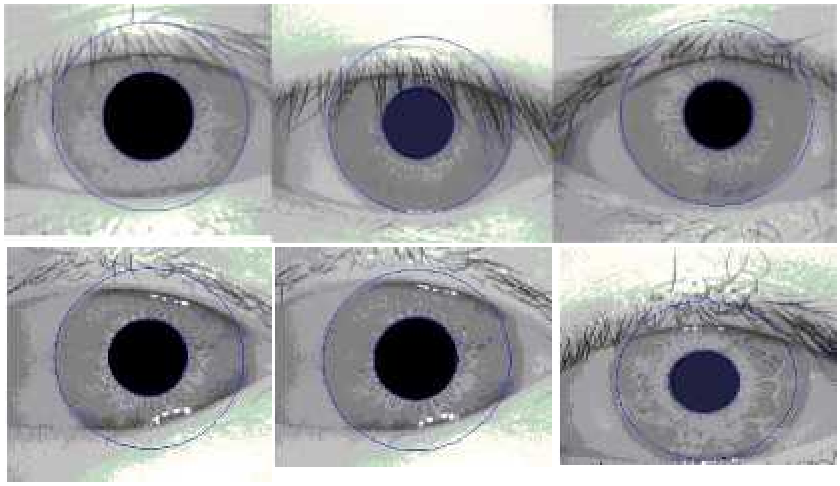


Figure 4.1: Segmentation results for different CASIA images.

Figure 4.2 shows the steps for obtaining the iris code and the stages that one of the CASIA images went through, which includes the Segmentation stage, and then the Normalization process.

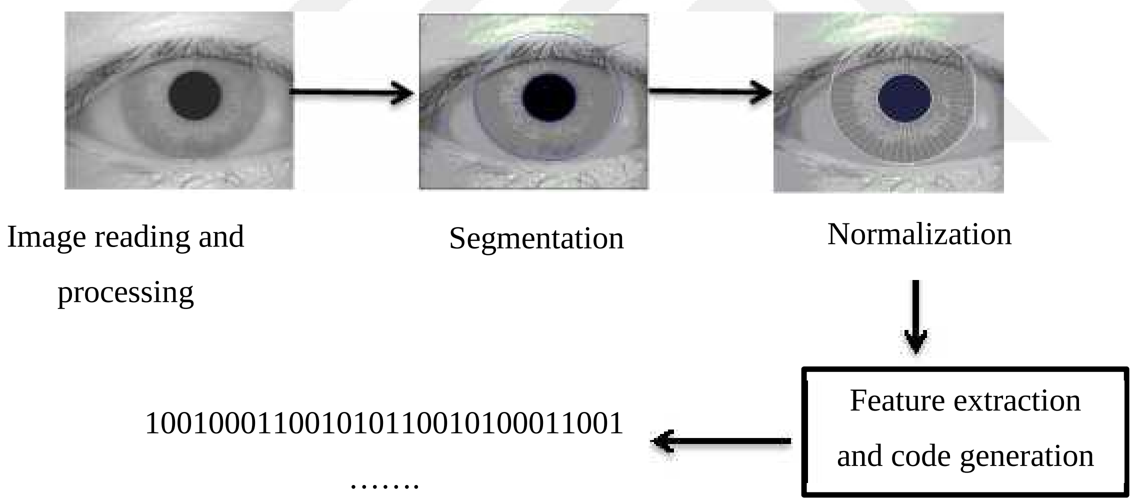


Figure 4.2: The stages of extracting the iris code.

4.3 INSERT THE IRIS CODE IN THE COVER IMAGE

After obtaining the iris blade, this code is inserted as a watermarking in the image of the cover to be protected by using the LSB method that adopts XOR. Figure(4.3)shows the result of applying the process of inserting yhe iris code to several CASIAI image of the type (bmp). And dimensions(320*280), the figure shows the pictures before and after the insertion process.

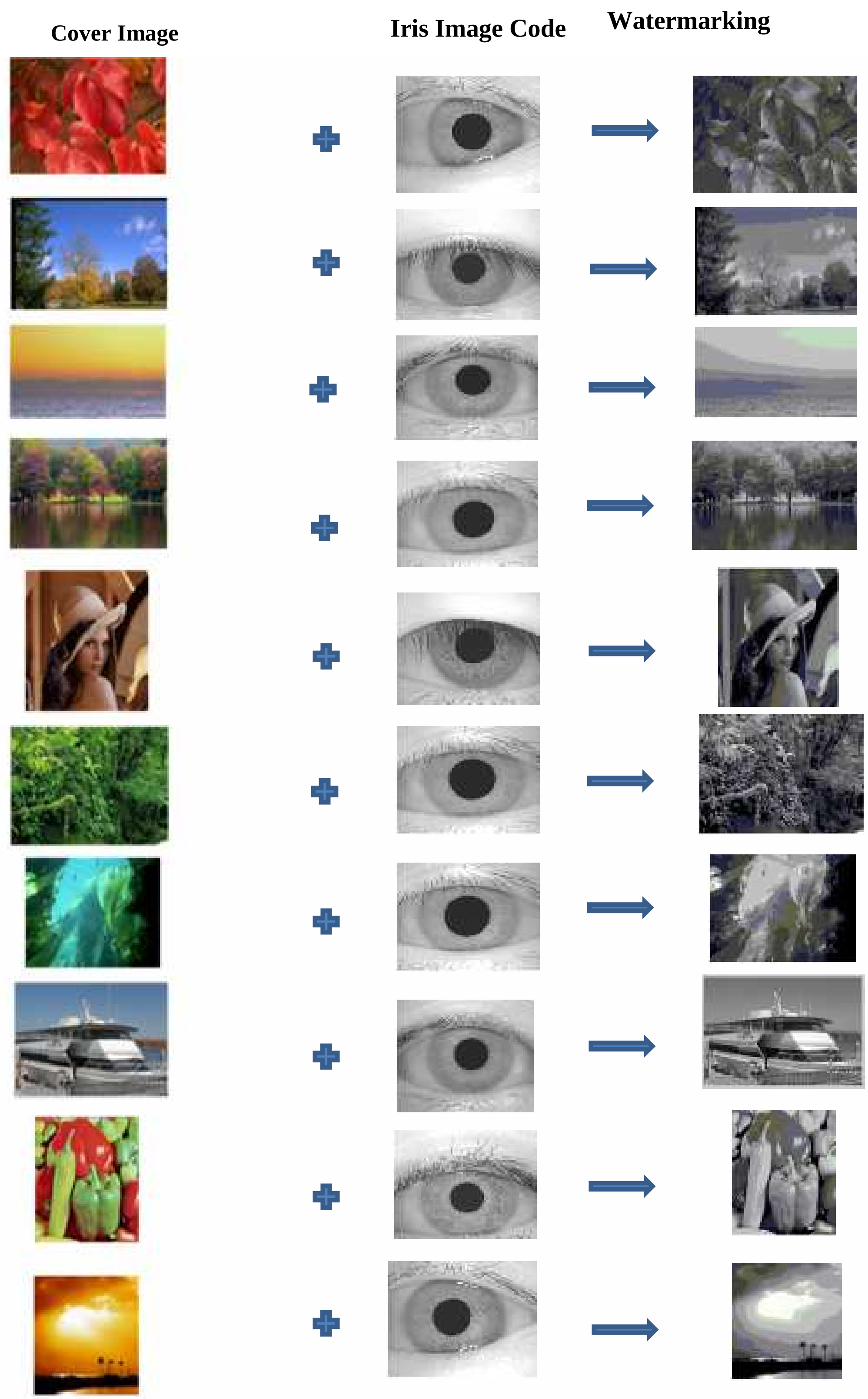


Figure 4.3: Embedding the iris code of a number of CASIA1 images in several images whose ownership is to be protected.

4.4 QUALITY MEASURMENT TECHNIQUE

There are several image quality techniques that are used to great extent in the evaluation , to assess image quality, we used metrics such as Mean square error (MSE), peak signal to noise ratio (PSNR), and Normalized correlation (NC)[106].

MSE, PSNR and NC are standard criteria for estimating the efficiency of watermark algorithms.

A. Mean Square Error (MSE)

It is defined as the square of error between the cover image and the cover image embedded with iris cod (watermark image), and the amount of distortion in the image can be measured using MSE[107]. MSE can be calculated using the following equation[108]:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(Wxy - Cxy)^2 \qquad (4.1)$$

Note that M, N: represent the image dimensions.

Wxy, Cxy: Image represents the cap and image watermarking on the sequence.

B. Peak-Signal-to-Noise-Ratio (PSNR)

It is a measure of the quality of the watermarking image by comparing the cover image with the watermark image. PSNR can be calculated using the following equation[106]:

$$PSNR = 10\log_{10}\left(\frac{Cmax^2}{MSE}\right) \qquad (4.2)$$

Cmax: The highest color value in the image, and its default value for 8 bit images is 255.

C. Normalized Correlation (NC)

It is a measure of the similarity between the watermark image and the cover image and has a value between [0, 1], and it can be calculated using the following equation:

$$NC = \frac{\sum_{x=0}^{m-1}\sum_{y=0}^{n-1} waterim(x,y) * cover_{imm(xy)}}{\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}((cover\_im(xy))^2} \qquad (4.3)$$

If NC = 1 then the watermark image and the cover image are the same, in general if the value of NC = 1 then it is considered an acceptable value to extract an acceptable watermark.

Note that:

n, m: represent the image dimensions.

Waterim, coverimm: represent the watermark and cover image on the sequence[109].

4.4.1 Result analyses

To analyze the effect of adding the iris code in the cover image, the measurements mentioned in the previous paragraph of the images were calculated after applying the proposed system to them and adding the iris code from one of the CASIA1 images. Table (4-1) shows the metrics values (MSE, PSNR, NC). Which were calculated for the photos before it was attacked.

Table 4.1: Application of metrics (MSE, PSNR, NC) before the attack.

NO.	The name of the image	Dimensions/PIXEL	MSE	PSNR	NC
1	Boat	142*256	0.0052	60.3784	0.9976
2	Better reflections	292*459	0.0034	61.4342	0.9970
3	Sunset	388*616	0.0041	68.6055	0.9998
4	Peppers	487*507	0.0039	63.9899	0.9969
5	Sky	477*479	0.0048	70.9855	0.9974
6	Leaves	392*650	0.0023	69.7564	0.9984
7	Lena	512*512	0.0047	66.6997	1
8	Undersea	409*633	0.0038	67.1096	0.9978
9	Tree	400*764	0.0014	76.2312	1
10	Nature	323*529	0.0027	65.5637	0.9981

Through Figure (4-3), and noting the PSNR values that ranged between (60.3784) and (76.2312), we conclude that there are no noticeable distortions in the cover image after adding the iris code to it, meaning the inability to detect the presence of a watermark in the image. This indicates the efficiency of the proposed system in the inclusion of the iris blade in the cover image. Also, the NC values ranged between (0.9969) and (1), which means that the secret message (iris code) is stable and not subjected to a clear, and that the MSE values ranged between (0.0014) and (0.0052), which means that there is no noticeable distortion in the cover image. In addition to the above, the values mentioned in Table 4.1 prove that the proposed system is capable of extracting the watermark in the cover image with the lowest possible error rate.

4.4.2 Analysis of the Attack

A salt & pepper attack type added noise to the watermarked images. This is in order to verify the efficiency of the system. After inserting the watermark in the image, the cover adds salt and pepper noises, which are one of the most common types of attacks used[110].

Figure (4.4) shows a picture of the watermark after it was attacked.

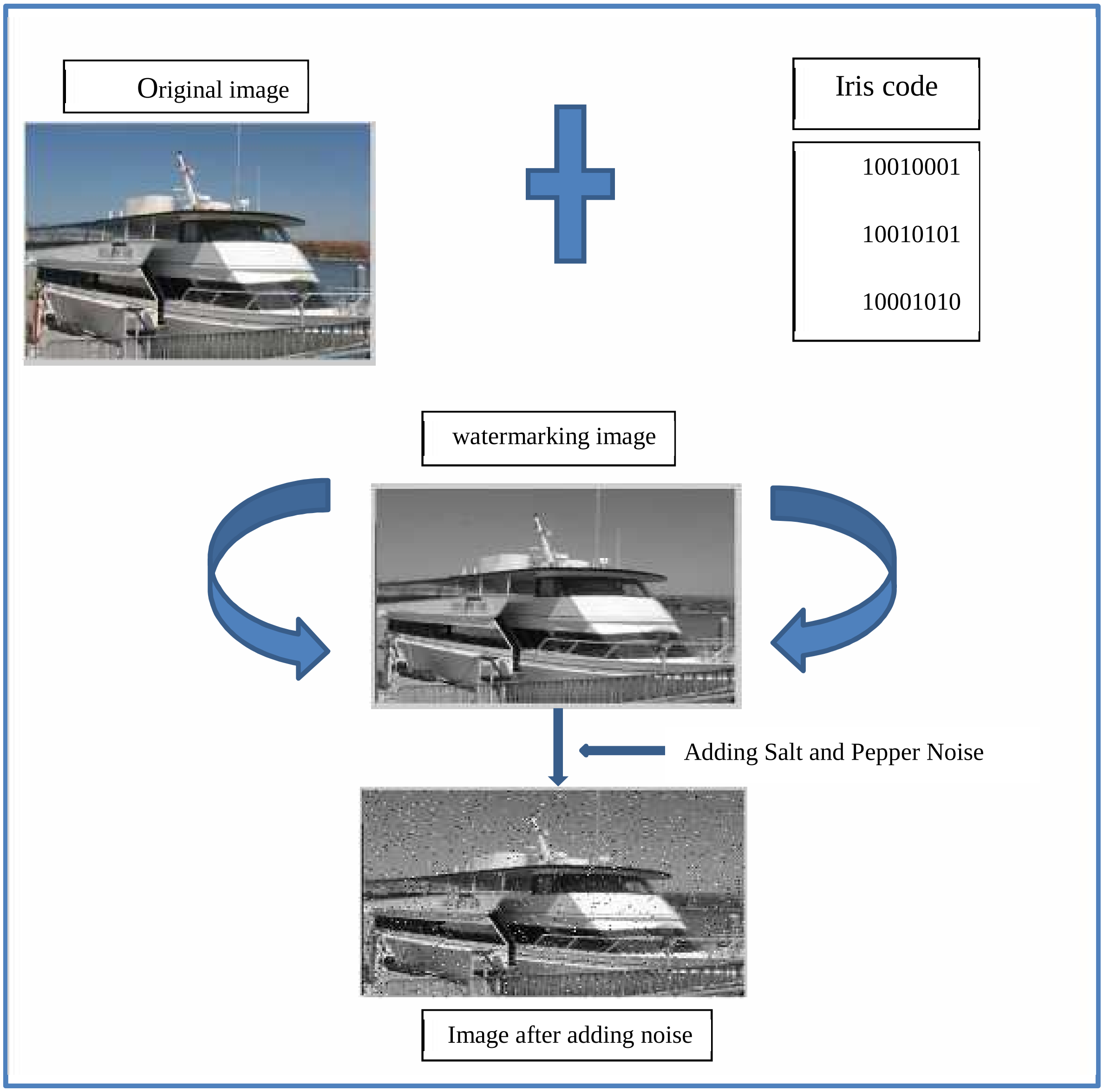


Figure 4.4: Adding salt and pepper noises to the hood image after embedding the iris code in it.

Both Table (4-2) and Figure (4-5) show the effect of noise of the type Salt and Pepper = 0.01)) in a group of ten images for which the watermark was added, by adopting the calculation of the value of (MSE, PSNR, NC) before the attack. And after. From the analysis of the values in Table (4-2), it can be concluded that the proposed system is efficient and that no major distortions will occur, which will ensure that adding a watermark to the images whose ownership is to be protected is not detected. Certainly, there must be a slight effect before and after the attack.

Table 4.2: Application of metrics (MSE, PSNR, NC) after the attack for the salt and pepper noise value = 0.01

NO.	The name of the image	Dimensions/PIXEL	MSE	PSNR	NC
1	Boat	142*256	0.9998	57.3871	0.9969
2	Better reflections	292*459	0.9969	58.9989	09961
3	Sunset	388*616	0.8976	60.9899	0.9989
4	Peppers	487*507	0.9089	59.9870	0.9962
5	Sky	477*479	0.8988	65.0045	0.9970
6	Leaves	392*650	0.9845	63.8745	0.9979
7	Lena	512*512	0.8780	61.8707	0.9984
8	Undersea	409*633	0.8785	61.6453	0.9960
9	Tree	400*764	0.7898	6602731	0.9988
10	Nature	323*529	0.8974	60.0001	0.9973

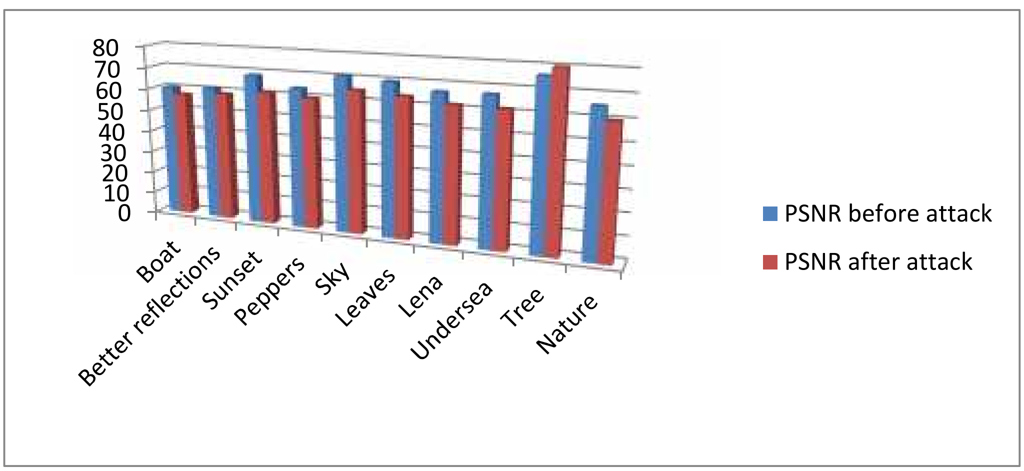


Figure 4.5: Scheme representing pre- and post-attack PNSR values.

And by noting Table (4.2) and Figure (4.5), the following is evident:

. The PSNR values ranged between (57.3871) and (66.2731), indicating that the algorithm was implemented correctly and efficiently.

. The PSNR values between the cover image and the Watermarking image were large indicating that there were no noticeable distortions, that is, the algorithm achieved a high percentage in the inability to distinguish the cover image from the Watermarking image, or in other words the inability to detect.

. It must be remembered that the main purpose of watermark algorithms is to include data in the overlay image in a manner that does not raise suspicion, and to extract the embedded data in the highest possible proportion.

. The NC values ranged between (0.9960) and (0.9989), which means that the secret message is stable and not exposed to obvious change.

. The MSE values ranged between (0.7898) and (0.9969), which means that there is no noticeable distortion between the cover image and the Watermarking image.

. The expected attack on such types of Watermarking may include many types. Therefore, the Salt & Pepper attack was chosen as one of the most common and
Used types of attack.

. The difference can be observed with the PSNR values before and after the attack, which is an indication of the efficiency and ability of the algorithm to be exposed to other types of attack.

And Table (4.3) and Figure (4.6) show the metric values after the attack value changed to 0.03.

Table 4.3: Scales Application Post-attack for Salt and Pepper Noise Value = 0.03.

NO.	The name of the image	Dimensions/PIXEL	MSE	PSNR	NC
1	Boat	142*256	1.8102	51.7638	0.9289
2	Better reflections	292*459	1.6607	51.7127	0.9293
3	Sunset	388*616	1.2723	57.6551	0.9476
4	Peppers	487*507	1.8703	50.7638	0.9301
5	Sky	477*479	1.8334	50.9989	0.96744

6	Leaves	392*650	1.1567	60.9876	0.9899
7	Lena	512*512	1.1904	58.3092	0.9899
8	Undersea	409*633	1.4573	58.8954	0.9398
9	Tree	400*764	1.0012	59.8721	0.9784
10	Nature	323*529	1.1724	57.9984	0.9549

And the Figure (4.6) is a chart showing the difference between the PSNR values after the attack when its value changes.

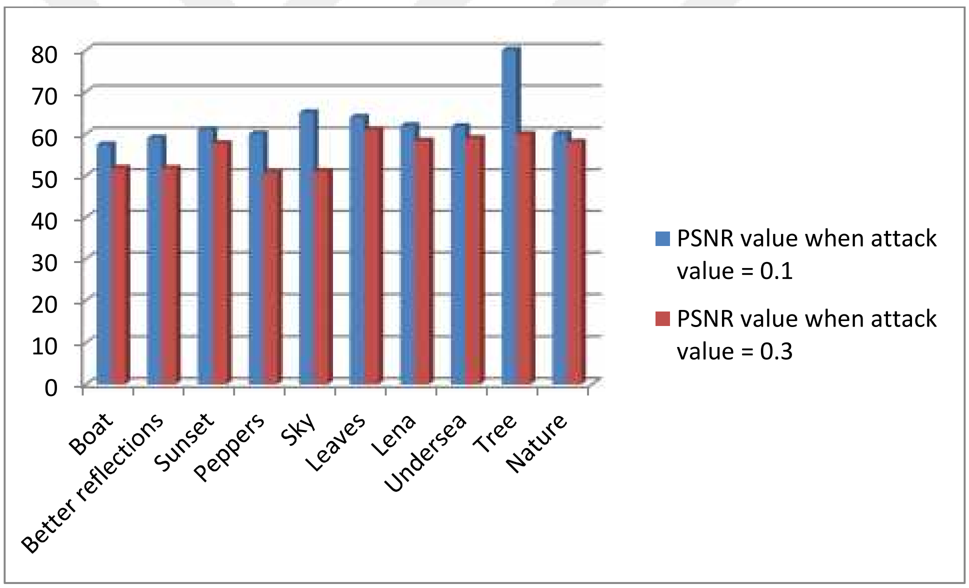


Figure4.6: The difference between PSNR values for two attack values.

By noting Table (4.3) and Figure (4.6), after the attack value has changed, the following is evident:

. The PSNR values ranged between (50.7638) and (60.9876) indicating that the algorithm was implemented correctly and efficiently after increasing the ratio of the noise value.

. The PSNR values between the cover image and the Watermarking image were large indicating that there were no noticeable distortions, meaning that the algorithm achieved a high percentage in the inability to distinguish the cover image from the Watermarking image, or in other words, the inability to detect.

. It must be remembered that the main purpose of watermark algorithms is to include data in the overlay image in a manner that does not raise suspicion, and to extract the embedded data in the highest possible proportion.

. The NC values ranged between (0.9289) and (0.9899), which means that the secret message is stable and not exposed to obvious change.

. The MSE values ranged between (1.0012) and (1.8703), which means that no noticeable distortion occurred between the overlay image and the Watermarking image after increasing the noise value ratio.

. The expected attack on such types of Watermarking may include many types, so the Salt & Pepper attack was chosen as one of the most common and used attack types.

Certainly there must be even a slight impact before and after the attack. The difference can be observed in the PSNR values before and after the attack after the noise value has changed and is an indication of the efficiency and ability of the algorithm to be exposed to other types of attack.

4.5 HAMMING DISTANCE

By implementing the proposed system, (10) Iris Code was hidden from CASIA1 images in different cover images, after retrieving the iris code from Watermarking Images and calculating Hamming Distance between the original and recovered iris code after adding noise. The HD values ranged from 0.0041 to 0.0053, indicating the efficiency of the Watermarking process.

5. CONCLUSIONS

As it is known, there are many and many algorithms for hiding in the watermark, but by representing the proposed system the results obtained from the practical implementation of the programs, the following was concluded: The algorithm used achieved good results in the concealment ratios, based on the analysis of the results, as well as through a comparison between the original iris code And extracted from Watermarking) by calculating the (Hamming Distance), we notice the result is zero without adding noise, and in the case of noise, we notice a small change between the values (0.0041)) and (0.0035). That ensures protection and reliability high prevents piracy of precious images and thus guarantee the property rights of the person. As well as the high-capacity embedding method in the spatial domain, and the strength of the algorithm used was proven.

5.1 RECOMMENDATIONS AND FUTURE WORKS

Through working in the stages of designing and representing the current system, a set of recommendations for future work were proposed with the aim of developing the work of the current system as follows:

Other biometrics types use behavioral biometrics (voice, signature). In addition to adding a step to encrypt data before embedding it to achieve a high level of security.And the use of a number of clever techniques, such as a genetic algorithm, to choose suitable areas to hide.

REFERENCES

[1] N. S. Kamaruddin, A. Kamsin, L. Y. Por, and H. Rahman, "A review of text watermarking: theory, methods, and applications," *IEEE Access*, vol. 6, pp. 8011–8028, 2018.

[2] A. Review, "A Review of Comparative Spatial Domain Techniques of Steganography and Watermarking," no. October, 2020.

[3] M. Kalita and T. Tuithung, "A comparative study of steganography algorithms of spatial and transform domain," *Int. J. Comput. Appl.*, vol. 975, 2016.

[4] S. A. A. Sma and B. R. A. R. Eddy, "Watermarking of Iris data in Hand Vein Images for Protection in Biometric Recognition," vol. 04, no. 17. pp. 3268–3273, 2016.

[5] M. R. M. Isa, S. Aljareh, and Z. Yusoff, "A watermarking technique to improve the security level in face recognition systems," *Multimed. Tools Appl.*, vol. 76, no. 22, pp. 23805–23833, 2017.

[6] S. Li, X. Chen, Z. Zheng, Z. Qian, G. Feng, and X. Zhang, "Data hiding in Fingerprint Minutiae Template for Privacy Protection," *arXiv Prepr. arXiv1710.00516*, 2017.

[7] O. Hosam, "Attacking image watermarking and steganography-a survey," *Int. J. Inf. Technol. Comput. Sci.*, vol. 11, no. 3, pp. 23–37, 2019.

[8] M. R. Soni and M. K. Gupta, "Digital watermarking of wavelet transforms based on coding and decoding techniques," *Int. J. Comput. Sci. Mob. Comput.*, vol. 3, no. 3, 2014.

[9] S. Majumder, K. J. Devi, and S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking," *IET biometrics*, vol. 2, no. 1, pp. 21–27, 2013.

[10] P. Ayubi, M. J. Barani, M. Y. Valandar, B. Y. Irani, and R. S. M. Sadigh, "A new chaotic

complex map for robust video watermarking," *Artif. Intell. Rev.*, vol. 54, no. 2, pp. 1237–1280, 2021.

[11] X. Zhong, P.-C. Huang, S. Mastorakis, and F. Y. Shih, "Sunesh and R. R. Kishore, "A Novel and Efficient Blind Image Watermarking in Transform Domain," *arXiv Prepr. arXiv2007.02460*, 2020.

[12] Sunesh and R. R. Kishore, "A Novel and Efficient Blind Image Watermarking in Transform Domain," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 1505–1514, 2020, doi: 10.1016/j.procs.2020.03.361.

[13] M. Marimuthu and A. Kannammal, "WATERMARKING BASED ENHANCED MULTIMODAL BIOMETRIC AUTHENTICATION TECHNIQUE."

[14] K. Seetharaman and R. Ragupathy, "Iris recognition based image authentication," *Int. J. Comput. Appl.*, vol. 44, no. 7, pp. 1–8, 2012.

[15] M. Ingale, R. Cordeiro, S. Thentu, Y. Park, and N. Karimian, "Ecg biometric authentication: A comparative analysis," *IEEE Access*, vol. 8, pp. 117853–117866, 2020.

[16] A. Dixit and R. Dixit, "A Review on Digital Image Watermarking Techniques.," *Int. J. Image, Graph. Signal Process.*, vol. 9, no. 4, 2017.

[17] Y. Zhang, S. Wang, T. Li, B. Liu, and D.-B. Pan, "Modulus Calculations on Prime Number Algorithm for Information Hiding With High Comprehensive Performance," *IEEE Access*, vol. 8, pp. 85309–85320, 2020.

[18] H. Unno, R. Yamkum, C. Bunporn, and K. Uehira, "A new displaying technology for information hiding using temporally brightness modulated pattern," *IEEE Trans. Ind.*

Appl., vol. 53, no. 1, pp. 596–601, 2016.

[19] M. S. Taha, M. S. M. Rahim, M. M. Hashim, and H. N. Khalid, "Information Hiding: A Tools for Securing Biometric Information," *Technol. Reports Kansai Univ.*, vol. 62, no. 04, pp. 1383–1394, 2020.

[20] A. K. Singh, "Data hiding: current trends, innovation and potential challenges," *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 16, no. 3s, pp. 1–16, 2020.

[21] X. Zhou, W. Gong, W. Fu, and L. Jin, "An improved method for LSB based color image steganography combined with cryptography," in *2016 IEEE/ACIS 15th international conference on computer and information science (ICIS)*, 2016, pp. 1–4.

[22] M. Taleby Ahvanooey, Q. Li, H. J. Shim, and Y. Huang, "A comparative analysis of information hiding techniques for copyright protection of text documents," *Secur. Commun. Networks*, vol. 2018, 2018.

[23] M. Mahajan and N. Kaur, "Adaptive steganography: a survey of recent statistical aware steganography techniques," *Int. J. Comput. Netw. Inf. Secur.*, vol. 4, no. 10, p. 76, 2012.

[24] W. Domain, "A review and open issues of diverse text watermarking techniques in spatial domain," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 17, 2018.

[25] M. Begum and M. S. Uddin, "Digital image watermarking techniques: a review," *Information*, vol. 11, no. 2, p. 110, 2020.

[26] O. O. Evsutin, A. S. Melman, and R. V Meshcheryakov, "Digital steganography and watermarking for digital images: a review of current research directions," *IEEE Access*, 2020.

[27] N. Harini and T. R. Padmanabhan, “2CAuth: A New Two Factor Authentication Scheme Using QR-Code,” *Int. J. Eng. Technol.*, vol. 5, no. 2, pp. 1087–1094, 2013.

[28] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-factor authentication: A survey,” *Cryptography*, vol. 2, no. 1, p. 1, 2018.

[29] S. Bhattacharyya, “A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier,” *J. Glob. Res. Comput. Sci.*, vol. 2, no. 4, 2011.

[30] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, “A survey of internet of things (IoT) authentication schemes,” *Sensors*, vol. 19, no. 5, p. 1141, 2019.

[31] T. Zhang, Y. Hu, C. Zhang, H. An, and W. Xu, “A New Method for Iris’ Location Based on Pointwise Detection,” in *2010 4th International Conference on Bioinformatics and Biomedical Engineering*, 2010, pp. 1–4.

[32] N. A. Lal, S. Prasad, and M. Farik, “A review of authentication methods,” *vol*, vol. 5, pp. 246–249, 2016.

[33] K. M. Sudar, P. Deepalakshmi, K. Ponmozhi, and P. Nagaraj, “Analysis of Security Threats and Countermeasures for various Biometric Techniques,” in *2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES)*, 2019, pp. 1–6.

[34] A. Hadid, N. Evans, S. Marcel, and J. Fierrez, “Biometrics systems under spoofing attack: an evaluation methodology and lessons learned,” *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 20–30, 2015.

[35] L. K. Ballard, *Robust techniques for evaluating biometric cryptographic key generators*.

Johns Hopkins University, 2008.

[36] J. Harvey, J. Campbell, and A. Adler, “Characterization of biometric template aging in a multiyear, multivendor longitudinal fingerprint matching study,” *IEEE Trans. Instrum. Meas.*, vol. 68, no. 4, pp. 1071–1079, 2018.

[37] X. Zhang, D. Cheng, P. Jia, Y. Dai, and X. Xu, “An efficient android-based multimodal biometric authentication system with face and voice,” *IEEE Access*, vol. 8, pp. 102757–102772, 2020.

[38] D. Blackburn, C. Miles, B. Wing, and K. Shepard, “Biometrics History,” no. 31 March, pp. 1–27, 2006, [Online]. Available: https://www.hsdl.org/?view&did=463907.

[39] A. Babich, “Biometric Authentication. Types of biometric identifiers,” 2012.

[40] R. Saini and N. Rana, “Comparison of various biometric methods,” *Int. J. Adv. Sci. Technol.*, vol. 2, no. 1, p. 2, 2014.

[41] Z. Sun, Y. Wang, G. Qu, and Z. Zhou, “A 3-D hand gesture signature based biometric authentication system for smartphones,” *Secur. Commun. Networks*, vol. 9, no. 11, pp. 1359–1373, 2016.

[42] T. Sabhanayagam, V. P. Venkatesan, and K. Senthamaraikannan, “A comprehensive survey on various biometric systems,” *Int. J. Appl. Eng. Res.*, vol. 13, no. 5, pp. 2276–2297, 2018.

[43] V. M. Patel, N. K. Ratha, and R. Chellappa, “Cancelable biometrics: A review,” *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, 2015.

[44] S. S. Harakannanavar, P. C. Renukamurthy, and K. B. Raja, “Comprehensive Study of

Biometric Authentication Systems, Challenges and Future Trends," *Int. J. Adv. Netw. Appl.*, vol. 10, no. 4, pp. 3958–3968, 2019.

[45] N. Singh, A. Agrawal, and R. A. Khan, "Voice biometric: A technology for voice based authentication," *Adv. Sci. Eng. Med.*, vol. 10, no. 7–8, pp. 754–759, 2018.

[46] P. S. Lozhnikov and A. E. Sulavko, "Generation of a biometrically activated digital signature based on hybrid neural network algorithms," in *Journal of Physics: Conference Series*, 2018, vol. 1050, no. 1, p. 12047.

[47] S. Bianco, F. Gasparini, and R. Schettini, "Adaptive skin classification using face and body detection," *IEEE Trans. Image Process.*, vol. 24, no. 12, pp. 4756–4765, 2015.

[48] R. Subban and R. Mishra, "Face detection in color images based on explicitly-defined skin color model," in *International Conference on Advances in Computing, Communication and Control*, 2013, pp. 570–582.

[49] S. K. Singla, M. Singh, and N. Kanwal, "Biometric System-Challenges and Future Trends," in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2021, pp. 647–651.

[50] C.-A. Toli and B. Preneel, "Privacy-preserving Biometric Authentication Model for e-Finance Applications.," in *ICISSP*, 2018, pp. 353–360.

[51] G. M. Mir, A. A. Balkhi, N. A. Lala, N. A. Sofi, M. M. Kirmani, and I. A. Mir, "The Benefits of Implementation of Biometric Attendance System," *Orient. J. Comput. Sci. Technol.*, vol. 11, no. 1, pp. 50–54, 2018.

[52] G. B. Iwasokun, S. S. Udoh, and O. K. Akinyokun, "Multi-Modal Biometrics:

Applications, Strategies and Operations," *Glob. J. Comput. Sci. Technol.*, 2015.

[53] J. D. Woodward Jr, C. Horn, J. Gatune, and A. Thomas, "Biometrics: A look at facial recognition," RAND CORP SANTA MONICA CA, 2003.

[54] P. Drozdowski, C. Rathgeb, A. Dantcheva, N. Damer, and C. Busch, "Demographic bias in biometrics: A survey on an emerging challenge," *IEEE Trans. Technol. Soc.*, vol. 1, no. 2, pp. 89–103, 2020.

[55] J. Priesnitz, C. Rathgeb, N. Buchmann, C. Busch, and M. Margraf, "An overview of touchless 2D fingerprint recognition," *EURASIP J. Image Video Process.*, vol. 2021, no. 1, pp. 1–28, 2021.

[56] A. Dantcheva, P. Elia, and A. Ross, "What else does your biometric data reveal? A survey on soft biometrics," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 3, pp. 441–467, 2015.

[57] M. B. Fisher, B. H. Mann, R. D. Cronk, K. F. Shields, T. L. Klug, and R. Ramaswamy, "Evaluating Mobile Survey Tools (MSTs) for field-level monitoring and data collection: development of a novel evaluation framework, and application to MSTs for rural water and sanitation monitoring," *Int. J. Environ. Res. Public Health*, vol. 13, no. 9, p. 840, 2016.

[58] S. Z. Li and A. Jain, *Encyclopedia of biometrics*. Springer Publishing Company, Incorporated, 2015.

[59] K. Huang, X. Tian, H. Yu, M. Yu, and A. Yin, "A High Capacity Watermarking Technique for the Printed Document," *Electronics*, vol. 8, no. 12, p. 1403, 2019.

[60] Y. Xia, "Watermarking federated deep neural network models," 2020.

[61] R. K. Singh, D. K. Shaw, and M. J. Alam, "Experimental Studies of LSB Watermarking

with Different Noise," *Procedia Comput. Sci.*, vol. 54, pp. 612–620, 2015, doi: 10.1016/j.procs.2015.06.071.

[62] L. K. Saini and V. Shrivastava, "A survey of digital watermarking techniques and its applications," *arXiv Prepr. arXiv1407.4735*, 2014.

[63] R. Patel and P. Bhatt, "A review paper on digital watermarking and its techniques," *Int. J. Comput. Appl.*, vol. 110, no. 1, pp. 10–13, 2015.

[64] R. F. Olanrewaju, "Development of intelligent digital watermarking via safe region," 2011.

[65] A. Rashid, "Digital watermarking applications and techniques: a brief review," *Int. J. Comput. Appl. Technol. Res.*, vol. 5, no. 3, pp. 147–150, 2016.

[66] R. Artru, A. Gouaillard, and T. Ebrahimi, "Digital watermarking of video streams: review of the state-of-the-art," *arXiv Prepr. arXiv1908.02039*, 2019.

[67] S. S. Katariya, "Digital watermarking," *Int. J. Eng. Innov. Technol.*, vol. 1, no. 2, pp. 143–153, 2012.

[68] H. Nyeem, W. Boles, and C. Boyd, "Digital Image Watermarking Techniques: A Review," in *2011 International Conference on Digital Image Computing: Techniques and Applications*, 2011, pp. 468–473.

[69] P. Lipiński, "Watermarking software in practical applications," *Bull. Polish Acad. Sci. Tech. Sci.*, vol. 59, no. 1, pp. 21–25, 2011.

[70] R. Sreejith and S. Senthil, "A novel tree based method for data hiding and integrity in medical images," in *2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE)*, 2017, pp. 1–4.

[71] U. Khadam, M. M. Iqbal, M. A. Azam, S. Khalid, S. Rho, and N. Chilamkurti, "Digital watermarking technique for text document protection using data mining analysis," *IEEE Access*, vol. 7, pp. 64955–64965, 2019.

[72] H. K. Rana, M. S. Azam, M. R. Akhtar, J. M. W. Quinn, and M. A. Moni, "A fast iris recognition system through optimum feature extraction," *PeerJ Comput. Sci.*, vol. 5, p. e184, 2019.

[73] G. Malathi, D. Mavaluru, and K. Srinivasan, "IRIS PATTERN RECOGNITION: A QUANTITATIVE REVIEW ON HOW TO IMPROVE IRIS-BASED PATTERN RECOGNITION SECURITY SYSTEM," 2020.

[74] R. Tobji, W. Di, and N. Ayoub, "FMnet: iris segmentation and recognition by using fully and multi-scale CNN for biometric security," *Appl. Sci.*, vol. 9, no. 10, p. 2042, 2019.

[75] A. A. Nithya and C. Lakshmi, "Iris recognition techniques: A literature survey," *Int. J. Appl. Eng. Res.*, vol. 10, no. 12, pp. 32525–32546, 2015.

[76] S. J. Al-Hijaili and M. AbdulAziz, "BIOMETRICS IN HEALTH CARE SECURITY SYSTEM, IRIS-FACE FUSION SYSTEM.," *Int. J. Acad. Res.*, vol. 3, no. 1, 2011.

[77] Y. U. Sonmez, "Research on Retinal and Iris Identification Systems," *Eur. J. Eng. Nat. Sci.*, vol. 2, no. 1, pp. 167–180, 2017.

[78] B. E. Mathew, "Securing Web Services by Iris Recognition System," *Int. J. Comput. Appl.*, vol. 13, no. 7, pp. 23–28, 2011.

[79] R. Vyas, T. Kanumuri, and G. Sheoran, "Iris recognition using 2-D Gabor filter and XOR-SUM code," in *2016 1st India International Conference on Information Processing*

(IICIP), 2016, pp. 1–5.

[80] D. Bhattacharyya, P. Das, S. K. Bandyopadhyay, and T. Kim, “IRIS texture analysis and feature extraction for biometric pattern recognition,” *Int. J. Database Theory Appl.*, vol. 1, no. 1, pp. 53–60, 2008.

[81] S. O. Olatinwo, O. Shoewu, and O. O. Omitola, “Iris recognition technology: implementation, application, and security consideration,” *Pacific J. Sci. Technol.*, vol. 14, no. 2, pp. 228–233, 2013.

[82] J. Daugman, “High Conf Visual Recog of Persons by a test of statistical significance,” *IEEE Trans. Pattern Anal. Mach. Intell*, vol. 15, no. 11, pp. 1148–1161, 1993.

[83] H. B. Kekre, S. D. Thepade, J. Jain, and N. Agrawal, “Iris recognition using texture features extracted from walshlet pyramid,” in *Proceedings of the International Conference & Workshop on Emerging Trends in Technology*, 2011, pp. 76–81.

[84] V. K. Sinha, R. Jeet2D, P. Bhambri, and M. Mahajan, “EMPOWERING INTRUSION DETECTION IN IRIS RECOGNITION SYSTEM: A REVIEW,” *J. Nat. Remedies*, vol. 21, no. 2, pp. 131–153, 2020.

[85] C. Kant and S. Chaudhary, “A Watermarking Based Approach for Protection of Templates in Multimodal Biometric System,” *Procedia Comput. Sci.*, vol. 167, pp. 932–941, 2020.

[86] V. R. E. Chirchi, L. M. Waghmare, and E. R. Chirchi, “Iris biometric recognition for person identification in security systems,” *Int. J. Comput. Appl.*, vol. 24, no. 9, pp. 1–6, 2011.

[87] J. Lu, T. Qu, and H. R. Karimi, “Novel iris biometric watermarking based on singular

value decomposition and discrete cosine transform," *Math. Probl. Eng.*, vol. 2014, 2014, doi: 10.1155/2014/926170.

[88] N. Lalithamani and M. Sabrigiriraj, "Embedding of iris data to hand vein images using watermarking technology to improve template protection in biometric recognition," in *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2015, pp. 1–7.

[89] A. Kumar, A. Potnis, and A. Singh, "Iris recognition and feature extraction in iris recognition system by employing 2D DCT," *IRJET Int. Res. Comput. Sci. Softw. Eng. Technol*, vol. 3, no. 12, pp. 503–510, 2016.

[90] J. Sang, X. Wu, C. Song, and S. Sudirman, "Multiparty Multilevel Watermarking Protocol for Digital Secondary Market Based on Iris Recognition Technology," *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)*, vol. 10, no. 1. 2017, doi: 10.2174/2352096510666170315130131.

[91] S. Pandey, "Embedding of Iris Data to Ear Image using Watermarking Technology, Pre-Processing Step," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 6, no. 4, pp. 3907–3911, 2018, doi: 10.22214/ijraset.2018.4641.

[92] A. Dwivedi, A. Singh, and M. K. Dutta, "Wavelet-SVD based Zero-Bit Watermarking for Securing Biometric Images," in *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, 2019, pp. 467–472.

[93] A. Singh, A. Kumar, and M. K. Dutta, "DWT, DCT and PBFO based approach for biometric image security," in *2020 International Conference on Contemporary Computing and Applications (IC3A)*, 2020, pp. 298–303.

[94] W. Zhou, X. Ma, and Y. Zhang, "Research on Image Preprocessing Algorithm and Deep Learning of Iris Recognition," *J. Phys. Conf. Ser.*, vol. 1621, no. 1, 2020, doi: 10.1088/1742-6596/1621/1/012008.

[95] M. Huber, "Nonlinear Gaussian Filtering : Theory, Algorithms, and Applications," no. March, 2014, doi: 10.5445/KSP/1000045491.

[96] Z. Zainal Abidin, M. -, A. Shibghatullah, S. -, S. -, and Z. -, "Iris Segmentation Analysis using Integro-Differential Operator and Hough Transform in Biometric System," *Jtec*, no. January, pp. 1–8, 2012.

[97] B. Chouhan and S. Shukla, "Analysis of statistical feature extraction for Iris Recognition System using Laplacian of Gaussian filter," *Int. J. Appl. Eng. Res. DINDIGUL Vol. 1, No 3, 2010*, vol. 1, no. 3, pp. 528–535, 2010.

[98] H. Al-Mamory, "Iris Detection Using Morphology," *J. Babylon Univ. Pure Appl. Sci.*, vol. 22, no. 9, pp. 2277–2282, 2014.

[99] I. J. Shaikh and A. H. A. R. Shaikh, "Iris Localization Using Segmentation & Hough Transform Method," vol. 5, no. 2, pp. 79–84, 2014.

[100] S. Al Mamun and S. M. Tareeq, "An Efficient Iris Segmentation Approach to Develop an Iris Recognition System," no. February 2015, 2012.

[101] A. Kumar, A. Potnis, and A. Singh, "Iris recognition and feature extraction in iris recognition system by employing 2D DCT," *IRJET Int. Res. Comput. Sci. Softw. Eng. Technol.*, vol. 3, no. 12, pp. 503–510, 2016.

[102] S. M. Arts, "Biometric Iris Recognition System Using Edge Detection and Gabor Filter for

High Security," vol. 12, no. 1, pp. 7–21, 2019.

[103] G. HR and M. CN, "Iris Code Generation and Recognition," *Int. J. Mach. Intell.*, vol. 3, no. 3, pp. 103–107, 2011, doi: 10.9735/0975-2927.3.3.103-107.

[104] M. M. Alrifaee, M. M. Abdallah, and B. G. Al Okush, "A Short Survey of IRIS Images Databases," *Int. J. Multimed. Its Appl.*, vol. 9, no. 2, pp. 01–14, 2017, doi: 10.5121/ijma.2017.9201.

[105] W. Zhou, X. Ma, and Y. Zhang, "Research on image preprocessing algorithm and deep learning of iris recognition," in *Journal of Physics: Conference Series*, 2020, vol. 1621, no. 1, p. 12008.

[106] U. Sara, M. Akter, and M. S. Uddin, "Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study," *J. Comput. Commun.*, vol. 7, no. 3, pp. 8–18, 2019.

[107] Z. T. R. AL-Windawi, "Security Enhancement of Image Steganography Using Embedded Integrity Features. Middle East University, Amman - jordan," *Middle Easr Univ.*, 2017.

[108] N. A. Memon and A. Alzahrani, "Prediction-based reversible watermarking of CT scan images for content authentication and copyright protection," *IEEE Access*, vol. 8, pp. 75448–75462, 2020.

[109] Y. Perwej, "An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection," *Int. J. Multimed. Its Appl.*, vol. 4, no. 2, pp. 21–38, 2012, doi: 10.5121/ijma.2012.4202.

[110] M. Sharma and S. Shiwani, “Noise Attack Analysis on Non Blind DWT Watermarking Algorithm,” *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 7, pp. 374–378, 2013.