Republic of Iraq

Ministry of Higher Education and Scientific Research

University of Diyala

College of Science

Document Signing Using ESSO Algorithm

A Thesis

Submitted to the Computer Science Department\ College of Science\ University of Diyala

In a Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer.

By

Israa Nazeeh

Supervised by

Asst. Prof Jamal Mustafa Abbas

2020 A.D. 1442 AH.

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿ وَقُلِ الْحَمْدُ لِلَّهِ سَيُرِيكُمْ آيَاتِهِ فَتَعْرِفُونَهَا ﴾

[سورة النمل الآية : 93]

Dedication

I dedicate my humble effort

To the light that illuminates me the path of success **…..** my dear father

To whom was her prayer the secret of my success**.. …**my dear mother

To those who were lighting the road for me and supporting me, to the true companions, who prove the deep meaning of friendship. **…..** my dear sisters

To whom I loved **…..**my dear family

To whom illuminated the way of science **…..** my dear teachers

With all my love and respect

Israa Nazeeh

2020

Acknowledgements

I would like to thank my supervisor Asst. Pro Dr.Jamal Mustafa Abbas for his sincere help and encouragement throughout my study and the writing of this thesis. I thank him for his beautiful attitude and continuous follow-up. This work would not have been possible without his support.

Abstract

Biometrics lack revocability and privacy while cryptography cannot detect the user's identity. By obtaining cryptographic keys using biometrics, one can achieve the properties such as revocability, assurance about user's identity, and privacy. In addition, the Multi-biometric systems alleviate a few of the problems observed in unimodal biometric systems. Besides improving matching performance and its can integrate information at various levels.

In this thesis presents Document Signing Using ESSO Algorithm, its aims to introduce a new technique to generate stream cipher key by using a multi – biometric identification system that consists of (sclera and palm) images and using the best coordinates is produced by an enhancement of shark smell optimization algorithm (SSO) based on 3d logistic chaotic map.

The stages of implementation the proposed system include feature extraction from sclera and palm biometric images of same personal using proposed sclera – identification system and palm –identification system, each system has different preprocessing techniques to preparing images to exacted features.

In addition , the scale-invariant feature transform (SIFT) algorithm in multibiometric identification system extract features from the sclera and palm biometric images and to get fast access to the important regions inside the sclera and palm biometric images. These features are used to find the optimal solution by using enhancement shark smell optimization algorithms(SSO) based on chaotic function.

The enhancements shark smell optimization algorithm (SSO)consists from three steps: 3d logistic map to generate set of random numbers to seed random parameters (R1,R2,R3) in SSO algorithm this step aims to enhance the

performance of SSO , the features that extracted from sclera and palm biometric images dropping on secret image to connected between sclera feature that represent (shark position) and palm feature that represents (fish position) this step aims to find set of optimal solution .

To generate stream cipher key, the proposing system presents new technique to generating variable and unpredictable stream key based on convert to binary the values of all optimal solution (fitness value, objective value, solution point coordinate (x,y)) .

The final stage in the proposed system is the document signature by using the MD5, the proposed system has the ability to generate a unique digital signature for each user.

The proposed system using the stream key in document signature to protect personal information in a completely safe manner.

The implementation the proposed system and results of Random Number Generation Tests (NIST) National Institute of Standards and Technology shown the proposed system has ability to generating stream key for multiply users that has several proprieties likes: unique, unpredictable, strong, and various length.

Contents

List of Figures

List of Tables

List of Algorithms

List of Abbreviations

Abbreviations	Meaning
C#	C sharp
R1,R2	Constants
DB	Data Base
DOG	Difference of Gaussian
•	Eat
ESSO	Enhancements shark smell optimization
EER	Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
•	Fish
MM	Mathematical Morphology
μ	Mean Value
NIST	National Institute of Standards and Technology
ND	Number of decision
NP	Number of Population
——	Path
RGB	Red, green, blue
SIFT	Scale Invariant Feature Transform
¤	Shark
SSO	Shark Smell Optimization
SURF	speeded up robust features
σ	Standard Deviation
SE	Structure Element
Xi	The random neighbor
3D	Three Dimension
T	Threshold
2D	Two Dimension
MD5	Message-digest algorithm

List of Symbols Table

Symbol	Meaning
+	Addition operation
+	Addition operation
Δ	Delta
/	Division operation
=	Equality sign
*	Multiplication operation
%	Percent sign
Σ	Sigma
√	Square root
-	Subtraction operation
∑	Summation
|X|	The absolute value
Θ	Theta

CHAPTER ONE

GENERAL INTRODUCTION

Chapter One

General Introduction

1.1 Overview

Network and computer security are highly dependent on the user's authentication. Now, token-based techniques (smartcards) and knowledge-based techniques (passwords) have been the major significant methods. Yet, such approaches have some security drawbacks. For instance, a password can be simply forgotten, stolen, and shared. Comparably, the smart-cards might be lost, stolen, shared, or duplicated. To circumvent such problems, some biometric authentication login approaches are applied [1].

The biometric verifications are referring to the person's automatic verification based on certain biometric features that are obtained from their behavior and/or physiological properties. A system of biometric verification has the ability of distinguish between imposters and authorized individuals in comparison to conventional systems which are using passwords or cards. About biometrics, and an individual might be identified on the basis of who they are instead of having an ID card or passwords [2].

Behavioral biometrics and physical biometrics are the two branches of biometrics. The latter includes face recognition, hand recognition, iris, fingerprints, and sclera. While the first one consists of key-stone and signatures. The biometrics, which are on the basis of ***physical behavior*** are of high importance, consisting of hand's geometrics, fingerprint's ridges, iris patterns, face's structure, voice as well as sclera vein patterns [3].

The biometric authentication system might be specified as multi-modal and uni-modal, basd on some biometric traits or applied modalities. The uni-modal biometric system is using one of the biometric characteristics of the individual to identify and verify identity, but the multi biometric system has ability to use two or more multiple biometric system characteristics to identify a person [4].

The multi-modal systems are better than of the other type (uni-modal systems), because of unacceptable false acceptance rates (FAR), and large false rejection rates (FRR). Yet, more information offer to the classifier increasing the recognition accuracy as well as decreasing the error rates, The identity proof has been strengthened as data, whereas it is obtained from various sources [5].

The biometric cryptosystems, including key binding, and the key generation systems are combining high security level. It is offered via cryptography in addition to the non-repudiation offered via biometric. The systems of key generation are producing stable cryptographic key which has been obtained from the biometric data. The systems of key binding are bound a cryptographic key that is randomly generated to biometric template [5].

Concerning the presented thesis, authentication and integrity are achieved by using (MD5-256) message-digest algorithm and the proposed cryptographic key generation algorithm based on the biometric features of users. Since two different biometric traits are obtained from the same user, different extraction techniques that best suit each of these is applied in this work. Sclera features are extracted using the sclera Identification System which is using different techniques to preprocessing sclera image of user and

to determine strong features and their descriptions based on the Scale Invariant Feature Transform algorithm (SIFT). Also, palm features are extracted using palm Identification system, which is using different techniques to preprocessing palm image of same user and to determine strong features and their descriptions based on the Scale Invariant Feature Transform algorithm (SIFT). Following the feature extractions and their descriptions from of both proposed identification systems (sclera and palm), dropping these features on the secret image to combine between them, and using shark smell optimization based on the chaotic map to find a set of optimal solutions. In this work, the proposed algorithm for generation 128-bit cryptographic key is based on an optimal solution that is found by using the Shark Smell Optimization Algorithm (SSO) with chaotic maps to enhancement security architecture of the proposed system. Finally, the proposed document signature using message-digest algorithm (MD5-256) is to obtain high security and integrity of data.

1.2 Related Work

Many approaches are proposed in different studies to improve security data based on biometrics:

- In (2015), G. Radha, B. Suganyadevi, and C. Saranya, [6] have proposed a secure multi-modal biometrical system through the fusion of the Finger vein and eye vein images. In this fusion system, has taken under consideration eye veins as well as finger veins

characteristics for the verifications, the user maybe authenticated by the recognition of the sclera veins with the use of a scale and rotation-invariant Y-shape descriptor based approach of feature extractions sufficiently removes the most unlikely match instances. The suggested model enhanced the system security as verified. It is possible to conduct the automatic authentication with state of the art approaches, such as the recognition of the sclera on the move and the scanner of the finger veins on the car steering.

- In (2016), Sujata Kataria and Ashok K. Goel [7] proposed a new multi-biometric system based on fingerprint and signature. The signature uses SIFT (Scale-invariant Feature Transform) and fingerprint uses minutia extraction. The researchers propose using two different datasets. In the fingerprint, the dataset is made up of 10 images. A signature dataset is made up of 10 images.
- In (2017), K. Tamilsevan, et al. [8] suggested a hybrid method of utilizing the palm and finger veins for designing a biometrical system. The suggested system method was performed the simultaneous acquisition of palm and finger vein database. Also, it had resulted in the combination of those 2 pieces of evidence with the use of a hybrid method of comparison for increasing system's sensitivity, and accuracy at the same time as decreasing time harmfulness, and complexity to the user.
- In (2018), M. Madhivhanan and R. Ravi [9] proposed a new hybrid technique in multi- biometrics, which are fingerprint and sclera. The whole process was implemented in the FPGA SOC. The dataset has consisted of 50 fingerprint images and 50 sclera images. Another

dataset has contained 10 fingerprint images, and sclera images of the same finger and the same eye from 6 different users.

- In (2018), Roh, et al. [10] have introduced an approach with recurrent neural network (RNN) and convolutional neural network (CNN) for the generation of the cryptographic keys from the biometrics of the face. CNN has been utilized for the extraction of feature vector from the images of the face, and the RNN results in key generation from feature vectors. In the procedure of the registration, RNN is trained in an iterative manner.
- In (2019), Jaswal et al. [11] are presented a new method for a multi-modal biometric system that has been suggested. The feature-level fusion of geometry, palm print, and hand shape features were carried out. The much-unrelated characteristics have been chosen from a fused set of features. This work achieved results that are matched with other formal art systems.
- In (2019), Pager et al. [12] have been focused on generating cryptographic keys according to the fusion method of the finger-prints reducing other conventional crypto-systems' complexity. The biometrical characteristics such as the finger-prints are permanent during the life-span of the person. In this study, a finger-print key generation approach has been presented, it is robust and utilized to encrypt and decrypt in the elliptic curve approach of cryptography The experimentation has been carried out on the available data-set. The obtained results have shown the significance concerning efficiency, producing a strong key of cryptography.

1.3 Problems statement

Biometric is the measure of behavioral and physiological features for the individual, commonly utilized biometric features for identification or verification, but it is at the same time can be employed as a key for various security applications. However, the unimodal biometric system is suffering from noise, interclass variations, non-universality attacks, so to overcome these attacks, the multimodal biometrics system is joining of two or more modalities biometrics. Among various biometric properties like as, fingerprint, face, voice, area, etc., hybrid techniques represent combinations of two biometric-identification systems (sclera and palm) based on Shark Smell Optimization (SSO) with chaotic maps to overcome many difficulties in individual biometrics .the sclera and palm print biometrics can provide a higher level of security because of its inherent robustness.

1.4 Aims of thesis

The aim of the thesis is to build a strong identity system based on a hybrid technique by using proposed Sclera and Palm identification systems, where each identification system has different techniques to extract features for each user). Enhancement shark smell optimization (ESSO) algorithms based on the 3-dimension logistic chaotic map to enhance the performance of SSO algorithms to generate a stream cipher key. It is used for many purposes and make the system more secure and authentication.

1.5 Layouts of Thesis

The thesis has been organized into five chapters., as follow:

Chapter One: This chapter includes the basic introduction, aim of the thesis, related work, and the layout of the thesis.

Chapter Two: This chapter includes theoretical background and discusses the algorithms that we use.

Chapter three: This chapter illustrated all tools and algorithms used in the design and implementation of proposed document signature based on hybrid identification techniques (sclera and palm–identification system).

Chapter Four: This chapter presents the tests and results.

Chapter Five: This chapter offers conclusions and suggestions for future work.

CHAPTER TWO

THEORETICAL BACKGROUND

Chapter Two

Theoretical Background

2.1 Introduction

Bio-cryptography can be defined as a progressive technology that combines biometrics with cryptography. The multi-biometric system used for security purpose has become increasingly popular. The use of multi-biometric data in generation cryptography key is a new growing and promising area of research. Yet, this growth depends on the theoretical base. Thus, the presented chapter is providing the work's theoretical background. The Biometric is presented in subsection (2.2), while, subsection (2.3) gives the preprocessing methods. Morphology Operations are shown in subsection (2.4). To find the object we provide the sub-section (2.5) to satisfy this goal. Also, the sub-section (2.6) is shown Feature Extraction. The two-dimensions maximum entropy threshold methods are covered in subsection (2.7). Furthermore, the shark smell optimization SSO algorithm and Chaotic Maps are clarified in subsections (2.8) and (2.9) respectively. In subsection (2.10), we show the digital signature. In subsection (2.11), we introduce the MD5 algorithm. Finally, in subsection (2.12), Random number generation tests.

2.2 Biometric

the science which involves the statistical analysis that is related to biological characteristics. Therefore, the individuals biometric recognition should be indicated, because of the security applications analyzing the characteristics of individuals for verifications and identifications of identities. Yet, the term "biometrics" will be used for indicating "biometric recognition of people" [13].

The biometric recognition provides a significant method with regard to the security applications in addition to certain benefits in comparison to the conventional approaches, that is based on something the person has (cards, keys, and so on), or something the person knows (PINs, passwords, and so on). One significant feature related to biometric traits is that it has been on the basis of something done, or something the person has, Thus, there is no requirement for remembering or holding a token [14]. Furthermore, the authentication techniques with regard to biometrics have been specific portions related to the security systems in addition to some benefits in comparison to the traditional approaches. Yet, there are some disadvantages as can be seen in the table below:

Table (2.1) Advantages and Disadvantages of 3 major authentication techniques.[14]

Authentication Approach	Advantage	Disadvantage
Hand-held token (Passports, IDs, cards, and so on) Knowledge-based (PINs, passwords, and so on)	♣ Economical and easy-to-implement approach ♣ Standard, even though moving to another facility, nation, and so on ♣ New one might be provided ♣ Easily replaced by new one when problems exist.	♣ Might be shared. ♣ Fake one could be provided. ♣ Might be stolen. ♣ Single individual register with various identities. ♣ It might be cracked or guessed.

		♣ Hard to remember the effective passwords.
Biometrics	♣ In comparison to other techniques, it is providing more security. ♣ If an individual has many identities, he/she might be easily detected. ♣ It might not be forgotten or lost, stolen, guessed.	♣ In certain conditions, fake one might be provided. ♣ It is not secret, nor replaceable. ♣ When the biometric data of individual is stolen, then there is no possibility for replacing it.

The biometric system is an advanced way to identify the individual on the basis of certain behavioral or physiological properties. Biometrics have been a reliable solution for protecting the identity and rights of individuals because they recognize the unique characteristics of people. The biometric is divided into two basic categories [15].,which are:

i. Physiological

Physiology is the characteristic of the body and thus it varies from person to person, including the following examples:

1. Features of the Face
2. Retina
3. Iris
4. Palm geometry
5. Fingerprints
6. DNA
7. Odor/scent.

ii. Behavioral

Behavioral biometrics are the behavioral characteristics that related to the pattern of people doing something, such as following examples:

1. Keystrokes/Typing patterns
2. Voiceprint
3. Typing rhythm
4. Gait
5. Handwritten signature.

2.2.1 Sclera Biometric

Sclera blood vessels are present effective biometric trait. The sclera is the white regions around the eyeball contain blood vessel patterns which might be utilized for personal identification, Also it might be defined as the opaque and white areas of connective tissue and blood vessels in the eyes, Such part of the eye is surrounding the iris that is defined as a colored tissue around the pupil, as shown in Fig (2.1)., It has a rich pattern of blood vessels that has various layers and orientations. Thus, the discriminant properties related to such blood vessels have been bright factors for the eye's recognition as shown in Fig (2.1) [16].

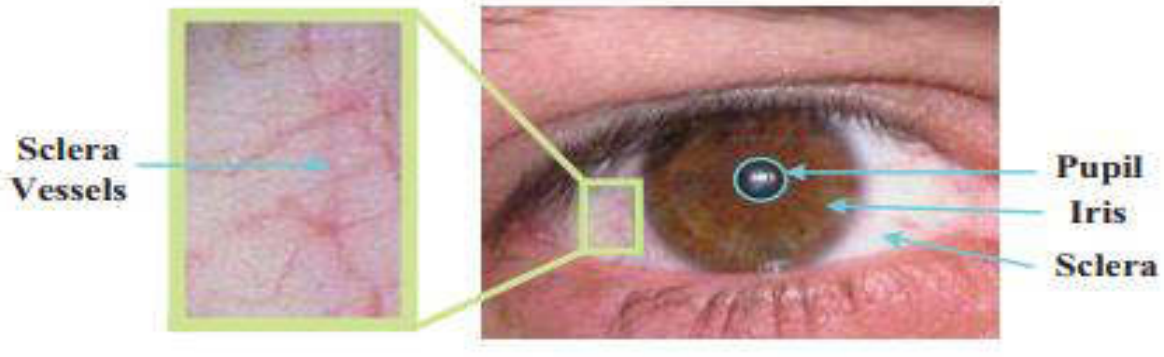


Figure (2.1) Sclera vessels and eye structure [17]

The sclera's veins might be imaged in the case when an individual is glancing to either side, offering four patterns' regions: one for each of the eye's sides. The verification uses digital templates from such patterns, also the templates are going to be encoded with statistical and mathematical algorithms. This enables confirming the proper users identify and rejecting anyone else. Advocates of eye vein's verifications indicating that one of the strengths related to technology has been the stability regarding the pattern of eye's blood vessels; patterns are not changing with redness, alcohol consumption, age, and allergies. [17]. Furthermore, eye vein verification, similar to other biometric authentication approaches, might be utilized in a lot of security situations, such as healthcare environment, government security, and mobile banking [18]. The benefits of these approaches are as follows [19]:

1- Each individual has distinctive eye vein patterns

2- The patterns are not changing with time and can be read even with redness

3- Used with glasses and contacts/

4- High-resistance against false matches.

2.2.2 Palm Biometric

The palm print-based individual identifications can be defined as an efficient approach to identify individuals with high effectiveness. The palm prints are specified to have a lot of features: minutiae points, wrinkles, principal lines, singular points, and ridges, as can be seen in the Figure (2.2). The surface area of palm prints is large in comparison to a fingertip, Yet, it is covered with some type of skin related to the fingers [20]. The data set is a palm dataset version 1-0 of 100 subjects [21].

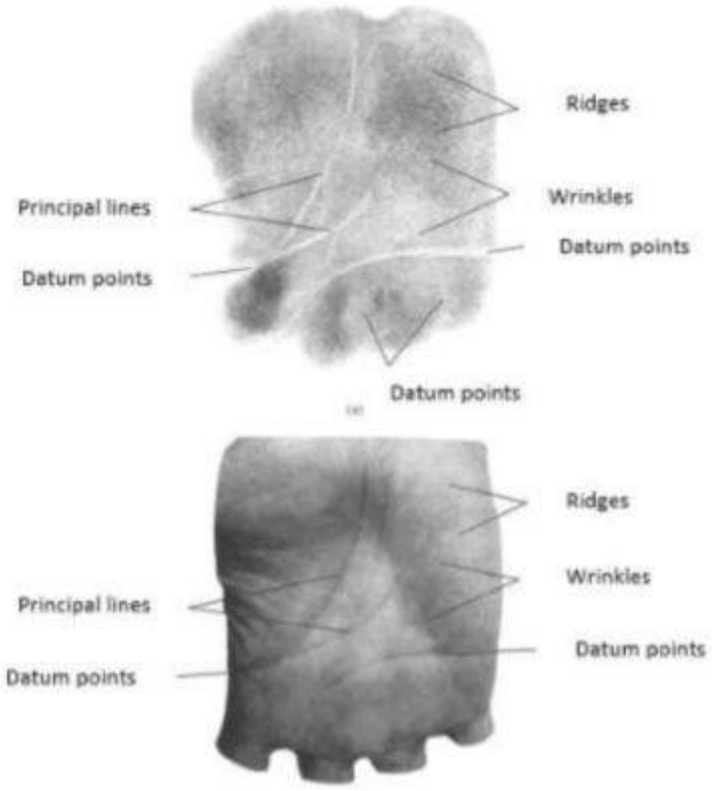


Figure (2.2) Different features of palm print (a) inked palm print (b) inked less palm print [21].

There are two acquisition methods for palm prints [18]:

i. **Offline Palm Print:** In 1996, the offline palm print started utilizing the inked images, as can be seen in Figure (2.3). The offline approach collects the samples via pressing the palm of the user on a sheet of white paper following inking it. After that, the ink will be dried, and the palm print's image on the paper is going to be digitized with a scanner as well as being stored in the PC. With a regard to real-time application, including physical access control, the approach has not been adequate. Along with the number of involving steps, the palm print has an unsatisfactory quality because

it may be affected by how much ink has been used. Too little or too much ink can produce low quality palm prints.

Figure (2.3) Offline Palm Print Acquisition [21].

ii. **Online Palm Print Acquisition:** It is the most direct method for digitizing data of palm print, makes the requirement for a 3rd medium such as a paper pointless. It might be achieved through the use of a scanner that directly scans a palm print, or the use of a video camera to generate the data of palm print.

2.2.3 Biometric System

These systems are mainly pattern-recognition systems recognizing an individual on the basis of feature vector obtained from certain behavioral or physiological features of the individual. On the basis of the application context, the biometric systems are generally operating in one of the two modes: identification and verification as can be seen in Figure (2.4) [22].

i. **In verification mode**: The system will be validating the identity of an individual through putting to compare the obtained biometric

features with the biometric template of the person, that has been pre-stored in the system's database, such model is referred to as matching model. For instance, an individual might be provided with physical access to the building's secure area with the use of a finger scan or might be accessing a bank account at an ATM by using a retinal scan [23].

ii. I**dentification mode,** systems are recognizing individuals through attempting to find a match in the whole template data-base. Also, the system is conducting one-to-many comparisons for establishing the identity of a person. For instance, use a camera to scan a crowd as well as utilizing the technology of face recognition, one might be determining matches against certain data-base. [23].

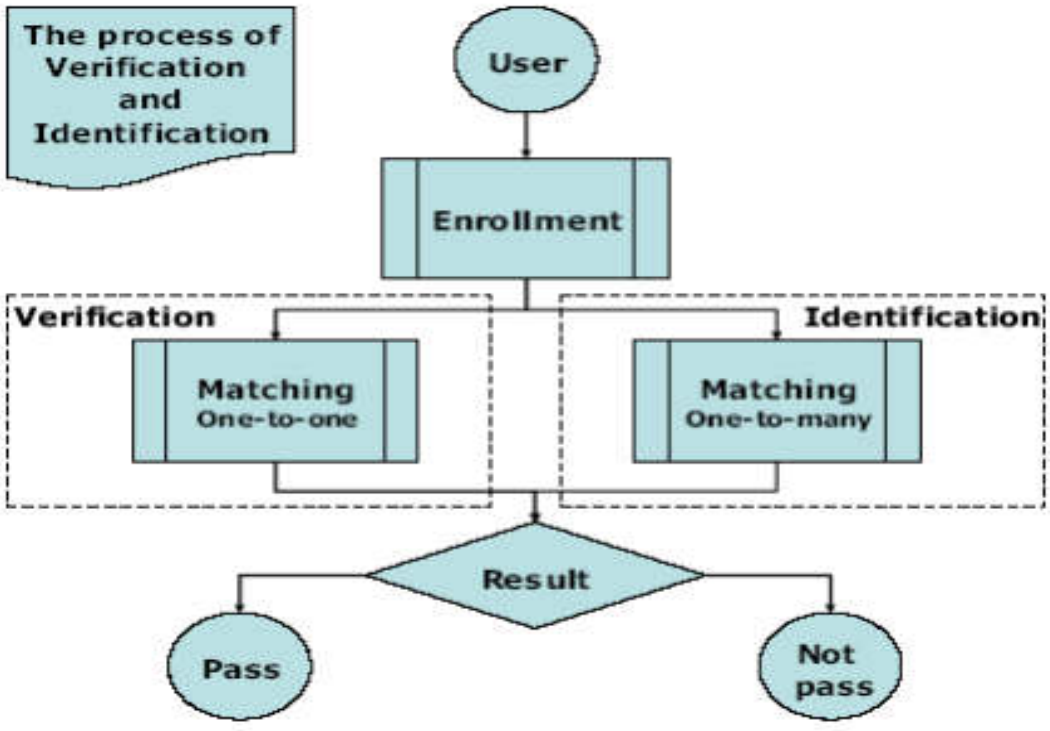


Figure (2.4) Block diagrams of Biometric system [24].

As an illustration in Figure (2.4), a new biometric user should first be enrolled prior to utilize biometrics. Generally, this is achieved through authorized individuals enrolling new users on biometric device, such authorized individual controlling and verifying the identity of an enrollee. In the case for elucidation, when enrolling a template has been generated, and has been stored either in smart-card, data-base, or another medium of storage, As users are enrolled successfully, they will be authorized to start logging in with the use of biometrics [24].

2.2.3.1 Requirements of Biometric Characteristic

Behavioral or physical features are required for meeting certain requirements for the purpose of being applied as biometrics approaches, such requirements might be practical or theoretical [23].

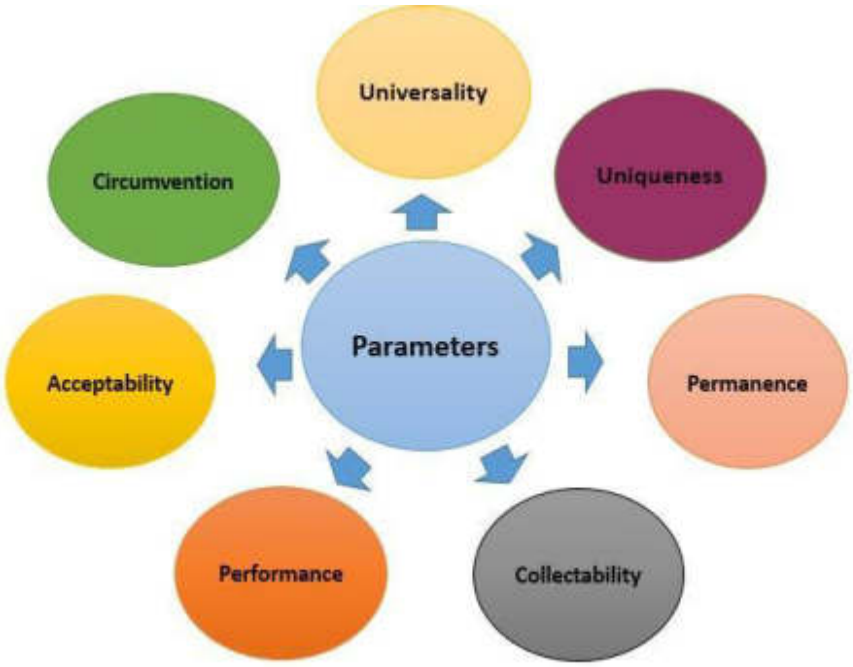


Figure (2.5) Biometrics requirements [23].

Basically, there are 7 theoretical requirements as follows: [23]

i. **Universality:** All individuals must have biometric features. There are individuals with injured eyes, individuals with no fingers, or mute people. Getting 100% coverage is difficult.

ii. **Uniqueness:** Indicating that no 2 individuals must be the same with regard to biometric features, specifying how distinctively and differently biometric systems have the ability for recognizing each of the users in groups of users.

iii. **Permanence:** It is needed for each one of the traits or features that has been recorded in the system's data-base and should be constant for a specific time period, indicating that the features must be invariant with the time.

iv. **Collectability** Indicating that the features should be quantitatively evaluated and acquired the characteristics must be simple.

v. **Performance** Indicating possible identification/verification accuracy as well as resources, working or environmental conditions required for achieving adequate accuracy.

vi. **Acceptability** Choosing the field, where biometric approaches have been acceptable.

vii. **Circumvention** Deciding how simplify each one of the features and traits offered via users might fail throughout verification.

2.3 Image Preprocessing

The approaches of image enhancement enhancing image' quality as seen via individuals. Typically, the approaches of image enhancement have been utilized for getting details that are obscured, or for highlighting some image's features of interest. With regard to the process of image enhancement, one or Two image's attributes have been changed. The major aim of image enhancement is bringing out the

image's details hidden in the image or increasing the contrast in images of low contrast. In the case when converting the image from a form to another, like digitizing the image, a degraded form will happen at output [25].

2.3.1 Converting Image to Gray scale

The most important benefit of converting a colored image into a grayscale domain is to less amount of data because there is only one channel in the grayscale domain rather than three as in the RGB domain [26].

Two principles for converting color to grayscale are such as [27]:

i. The approach of lightness will be averaging the lest prominent and most prominent colors as in equation (2.1):

$$Grayscal(i,j) = 1/(max - min) * (I(i,j) - min) \qquad (\mathbf{2.1})$$

ii. The average method averages the color values as in equation (2.2):

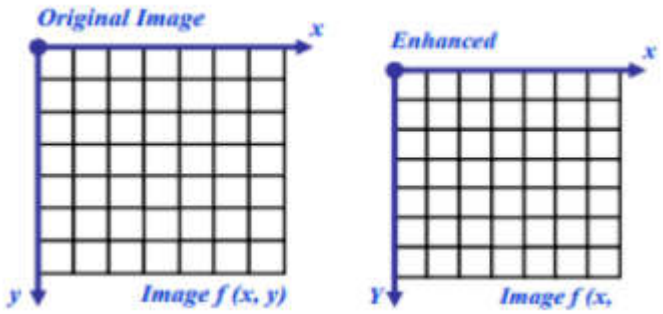
$$Grayscale\ (i,) = (R + G + B) / 3 \qquad (\mathbf{2.2})$$

2.3.2 Banalization

Digital Image Processing is aiding the algorithms of computers for performing image processing on the digital images. The major goal of image enhancement approaches is majorly applied in various applications related to image processing, in which the image's subjective quality has been of high importance to the human interpretation or for providing better input with regard to other systems of automated image processing [28].

The approaches of image enhancement might be categorized into two categories: Frequency domain approaches operating on image's Fourier transform, and the Spatial domain approaches operating directly on the pixels. Thresholding can be defined as the simplest approach of the segmentation. It has been achieved via threshold values that have been acquired from

histogram of the original image's edges. Thus, in the case when edge detections have been precise, then the threshold will also be precise. Furthermore, the thresholding transformations have been of high importance to segmentation for isolating objects of interest from a background as can be seen in Figure (2.6).



(a) (b)

Figure (2.6) Isolating object from background [28].

2.3.3 Remove Noise

Eliminating image noises is of high importance in image processing. Images might be corrupted through random changes in the pixel's illumination, intensity, or because of bad contrast and might be directly utilized. Thus, noise is a major issue in image processing. It is resulting in random modifications in the images, thus the original values fluctuating to certain distinctive values. A solution to such a problem has been developing a robust algorithm that has the ability for processing images even with the existence of noise. An alternate solution to this problem is to design a filter that is eliminating the noise along, also preserve the image features, edges, and details [29]. With regard to this work, the suggested system applies two major approaches for removing noise from the input biometric images, such approaches are indicated in sub-sections bellow (i and ii).

i. A Median Filter

Basically, the filters are of two types, non-linear and linear filters. The latter, also indicated as averaging low pass filter, the issue with such type of filter has been the edge's blurring and losing the image's content, thus reducing the output's correctness. Whereas the first type of filters has better results in comparison to latter, since they are eliminating noisy pixels without resulting in edge blurring. Also, median filters are examples of non-linear filters, also they are of high importance in retaining image's features. The median filter is considered to be a simple implementation related to non-linear filters with regard to noise removal. The targeted noisy pixels have been substituted via its neighbors' median value. The number of neighbors is determined via the filtering window size. Median value has been easily specified as a mid value in the sorted sequence [29].

$$Median\{P\} = Med\{P_i\}$$

$$Median\{P\} = Med\{P_i\}$$

$$= P_i\left(\frac{k+1}{2}\right), k\ is\ odd$$

$$= \frac{1}{2}\left[P_i\left(\frac{k}{2}\right) + P_i\left(\frac{k}{2}+1\right)\right], k\ is$$

Where P1, P2, P3 ……Pk representing the neighbor pixels' sequence. All the image's pixels must be arranged in descending or ascending order, prior to using filtering. Following achieving sorting, resulting image pixel sequence is going to be Pi1≤Pi2≤Pi3≤....Pik, .k has been typically odd [29].

ii. Fill Flood Algorithm

This is the major utilized approach of image processing to find the connection as well as the shortest path between 2 points [30]. It is considered as a major region filling algorithm that has been typically based on the notion of 4-connectivity or 8-connectivity. Mathematically, assuming that P = (x,y) denotes the pixel's coordinate, the it is 4-Connected regionC_4(P) in bitmap and specified in the following way [31]:

$$C_4(P) = \{(x, y-1), (x, y+1), (x-1, y), (x+1, y)\} \quad \textbf{(2.3)}$$

and its 8-Connected region C_8(P) in bitmap specified in the following way [31]:

$$C_8(P) = C_4(P) \cup \{(x-1, y-1), (x+1, y+1), (x-1, y+1), (x+1, y-1)\} \quad \textbf{(2.4)}$$

Visual illustration will be provided in Figure (2.7).

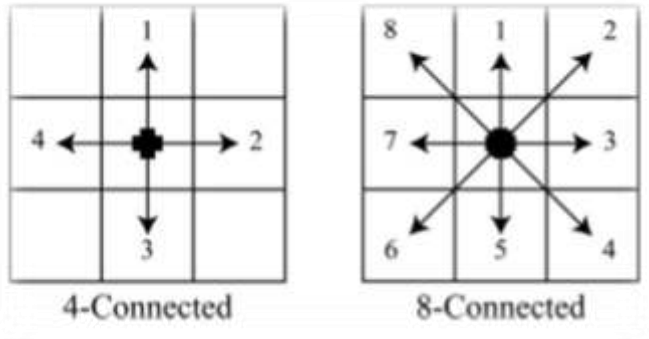


Fig (2.7) Concept of connectivity.

Pixel of interest is the pixel in the box's middle, also its 4-connected of the 8-connected region includes all the pixels which might be reached through arrows which start from it [31]. Also, the flood fill algorithm is starting from a recognized pixel in the closed area, as well as

recursively finding all pixels in connecting region related to the known pixel. For the purpose of reaching all pixels in each of the regions (typically in 4-connected or 8-connected region as indicated earlier), a stack might be needed, also pixels in the region might be recursively visited [31].

.2.4 Morphology Operations

The Mathematical morphology (MM) can be defined as an image components extraction tool which are beneficial in the description and representation of the shape of the area, like the skeletons, boundaries, as well as the convex hull. In addition to that, morphological approaches are interested in preprocessing or post-processing like thinning, morphological filtering, and pruning [31]. The morphological processes are logical transformation operations which are based upon comparing the neighborhoods of the pixel against a specific pattern. The majority of the morphological processes are focused upon the binary images. The morphological processes provide a powerful and unified method for many requirements of image processing [32]. The Mathematical Morphology (MM) is using a formulate operation which is based upon a selection of structuring elements (SE_s), which is a small group of sets or sub-images, and it is utilized for examining an image for the relevant characteristics. There are numerous SE_s examples due to the fact that it may be characterized in a variety of shapes based on the object which exists in the considered image. In Figure (2.8), we illustrates various structure element examples [32].

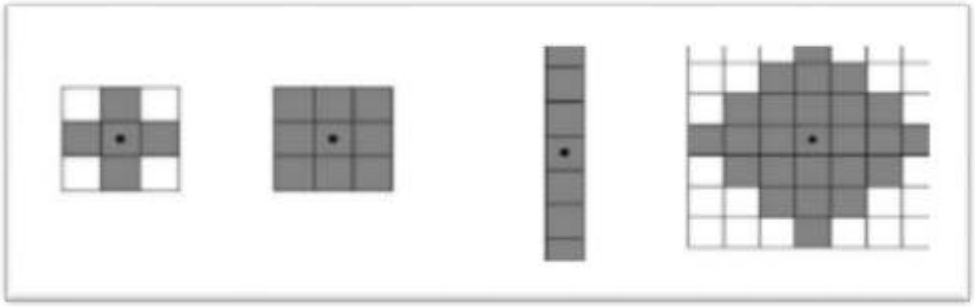


Figure (2.8) SE_s examples [32].

Every one of the shaded squares in Figure (2.8) represents an SE_s member. To define the elements that are SE members, the structuring elements' origin must be provided. In addition to that, the origins of the variety of the SE_s have been characterized with black dots as can be seen Figure (2.8), SE_s has to be rectangular arrays accomplished with the appending of smallest possible background elements' number [32].

i. Morphological dilation

Dilation can be defined as an operator in the MM area, the other is the erosion. Which is often implemented on the binary images, however, there are versions working on the gray-scale images. The operator's main impact of a binary image is gradually enlarging the regions' boundaries of the pixels of the foreground. This is why the foreground pixel areas will increase in the size whereas the holes inside these areas decrease in the size. In the dilation white pixel is increased in image making, it looks broader. Each one of the background pixels which is touching a pixel of the object is changed to a pixel of the object [33].

Dilation is utilized for growing the input image region. SE is utilized by the dilation to probe and expand shapes. While SE size specifies the matrix

dimension and the shape characterizes a pattern of 0s and 1s [34]. In the case where the SE is implemented on the image A, new image I will be

$$I = A \oplus S = \bigcup_{s \in S} A_s \qquad (2.5)$$

ii. Morphological Opining Operation

The image opening operation is a combination of erosion and dilation operation by using intersection and complementation [34]. Let assume A consists of set elements of the 8-connected boundary, each element in boundary enclosing a background. The conditioned dilation (opining) is beginning by producing matrix X_0 of 0s which size is equal size A

$$x_{i=}(X_{i-1} \oplus S) \cap A^C \qquad (2.6)$$

final step: $X_i = X_{i+1}$, where X_i contains all the filled holes.

iii. Morphological closing

The morphological erosion comes after dilation operation using the same structuring element [34]. The closing operation is

$$A.S = (A \oplus S) \ominus \boldsymbol{S} \qquad (2.7)$$

iv. Morphological Erosion

Morphological erosion operation aims to shrink the image [34]. The output of erosion operation is an image I is

$$I = A \ominus S = \bigcap_{s \in S} A_{-S} \qquad (2.8)$$

2.5 Find Objects (Localization)

The present world is surrounded by massive amounts of the digital visual data. The image content specifies the importance of the majority of possible utilizations. One of the significant aspects of the image content is

image objects. Which why, object recognition methods are necessary. The process of the object recognition can be defined as one of the significant tasks in computer vision and image processing. It is specified for the determination of object identity which is being observed in the image from a group of the known tags. Humans have the ability of the recognition of different objects in real world simply with no effort; in contrast, a machine by itself has no ability of recognize the objects. The algorithmic recognition task descriptions are applied to the machines [35].

Object recognition can be defined as a general term for the description of a set of the associated tasks of the computer vision involving the identification of the objects in the digital images. The classification of the Images is involved with the prediction of one object class in the image. The localization of the objects means the identification of locations of one object or more in the image and drawing a bounding box that surrounds their extents. The detection of the objects means the combination of those two tasks and performs the localization and classification of one object or more in the image [36]. In the image processing, the object can be defined as an identifiable part of that image which may be represented as one unit [35].

2.6 Feature Extraction

In the processes of machine learning, pattern recognition, in image processing, and feature extraction begins with an initial group of the measured data and produces derived values (i.e. features) Thy have been intended as non-redundant and informative, which facilitate successive generalization and learning steps, and in some of the cases lead to more sufficient human interpretation types. The feature extraction is associated with the reduction of the dimensionality, in the case where input data to the algorithm is extremely

large for the processing and it is expected as redundant (for example, the same measurements in feet as well as meters, or image repetitiveness presented as pixels), in this case, it may be converted to a decreased group of the characteristics (referred to as feature vector as well). The determination of a sub-set of initial characteristics is referred to as the feature selection. The features that have been selected are suspected to be containing related information from input data, for the sake of the desired task being carried out with the use of this reduced representation rather than complete initial data [37].

2.6.1 Scale Invariant Feature Transform Algorithm (SIFT)

SIFT has been suggested by Lowe, it solves the issues of image rotation, intensity, affine transformations, and view-point changes in the matching of the features. SIFT includes four main steps illustrated in the following subsection (i, ii, iii, and iv) [38].

i. **First Step**: Estimation of scale-space extrema with the use of Difference of Gaussian (DoG), the locations of the features is specified as local extrema of the DOG pyramid as specified by equation (2.11). To implement the pyramid of the DOG, the input image will undergo iterative convolution with a Gaussian kernel as can be seen in equation (2.10). This process will be done again as long as there is a possibility for the down-sampling. Every set of same-size images is referred to as the octave. All of those octaves combine what is known as the Gauss pyramid by equation (2.11), represented by a 3-D function L(x,y,σ) [27].

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \qquad (2.9)$$

$$G(x,y,\sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2} \quad (2.10)$$

$$D(x,y,\sigma)=(G(x,y,\sigma) - G(x,y,\sigma)) * I(x,y) \quad (2.11)$$

DOG function's local extrema (minima or maxima) are found from the comparison of every one of the pixels against its 26 neighboring pixels in scale-space as can be seen in Figure (2.9). The searches for the value of the extrema excludes first and last image in every one of the octaves due to the fact that they do not have scale above and scale below respectively. The detection of the scale-space extrema results in too many candidate key-points, some of them are less useful and unstable [39].

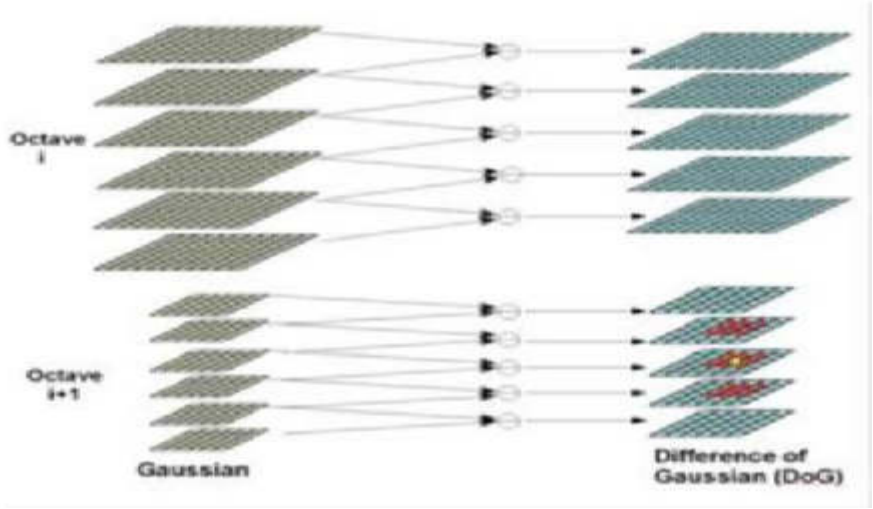


Figure (2.9) The scale space of SIFT [39].

ii. **Second Step:** Adetailed fit is performed to nearby data in order to find the precise location, ratio, and the scale of the principal curvatures. That information is useful to the points which are of low contrast or for every one of the candidate key-points, the interpolation of nearby data is utilized for the accurate estimation of the position. This interpolation is performed with the use of the

quadratic Taylor expansion of the scale-space function of the DoG, $D(x,y,\sigma)$ with candidate key-point as an origin. This Taylor expansion has been provided as in eq. (2.12) [39]:

$$D(x) = D + \frac{\delta D^T}{\delta x}x + \frac{1}{2}x^T\frac{\delta^2 D}{\delta x^2}x \qquad \textbf{(2.12)}$$

D and its derivative values are assessed at candidate key-point and x=(x, y, σ) is off-set from that point.

iii. **Third Step:** For every one of the key-points, one or several orientation values are assigned on the basis of the directions of the local image gradient. This is a beneficial step towards the achievement of the invariance to the rotations as a description of the key-points may be characterized based on that orientation and as a result, achieved the invariance to the rotations of the image. Initially, Gaussian-smoothed image L(x,y,σ) at the key-point scale σ will be taken in order to perform the computations in a scale-invariant way [39].

iv. **Fourth Step :** For a sample of the image L(x,y) at the scale σ, orientation $\theta(x,y)$, and gradient magnitude m(x,y), are pre-computed with the use of the pixel differences in the following form:

$$m(x,y) = \sqrt{\left((L(x+1,y) - L(x-1,y)\right)^2 + (L(x,y-1) - L(x,y-1))2} \qquad \textbf{(2.13)}$$

$$\theta(x,y)\tan^{-1}\left[\frac{L(x,y+1)-L(x,y-1)}{L(x+1,y)-L(x-1,y)}\right] \qquad \textbf{(2.14)}$$

2.7 Two dimensions Maximum Entropy Threshold Method

Image segmentation and feature extraction represent the initial step in many applications in the area of image processing. Thresholding is an important and simple approach to feature extraction and image segmentation. One dimensional entropy thresholding does not take into consideration spatial

correlations amongst image pixels. This why, efficiency can rapidly worsen while spatial interactions between the pixels become of a higher level of dominance compared to the grey-level values. Thereby, it will become harder to separate objects from the background and it can be found that human interference is necessary, 2-D entropy thresholding utilizes the gray value of the pixel and its local mean gray value, thereby providing more sufficient results [40].

The first step of 2D entropy thresholding segmentation is to build 2D histogram through computing the frequent occurrence of each pair of grey level of every one of the pixels and the neighborhood's mean grey-level value. The second step is to compute 2D entropy through the following formals:

Suppose mi represents the number of the pixels in which the grey level value equals i. The likelihood of the grayscales has been characterized by the formula (a). f_{ij} represents the number of the pixels where the value of the grayscale = i and the mean gray value = j.

$$M = \sum_{i=0}^{L-1} mi,\ p_{ij} = {f_{ij}}/{M} \qquad \textbf{(2.15)}$$

Assuming that s represents a pixel's gray value. Let t represent a mean gray value of the pixel. To a pair of the value (s, t), calculating information entropy has been characterized according to the formula (b) [44]:

$$\emptyset(s,t) = \ln(\sum_{i=0}^{s}\sum_{j=0}^{t} p_{ij}) + \ln(\sum_{i=s+1}^{L-1}\sum_{j=t+1}^{L-1} p_{ij}) - \frac{\sum_{i=0}^{s}\sum_{j=0}^{t} p_{ij}\ln p_{ij}}{\sum_{i=o}^{s}\sum_{j=0}^{t} p_{ij}} - \frac{\sum_{i=s+1}^{L-1}\sum_{j=t+1}^{L-1} p_{ij}\ln p_{ij}}{\sum_{i=s+1}^{L-1}\sum_{j=t+1}^{L-1} p_{ij}} \qquad \textbf{(2.16)}$$

2.8 Shark Smell Optimization SSO Algorithm

In general, each animal has capabilities ensuring their survival in nature. Some of the animal species have certain capabilities distinguishing them from other species. The detection of the prey and the hunter's movement in its direction are two significant aspects in the process of hunting. The animals which have the ability of finding their prey in a short period with an accurate movement, can be considered as successful hunters. Sharks are one of the most superior and well-known hunters in nature. Such superiority is a result of their capability in finding their prey in a short time, according to its strong sense of the smell in large search spaces. According to the abilities of that shark [42].

The shark smell optimization algorithm can be defined as a new meta-heuristic algorithm that has been developed by Abedinia et al. (2014) [42]. It has obtained inspiration from the sharks' superior hunting behaviors and their capability in sensing the prey's odor even from massive distances that can reach miles. In the case where the prey has been injured and its blood has been injected into the water, a shark will smell the blood odor and move in the prey's direction. The shark's movement in the prey's direction is fundamentally based upon the blood odor's gradient and concentration in the particles of the water. In the case of the increase of the concentration with the movement of the shark, this will mean that this movement is correct. That behavior of the shark has been utilized in the algorithm of the SSO. The assumptions below have been made while modelling the sharks'movements [42].

1- The prey has been injured and its blood has been injected in the sea (i.e. the environment of the search). Therefore, the prey movement's velocity will be low and can be neglected compared to the velocity of the shark. Which is why, the source (i.e. the prey) is assumed to be nearly steady.

2- The injection of the blood happens in a regular manner to the water and the impact of the flow of the water on distorting the particles of the odor can be disregarded.

3- There is only a single source of the blood (in other words, a single injured prey) in the shark's search environment.

The SSO algorithm has been depicted in Figure (2.10) in detail [45].

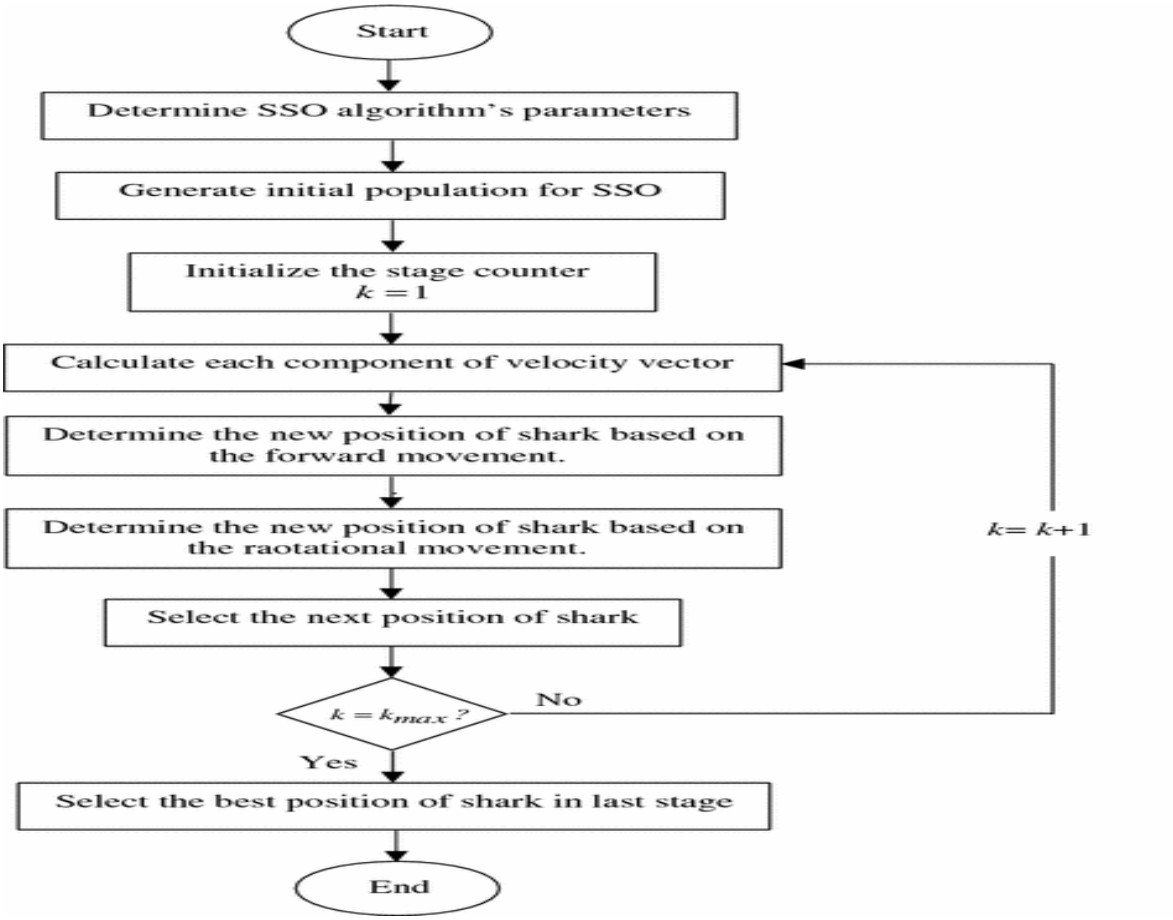


Figure (2.10) Flowchart of the SSO algorithm [45].

The method of the SSO is briefly explained in following steps [43], [44]:

- **Initializing**

The process of the search begins by the shark finding a smell of the odor particle of injured prey. An initial solution's population will be haphazardly produced in the potential environment of the seeking. Every one of them responds represents a potential shark's position. The vector of the starting position has been given by [43], [45]:

$$X_i = [X_1^1, X_2^1, \ldots\ldots, X_{NP}^1] \text{ and NP= size of the population} \quad \textbf{(2.17)}$$

X_i^i represents *i*-th starting location vector, in other words, *i*th initial potential solution. The speed of every one of the individuals of the populations is represented by:

$$SP_i = \left[SP_{i,1}^1, SP_{i,2}^1, \ldots\ldots, SP_{i,ND}^1\right] \text{ ,i=1,..,NP} \quad \textbf{(2.18)}$$

where$SP_{i,j}^1$ is the *j*-th dimension of shark's *i*-th position or *j*-th decision variable of the *i*-th position of shark X_i^1; and ND = number of the decision variables in the issue of the optimization [45]. Although, the relevant individual's objective function may be characterized by the OF (X_{NP}) and is going to be conserved for every one of the individuals following the iteration. It is assumed that the initials of the algorithm at iteration 0 [44].

- **Shark Movement Toward the Prey**

The phase that follows the initialization will be the shark's moving towards the prey to get is. Its movement comprises the forward movement as well as the rotational one. The shark is moving towards the prey in such a way that the odor concentrated and computed from:

$$SP_{i,j}^m = \mu_m . R1 . \frac{\vartheta(OF)}{\vartheta X_j}\left[X_{i,j}^m + \alpha m . R2 . SP_{i,j}^{m-1}\right] \quad \textbf{(2.19)}$$

i = 1, ⋯, NP, m = 1, ⋯,M, j = 1, ⋯,ND, μ_m represents the coefficient of the gradient, ∇(OF) represents the objective function's gradient, m represents the number of stages, M represents maximal numbers of stages in the shark's forward movement, μ_m, and am belongs to the interval of (0, 1], and R1&R2 are constants that have been generated randomly in the [0, 1] interval [44].

There is a constraint for the speed of the shark, represented in the following form [44]:

$$\left|SP_{i,j}^{m}\right| = \left[\mu_m . R1 . \frac{\vartheta(OF)}{\vartheta X_j}\left|X_{i,j}^{m} + \alpha m . r2 . SP_{i,j}^{m-1}, \left|\gamma_m . SP_{i,j}^{m-1}\right|\right|\right] \quad \textbf{(2.20)}$$

Where i = 1, ⋯, NP , m = 1, ⋯, M, j = 1, ⋯, ND, Parameter γ_m indicates the higher current speed boundary concerning the previous speed. Every one of the constituents $SP_{i,j}^{m}$ of SP_i^m will be calculated based on (Eq 2.20). For the shark's universal seeking, the evaluation of the updated position may be represented by:

$$GY_i^{m+1} = X_i^m + SP_i^m . \Delta \boldsymbol{tm} \quad \textbf{(2.21)}$$

The *m-th* time interval stage is denoted by Δtm. Therefore, the shark's local seeking may be characterized by[44]:

$$NX_i^{m+1,l} = GY_i^{m+1} + R3 . \Delta \mathbf{GY_i^{m+1}} \quad \textbf{(2.22)}$$

l = 1, ⋯,L, R3 represents a constant which has been randomly generated in the interval of (−1, +1); and L represents the number of points in every stage's local seek. The optimum values of points, studied in forward movements and the local search are selected by the shark and then modeled in the approaches of shark smell optimizations in the following form [44]:

$$X_i^{K+1} = \text{org max}\left\{OF\left(GY_i^{m+1}\right), OF\left(NX_i^{m+1,1}\right), .., OF\left(NX_i^{m+1,L}\right)\right\} \quad \textbf{(2.23)}$$

i =1, 2, .. , NP

2.9 Chaotic Logistic Map

The present section discusses the chaotic maps which are employed in this thesis. The chaotic sequences have a variety of the beneficial characteristics of the applications based upon security. Those characteristics are:- (a) chaotic is a dynamic system in the discrete time for the generation of the complex sequences behaving in a random manner in a simple and easy way. (b) Chaotic signals are not random. However, they are known for being deterministic, this characteristic permits regenerating them. (c) Chaotic signals are of high initial condition sensitivity, which leads to the fact that any changes in the initial states will produce different sequences. This characteristic will make the prediction of the chaotic sequence by the attackers very difficult to regenerate them and raise the level of security. (d) The path of the chaotic sequence behaves randomly in the specific space, which will cause the impossibility of restoring that sequence in its particular space [46]. The chaotic maps are split into two categories, 1-D and multi-dimensional maps. In this subsection, discussed the logistics 3d chaotic maps.

2.9.1 3d Logistic Chaotic Maps

The 3D Logistic Formulation logistic map is used for increasing the encryption method's level of security. The 3-D map is detailed in the formula as given in equation (2.24, 2.25, 2.26) as follows [47]:

$$x_{i+1} = \lambda x_i(1\text{-}x_i) + \beta y_i^2 + x_i + a z_i^3 \quad \textbf{(2.24)}$$

$$y_{i+1} = \lambda x_i(1\text{-}x_i) + \beta z_i^2 + x_i + a x_i^3 \quad \textbf{(2.25)}$$

$$z_{i+1} = \lambda x_i(1\text{-}x_i) + \beta x_i^2 + x_i + a y_i^3 \quad \textbf{(2.26)}$$

There are 3 quadratic coupling constant characteristics obtainable for the strengthening of the security and complexity of the 3-D

Logistic maps. This system offers chaotic behavior in $0.0 < \beta < 0.022$, $3.530 < \lambda < 3.810$, $0.0 < \alpha < 0.015$ and produces X & Z chaotic sequences in the [0, 1] range.

2.10 Digital Signature

The digital signatures can be defined as the most secure and sophisticated electronic signature type. It performs a unique identification of the document'sowner, in other words, it can identify who has sent that document. It is of comparable characteristics of the handwritten signatures. The digital signature is a cryptography application. Cryptography has been defined as the art of changing texts to unreadable forms. It has been generally classified into two categories, Symmetric, and Asymmetric Cryptography methods. Identical keys are utilized for the encryption of the data and the decryption of encrypted data in the symmetrical methods of cryptography, while the asymmetric cryptography methods have a pair of keys: the encryption is performed with the use of the Private Key and the Decryption is performed with the use of the Public key. The digital signatures use the hash function that performs the creation of the hash value and the Asymmetric cryptography that is referred to as the as public key cryptography (PKC) as well. One secret key is utilized for the encryption of the hash value that is referred to as the Digital Signature. No two persons can have identical signatures because every one of them will have a distinctive set of the PKC keys. The main digital signature objective is providing the data with security and validation [48].

2.11 Message digest 5 (MD5) Algorithm

MD-5 is a message-digest algorithm type which has been proposed first in 1991 by R. Rivest. This algorithm operates by taking any length input and producing a digest output which is 128-bit long. The input which is obtained by the algorithm undergoes processing in a 512-bit block, which will later be split into 16 sub-blocks, every one of which is 32-bit long [49]. MD-5 function produces large information amounts to be compressed to confidential format and after that, the secret key will be signed with the digital signature [50]. Figure (2.11) is shown block diagrams of MD5 algorithm [51] and Figure (2.12) illustrated the general steps of MD5 algorithm [51].

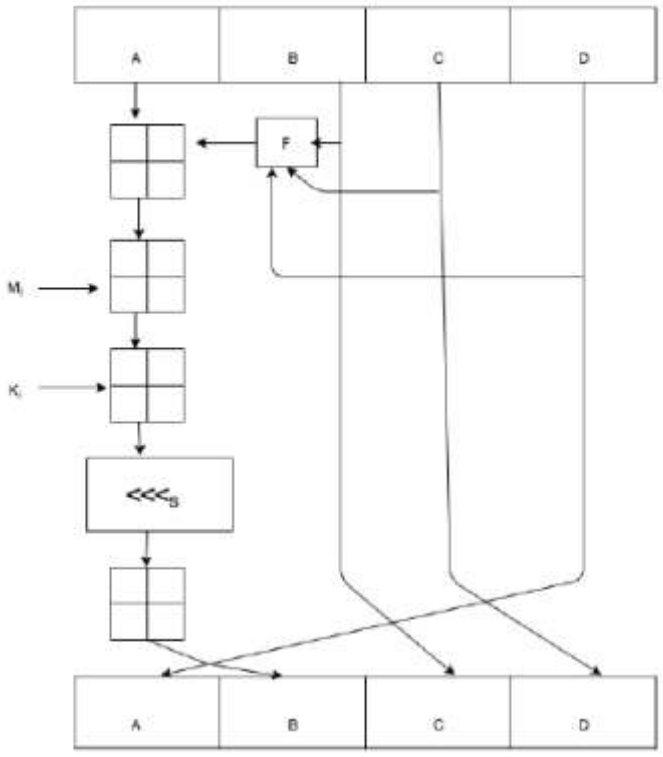


Figure (2.11) The block diagrams of MD5 algorithm [51].

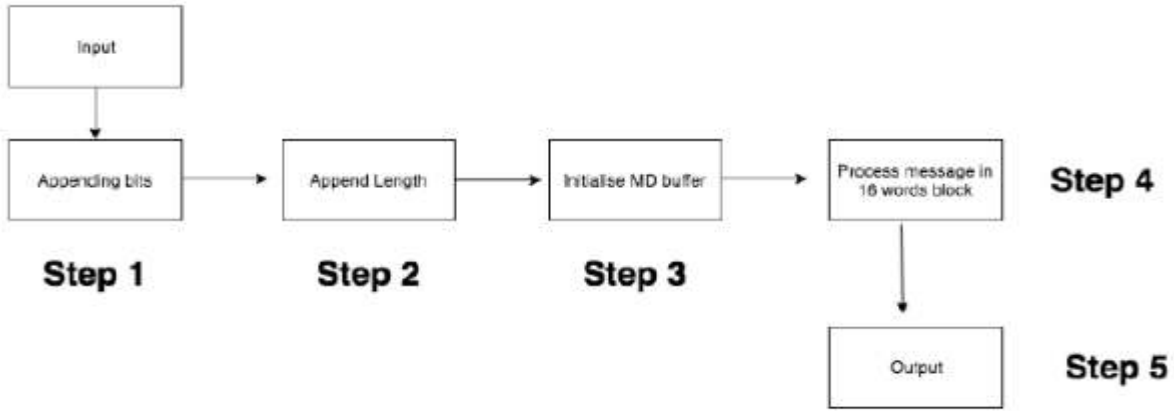


Figure (2.12) The general steps of MD5 algorithm [51].

As shown in Figure (2.10), MD5 algorithm is consisted from five main steps illustrated as following [50, 51] :

Step 1: Appending the padded bits

The message will be filled in such a manner to congruent its length to 448 mod 512. That padding is a single bit of 1, which is added into the message's end, followed with as many zeroes as needed until the length of the bits = 448 mod 512.

Step 2: Appending the length

A 64-bit message length representation will be appended to result. This step to make the length of the message a precise multiple of 512 bits in the length.

Step 3: Dividing the message

The MD-5 performs the processing of the string of the input in blocks of 512-bits long, splits it to 16 of the 32-bit sub-blocks. The algorithm's output represents a group of 4 of the 32-bit blocks, forming one 128- bit hash value.

Step 4: Initialization of the MD Buffer

Four of the 32-bit variables will be initialized in this phase:

$A = 0x01234567$

$B = 0x89ABCDEF$

$C = 0xFEBCDA98$

$D = 0x76543210$

Those are referred to as the chaining variables.

Step5 : Processing the Message

The algorithm's prime loop starts and proceeds for as many 512-bit blocks as are in that message. The 4 will be copied to the variety of the variables: a will get A, b will get B, c will get C, and d will get D. The basic loop is of 4 rounds; which all are quite comparable. Every one of the series uses a different operation for 16 times. A non-linear function is performed by each operation on 3 of a, b, c, and d. After that, it will add that result to the right a variable number of bits and adds the result to one of a, b, c, and d. ultimately, the result will replace one of the a, b, c, and d. There are 4 of the non-linear functions:

$G(X,Y,Z) = (X \wedge Z) \ (Y \wedge (\sim Z))$

$F(X,Y,Z) = (X \wedge Y) \vee ((\sim X) \wedge Z)$

$I(X,Y,Z) = Y \oplus (X \vee (\sim Z))$

$H(X,YZ) = X \oplus Y \oplus Z$

$(\vee \ is \ OR, \wedge is \ AND, \oplus \ is \ XOR, \sim \ is \ NOT)$

Step 6: Output message

The digest will be represented as output: A, B, C, D. which means that the output will begin with A low order byte, and end with the high-order byte D.

2.12 Random number generation tests

Randomness is related to several aspects of the computer sciences, particularly with the cryptography. This is why, the testing of randomness has a significant impact on the cryptography. Usually, the randomness is observed with sequences of the statistical tests. A very often utilized set is NIST Statistical Testing Suite [52]. Randomness tests have to be relatively fast due to the fact that they typically perform the processing of large data volumes. The tests are explained as follows:

1-Approximate entropy

This test has been focused on finding the frequency of all of the potential overlapping patterns of m-bits long over the whole sequence of the bits. This test has the aim of comparing the overlapping blocks' frequency of 2 successive/adjacent lengths (m&m+1) with a projected result for an arbitrary sequence. [53]

2-Frequency Test in a Block

The focus of this test is evaluating the amount of the 1's in blocks of M–bits long. It aims at determining whether or not the rate of the 1's in that M-bit block is nearly M ÷ 2 as it would be anticipated under considering the randomness. For bock of M equal to 1 size, the frequency testing performs the degeneration to Frequency (Mono-bit) Testing. [54].

3-Cumulative Sums (Cusum) Testing

This testing is performed in the counting of maximum excursions (from 0) of an arbitrary walk which has been characterized with cumulative summation of the adjusted digits (-1, +1) in a bit-sequence. This test aims at determining if the cumulative summation of partial sequences which occur in a tested sequence is excessively small or excessively large compared with the

predicted behavior of cumulative summation for the arbitrary sequences, the random walk excursion has to be close to 0. For specific non-random sequence types, this random walks' excursion from 0 is going to be high. [54]

4-Fast Fourier Transform (FFT) Test

An impulse's FFT at origin is unchanged in the domain of the transformation. In the discrete forms, impulse is a non-0 sample of the REAL [0]. The program for the testing performs the calculation of the DFT of the eight-element vector. The resulting value has to be constant in the domain of the transformation; in such case, 8 of the real values, each one of which equals 0.1250 [55]

5-Frequency Test

The focus of this test is an evaluation of the amount of 0's and 1's for the whole sequence. This testing aims at the determination of whether the rate of the 1's and 0's in the sequence is nearly equal, In the same way, it would be predicted for a sequence with actual randomness. This test performs the assessment of how close the fraction of the 1's is to 0.50, which means that the amount of the 1's and the 0's in a sequence have to be approximately equal. [54].

6-Lempel-Ziv Testing of Compression

This test is responsible for the determination of the degree to which it is possible to compress the tested sequence, which can be viewed as non-random in the case where it may be highly compressed. [54].

7-Runs Test

This test performs a measuring of the whole amount of the runs in a sequence, in which the run can be considered as an uninterrupted stream of similar bits. A k-long run includes precisely k of the similar bits and it is bounded before and after by an opposite value bit. The aim of this testing is the determination of whether the amount of the runs of 0's and 1's of different length values is like it is predicted for the arbitrary sequence. Particularly, it performs the determination of whether the oscillation between those 1's and 0's is too slow or fast.[54].

8-Serial Test

This testing determines whether or not the number of the occurrences of 2 mm-bit overlap patterns is nearly equal to what it would be anticipated for the random bit-stream. The random sequences are uniform; which means that each one of the m-bit patterns has an equal possibility to appear as other patterns of m-bits long. For the case where m is equal to 1, this test can be considered as equivalent to Frequency Testing. [53].

CHAPTER THREE

THE PROPOSED SYSTEM

Chapter Three
The Proposed System

3.1 Introduction

This chapter is focusing on the implementation requirements and design considerations of the proposed system. The proposed system: (document signature using ESSO Algorithm) is associated with many technologies that rely on extracting palm and sclera print features as keys using security approaches. These keys are used as a digital signature for documents.

3.2 The Proposed System

In figure (3.1),will be illustrate a general block diagram of the proposal system.

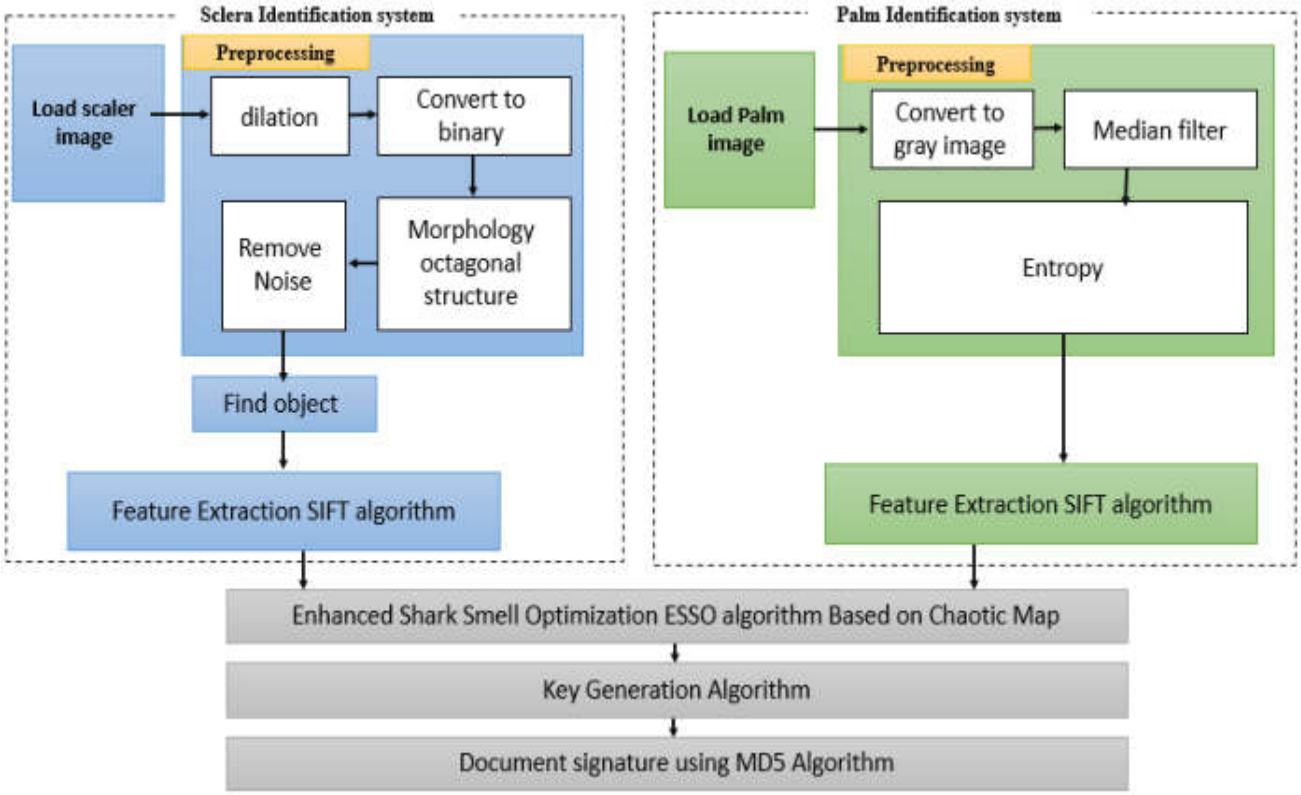


Figure (3.1) : The Proposed Block Diagram of the document signature using hybrid identification systems.

Generally, the proposed hybrid identification model includes two proposed systems: sclera identification system and palm identification system as illustrated in Figure (3.1) Each of these identification systems has different pre-processing steps than the other to extract features from its biometrics and meet in the Enhancement Shark Small Optimization (ESSO) algorithm to find the best coordinates in the secret image that used in stream key producing, and finally apply stream key in digitald signature using the MD5 algorithm.

3.2.1 The Proposed Sclera Identification System

In Figure (3.2), we clarify a general block diagram of the proposed Sclera identification system

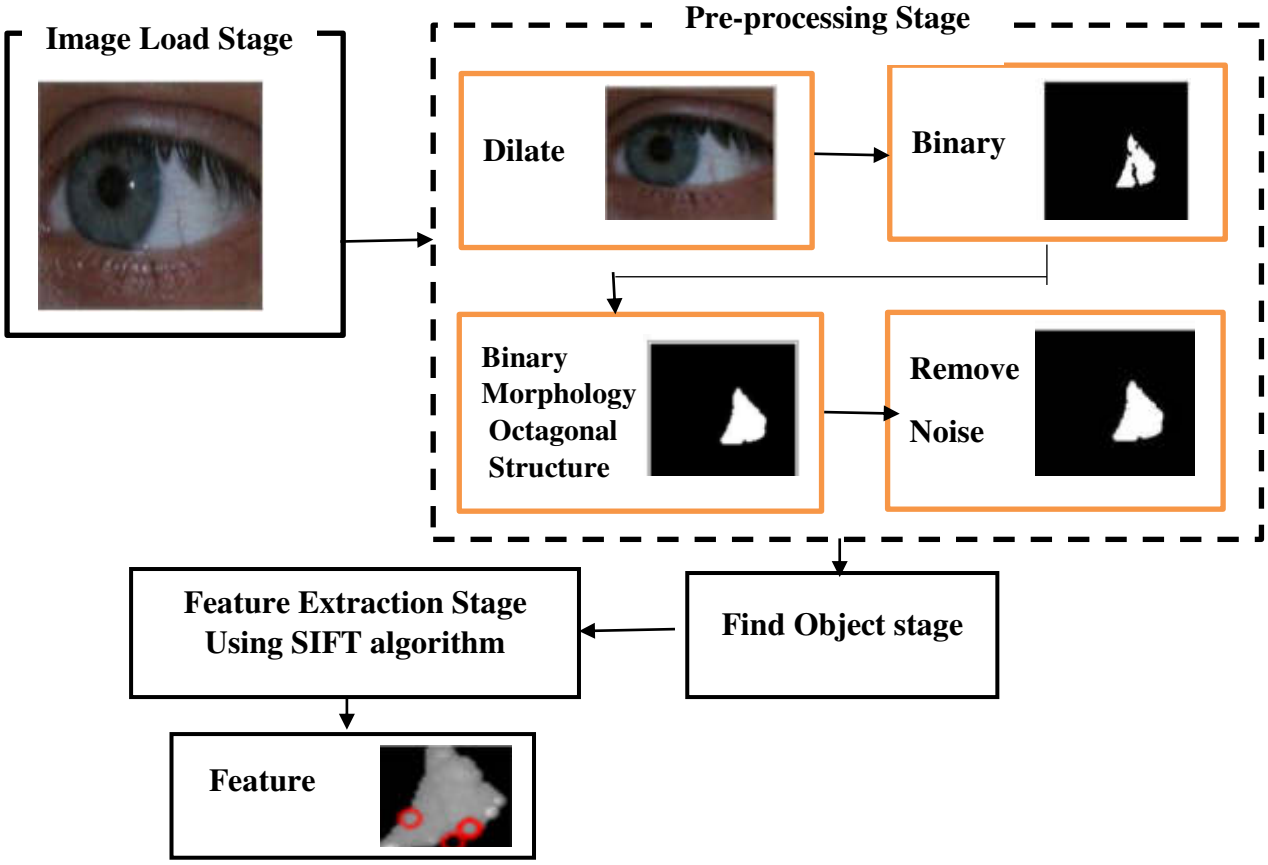


Figure (3.2): Block Diagram of the Proposed Sclera Identification System.

As shown in Figure (3.2), the sclera identification system includes four stages, these stages are:

3.2.1.1 Input Stage or (Load sclera Image)

The first stage in the proposed sclera identification system is the load sclera image form dataset in RGB color form with (.tiff) image type The {UBIRIS.v2}: A Database of Visible Wavelength Images Captured On-The-Move and At-A-Distance "Department of Computer Science, University of Beira Interior, Covilha , Portugal [56].

3.2.1.2 Image Pre-Processing Stage

The preprocessing stage is necessary to prepare the input image for further processing. This stage consists of four steps: Morphology dilate operation, binary, binary morphology octagonal structure, and remove noise as shown in subsection (i, ii, iii, and iv).

i. Morphology Dilation Operation

Dilation operations that process images based on the shapes. This step aims to make an object (white area) more visible, fills in small holes in objects, and remove small regions which considered as unimportant areas or noise on the resulting image and keep the useful areas for processing in the next steps. A dilation operation expands the image pixels and extended the object boundaries by adding pixels to it . For more, the result pixel value is equal to the maximum value of all the neighborhood pixels. The Algorithm (3.1) is illustrated the dilation operation in details.

Algorithm (3.1): Dilation Operation

Input: image bin , Kernel **Output:** output image
Begin **Step 1:**for each element in image do **Step 2**: get neighborhood from element base on kernel do

Step 3: for each elem_neigh in neighborhood do
Step 4 :if elem_neigh=0 then
elem_neigh=255
else
continue
endif
End Algorithm

In Algorithm (3.1), the dilation operation takes two inputs. (1) sclera image in (RGB) format is input to the dilation morphology operation algorithm. (2) a structuring element or (kernel) which is a set of coordinate pixels. The dilation operation results in a grayscale image. Figure (3.3) clarifies an example of the dilation of an input image with kernel size 3×3, so the offset value at each pixel location in the kernel is added to the value of its corresponding pixel in the source image. This yields a sum for each pixel location in the kernel. The result is the maximum of these sums replaced with process pixel.

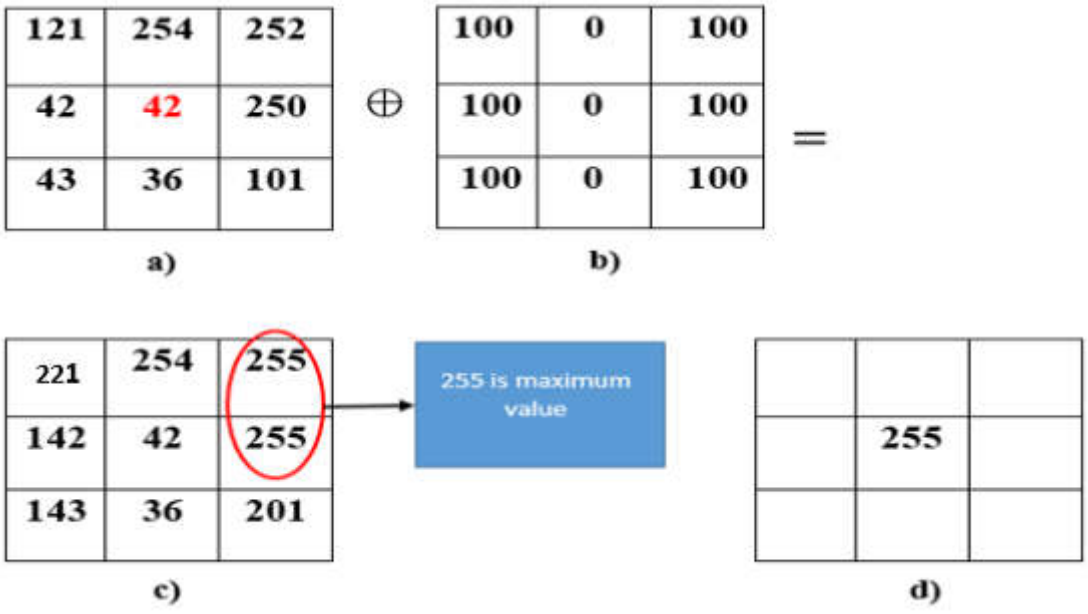


Figure (3.3): Example of a 3x3 dilation kernel for a single destination pixel: a) Source Image,b) kernel 3*3, c) intermedia results ,and d) output image

Figure (3.4) is illustrated as an example of effect that caused by the kernel resizing through dilation operation of the original sclera image.

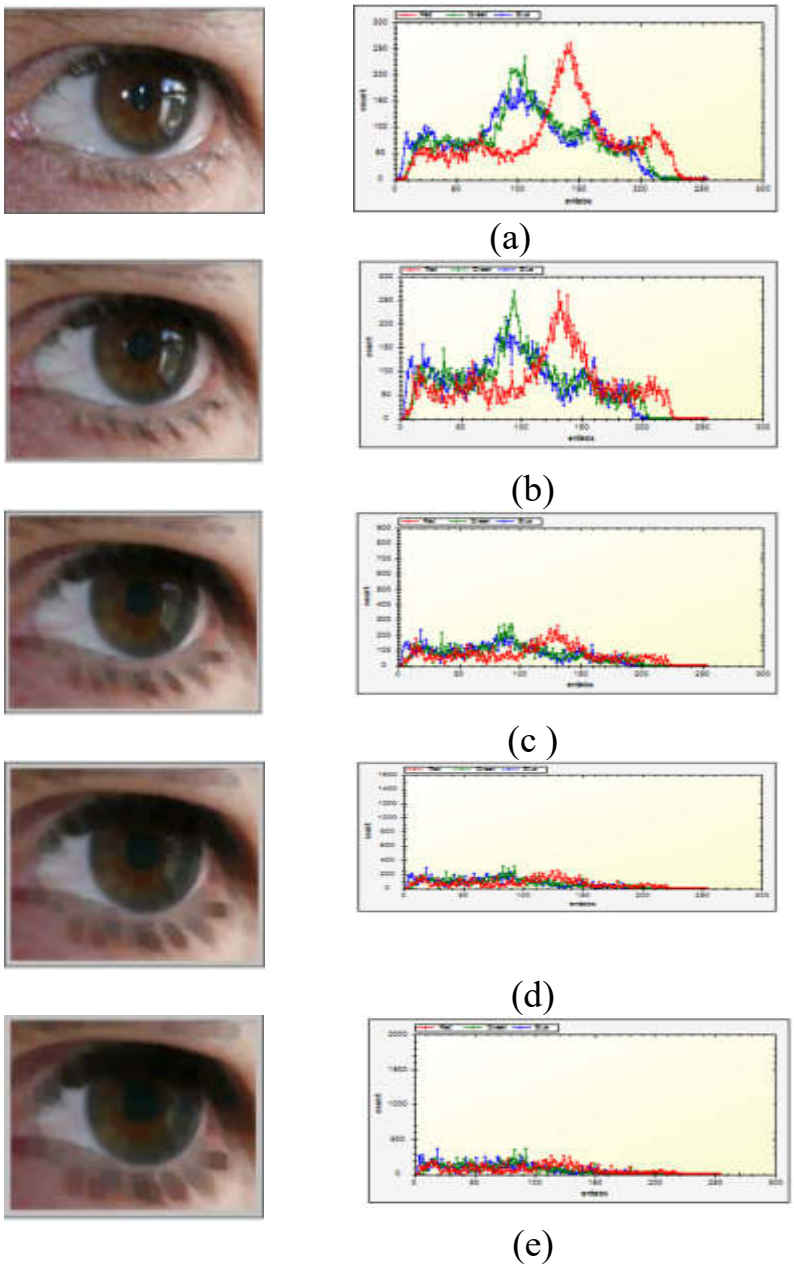


Figure (3.4) : An Example of dilation operation ,(a) input image with its histogram ,(b) dilation image with kernel[3*3] with its histogram, (c) dilation image with kernel[5*5] with its histogram ,(d) dilation image with kernel[7*7] with its histogram ,(e) dilation image with kernel[9*9] with its histogram.

As shown in figure (3.4) the proposed system gives flexibility to apply dilation operation with varying size of kernel ={[3*3],[5*5],[7*7],[9*9], },the consequence of this process is to set the foreground color to any back pixels that have an adjacent front pixel (assuming 8 connections). These pixels should lie on the edges of the white areas, so the practical result is that the front areas grow (and the holes inside the area contract). When the mask size increase the Whiteness of the result image in the front areas is increase .

ii. Convert to Binary Image

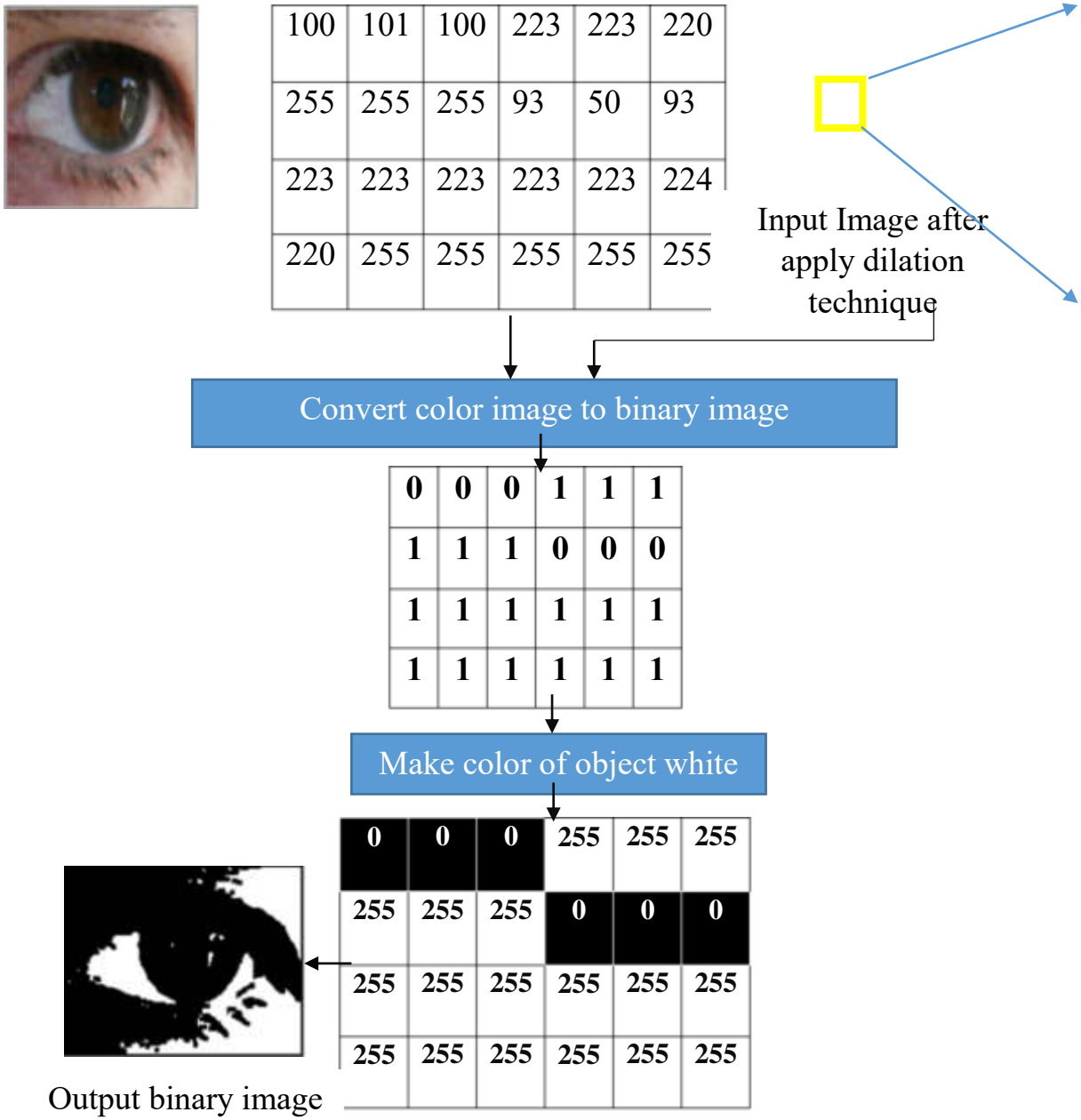
The result of previous step is a grayscale image, in this step convert it to binary using the threshold value, where the threshold value =128. This step aims to produce a binary image consist from the black pixel with value (0) and white pixel with value (255) through scanning a whole pixels of the greyscale image and test each value of the pixel; if it is greater or equal than the value of threshold then set the pixel to white color (255) otherwise set this pixel to black color (0) as shown in Algorithm (3.2) and Figure (3.5).

Algorithm (3.2): Binary Step

Input : sclera image in RGB color ,iw: weight , ih:hight ,threshold =128
Output: binary image

```
Begin
 Step 1: convert image to binary
        for each elementR , elementG, elementB in image  do
              tem =( elementR + element+ element) / 3
              IF (tem > threshold) Then
                    im=0;   //Background color is 0
              Else
                   im =1;   //The foreground color is 1
              Endif
          Endfor
Step 2: //determined object using white pixel and back ground black  pixel
        for each element in im do
```

```
            if (element =1) then
                bm.SetPixel(Black)
            Else
                bm.SetPixel(white)
            End if
        Endfor
End Algorithm
```



Figure

(3.5): Example of Binary Step with Threshold Value = 128.

iii. Binary Morphology Octagonal Structure Step

The third step in preprocessing image is the morphology octagonal structure which is a type of Erosion operation. This step aims to enhancement the edges of the image, create a harmonious, and gap - free object. The Octagon kernel size is 5×5, this octagonal kernel values multiply by values of a binary image obtained in the previous step as shown in Algorithm (3.3)

Algorithm (3.3): Binary Morphology Octagonal Structure Step

Input : Binary image

Output: Bitmap image

Begin

Step1: morph_Erosion $=\begin{bmatrix}50 & 50 & 10 & 50 & 50\\ 50 & 10 & 10 & 10 & 50\\ 10 & 10 & 10 & 10 & 10\\ 50 & 10 & 10 & 10 & 50\\ 50 & 50 & 10 & 50 & 50\end{bmatrix}$,morph_ Dilation$=\begin{bmatrix}50 & 50 & 10 & 50 & 50\\ 50 & 10 & 10 & 10 & 50\\ 10 & 10 & 80 & 10 & 10\\ 50 & 10 & 10 & 10 & 50\\ 50 & X1 & 10 & 50 & 50\end{bmatrix}$

Step2: GrayErode

```
For each elementR   in image  do
    min= 255
    get neighborhood from element base on offse do
    For each Xcolor,Y   in neighborhood,morph_Erosion do
        Z=Xcolor-Y
        If  Z<min  then min = Xcolor
    End For
    resultBitmap.SetPixel(min)
End for
```

Step3: GrayDilate

```
For each elementR   in image  do
    Max= 0
    get neighborhood from element base on offse do
    For each Xcolor,Y in neighborhood,morph_Erosion do
        Z=Xcolor-Y
        If  Z > Max then Max = Xcolor
    End For
    resultBit.SetPixel(Max)
End for
```

End algorithm

iv. Remove Noise Step

The binary image resulting from the previous pre-processing steps, after applying the morphological processes (dilation and erosion) is a harmonious image, but the noise problem remains at the edges in the image, so the edges of the cropped image are not important for the sclera image. Further, we get rid of this problem by filling the area outside the given boundary by using (flood fill algorithm) as clarified in the Algorithm (3.4).

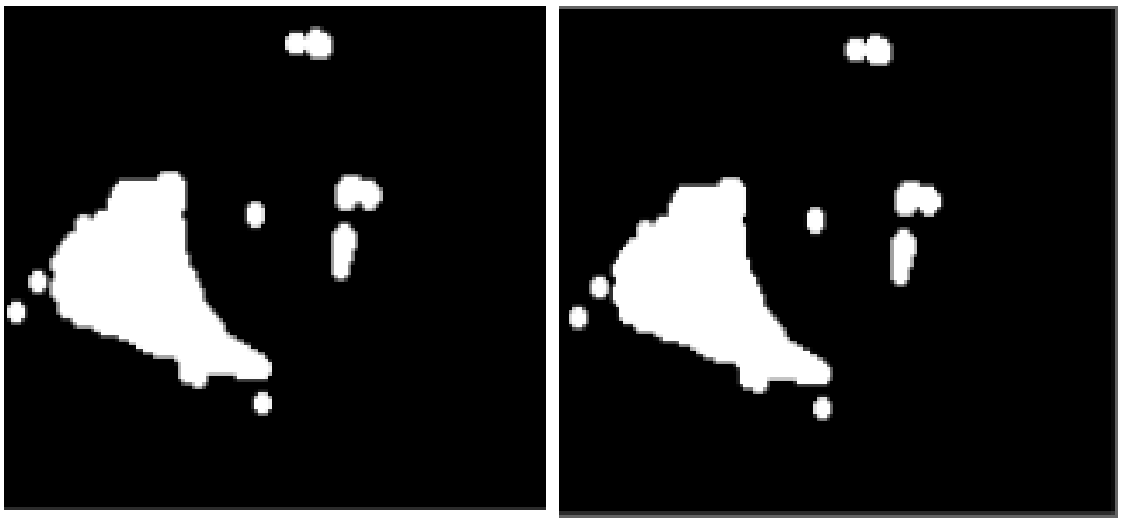
Algorithm (3.4): Remove Noise using Flood Fill using 4-connectivity.

Input : Binary image
Output: Bitmap image

Begin
Step 1: Initialize the value of seed pixel (seedx, seedy), fill-color and default-color.
Step 2: Define the boundary values of the polygon
Step 3: Check if the current seed pixel is of default color, then repeat the steps 4 and 5 till the boundary pixels reached.
Step 4: Change the default color with the fill color at the seed pixel
Step5: Foreach four neighborhood pixels do
FloodFill (seedx – 1, seedy, fill-color, default-color)
FloodFill (seedx + 1, seedy, fill-color, default-color)
FloodFill (seedx, seedy - 1, fill-color, default-color)
FloodFill (seedx – 1, seedy + 1, fill-color, default-color)
End for
End algorithm

The color of the object is different from color of its boundary, so in a flood fill technique picks a pixel internal an object (white area) and Initial fill until it reaches the boundaries of the object, where the fill color represents the same color as the object and is white. The Algorithm (3.4) depends on 4-conduct technology to fill in pixels, while searching for bord color; it searches for all adjacent pixels that are part of the interior.

In the 4-connect technique arranged neighbor pixels by placing the pixels up, down, to the right, and the left side of the process pixel and this processed will go on until the algorithm detects a boundary with various colors. Figure (3.6) shows example of flood fill algorithm with 4-connect technique of binary sclera image.



(a) **(b)**

Figure (3.6): An Example of Remove Noise using Flood Fill using 4-connectivity (a) Binary sclera image,(b) Binary sclera image without noise.

3.2.1.3 Find Object Stage using Localization technique

The third stage in proposed sclera identification system is found object. In this step, each unnecessary object (small) and does not relate to main one should be eliminated. In Figure (3.7) the object can be identified by

considering it as a matrix. The values in this matrix can be obtained from true and false answers by using the Boolean algorithm. Next, the white color pixels will be neighbored to each other in a separate layer as a group. These pixels configure non-uniformly, they may take place most left or right and top and bottom in each layer once they are set to true. However, is considered a layer that has a big number of true cases (values).

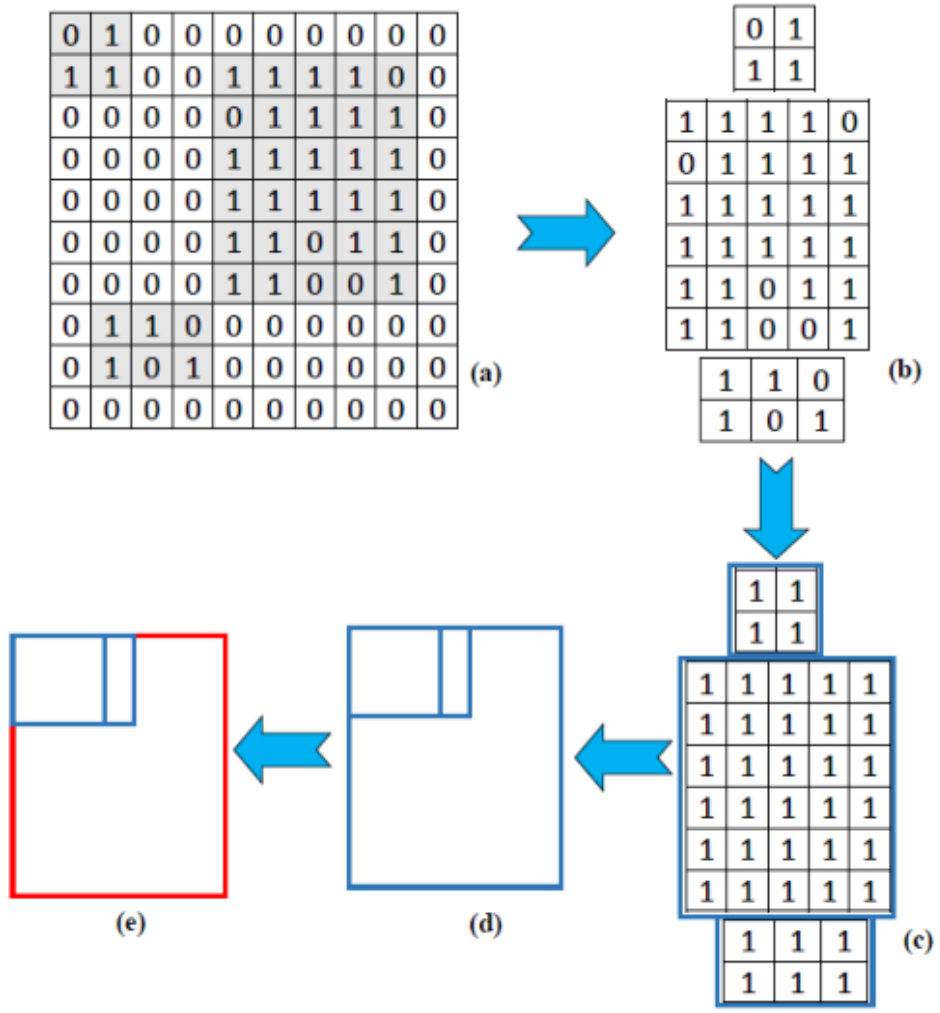


Figure (3.7): Schematic Structure for the Identifying Process, (a) the objects are detected, (b) the objects are separated into layers, (c) the objects are corrected, (d) the objects are redrawn, and (e) the largest object is chosen as sclera image.

Algorithmically, the splitting process can be achieved depending on the whiteness and the darkness in targeted images. For sclera image, the region the sclera as white color. Thus, it is simple to identify this color since the targeted images are binary image type and contain low noise. In other words, the white color in the sclera is represented by logic "1". In another method, once the denoised image is a gray-scale image, the threshold value should be stable on a certain value then compare all objects with it in order to convert the image from gray-scale into binary one. After that, the whiteness or darkness regions can be detected by identifying the logic "1" from logic "0" to form image. The Algorithm (3.5) is illustrated in details in the detection sclera image. Figure (3.8) shows an example of finding an object in binary sclera image.

Algorithm (3.5): Find Object algorithm

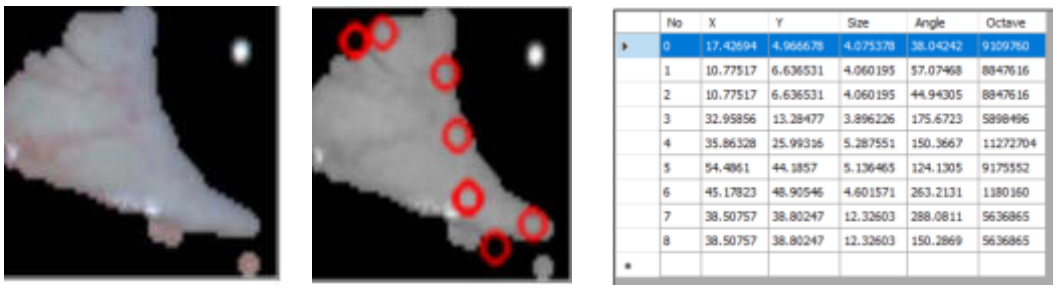
Input : Binary sclera Image
Output: Sclera part
Begin **Step 1:** Read the binary image. **Step 2:** Use Boolean algebra to add each threshold pixel (object). **Step 3:** If the result is true then is logic "1", otherwise is logic "0". **Step 4:** Applied steps 3 and 4 on every layer. **Step 5:** In each layer, change every logic "0" to logic "1" in each set has large number of logic "1". **Step 6:** The set that has the biggest number of adjacent logic "1" represents the white part. **Step 7:** Change every other logic "1" objects to logic "0". **Step 8:** All other sets denote the black part. **Step 9:** Configure the white part image by drawing all objects of the biggest set. **Step10:** Obtain the white part image **Step11:** Configure the black part image by drawing all objects of other sets **Step12:** Obtain the black part image. **End algorithm**

(a) (b)

Figure (3.8): An Example of output of find object step when No. of object =4 (a) Binary image ;(b) sclera objects.

3.2.1.4 Feature Extraction Stage

The final stage in the proposed sclera identification system is feature extraction using Scale-Invariant Feature Transform (SIFT). This step aims for detecting energy points or key points in the important area (object) that is founded in the previous step, also this step supplies a set of "important features or energy point" and "characterize/describe" of the tiny image area around the energy point. The features that detected using the SIFT algorithm are invariant to using for image matching. Figure (3.9) illustrates an example of the output of feature extraction by using the SIFT Algorithm.



	No	X	Y	Size	Angle	Octave
▸	0	17.42694	4.966678	4.075378	38.04242	9109760
	1	10.77517	6.636531	4.060195	57.07468	8847616
	2	10.77517	6.636531	4.060195	44.94305	8847616
	3	32.95856	13.28477	3.896226	175.6723	5898496
	4	35.86328	25.99316	5.287551	150.3667	11272704
	5	54.4861	44.1857	5.136465	124.1305	9175552
	6	45.17823	48.90546	4.601571	263.2131	1180160
	7	38.50757	38.80247	12.32603	288.0811	5636865
	8	38.50757	38.80247	12.32603	150.2869	5636865
*						

(a) (b) (c)

Figure (3.9): An Example of SIFT algorithm (a) Sclera object;(b) Determined key points of sclera Area;(c) description [No, Location(x,y) ,Size, angle ,octave]

3.2.2 The Proposed Palm Authentication System

Figure (3.10) illustrates block diagram of the proposed palm identification system.

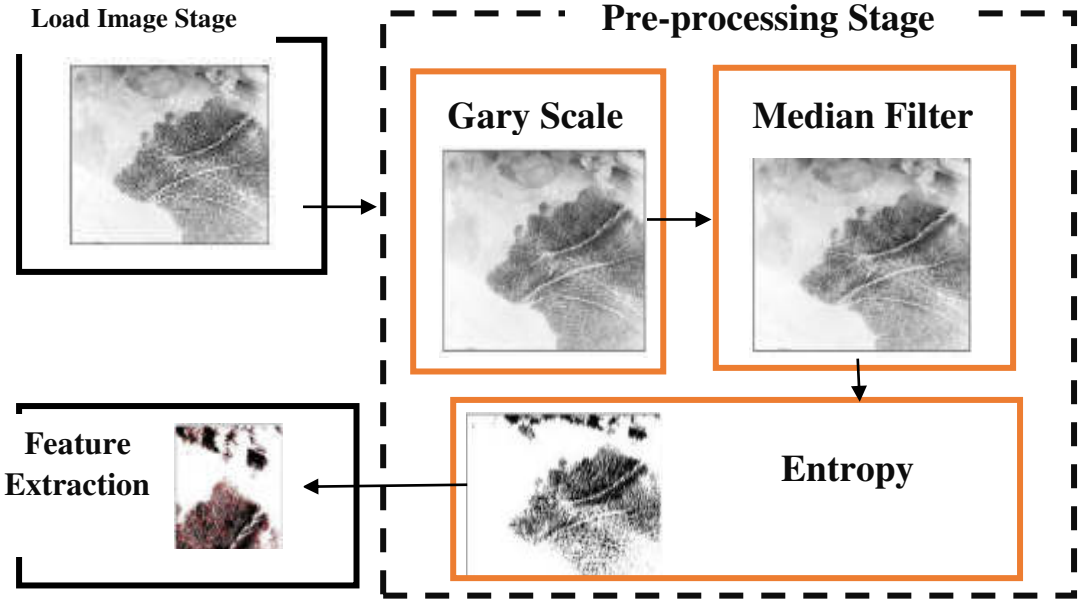


Figure (3.10): Block Diagrams of the proposed palm Identification System.

As presented in Figure (3.10) the proposed palm authentication system includes three stages, these stages are:

3.2.2.1 Input Stage or (Load Palm Image)

The first step in the proposed palm authentication system is load palm image from data set in RGB color form with bmp type the THUBALMLAP database The Tsinghua Palm print Database. Tsinghua University in Beijing China .This database contains 1,280 palm print images from 80 subjects (two palms per person and eight impressions per palm) captured using a commercial palm print scanner of Hisign. All the palm print images are of 2040x2040 pixels and 500 ppi. [21].

3.2.2.2 Image Pre-Processing Stage

The pre-processing stage is necessary to make the palm image suitable for further processing. In this proposed system, the palm image preprocessing consists of three steps: Convert the image from RGB to grayscale image, use the Median filters to enhancement image and finally apply maximum 2d entropy thresholding to find the best threshold to input palm image as shown in subsection (i, ii, and iii).

i. Convert input palm image to Grayscale color space

The first step in preprocessing palm image is the transform it into grayscale. This process allows the proposed system to reduce the color space applied for recording information obtained in the image. The color pixels demand 24 bits to be fit to represent the various layers of colors, but the grayscale image need only 8 bits for each pixel. Algorithm (3.6) shows the implementation stages to convert palm RGB color to grayscale color image.

Algorithm (3.6): Convert to Grayscale Image.

Input : Color Palm image
Output : Grayscale Palm image
Begin **Step1:** read palm image from database pixel by pixel. **Step2:** apply equation (2. 1) on each pixel of palm image. **Step3:** return gray scale image. **End Algorithm**

ii. Apply Median Filter on Grayscale Palm Image

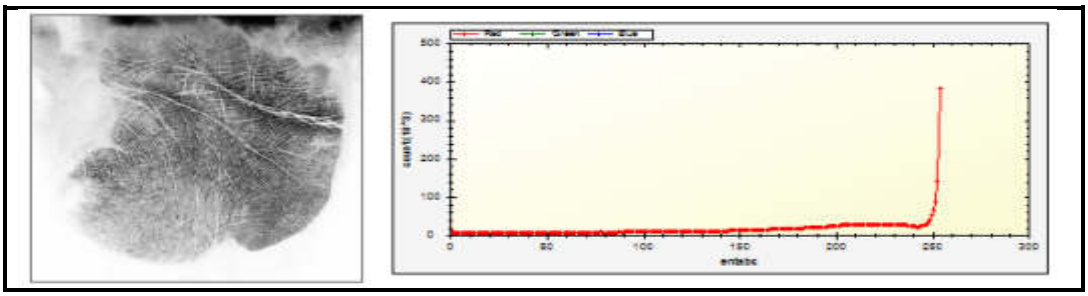
Each pixel in the palm image has gray value, this value is very close to neighboring pixels, and the pixels of the edge have the same characterizes. If the pixel value is greater or less than the value in the

neighborhood, the pixel is polluted with noise, else that the pixels are ripe in the remove noise operation, each pixel in palm image hack sequentially, if the results of compared with average value in the mask are greater or equal, then decided that the pixel is ripe with noise and replace it with the average value of the mask; else keep the value of the original pixel without change. The benefits of this method to decrease the calculations time, but also keeps the image details as farther away. The value of the original pixel is an exchange with the average value of the mask as introduce in the Algorithm (3.7). Figure (3.11) illustrates the Global Median filter on the Palm Grayscale image.

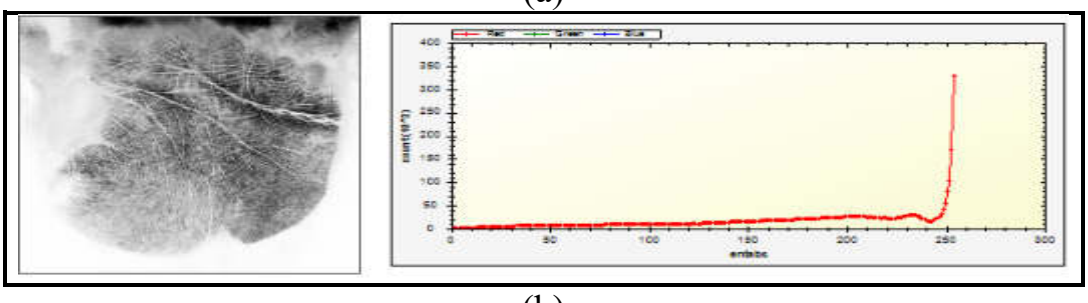
Algorithm (3.7): Apply Median filter on Palm Grayscale image.

Input : Grayscale Plame Image ,Median Mask [k,k]
Output : filtered Gray Palm Image

Begin
Step 1: For each pixel in input image
Sort neighbors pixel values in the mask [k,k]
Pick the middle one in the sorting list
Replace the pixel value with median one
End for
End algorithm



(a)



(b)

Figure (3.11): An example of the Apply Median Filter with mask size [3*3] on Palm Image (a) Grayscale image with its histogram ,(b) Filtered image with its histogram.

iii. Maximum Entropy Threshold

The final step in the pre-processing stage of the palm identification system is apply entropy method on a filtered palm image. The aim of this step is to obtain processed data to extract a few significant features from the palm image. Two dimensions' maximum entropy threshold method is utilized for analyzing palm models and extracting features from them. Entropy is utilizing to quantum the amount of noise data. Entropy is known in expression of the probabilistic behavior of original information. This proposed system is using 2D maximum entropy threshold method.

The first step in this method is found the 2D histogram for the input grayscale palm image. The histogram is normalized and the entropy equation that mentioned in (2.8) is calculated in the range (0-255). It represents the start and end. A new histogram will have to compute for the entropy function results. The histogram will be equalized and the value of the maximum entropy is taken from the outcome. The Algorithm (3.8) illustrates entropy steps in details.

Algorithm (3.8): Entropy algorithm

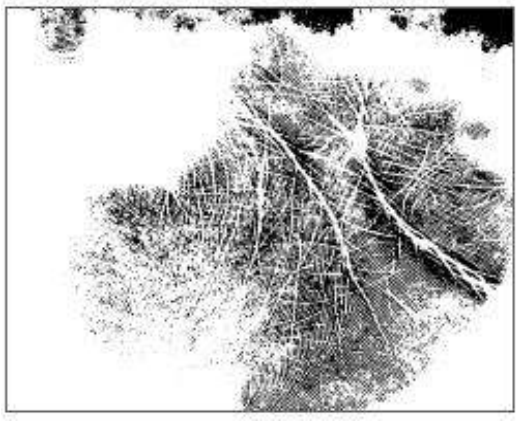
Input: Image Grey call Grey **Output** : image Equilized call EquilizeH2D

Begin
Step1:for (i = 0; i < 256; i++) HiGrey[i] = 0
Step2:find Hisgram Image Grey
For all(i=0,j=0;i< Grey.Width , j< Grey.Higth ; i++ , j++)
HiGrey[Grey[i, j]] = HiGrey[Grey[i, j]] +1;
Endfor
Step3:Hisgram Normalize
for (i = 0; i < 256; i++)
HiGreyN[i] = HiGrey[i]/(Grey.Width * Grey.Higth)

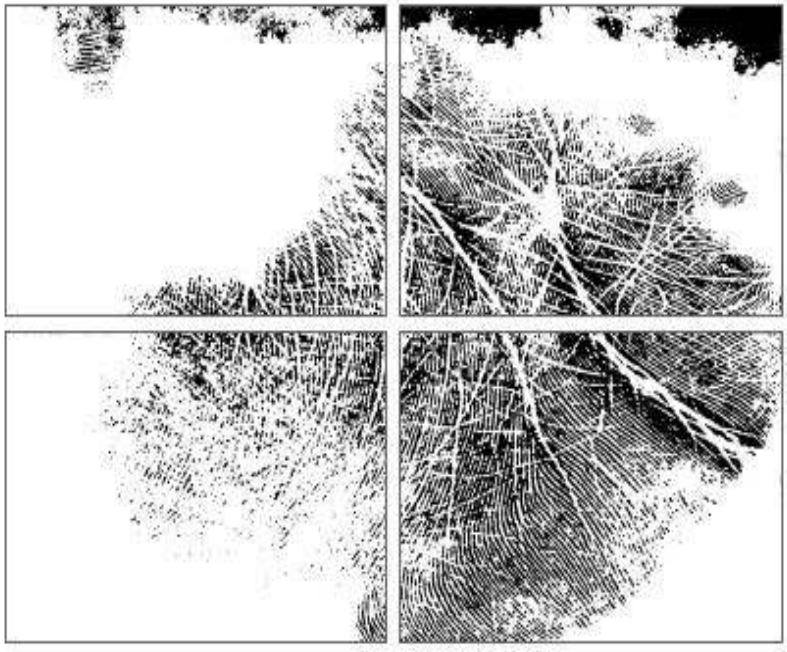
```
    Endfor
Step4:Calculate Entropy of 2D histogram
    Sum_prob_1k = 0
    Sum_prob_kl = 0
    Sum_prob_ln_1k = 0
    Sum_prob_ln_kl = 0
    for (k = 0; k < 256; k++)
      for(i = 1; i < k; i++)
       Sum_prob_1k = Sum_prob_1k + HiGreyN[i]
       if (HiGreyN[i] != 0)
         Sum_prob_ln_1k= Sum_prob_ln_1k + (HiGreyN[i] *
Log(HiGreyN[i]))
       End for
       for (int i = k; i < 256; i++)
          Sum_prob_kl = Sum_prob_kl  + HiGreyN[i];
          if (HiGreyN[i] != 0)
            Sum_prob_ln_kl = Sum_prob_ln_kl +(HiGreyN[i]
*Log(HiGreyN[i])
        end for
        EiGrey[k] =Log(Sum_prob_1k) +
                Log(Sum_prob_kl)-
                (Sum_prob_ln_1k/Sum_prob_1k)-
                (Sum_prob_ln_kl/ Sum_prob_kl)
           if (EiGrey[k] < 0) EiGrey[k] = 0;
    end for
Step5  Entropy Max Pos
   for(i=0; i < 256; i++)
      if (EiGrey[i] > tmp)
          tmp = EiGrey[i];
          max_pos = i
       endif
    end for
    for (i = 0; i < 256; i++)
      if (i <= tmp) HiGrey[ i] = 0;
      if (i > tmp )HiGrey[i] = 255
   end for
Step6 apply for image
    For all(i=0,j=0;i< Grey.Width , j< Grey.Higth ; i++ , j++)
     EquilizeH2D.Pset.(I,j) HiGrey[1, Grey[i, j]]
      Endfor
End algorithm
```

3.2.2.3 Feature Extraction Stage

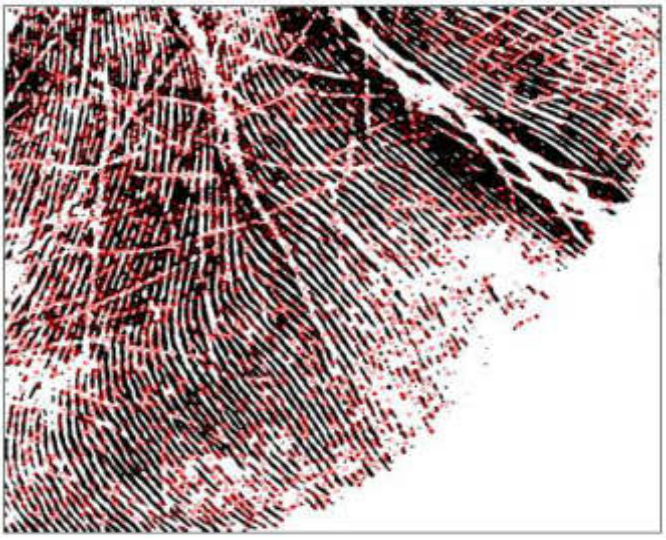
The final stage in the proposed Palm identification system is feature extraction using Scale-Invariant Feature Transform (SIFT). This step aims for detecting energy points or key points in palm image that are resulting in the previous step, also this step supplies a set of "features" that "characterize/describe" a tiny image area around the pixel which are [No, location of key points [x, y], size, angle and octaves] . Figure (3.12) clarifies the example of the feature extraction of the palm image by using SIFT algorithm.



(a)



(b)



(c)

	No	X	Y	Size	Angle	Octave
▶	0	35.16637	4.636881	3.875953	182.7917	5505280
	1	40.50309	6.093566	4.328823	172.6106	13500672
	2	73.60416	5.232244	4.087183	187.9556	9371904
	3	609.9854	6.462873	3.594019	4.35675	65792
	4	238.9135	6.815132	3.852153	324.5546	5046528
	5	238.9135	6.815132	3.852153	123.1516	5046528
	6	238.9135	6.815132	3.852153	8.964233	5046528
	7	402.0972	7.558844	3.838622	354.0357	4784384
	8	402.0972	7.558844	3.838622	167.1038	4784384
	9	796.9329	7.767213	4.606339	229.1789	1311232
	10	359.0701	9.387353	4.194162	354.4714	11206912
	11	359.0701	9.387353	4.194162	170.1328	11206912
	12	619.466	9.758923	4.651623	176.7159	1966592
	13	160.8479	9.706861	3.804516	4.799225	4129024
	14	365.1433	9.85751	4.432109	170.5821	15204608
	15	55.67271	10.54135	3.783625	325.0129	3735808
	16	55.67271	10.54135	3.783625	213.738	3735808
	17	49.70937	12.00136	4.011462	214.2965	7995648
	18	117.9837	11.82527	3.796045	343.5332	3997952
	19	117.9837	11.82527	3.796045	176.6178	3997952
	20	92.43592	15.81193	5.041585	178.2538	7799296
	21	319.9377	13.02139	3.946552	352.5988	6816000

(d)

Figure (3.12): Example of Feature Extraction of Palm Image using SIFT Algorithm(a)Binary Entropy image, (b) Four octaves of image, (c) energy point of image, (d) description [No, Location(x,y) ,Size, angle, octave].

3.2.3 The Proposed Hybrid Identification System

As shown in section (3.2), the proposed hybrid identification system consists of four main stages: (Preprocessing, enhancement shark smell optimization (SSO) algorithm based on 3d logistic chaotic function, and generate stream key and digital signature by using MD5 algorithm). The main stages of the proposed hybrid identification system are illustrated as following 'sub-sections (i, ii, iii, and iv)".

i. Preprocessing stage

The first stage in the proposed hybrid is preprocessing of both sclera and palm image, this step consists of two parts: The first part represents the proposed sclera identification system as clarifies in section (3.2.1) to get (key point and their description) of sclera image, and the Second part

represents the proposed palm identification system as clarifies in section (3.2.2) to get (key point and their description) of the palm image.

ii. The Proposed Enhanced Shark Smell Optimization Algorithm (ESSO) based on 3d Logistic Chaotic Function:

Figure (3.13) shows a block diagram of the ESSO algorithm based on 3d logistic function.

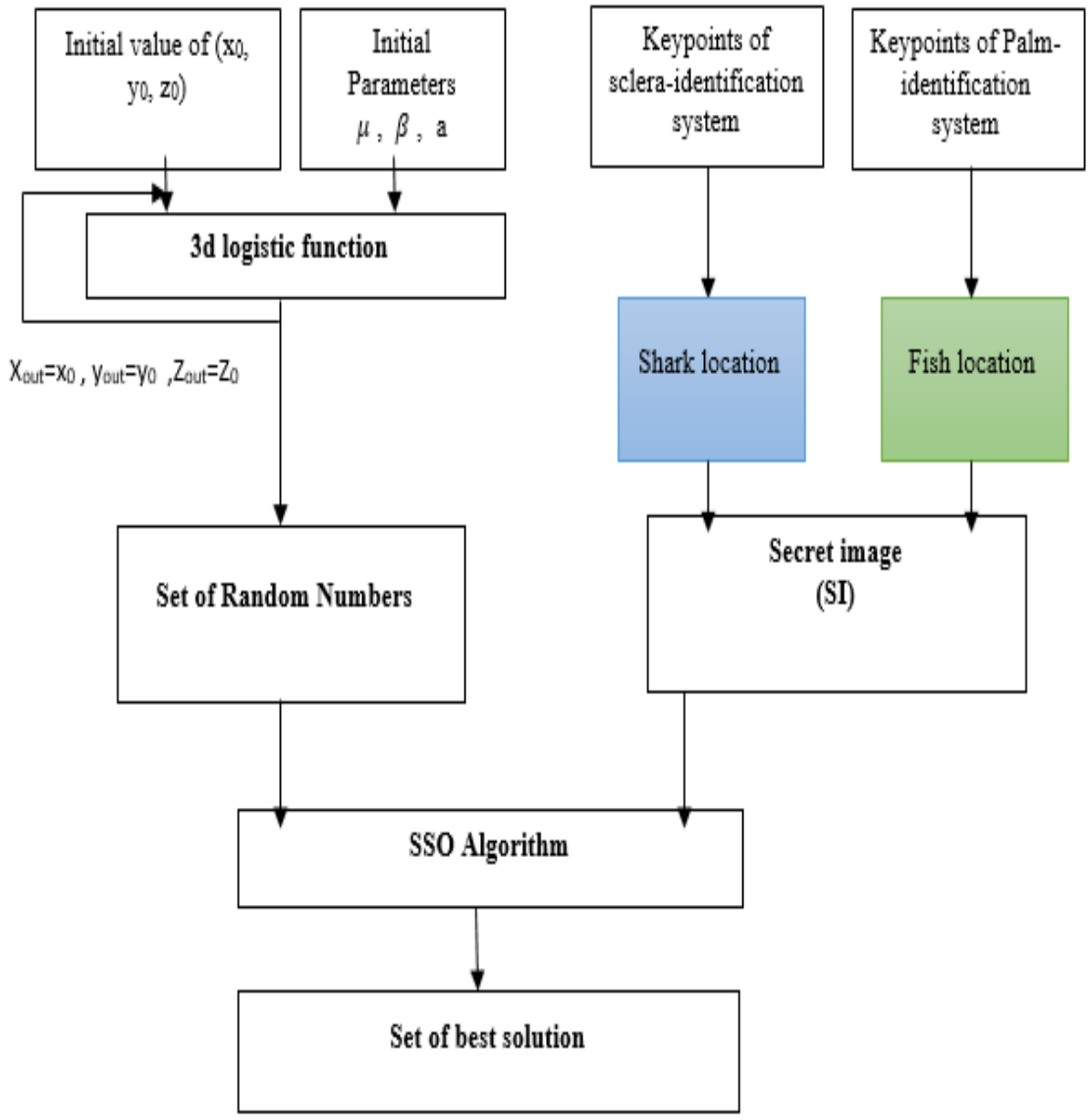


Figure (3.13) : General Block diagram of ESSO Algorithm based on 3d logistic Chaotic Map.

As shown in the block diagram of the proposed ESSO algorithm, firstly generating a sequence of random numbers as illustrated in the Algorithm (3.9), This sequence is representing the random parameter of ESSO to increase the randomization of the original SSO algorithm as illustrated and find the best solution in a faster time.

Algorithm (3.9): Generate random number based 3d logistic maps

Input set of parameter of the 3d logistic maps
$\mu = 3.6$, where $3.53 < \mu < 3.81$
$\beta = 0.0001$, where $0 < \beta < 0.002$
a=0.0012 , where $0 < a < 0.002$
$x_0 = 0.5$ // initial value for x
$y_0 = 0.001$ // initial value for y
$z_0 = 0.8$ // initial value for z
iteration =100
[] x array 1d of integer number
[]y array 1d of double number

Output: databased (RowCount, x, y, z, x)

Begin

Step1 for i = 0 to iteration
{
Logistic _ x_1 = apply equation (2. 24)
Logistic _ y_1 = apply equation (2. 25)
Logistic _ z_1 = apply equation (2. 26)
Databased.Add (RowCount, x_0, y_0, z_0, x_0)// for first element in databased
x[i] = i
y[i] = x_0
x_0 = Logistic _ x_1
y_0 = Logistic _ y_1
z_0 = Logistic _ z_1
Databased.Add (RowCount, x_0, y_0, z_0, x_0)
}
Return databased (RowCount, x, y, z, x)

In this work, we use two biometric images. Each of them has different features from another, Thuse the combination between them is done by

drooping all features on an image at the same time these features are classified into strong or weak features , Hemce we determine the strongest features for both biometrics images by using ESSO. The ESSO needs to create a suitable environment to work on it. , This is done by getting the feature or (key point) that is extracted from sclera identification system and feature or (key point) that is extracted from palm identification system. The connected between these features by dropping them on the image is called secret image for shoring referred as (SI) as shown in Figure (3.14), where yellow pixel represent shark location get from Keypoint of sclera-identification system and all blue pixels represent fish location get from Keypoints of palm identification systems.

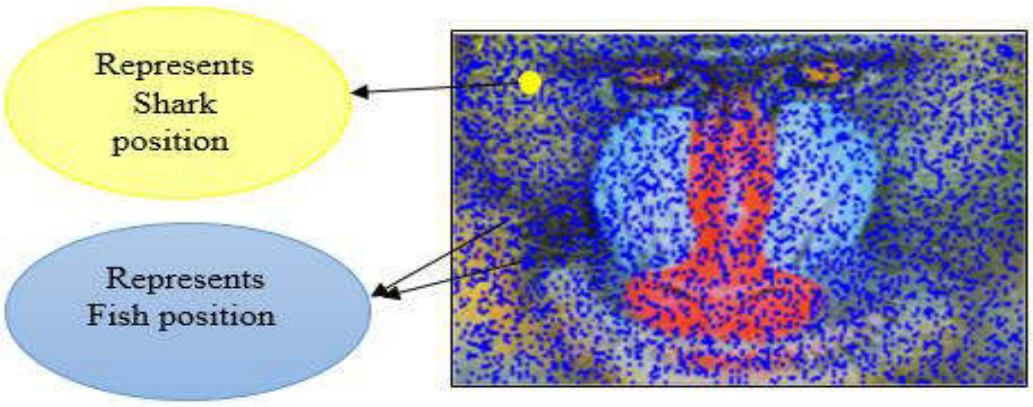


Figure (3.14): Example of dropping Features on Baboon Image

After Dropping all key points on the secret image, the secret image (SI) represents the search space that used by ESSO algorithm to find a set of optimal solutions through takes an initial key point extracted from the sclera biometric as the primary location for the shark to use in searching for fish locations, where the fish locations represent the key points extracted from the palm biometric, each a fish eaten by a shark represents a solution.

In the search space of ESSO, the shark moves toward the fish, so the search algorithm provides the shark with only two movements (movement and rotation). The shark can be reach to fish directly, also, it can move to the left or right to detect the nearest location to reach the target (fish). To achieve this propose, ESSO depends on specific steps to move to the right or the left as follows:

1- Determined locations of both shark for example, let x = {16,25}and fish f = {2,18}
2- Determined sharks neighbors with mask size [3*3] for example sharks neighbors = {X= 15, Y = 24}, {X=15, Y = 25} , {X=15, Y =26}
, {X = 16, Y = 24}, {X = 16, Y = 26} , {X = 17, Y = 24},{X = 17, Y = 25} , {X = 17, Y = 26}
3- compute the distance between each shark neighbors location and fish location by using equation (3.1)

Local distance= $\sqrt{(x2-x1)^2+(y2-y1)^2}$ ----Eq(3.1)

4- Find the minimum distance value of all Local distance value of the shark's neighbors, for example min distance for location {17,24} the location of shark replaced with its neighbor's that has min local distance.

Algorithm (3.10) shows details of proposed ESSO algorithm.

Algorithm (3.10): ESSO Algorithm based on 3d Logistic Chaotic Map.

Input : energy points description, *Is* //secret image ,random number
Output: dataset(No, location, fitness value)
Begin **Step 1:** load secret image *Is* **Step 2:** Get location of the first key point from sclera identification system

and considered it as shark location and get location of all key points from palm identification system and considered as fishes

Step 3: Randomly distributed all key points of on *Is*

Step 4: Find mean value for (*Is)*

Step 5: For Each pixel in *Is*

Fitness.pixel [x,y] =(pixel[x,y].value – mean)2/(*Is* high * *Is* width)

object_function.pixel[x,y] = R1 * αk* pixel [x,y].fitness;

end for

Step 6: Get SSO algorithm parameter which are: NP, βk , Δtk , Kmax; mask,

Step 7: Set NP=24336, ND=50, $\beta k = 1$, η=1,Kmax=10 ,K=1, $\Delta tk = 3$, $MASK = 1, i = 1, j = 1$

Step 8: Generate R1,R2,and R3

Step 9: Generate the initial population $X_i = [X_1^1, X_2^1, \ldots\ldots, X_{NP}^1]$

Step 10: Compute objective function OF(X_i)

10-1 neighbor = get neighbors of shark location (xPoint.X , xPoint.Y, mask)

10-2 Get distance between neighbors of shark neighbors pixel [x1,y1] and fishpixel [x2,y2]

a =$fishpixel\,.x_2$ -$sharkpixel.x_1$

b=$fishpixel\,.y_2$ -$sharkpixel.y_1$

Distance =$\sqrt{a^2 \times b^2}$

10-3 Get minimum Distance

Step 11: Calculate the initial velocity vectors

V_i^k= ηk.R1$\nabla(OF)/x_i^k$

Step 12: while (k<= Kmax)

For i=1 to NP

$$\left|V_{ij}^k\right| = \min\left[\left|\eta k.R1\,.\frac{\partial(OF)}{\partial x}\right| x_{i,j}^k + \propto k.R2.V_{i,j}^{k-1}, \left|\beta k.V_{ij}^{k-1}\right|\right]$$

$y_i^{k+1} = x_i^k + V_I^K.\Delta tk$,where k=1,..,kmax and i=1,.. NP

End for

K=k+1

End while

Step13: The best position of shark in the last step (kmax) which has minimum (OF) value is selected as final solution for optimization algorithm

$$\left|V_{ij}^k\right| = \min\left[\left|\eta k.R1\,.\frac{\partial(OF)}{\partial x}\right| x_{i,j}^k + \propto k.R2.V_{i,j}^{k-1}, \left|\beta k.V_{ij}^{k-1}\right|\right]$$

where k=1,..,kmax ; i=1,.. NP; j=1,..ND

End algorithm

iii. The Proposed Generate Stream Key Algorithm

In this step, proposed an efficient algorithm to generate a cryptographic key with variable length using a set of optimal solutions which are founded in the previous step. The Algorithm (3.11) illustrateS details to generate the key.

Algorithm (3.11): Key Generating

Input : dataset(No, location, fitness value, objective value) , k_{max}=10
Output: Stream key

Begin
Step 1: For k=0 to k_{max}
String xkey = "";
xkey = Convert location of (init_point.X)to binary
xkey += Convert location of(init_point.y)to binary
xkey += Convert(data[0][init_point.X][init_point.Y].fitness) to binary
xkey+=Convert(data[0][init_point.X][init_point.Y].object_function)
to binary
end for
return key stream =xkey
End algorithm

In Algorithm (3.11), we convert a solution location [x, y] that is founded by using ESSO algorithm to binary as well as convert the value of its fitness and objective function to binary as the following example: Let assume location .point be [40,6] then:

1- Xkey= convert (40) to binary="01000110 00111101 01100110 100110 10010 1110 10 01111010110011010011010011011101"

2- Xkey += convert (6) to binary ="101000110001111010110011 010 011010010111010011110101100 1101 0011010 01011101 "

3- Fitness value of (point [40,6]) is 0.056299555724630933
Convert (*0.056299555724630933*) to binary= "1010001100011 1101 010011010011010010111010011110101100110100110 10 01011101"

4- objective value of (point [40,6]) is 0.056299555724630933
Convert (*0.056299555724630933*) to binary= "1010001100011 1101011001101001101001011101001111010110011010011 0 1 0 0 1011101".

The length of generating stream key depending on the number of iterations of the proposed ESSO algorithm. Figure (3.16) shows an example of a stream secret key that is generated by using the Algorithm (3.11).

```
10100111000111101101100100011000000100011001111011011001000110000001000111
11000100000011000100110110111100110001000000110001001101101111000111001011
10100011000111101011001101001101001011101001111010110011010011010010111011
10111010010110010110011010111100101110100101100101100110101111000110001011
10011110000111000001100011000100111111101001110000011000110001001111111011
10111111100100011000110000011100101111111001000110001100000111000011110011
10011010000111101001011001000001011000010001111010010110010000010110000102
01000011010000010011010010111100010000110100000100110100101111000010110011
10010110000111011001011001111111010000101001110110010110011111110100001011
10100001011111110011010011011100101000010111111100110100110111000011010011
10010010100111100111000111101000100110100001111001110001111010001001101000
00101100100010111100011100111100001011001000101111000111001111001010010011
10001110000111100010110100111111000010100001111000101101001111110000101000
00101000011111100101101000111100001010000111111001011010001111000011100011
10010010100111100010110100111111000010100010001100001110001000000000000000
00000000000000100011100001100010001010000111111001011010001111001010010011
10010111000111101001101110111010010111010001111010011011101110100101110100
01011101001011101110110010111100010111010010111011101100101111000111010011
```

Figure (3.16): An Example of a stream key.

iv. Document signature using MD5 algorithm

The final step in the proposed hybrid identification system is a document signature by using the MD5 algorithm as shown in subsection (2.11) based on the stream cipher key that produced in previous step. The document selects to approve it for signature, and requests from proposed system the digital signature program to sign it.

CHAPTER FOUR

IMPLEMENATION OF PROPOSED SYSTEM

Chapter Four

Implementation and Results

4.1 Introduction

This chapter is dedicated to present the results and tests that evaluate the proposed system. The experimental tools are used in the proposed system , which contains image preprocessing for both (sclera and palm identification system), SIFT algorithm, enhanced shark small optimization (ESSO) algorithm, key stream generation , and document signature using the MD5 algorithm.

4.2 System Implementation

The implementing of the proposed system is using a programming language (#C) and applied in windows ten (Win10) operating system. (#C) Language deals with an easy path to access the image data of every digital image format. A software language first appeared in 2000 by Microsoft. The programming language (#C) is similar to Java language, as it is fast, and simple, and running on windows. C# Language with version Microsoft Visual Studio 2013 Visual, and Microsoft 2016.

4.3 Results of the Proposed Sclera–Identification System

The proposed system results will show sequentially in "subsections: (4.3.1, 4.3.2, 4.3.3, and 4.3.4)".

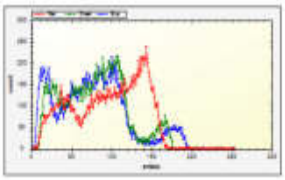
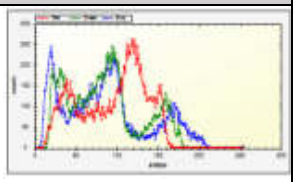
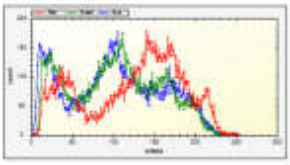
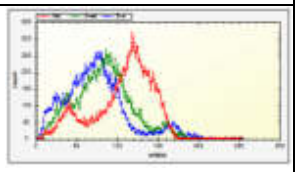
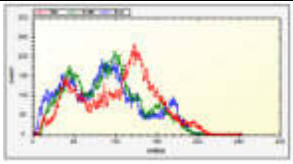
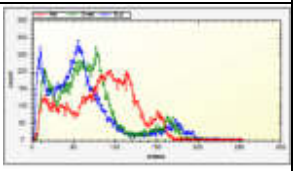
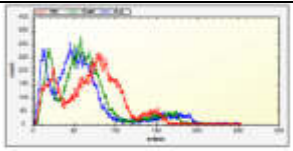
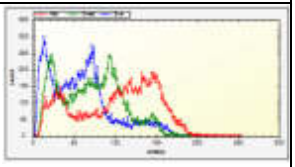
4.3.1 Loading Original Images

The following table, Table (4.1) obtains eight samples of the sclera images in RGB color space and (.tiff) image type with resolution 12.7 MP that selected

from the UBIRIS.V2 database to be implemented in the sclera identification system. The {UBIRIS.v2}: A Database of Visible Wavelength Images Captured On-The-Move and At-A-Distance "Department of Computer Science, University of Beira Interior, Covilha , Portugal.[56]

As shown in table (4.1) , the main reason for choosing eye images is that the direction of view is to the right or left, so that the white area inside the eye is greater and it is possible to extract more features from this area.

Table (4.1): Original sclera Image samples.

Image .ID	*Original Sclera image*	*Frequency*	*Image .ID*	*Original Sclera image*	*Frequency*
#1			#5		
#2			#6		
#3			#7		
#4			#8		

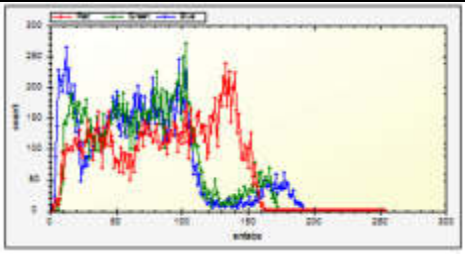
4.3.2 Sclera Image Pre-Processing Stage

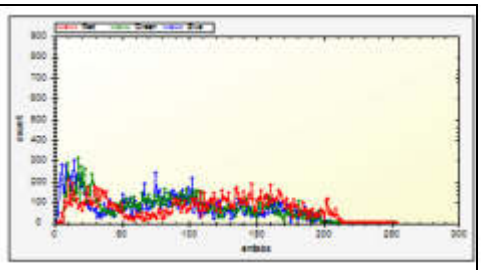
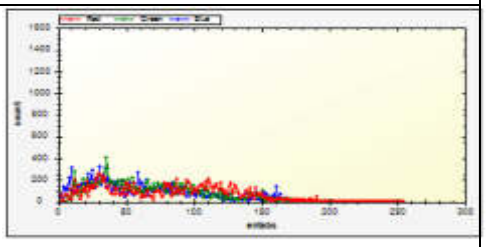
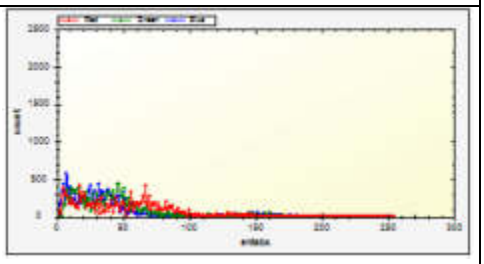
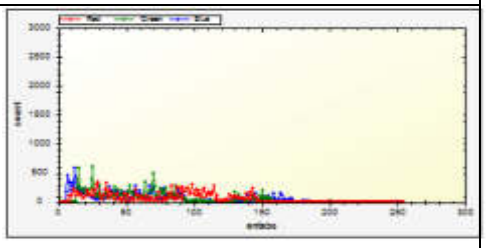
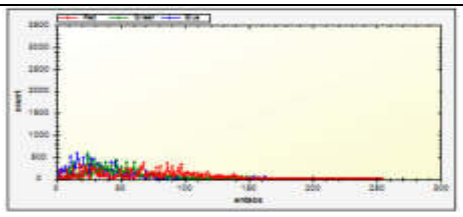
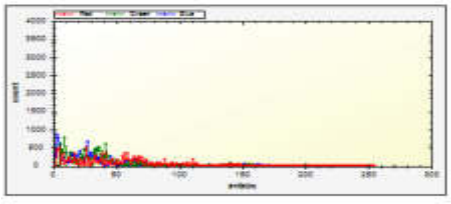
The results of sclera image preprocessing consist of four steps: Morphology dilate operation, convert image to binary, binary morphology octagonal structure, and remove noise as shown in subsection (i, ii, iii, and iv)

i. Results of the Morphology Dilation Operation

RGB sclera image converted into sclera dilation image based on filter size , the filter size has been determined by try and test that value is taken between (***3*3,5*5,7*7,9*9,11*11,13*13,15*15***), The best value is chosen for the filter size that fits to image which is [3*3], converting color image into grayscale image is adopted for two reasons, firstly is to speed up the operation, secondly is producing image more smoothing by the separated areas are connecting with distances smaller than the structural element size. Table (4.2) illustrated the results of morphology dilation operation on test image with different filter sizes.

Table (4.2): Results of Morphology Dilation Operation of a Sclera Image

Image .ID	**Filter Size [k*k]**	***Dilation Sclera image***	***Frequency***
#1	**[3*3]**		

#2	[5*5]		
#3	[7*7]		
#4	[9*9]		
#5	[11*11]		
#6	[13*13]		
#7	[15*15]		

ii. Results of Convert Sclera Image to Binary

Table (4.3) shows the results of converting the grayscale dilation sclera with a filter size [3*3] into the binary image based on a global threshold value (128) to simplify the separation of object (sclera or white area) and its background within an image, in this table used five sample images.

Table (4.3): Results of Converted Grayscale Sclera Image into Binary Image based on Threshold Value (128).

	#1	#2	#3	#4	#5
Grayscale image					
Binary Image					

iii. Results of Binary Morphology Octagonal Structure

Table (4.4) illustrates the results of a binary morphology octagonal structure operation on binary images that own in Table (4.3).

Table (4.4): Results of Binary Morphology Octagonal Structure Operation.

	#1	#2	#3	#4	#5
Binary Image					

Erosion Binary image					

iv. Results of Remove Noise from Binary Image

Table (4.5) shows the result of implemented a flood fill algorithm to remove noise from the binary images that are illustrated in Table (4.4) .

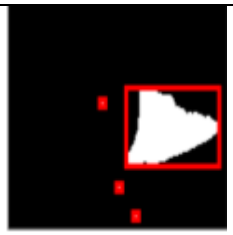
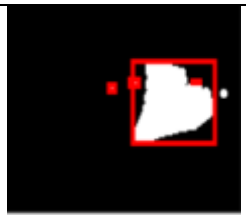
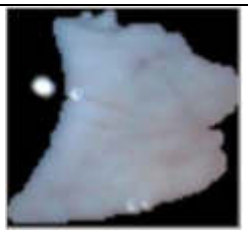
Table (4.5): Results of Remove Noise using Flood Fill Algorithm

	#1	**#2**	**#3**	**#4**	**#5**
Erosion Binary image					
Image without Noise					

4.3.3 Results of Find Object

Table (4.6) clarifies the results of finding a region of the interested ROI sclera images that represents the white area, where each image has number of object (ROI) and the results of this step represents find all objects (ROI) in an input image and inform of these objects, This information represents coordinates the object and object area value . As shown in Table (4.6),we have the best results when the size of object is large so ,the best value of find object when the number of objects = 8 , which is the largest area value = 5600.

Table (4.6): Results of finding objects

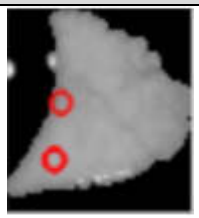
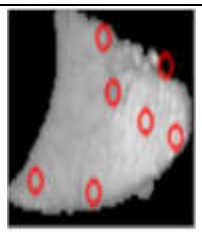
Image .ID	*Number of objects*	*ROI (white area)*	*Objects*	*Information of each objects*
#1	**4**			**No** | **X1** | **Y1** | **X2** | **Y2** | **Area** **1** 140 82 84 31 2856 **2** 98 33 97 32 1 **3** 86 50 80 45 30
#2	**5**			**1** 29 15 24 10 25 **2** 135 92 49 40 4472 **3** 153 49 148 44 25 **4** 119 51 115 50 4
#3	**6**			**1** 151 84 84 43 2747 **2** 69 53 65 49 16 **3** 81 97 77 93 16 **4** 93 112 89 108 16
#4	**7**			**1** 139 78 84 32 2530 **2** 109 32 107 32 0 **3** 88 46 82 42 24 **4** 129 44 124 43 5 **5** 123 44 123 44 0 **6** 72 49 68 45 16
#5	**8**			**1** 136 85 56 15 5600 **2** 87 29 73 16 182 **3** 79 24 72 18 42

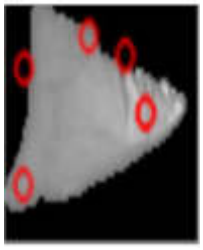
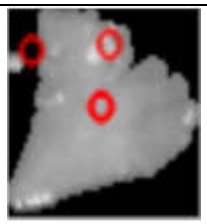
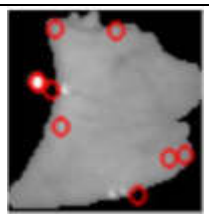
				4	108	20	98	20	0	
				5	72	44	64	37	56	
				6	142	73	138	69	16	
				7	59	78	57	76	4	

4.3.4 Results of Implementation Feature Extraction using SIFT Algorithm:

Table (4.7) shows results of feature extraction by using the SIFT algorithm, based on number of objects, this table depends on five samples of sclera biometric images. The images in this table are the results of the found object methods. The best results of SIFT algorithm when the increase size of object, for that the best results when the number of objects = 8.

Table (4.7): Results of Implementation of SIFT Algorithm.

Image .ID	*Number of objects*	*Octaves*	*Description of each Octaves*	*No.features*
#1	**4**		**No** / **X** / **Y** / **Size** / **Angle** / **Octave** **1** 16.19434 25.7035 4.843551 18.74561 4915712 **2** 14.20891 41.32967 10.84168 268.4457 13042177 **3** 14.20891 41.32967 10.84168 27.28824 13042177	**3**
#2	**5**		**`1** 74.158 14.23974 3.916359 112.8113 6226176 **2** 78.9186 32.63867 6.721629 235.8694 11928320 **3** 44.88605 6.944855 5.4487 113.7384 13435392 **4** 49.31932 21.0968 4.724291 56.42899 3080704 **5** 40.20074 46.82232 6.518385 266.2949 9700096 **6** 12.81202 43.81301 9.582843 39.09009 4129281 **7** 64.74069 28.54327 19.80455 112.1023 6488578	**7**

#3	6		`1	31.09151	6.120071	3.768978	109.4585	3473664	6
			2	44.70367	10.06152	4.849864	102.0301	4981248	
			3	7.050093	12.57722	4.575388	5.584595	786944	
			4	6.769567	36.10471	7.115308	265.1006	15991552	
			5	52.2459	21.59435	12.53903	246.2173	6882049	
			6	52.2459	21.59435	12.53903	110.5905	6882049	
#4	7		`1	6.784286	9.404441	4.231197	359.4238	11862272	5
			2	29.4122	7.985693	6.617125	134.5607	10748672	
			3	27.02433	22.22325	20.66721	232.5214	9568770	
			4	27.02433	22.22325	20.66721	139.5073	9568770	
			5	27.02433	22.22325	20.66721	13.41321	9568770	
#5	8		`1	44.28148	7.061563	3.924386	87.80426	6422784	8
			2	11.96867	25.40808	4.126865	287.7882	10027264	
			3	11.96867	25.40808	4.126865	88.07498	10027264	
			4	17.80005	28.31627	3.677315	4.304474	1704192	
			5	72.61665	51.43366	4.665385	175.5285	2228736	
			6	53.25276	65.81422	3.854784	247.9097	5112064	
			7	19.18774	6.464801	5.116055	352.3774	8847872	
			8	21.58114	41.34207	8.733161	17.75131	14156033	
			9	66.20298	52.59324	10.01035	238.0831	7275009	

4.4 Results of the Proposed Palm –Identification System

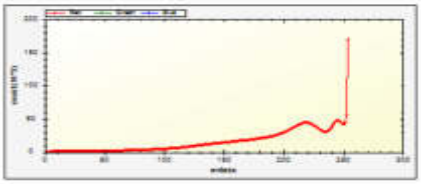
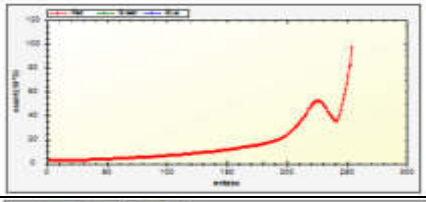
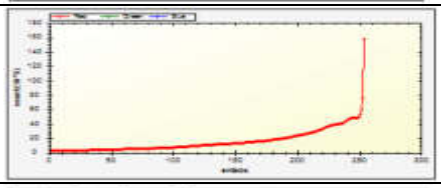
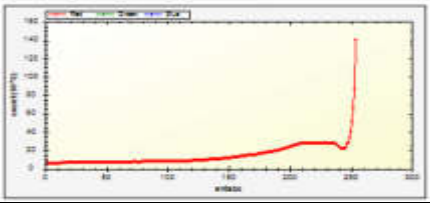
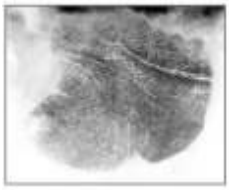
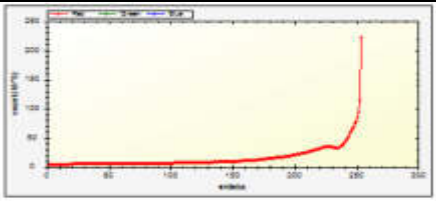
The results of the proposed system will show sequentially in "subsections: (4.3.1, 4.3.2, and 4.3.3)".

4.4.1 Load Image (Palm Image)

The following table, Table (4.8), obtains (Five) samples of the Palm images in RGB color space and (.bmp) image type selected from the THUBALMLAP database to be implemented in the palm identification system. The Tsinghua Palm print Database. Tsinghua University in Beijing China .This database contains 1,280 palm print images from 80 subjects (two palms per person and eight impressions per palm) captured using a commercial palm print scanner

of Hisign. All the palm print images are of 2040x2040 pixels and 500 ppi. shown in Table(4.8) [21].

Table (4.8): Original Palm Image Samples.

Image .ID	*Original Palm image*	*Frequency*
#1		
#2		
#3		
#4		
#5		

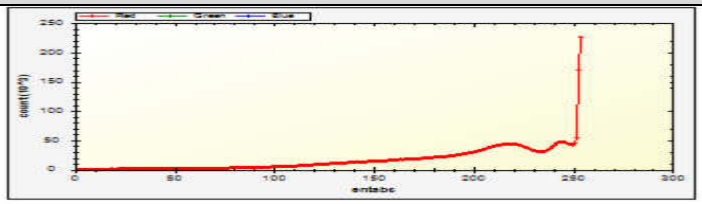
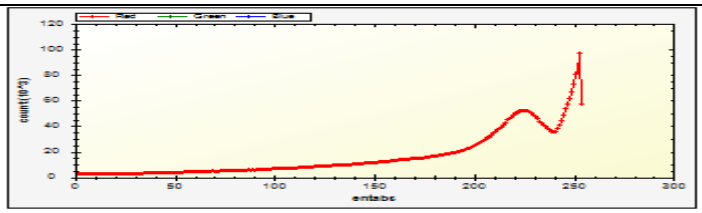
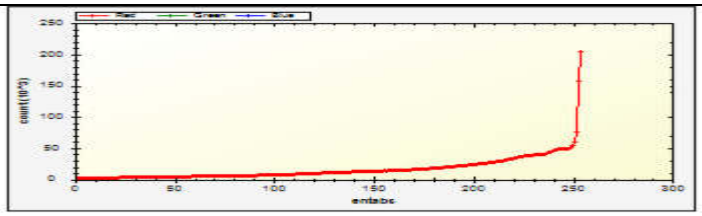
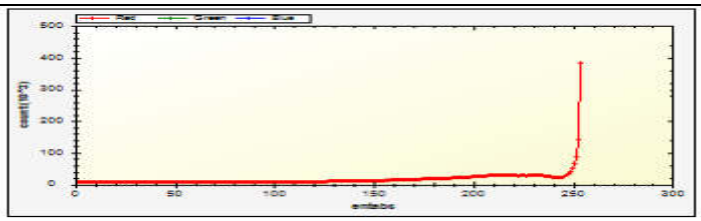
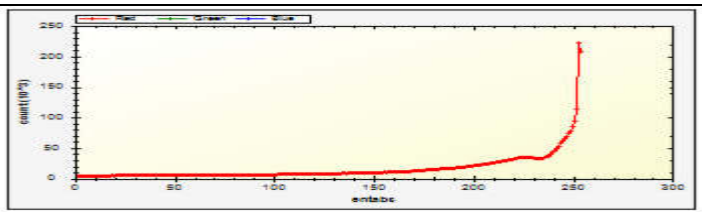
4.4.2 Palm Image Pre-Processing Stage

The Palm image preprocessing results are consisting of three steps: convert into Grayscale image, Median filter, and 2d maximum entropy threshold method as shown in subsection (i, ii, and iii)**.**

i. Results of the Convert Palm Image to Grayscale Image

Table (4.9) is shown the results of the implementation converted color palm image into a grayscale image on five sample palm images.

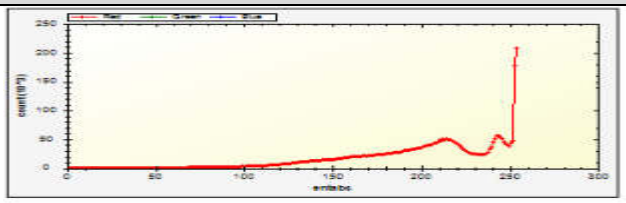
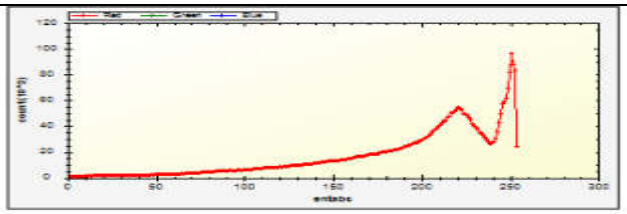
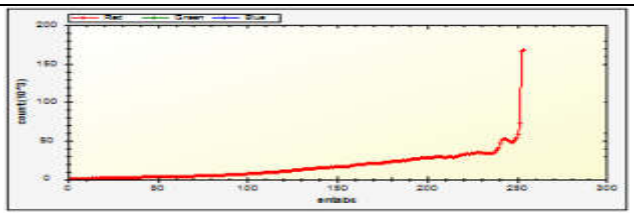
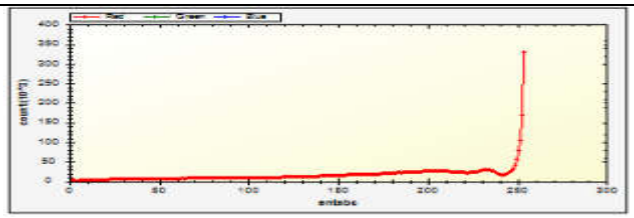
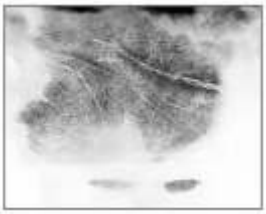
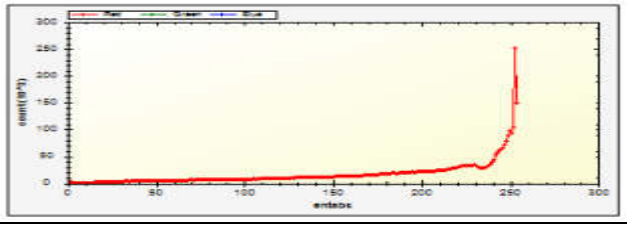
Table (4.9): Convert color palm into Grayscale Image.

Image .ID	*Grayscale Palm image*	*Frequency*
#1		
#2		
#3		
#4		
#5		

ii. Results of Implementation Median Filter

The results of applying the median filter on the grayscale palm image are clarified in Table (4.10).

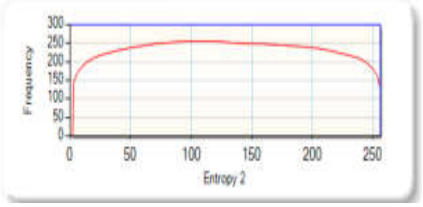
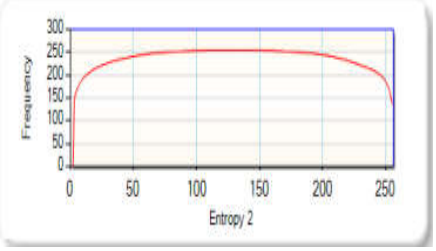
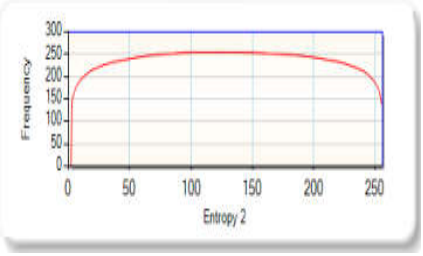
Table (4.10): Results of Implementations of Median Filter on Palm Grayscale Image.

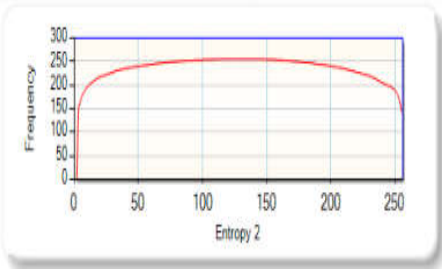
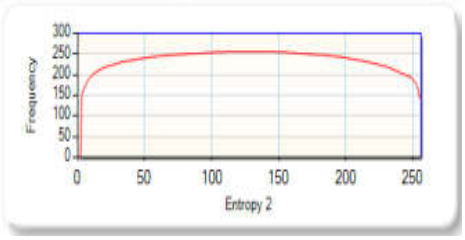
Image .ID	*Filtered Palm image*	*Frequency*
#1		
#2		
#3		
#4		
#5		

iii. Results of the Implementation of 2d Maximum Entropy Threshold Method

Table (4.11) illustrates the results of the implementation of an entropy algorithm on the filtered Palm images that are shown in Table (4.10), The entropy 2 algorithm is performed respectively to present an image with the highest entropy, so the resulted number of pixels will be minimized. In Table (4.11) , the histogram represents the number of energy pixels for each tonal value for each image which has changed a lot, also entropy execution time for each image.

Table (4.11): Results of Implementations of Entropy Filter on Palm Image.

Image Id.	Entropy Image	*Entropy Information*		*Histogram*
		Max Value	Location	
#1		9.15528261202978	108	
#2		9.32605423316691	128	
#3		9.27271844659328	121	

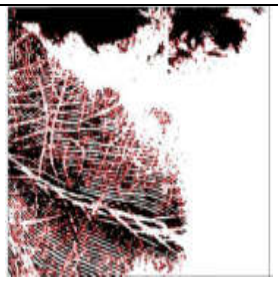
#4		9.31626838229224	130	
#5		9.24629428522355	133	

4.4.3 Results of Results of Implementation Feature Extraction using SIFT Algorithm:

The results of the performance of the SIFT algorithm are shown in Table (4.12), which is clarifying (the SIFT image and their description (x , y , size , angle, octave).

Table (4.12): Results of Implementation of the SIFT Algorithm (the SIFT image, and description).

Image ID	*Keypoints*	*Feature Description*						*No. Feature*
		No	*x*	*y*	*size*	*angle*	*octaves*	
#1		**0**	24.96943	4.629488	4.186714	97.85382	11075840	**1002**
		1	275.1685	7.045592	3.753722	183.3679	3211520	
		2	275.1685	7.045592	3.753722	73.20776	3211520	
		-----	-------	--------	------	--------	---------	
		1002	631.3099	115.1744	80.6683	132.4302	7799300	

#2		**0**	780.8946	5.110248	3.694515	31.93893	2031872	**1934**
		1	793.2253	8.459703	4.20813	231.7866	11469056	
		2	793.2253	8.459703	4.20813	105.9789	11469056	
		-----	-------	--------	------	--------	---------	
		1934	266.4464	270.3456	219.0846	112.4396	13239045	
#3		**0**	802.2112	5.397834	3.91212	165.726	6160640	**3901**
		1	596.2106	5.933159	4.172237	19.42505	10813696	
		2	851.9691	7.966488	4.134669	164.5971	10158336	
		-----	-------	--------	------	--------	---------	
		3901	788.0816	383.8926	158.7486	203.196	6619653	
#4		**0**	25.80912	14.04385	3.744941	1.886047	3014912	**5386**
		1	25.80912	14.04385	3.744941	178.9118	3014912	
		2	23.62295	20.50984	3.995263	111.816	7667968	
		-----	-------	--------	------	--------	---------	
		5386	487.3864	202.7255	164.2576	80.66333	9110021	
#5		**1**	19.54876	12.4029	4.424927	19.80304	15073536	**4344**
		2	632.9808	12.64426	3.807936	27.44049	4194560	
		3	861.8011	16.348	3.924419	325.8651	6422784	
		------	---------	-------	--------	------	--------	
		4344	543.6271	732.5382	205.941	322.5333	8782597	

4.5 Results of Implementation of Proposed Document Signature using Hybrid Identification System

The results of the performance of the proposed hybrid identification system consists of four main stages: (Pre-processing, Enhanced shark

smell optimization (ESSO) algorithm with a chaotic map, and a generate stream key as well as Documents signature by using the MD5 algorithm). The results of each stage are illustrated in sub sections (4.5.1, 4.5 .2, 4.5.3, and 4.5.4)

4.5.1 Results of Implementation of pre-processing

This step is combination results of two proposed identification systems to get feature from each system as illustrated in section (4.3 results of Sclera identification system) section (4.4 results of Palm identification system).

4.5.2 Results of Implementation of the Enhanced Shark Smell Optimization (ESSO) Algorithm based on chaotic map.

Figure (4.1) shows an example of 3d logistic behaviors, where initial parameters of 3d logistic map are r=0.7 and x_i=0.4.

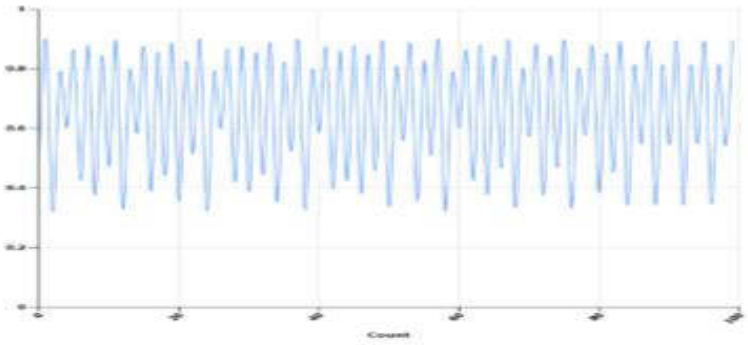


Figure (4.1): Results of the 3D Logistic Function.

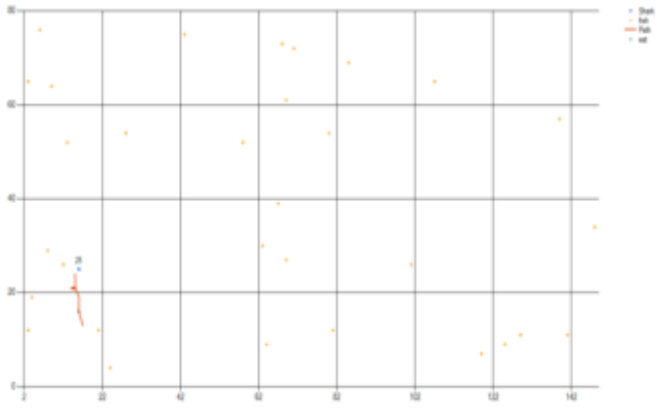
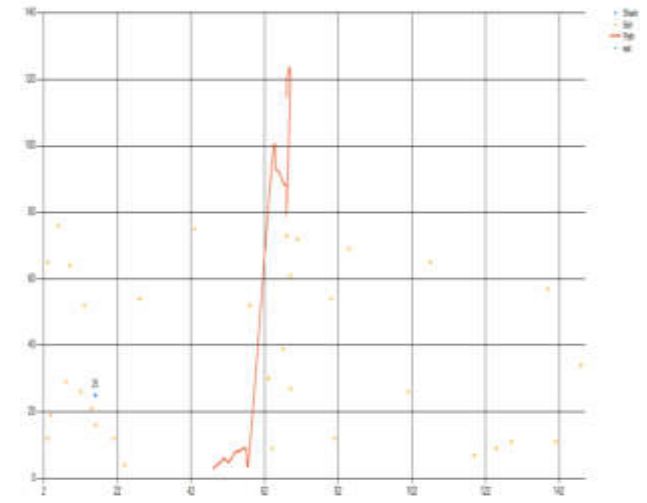
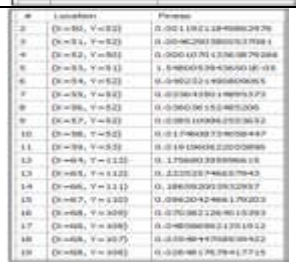
Figure (4.2) shows an example of the dropping coordinates of features extracted from both proposed sclera and palm–identification systems on image, in this figure used feature coordinates of (#1) as shown in Table (4.7) as shark positions and feature coordinates of (#1)

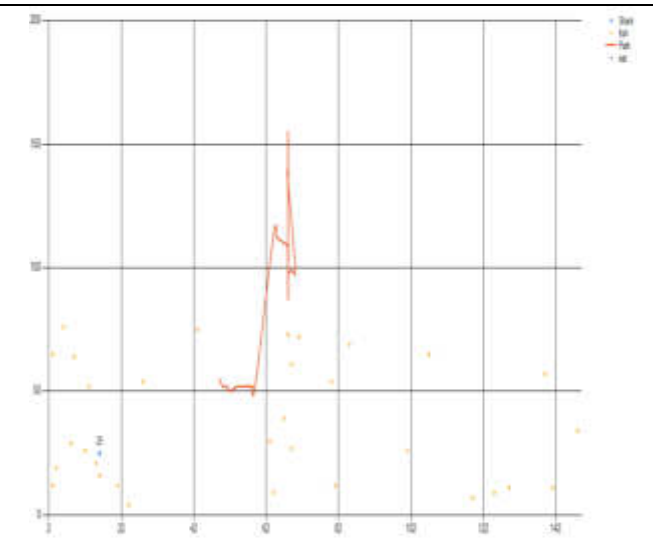
as shown in Table (4.12) as fish positions. The image used in this figure is 'Lena .jpg ' image in RGB color form.

Figure (4.2): An Example of dropping coordinate of ESSO

Table (4.13) shows fitness function of the ESSO algorithm for each location in Lena image as present in Figure (4.1) and the behavior of the ESSO algorithm based on the number of iteration (Kmax) , Table (4.14) illustrates the simulation of randomly behavior of the ESSO, where parameters of the ESSO algorithm are NP (number of population size)= 24336, ND (number of decision variables) = 50, βk(the velocity limiter) = 1, Δk (time interval) = 3, k = 1, 0, -1, and R1, R2, R3 represents the random parameters. In table (4.14) , if the number of iteration is increases, the chance of ESSO Algorithm to finding better solutions .

Table (4.13): Fitness function of all points and ESSO algorithm behavior based on No. iteration.

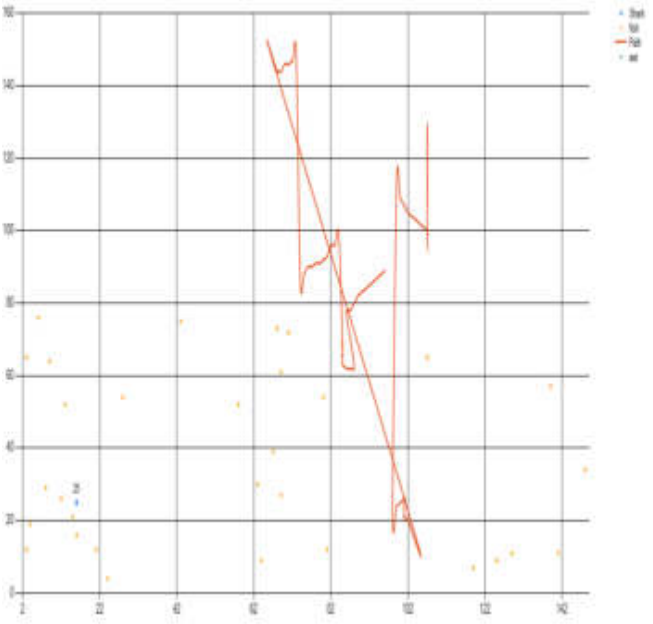
<table>
<tr><th>No of iteration</th><th>Fitness Function</th><th>ESSO behavior</th></tr>
<tr><td>10</td><td>
<table>
<tr><th>#</th><th>Location</th><th>Finess</th></tr>
<tr><td>0</td><td>{X=16, Y=25}</td><td></td></tr>
<tr><td>1</td><td>{X=15, Y=24}</td><td>0.118114608728395</td></tr>
<tr><td>2</td><td>{X=15, Y=21}</td><td>0.122561829086325</td></tr>
<tr><td>3</td><td>{X=14, Y=21}</td><td>0.127091232218746</td></tr>
<tr><td>4</td><td>{X=15, Y=21}</td><td>0.127091232218746</td></tr>
<tr><td>5</td><td>{X=16, Y=19}</td><td>0.131702818125657</td></tr>
<tr><td>6</td><td>{X=16, Y=18}</td><td>0.122561829086325</td></tr>
<tr><td>7</td><td>{X=16, Y=17}</td><td>0.122561829086325</td></tr>
<tr><td>8</td><td>{X=16, Y=16}</td><td>0.118114608728395</td></tr>
<tr><td>9</td><td>{X=17, Y=13}</td><td>0.0781624577460666</td></tr>
</table>
</td><td>  </td></tr>
<tr><td>30</td><td>
<table>
<tr><th>#</th><th>Location</th><th>Finess</th></tr>
<tr><td>0</td><td>{X=16, Y=25}</td><td></td></tr>
<tr><td>1</td><td>{X=48, Y=3}</td><td>0.0291047478216714</td></tr>
<tr><td>2</td><td>{X=49, Y=4}</td><td>0.036036152485206</td></tr>
<tr><td>3</td><td>{X=50, Y=5}</td><td>0.0410680028000148</td></tr>
<tr><td>4</td><td>{X=51, Y=6}</td><td>0.0410680028000148</td></tr>
<tr><td>5</td><td>{X=52, Y=5}</td><td>0.0313330332683591</td></tr>
<tr><td>6</td><td>{X=53, Y=6}</td><td>0.0385109862553652</td></tr>
<tr><td>7</td><td>{X=54, Y=8}</td><td>0.036036152485206</td></tr>
<tr><td>8</td><td>{X=55, Y=8}</td><td>0.0313330332683591</td></tr>
<tr><td>9</td><td>{X=56, Y=9}</td><td>0.0336435014895373</td></tr>
<tr><td>10</td><td>{X=57, Y=9}</td><td>0.0385109862553652</td></tr>
<tr><td>11</td><td>{X=58, Y=10}</td><td>0.0410680028000148</td></tr>
<tr><td>12</td><td>{X=64, Y=95}</td><td>0.439213964538588</td></tr>
<tr><td>13</td><td>{X=65, Y=93}</td><td>0.350723789527762</td></tr>
<tr><td>14</td><td>{X=66, Y=92}</td><td>0.272177730230282</td></tr>
<tr><td>15</td><td>{X=67, Y=89}</td><td>0.112767764923214</td></tr>
<tr><td>16</td><td>{X=68, Y=88}</td><td>0.0884155841122163</td></tr>
<tr><td>17</td><td>{X=68, Y=86}</td><td>0.0154431964982294</td></tr>
</table>
</td><td>  </td></tr>
<tr><td>60</td><td>


<table>
<tr><td>57</td><td>{X=43, Y=68}</td><td>0.000107013363879266</td></tr>
<tr><td>58</td><td>{X=43, Y=69}</td><td>0.00179742153091435</td></tr>
<tr><td>59</td><td>{X=43, Y=70}</td><td>0.00238205148779276</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>
</td><td>  </td></tr>
</table>

80

#	Location	Finess
0	{X=16, Y=25}	
1	{X=96, Y=89}	0.122561829086325
2	{X=95, Y=88}	0.150970989498207
3	{X=94, Y=87}	0.105266044301546
4	{X=93, Y=86}	0.0817878503590923
5	{X=92, Y=85}	0.0581359403322123
6	{X=91, Y=84}	0.036036152485206
7	{X=90, Y=83}	0.0313330332683591

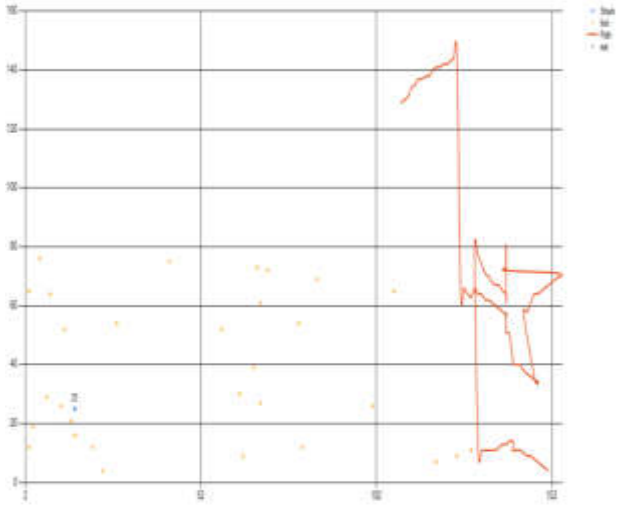
77	{X=107, Y=111}	0.0809556527044741
78	{X=107, Y=108}	0.117114101435764
79	{X=107, Y=107}	0.159929354900781



100

#	Location	Finess
0	{X=16, Y=25}	
1	{X=151, Y=4}	0.0269586451494741
2	{X=150, Y=5}	0.021013433779825
3	{X=149, Y=6}	0.0385109862553652
4	{X=148, Y=7}	0.036036152485206
5	{X=147, Y=8}	0.0313330332683591

96	{X=112, Y=134}	0.605465773243771
97	{X=111, Y=131}	0.397758416098128
98	{X=110, Y=130}	0.366073267286589
99	{X=109, Y=129}	0.144917958775361



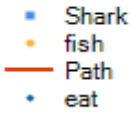
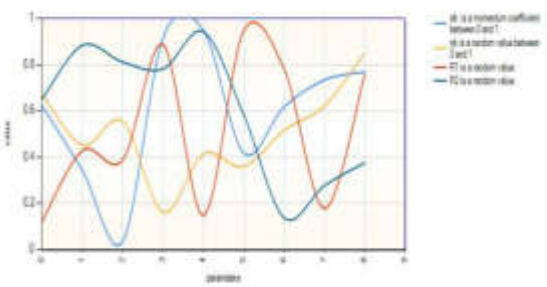
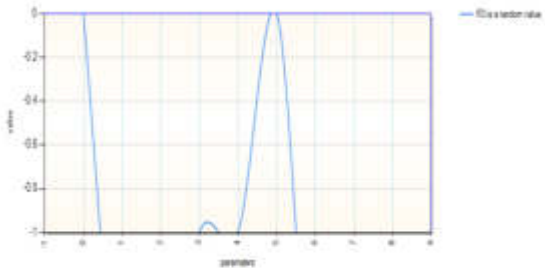
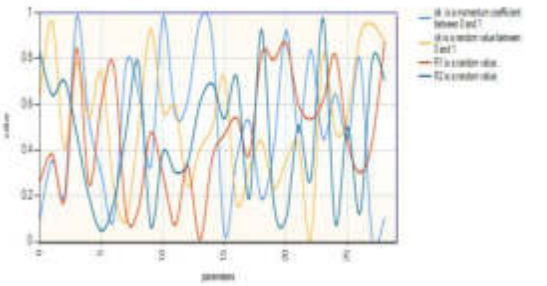
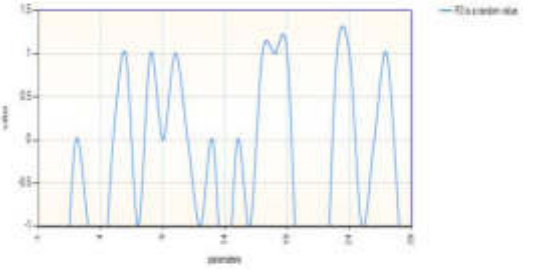
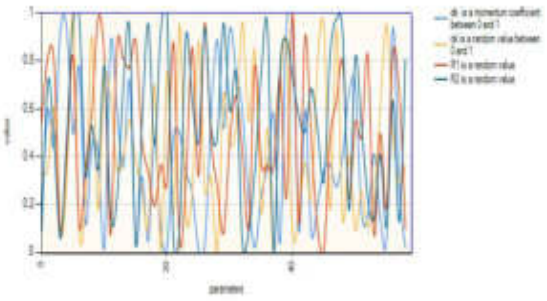
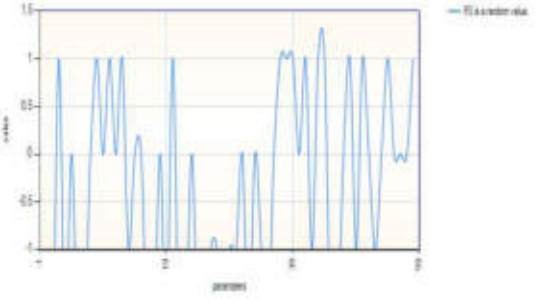
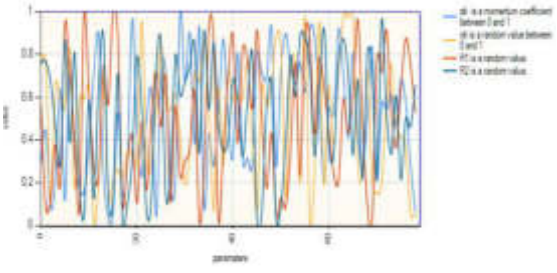
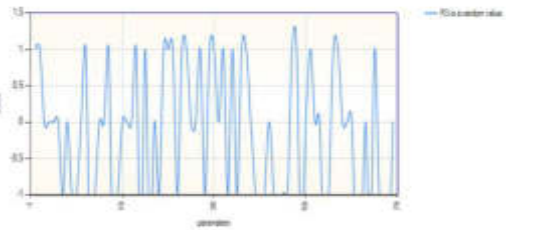
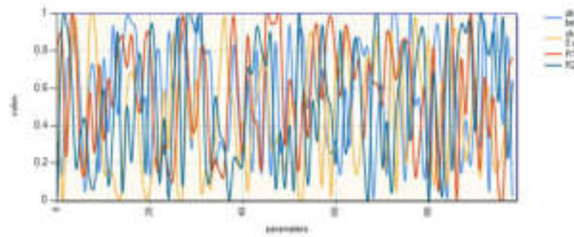
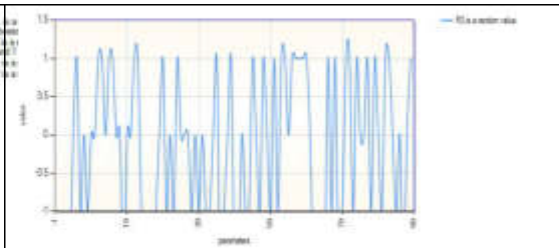


Table (4.14): ESSO algorithm Random behavior based random parameter

No. Iteration	Behavior of ESS0 based on Randomly Parameter	
	αk is momentum coefficient [0-1], ηk random value [0-1], R1,R2 random value	**R3 Random value**
10		
30		
60		
80		

100		

As illustrated in Table (4.13 and 4.14)" the behavior of the ESSO algorithm changes according to the number of iterations.

4.5.3 Results of the Key Stream Generating

Table (4.15) shows an example of the results of a generating key with two cases of the ESSO iteration (10,30).The length of secret key depending on number of iteration of ESSO algorithm.

Table (4.15): Key Stream Generating

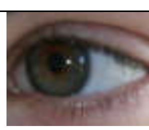
No. Iteration	No. Key	Key stream
10	K_1	11111100000111101111100011110011000010010001111011111000111100110000100100100100001100111100011111011110001001000011 00111100011111011110000011111111111010100111101111110110000000110110010001111011111101100000000110110010010011011000 00011011111101111000100110110000000011011111101111001010111111101010100111110000000010001001000011010000111111000000001 00010010000110100001011000010010001000000001111110000101100001001000100000000111110010101011111111010100111110000000100 01001000011010001000110000111000100000000000000000000000000001000111000011000100010110000100100010000000111110010101 11111000010100001111100000001101101110100011011001111100000001101101110100011011110110001011101101100000001111100110110 00101110110110000000111110000101000011000010011001111100000001101101110100011011001111100000001101101110100011011110110 00101110110110000000111110011011000101110110110000000111110011001000011000010011001111011111101100000000110110010001111 01111110110000000110110010010011011000000001101111110111100010011011000000001101111110111100110010000110000100010011111 011111101100000000110110010001111011111101100000000110110010010011011000000001101111110111100010011011000000001101111110 11110010001000011000010000000111101111100011110011000010010001111011111000111100110000100100100100001100111100011111110 11111000100100001100111100011111011110000000100001

30	K_2	1001011010011110011011100110110000110000000111100110111001101100001100000000001100001101100111011001111000000110000 1101100111011001111001011010011001111010011101011011011101010001010111100111010110110111010100010101111111010100010 1011101101101011100111101010001010111011011010111001011110011010011000011110100000111100111101110011000111101000011 11001111011100110011001110111100111100000101111000110011101111001111000001011110000110010110101110000111100100110011 11101011101101000111100100110011110101110110100101101110101111001100100111100010110111010111100110010011110000111 01011010011010011110011101010010111011100011100111100111010100101110111000111111000111011101001010111001111001110001 11011101001010111001111001011001011001111100011101001001111001111010100001000111010010011110011110101000010010000101 01111001111001001011100010000101011110011110010010111000111110011001011010011110100001001110011011100010100111101000 01001110011011100010110100011101100111001000010111100101000111011001110010000101111001011010011000111100011110110101 11100011000001110100011110110101111000110000011101001011100000110001111010110111100010111000001100011110101101111000 11110001100001101001111011110100011110101100010011001000110101111000101111011110010011110111101000111101011000100100111100100 1000110101111000101111011110010110000110000111000111101111100011110011000010010001111011111000111100110000100100 1001 00001100111100011111011110001001000011001111000111110111100011100001100001101001111011110100011110101100010011110 11110100011110101100010011001000110101111000101111011110010010001101011110001011110111100101100001100111100111001111 101110000011111111011001110011110111000001111111101111011111111000001110111110011100110111111110000011101111100 1110 011110011010010000111100100110011110101110110100011110010011001111010111011010010110111010111100110010011110000101 10111010111110011001001111000010010110101101001111000110001110010111011000110011110001100011100101110110001111000110 11101001110001100011110011000110111010011100011000111100101101011011010000111011100100010011111111111101001110111001 0001001111111111110110111111111111001000100111011100101111111111110010001001110111000010110110111100001110101 0011100 0100000011011100001110101001110001000000110111000011101100000001000111001010111000011101100000001000111001010111000011 11011100010000111000101001011001100001000101001110001010010110011000010001011010001000011001101001010001110010100010 00011001101001010001110000100011101111100011100101110101010101111010100100111001011101010101011110101001100101011110 10101010111010011100100101011110101010101110100111000111110110110111001110111100111010010011010010100011101111001110 10010011010010100101001011001001011100111101110001010010110010010111001111011100111011011010110000011110010101000101 10001111100000001111001010100010110001111110000000001111100011010001010100111100000001111100011010001010100111100000 1101 01101001000001111001011100000011010010111110011110010111000000110100101111111111010010110000001110100111100111110100 10110000001110100111100000100101100111000001110100100111100111101010000100011101001001111001111010100001001000010101 11100111100100101110001000010101111001111001001011100000111001100111000110011101110010001001111111111110100111011100 100010011111111111011011111111111100100010011101110010111111111111001000100111011100110001110011001010001100 1111001 1001011111100000000011000111100110010111111000000000011001100000000001111110100110011110001100000000011111101001100111 1001100010100110001100010001111011010011110000000001100011001111011010011110000000001100011110001100000000111100101101 11100110001100000000111100101101111000100011000110000100001001111011111101100000001101100100011110111111011000000011 01100100100110110000000110111111011110001001101100000001101111110111100100001000011111111100011110111010111100101011 011100100111101110101111001010110111001100111011010100111101011101111001001110110101001111010111011110001111111111 0 1101100111101111110110000000110110010001111011111101100000001101100100100110110000000110111111011110001001101 1000000 0110111111011110011011011111011101100111110000000010001001000011010000111110000000010001001000011010000101100001001000 10000000111110000101100001001000100000001111100110111011

4.5.4 Results of Document Signature Using MD5 Algorithm

Table (4. 16) results of the MD5 for five users with the number of iteration =10. The proposal system can be generated different document signature for each user based on user stream key.

Table (4.16): Results of MD5 Algorithm of 5 users

# User	Sclera biometric	Palm biometric	User key	User MD5
#1			0011111000111100101001001001010011110001111100100 1111000100101001111000111110010011110000011111111 1110111001111001001111100011110010100100011110010 0111110001111001010010010010100111100011111001001 1110001001010011110001111100100111100111011111111 1101100011110100001011000010010111010100111101000 0101100001001011101011010111010010000110100001011 110010101110100100001101000010111100011011111111 1010100111101011111001001111000101100001111010111 110010011110001011000011010001111001001111010111 100001101000111100100111101011110010101111110000 1001100111100100111110001111001010010001111001001 1111000111100101001001001010011110001111100100111 1000100101001111000111110010011110011001000011000 0100000011110011001110000011110101010100111100110 0111000001111010101011010101011110000011100110011 1100101010101111000001110011001111000000100001111 11000000111101111101111100000001011000000111101111 10111110000000101100000011010000000111101111011 1100000110100000001111011110111100000011111000 01000000111101111101111100000001011000010001100000 11100010000000000000000000000000000010001110000110 00100001101000000011110111101111000000100001	4A3C0DA2 50D3614C6 30DE51352 BF98EF
#2			0011101111001111101001111000011000111011110011110 0110011001101111100111101110101101100100111000100 0011110111010110110010011100010000100011100100110 110101110111100001000111001001101101011101110011 11101100110011101101001111011111010000010000110000 0100011110111101000001000011000001001000001100001 0000010111101111000100000110000100000101111011110 0101101110011001111110000111101111010000010000110 0000100011110111101000001000011000001001000001100 0010000010111101111000100000110000100000101111011 110000111110011010000101100111101110001100001111 0010111110011110111000110000111100101111111111010 01111000011000011101111001111101001111000011000111 0111100110100001011010001101000111101101101100001 1111010100110011110110110110000111110101001111001 0101111100001101101101111001100101011111000011011 0110111100010110001011010010100100111101110011100 1011110100001100011110111001110010111101000011001 1000010111101001110011101111000110000101111010011 100111011100100101001011010011100000111101101011 1001100000011011110011110110101110011000000110111 1111101100000011001110101101111001111011000000110 01101011011110000011100101	3D280663A 86FB2D406 EFC1756EB CD340
#3			111101100111011010111100000100110011001001110110101111000001001100 110011001100110010000011110101101110010011001100100000111101011011 1001101111111011010011101100101111110100110010101100111011001011111 11010011001010111101010011001011111010011011100110101001100101111 11010011011100101101111100110001110111000100011010001011010100011 101110001000110100010110101001010110100010110001000111011100010101 101000101100010001110111000110011111011101001110110101111000001001 100110010011101101011110000010011001100110011001100100000111101011 011100100110011001000001111010110111001011101111010101001110111010 0101010011110110110001110111010010101001111011011100111011011100 10101001011101110001110110111001010100101110111001010101111001110 011101110100101010011110110111000111011101001010100111101101110011 1011011100101010010111011100011101101110010101001011101110011100 111100011001110110101111000001001100110010011101101011110000010011 001100110011001100100000111101011011100100110011001000001111010110 111001100011101111010011101101011110000010011001100100111011010111 100000100110011001100110011001000001111010110111001001100110010000 011110101101110010111101101101100011101110100101010011110110111000 11101110100101010011110110111001110110111001010100101110111000111 01101110010101001011101110001101101	4E5E318DE D6E946F7F EC57F6B48 D2247

#4			111100000111101001100000101000111011010001111010011000001010 001110110100101101110001010000011001011110001011011100010100 000110010111100000111110001000001111010100011011001000100011 100011110101000110110010001000111001110001000100110110001010 111100011100010001001101100010101111000001000110011001001111 010101111010010111111101000011110101011110100101111111010000 101111111010010111101010111100001011111110100101111010101111 001001100110101010001111010100011011001000100011100011110101 000110110010001000111001110001000100110110001010111100011100 100010011011000101011110001010101101110100011110101000110110 010001000111000111101010001101100100010001110011100010001001 101100010101111000111000100010011011000101011110001011101110 010110011110100100101100101111100010000111101001001011001011 111000100001000111110100110100100101111000010001111101001101 001001011110011010011110111000011110100000111011011101000110 100111101000001110110111010001101101100010111011011100000101 111001011000101110110111000001011110000111011111011100011110 010011001101011010000001100111100100110011010110100000011110 000001011010110011001001111001100000010110101100110010011110 001110111111111110011110001111100100000010110100100111100011 110010000001011010011001011010000001001111100011110010010110 1000000100111110001111001111111	C2D00CC5 748EAC115 1577DB8FE 883D88
#5			10100000111000000000000000111000000101001011101111000000000 011100000101001011101111000000110110110111010100011110110 010100100011100010110000111101100101001000111000101100000 110100011100010010100110111100001101000111000100101001101 10 11110001010111011011111001001111100100100001101011000010 11001111100100100001101011000010111101000011010110000100 10011111001101000011010110000100100111110010011111011100 0010100011111010101010011110001000011000111110101010101001 1110001000011001100001000111001010101011111000110000100 011110010101010111110001010000111100011011001111101000000 110101101001001111001111101000000110101101001001111111100 1001011010110000001011111001111001001011010110000001011111 00110110001111001011010011111001001000011010110000101100 11111001001000011010110000101111010000110101100001001001 1111001101000011010110000100100111100101101001111001111 10001111101010111001000111100010100011111010101110010001 1110001010010100011110001001110101011111000101000111000 10011101010111110001111100111101001110001110000011000110 0010011111110100111000001100011000100111111101101111110 010001100011000001110010111111110010001100011000001110001 11001011110100100000011100000110001100010011111110100111 00000110001100010011111110110111111100100011000110000011 10010111111100100011000110000011100000001001011	A774D45D E5F2B4564 708A721DC 4A5C22

4.6 Random Number Generation Tests

Table (4.17) clarifies the test of the random number generation by enhancement shark smell optimization (ESSO). To apply the NIST test, firstly dropping features of (sclera and palm) of the (three) users on Lena and Baboon image samples and then measures the randomness of these images.

Table (4.17): Results of NIST test.

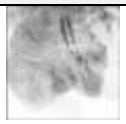
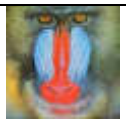
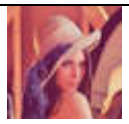
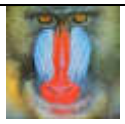
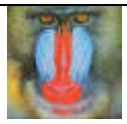
User		1		2		3	
Biometry							
Secret image							
NIST		P-value					
1	APPROXIMATE ENTROPY	1.00000	1.00000	1.00000	1.00000	1.00000	1.00000
2	BLOCK FREQUENCY	0.85968	0.50000	1.00000	0.21592	0.11161	0.21595
3	CUMULATIVE SUMS	0.59251	0.91915	0.31570	0.72994	0.98664	0.86350
4	FFT TEST	0.63817	0.15132	0.15132	0.32872	0.05521	0.34080
5	FREQUENCY	0.71015	0.15787	0.50351	0.15787	0.41357	0.60285
6	LEMPEL-ZIV	1.00000	1.00000	1.00000	1.00000	1.00000	1.00000
7	RUNS TEST	0.60975	0.59852	0.02096	0.33368	0.14564	0.08657
8	SERIAL TEST	0.49896	0.15862	0.92175	0.97786	0.92175	0.15862

Figure (4.3) shows results of NIST test for (3) users and Lena and baboon image samples. In figure (4.3) shown the proposed generation secret key algorithm able to create unique , unpredictable ,strong ,and randomly key for each user .

Figure (4.3): Results of NIST test.

CHAPTER FIVE

CONCLUSIONS AND FUTURE WORK

Chapter Five

Conclusions and Suggestions for Future Work

5.1 Introduction

This chapter finishes this thesis with some conclusions about the implementation and results of the proposed document signature using hybrid identification techniques. These conclusions are presented in section (5.2). While section (5.3) clarifies the suggestions for future work.

5.2 Conclusions

Some conclusions can be inferred from the results and tests of this work as follows:

1- The proposed sclera identification system is using to obtain feature from sclera image, this proposed system is including uploading a sclera biometric image. Preprocessing sclera image prepares it to more analysis, including dilation morphology operation to convert RGB image into grayscale, convert image to binary using thresholding value (128), binary morphology octagonal structure to enhancement edge of sclera image , and finally remove noise from an image by using flood fill algorithm. The SIFT algorithm is using to extract the feature key point.

2- The sclera image results after apply a different filter size of dilation morphology operation as shown in Table (4.2), the best value of filter size is 3*3 because its faster and more smoothing.

3- The proposed Palm identification system is using to obtain feature from palm image, including uploading a palm biometric image. Preprocessing of a palm image to prepare it for more analysis, including convert image into grayscale, using the median filter to remove noise from the image, finally using two dimensions of entropy to extract some important features from the palm image. SIFT algorithm is using to extract a set of key points.

4- Proposing enhancement shark smell optimization (ESSO) based on 3d logistic function: The key points of the sclera and palm biometric image that is extracted by using a proposed sclera and palm identification systems, a proposing ESSO algorithm to find the best coordinate position feature is used to find stronger features overall features of both biometric systems. As shown in Table (4.13) for calculate fitness function of all points and Table (4.14) as shown the effect of 3d logistic function on behaver of proposed ESSO to it more randomness and faster.

5- Generating stream secret key: The fitness function value, the objective function value, and the coordinates[x,y] for all points of optimal solution that finding by using the proposed ESSO algorithm are using to generating a variable size key which is called a stream cipher key. The length of the secret key is depending on the number of iterations of the proposed ESSO algorithm as illustrated in Tables (4.15).

6- Document signature: The final stage in the proposed system is the document signature by using the MD5 as shown in Table (4.16), the

proposed system has the ability to generate a unique digital signature for each user.

7- Results of NIST testing of generation random number are provided the proposed system enable to generate a unique, unpredictable, random, strong, and various length of the stream key.

5.3 Suggestions for Future Work

During this work, several subjects are identified that will yield large support to the field of a secure document signature based on multi-biometric systems. Among these, the following can be suggested:

1- Using optimization algorithms like Camel herds Algorithm(CHA).
2- The digital signature of the document by using the human brain.
3- Use SHA- 256 algorithm in generating a digital signature.
4- Using SURF algorithms to generate more features, Because it is many times faster than SIFT and more powerful against different image transformations, SURF also uses almost correct approximation and finally is used to reconstruct 3D scenes.
5- Can be found Entropy for finger vein recognition to extract the digital signature.
6- Two or more sharks can be used to get a faster and more perfect solution.

REFERENCES

References

[1] Christina Katsini, Marios Belk, Christos Fidas, Nikolaos Avouris, George Samaras.(2016). Security and Usability in Knowledge-based User Authentication: A Review. PCI '16: Proceedings of the 20th Pan-Hellenic Conference on Informatics.November 2016 Article No.: 63 Pages 1–6.

[2] Mir A.H, Rubab, S and Jhat, Z. A.(2018). Biometrics Verification: a Literature Survey. Journal of Computing and ICT Research, Vol. 5, Issue 2, pp 67-80. http://www.ijcir.org/volume5-number2 /article7.pdf

[3] Maghsoudi, J., & Tappert, C. C. (2016). A Behavioral Biometrics User Authentication Study Using Motion Data from Android Smartphones. 2016 European Intelligence and Security Informatics Conference (EISIC). http://doi:10.1109/eisic.2016.047

[4] Swati K. Choudhary , Ameya K. Naik.(2019) . Multimodal Biometric Authentication with Secured Templates — A Review.IEEE. International Conference on Trends in Electronics and Informatics (ICOEI). ISBN: 978-1-5386-9439-8.http:\\ DOI: 10.1109/ICOEI .2019. 8862563

[5] Nemanja Maček, Borislav Dorđevic, Jelena Gavrilovic, Komlen Lalovic.(2015). An Approach to Robust Biometric Key Generation System Design.Acta Polytechnica Hungarica . Vol. 12, No. 8, 2015

[6] G.Radha, C.Saranya, B.Suganyadevi.(2015). A New Multimodel Approach for Human Authentication: Sclera Vein and Finger Vein Recognition. IJRET: International Journal of Research in Engineering and Technology. Volume: 04 Issue: 03 | Mar-2015. http://www.ijret.org

[7] Tamilselvan, K., Krishnaraj, R., Sukumar, P., & Jayakumar, T.(2016). Security Method for Human Finger and Palm Images

Identification. International Journal of Emerging Technologies in Engineering Research (IJETER) Volume, 4, 77-80.

[8] Sarkar, A., Singh, B. K., & Bhaumik, U. (2017). RSA Key Generation from Cancelable Fingerprint Biometrics.IEEE, International Conference on Computing, Communication, Control and Automation (ICCUBEA) .Pp: 1-6.

[9] Madhivhanan, M., & Ravi, R. (2018). Fingerprint-Sclera based Multimodal Biometric Authentication System using Hybrid Genetic Intelligent Technique for System on Chip Application. Taga Journal, 14.

[10] Roh, J., Cho, S., & Jin, S.-H. (2018). Learning based biometric key generation method using CNN and RNN. 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE). http:// doi:10.1109/iciteed.2018.8534873

[11] Jaswal, G., Kaul, A., & Nath, R. (2019). Multimodal biometric authentication system using hand shape, palm print, and hand geometry. In Computational Intelligence: Theories, Applications and Future Directions-Volume II (pp. 557-570). Springer, Singapore.

[12] Yogita S. Pagar and G. V. Chowdhary.(2019). Strengthening Elliptic Curve Cryptography—Key Generation via Biometric Fusion Approach. Springer,Computing in Engineering and Technology, Advances in Intelligent Systems and Computing. volume 1025.pp 87-101.

[13] Solé-Casals, J., Vancea, M., & March Amengual, J. M. (2014). A Preliminary Review of Behavioural Biometrics for Health Monitoring in the Elderly.

[14] Faundez-Zanuy, M. (2009). Biometric security technology. In Encyclopedia of Artificial Intelligence (pp. 262-269). IGI Global.

[15] Mir, A. H., Rubab, S., & Jhat, Z. A. (2011). Biometrics verification: a literature survey. International Journal of Computing and ICT Research, 5(2), 67-80.

[16] Alkassar, S., Woo, W. L., Dlay, S. S., & Chambers, J. A. (2015). Robust sclera recognition system with novel sclera segmentation and validation techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 47(3), 474-486.

[17] Dong, W., Zhou, H., & Xu, D. (2018). A New Sclera Segmentation and Vessels Extraction Method for Sclera Recognition. 2018 10th International Conference on Communication Software and Networks (ICCSN).

[18] Alkassar, S., Woo, W. L., Dlay, S., & Chambers, J. (2016). Sclera recognition: on the quality measure and segmentation of degraded images captured under relaxed imaging conditions. IET Biometrics, 6(4), 266-275.

[19] Radu, P., Ferryman, J., & Wild, P. (2015, September). A robust sclera segmentation algorithm. In 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS) (pp. 1-6). IEEE.

[20] M. G. Kresimir Delac, "A survey of biometric recognition methods," in 46th International Symposium Electronics in Marine, Zadar, Croatia, 2004.

[21] https://www.kaggle.com/techmn/palm-dataset.

[22] Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: security and privacy concerns. IEEE Security & Privacy Magazine, 1(2), 33–42..

[23] Shilpa Shrivastava "Biometric: Types and its Applications" International Journal of Science and Research (IJSR), ISSN: 2319-7064, Index Copernicus Value: 6.14, (2013).

[24] Schuckers, 2001] Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001. (journal style)

[25] S. Kaur, P. Garg and S. sharma, "Image Enhancement Techniques Based On Histogram Equalization," International Journal of Engineering Sciences & Management Research, pp. 23-29, 2017

[26] Zahraa Naji Razoqi , Palm Vein Recognition Using Centerline Extraction, electronic thesis ,Computer Sciences, University of Technology,2017.

[27] D. John, "Three Algorithms for Converting Color to Grayscale" , Available at : www. .johndcook.com 2009.

[28] Shetter, A., Prajwalasimha, S., & Swapna, H. (2018). Finger Print Image Enhancement Using Thresholding and Binarization Techniques. 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) .doi:10.1109/ icicct.2018.8473286

[29] George, G., Oommen, R. M., Shelly, S., Philipose, S. S., & Varghese, A. M. (2018). A Survey on Various Median Filtering Techniques For Removal of Impulse Noise From Digital Image. 2018 Conference on Emerging Devices and Smart Systems (ICEDSS)

[30] Vuckovic, V., & Arizanovic, B. (2017). Heuristic-modified region filling algorithms for A-B connection searching problem. 2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS) . doi:10.1109/ telsks. 2017 .8246309

[31] Yixuan He, Tianyi Hu, Delu Zeng.(2019). Scan-flood Fill(SCAFF): an Efficient Automatic Precise Region Filling Algorithm for Complicated Regions.computer vision fundamental .

[32] AlAzawee, W. S., Abdel-Qader, I., & Abdel-Qader, J. (2015). Using morphological operations — Erosion based algorithm for edge detection. 2015 IEEE International Conference on Electro/Information Technology (EIT). doi:10.1109/eit.2015.7293391

[33] Pawar, S., & Banga, V. K. (2012). Morphology approach in image processing. In International Conference on Intelligent Computational Systems (ICICS'2012)(Dubai). Dubai (pp. 148-150).

[34] Singh, A., Singh, M., & Singh, B. (2016). Face detection and eyes extraction using sobel edge detection and morphological operations. 2016 Conference on Advances in Signal Processing (CASP). doi:10.1109/casp.2016.7746183

[35] Deepika, P. U., Chauhan, S., & Narayan, N. (2017, October). Artificial Intelligence techniques used to detect object and face in an image: A Review. In 2017 3rd International Conference on Computational Intelligence and Networks (CINE) (pp. 6-9). IEEE.

[36] Maier, A., Syben, C., Lasser, T., & Riess, C. (2019). A gentle introduction to deep learning in medical image processing. Zeitschrift für Medizinische Physik, 29(2), 86-101.

[37] Manikandan, G., & Abirami, S. (2018). A survey on feature selection and extraction techniques for high-dimensional microarray datasets. In Knowledge Computing and its Applications (pp. 311-333). Springer, Singapore.

[38] Jindal, R., & Vatta, S. (2010). Sift: Scale invariant feature transform. IJARIIT, 1, 1-5.

[39] Genovese, A., Piuri, V., Plataniotis, K. N., & Scotti, F. (2019). PalmNet: Gabor-PCA convolutional networks for touchless palmprint recognition. IEEE Transactions on Information Forensics and Security, 14(12), 3160-3174.

[40] Y F Zhang, Y Zhang. (2006). "Another Method of Building 2D Entropy to Realize Automatic Segmentation". International Symposium on Instrumentation Science and Technology.

[41] .Liping Zheng, Guangyao Li, Yun Bao. (2010). "Improvement of Grayscale Image 2D Maximum Entropy Threshold Segmentation Method". IEEE.

[42] Gnanasekaran, N., Chandramohan, S., Kumar, P. S., & Imran, A. M. (2016). Optimal placement of capacitors in radial distribution system using shark smell optimization algorithm. Ain Shams Engineering Journal, 7(2), 907-916.

[43] Bagheri, M., Sultanbek, A., Abedinia, O., Naderi, M. S., Naderi, M. S., & Ghadimi, N. (2018). Multi-objective Shark Smell Optimization for Solving the Reactive Power Dispatch Problem. 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe) .doi :10.1109 /eeeic.2018.8494502

[44] Rao, Y., Shao, Z., Ahangarnejad, A. H., Gholamalizadeh, E., & Sobhani, B. (2019). Shark Smell Optimizer applied to identify the optimal parameters of the proton exchange membrane fuel cell model. Energy Conversion and Management, 182, 1–8. doi:10.1016/j.enconman.2018.12.057

[45] Mohammad-Azari, S., Bozorg -Haddad, O., & Chu, X. (2017). Shark Smell Optimization (SSO) Algorithm. Studies in Computational Intelligence, 93–103. doi: 10. 10 07/978-981-10-5221-7_10

[46] Rui.Ye,"Image Watermarking using chaotic Watermark Scrambling and perceptual Quality Evolution",IRCCYN-Institute de Recherche 'en communications et encybernetique de Nantes ,IETR-Institute d' Electronique et detelecommunications deREnnes,2013

[47] GuodongYe ,KaixinJiao,ChenPan,andXiaolingHuang.(2018). An Effective Framework for Chaotic Image Encryption Based on 3D Logistic Map. Hindawi. Security and Communication Networks Volume 2018, Article ID 8402578, 11 pages https://doi.org/10.1155/2018/8402578

[48] Owolabi, O. Y., Shola, P. B., & Jibrin, M. B. (2017). Improved Data Security System Using Hybrid Cryptosystem. 201.7 IJSRSET, 3(3)

[49] Putri Ratna, A. A., Dewi Purnamasari, P., Shaugi, A., & Salman, M. (2013). Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple-O authentication based security system. 2013 International Conference on QiR.

[50] Zhong, L., Wan, W., & Kong, D. (2016). Javaweb login authentication based on improved MD5 algorithm. 2016 International Conference on Audio, Language and Image Processing (ICALIP). doi:10.1109/icalip.2016.7846653

[51] Asmin Bhandari, Moshiur Bhuiyan, P. W. C. Prasad. (2017). Enhancement of MD5 Algorithm for Secured Web Development. Journal of Software .Volume 12, Number 4.

[52] Sýs, M., & Říha, Z. (2014, October). Faster randomness testing with the NIST statistical test suite. In International Conference on Security, Privacy, and Applied Cryptography Engineering (pp. 272-284). Springer, Cham.

[53] Bassham III, L. E., Rukhin, A. L., Soto, J., Nechvatal, J. R., Smid, M. E., Barker, E. B., ... & Heckert, N. A. (2010). Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards & Technology.

[54] Rukhin, A., & Soto, J. (2016). A statistical test suite for random and pseudorandom number generators for cryptographic applications [Electronic resource]. Access mode: http://csrc. nist. gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a. pdf.

[55] Fouque, P. A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., ... & Zhang, Z. (2018). Falcon: Fast-Fourier lattice-based compact signatures over NTRU. Submission to the NIST's post-quantum cryptography standardization process.

[56]https://www.computer.org/csdl/journal/tp/2010/08/ttp2010081529/13rRUyogGBk

المستخلـــص

توقيـــع المســـتند باســـتخدام تحســـين خوارزميـــة ســـمك القـــرش تـــم اســـتخدام مجـــالات الأمـــان والخصوصـــية والمقـــاييس الحيويـــة للوســـائط المتعـــددة على نطاق واسع اليوم للمصادقة الشخصية.

تعتبـــر الصـــلبة (Sclera) والنخيـــل (Palm) مـــن البشـــر واحـــدة مـــن التقنيـــات البايومتريـــة الاســـرع والدقيقـــة والامنـــة لتحديـــد الهويـــة والتحقيـــق, بنـــاءا علـــى الميـــزات الفريدة

تقـــدم هـــذه الرســـالة توقيـــع المســـتند باســـتخدام تحســـين خوارزميـــة ســـمك القـــرش ESSO (Enhancement Shark Smell Optimization Algorithm)، وتهـــدف إلـــى تقـــديم تقنيـــة جديـــدة لتوليـــد مفتـــاح تشـــفير تيـــار(stream secret key)باســـتخدام نظـــام تحديـــد متعـــدد المقـــاييس يتكـــون مـــن صـــور (الصـــلبة sclera والنخيـــل palm) ويـــتم اســـتخدام أفضـــل الإحـــداثيات عـــن طريـــق التحســـين لخوارزميـــة ســـمك القـــرش (Enhancement Shark Smell Optimization) علـــى أســـاس خريطـــة فوضوية لوجستية ثلاثية الأبعاد (Chaotic Logistic Map) .

حيـــث تـــم اســـتخدام اثنـــين مـــن قاعـــدة البيانـــات الاولـــى قاعـــدة بيانـــات الصـــلبة sclera (UBIRIS.V2) مـــن جامعـــة بيرا.البرتغـــال والثانيـــة قاعـــدة بيانـــات النخيـــل palm (THUBALMLP) جامعة تستنغوا .بكين.

تتضـــمن مراحـــل تنفيـــذ النظـــام المقتـــرح اســـتخلاص الميـــزة مـــن صـــور الســـمات الصـــلبة sclera والنخيـــل palm مـــن نفـــس الشخصـــية وتســـقيط النقـــاط المســـتخرجة مـــن الصـــلبة sclera والنخيـــل palm علـــى صـــورة ســـرية (secret image) SI ، لكـــل نظـــام تقنيـــات معالجـــة مســـبقة مختلفـــة لإعـــداد الصـــور للميـــزات الدقيقـــة. بالإضافة إلى ذلك ، تستخرج خوارزمية تحويل الميزة الثابتة SIFT

(Scale Invariant Feature Transform Algorithm) فـــي نظـــام التعـــرف متعـــدد المقـــاييس ميـــزات مـــن الصـــلبة والحيويـــة وصـــور النخيـــل والحصـــول علـــى وصـــول ســـريع إلـــى المنـــاطق الهامـــة داخـــل الصـــلبة والنخيـــل. يـــتم اســـتخدام هـــذه الميـــزات لإيجـــاد الحـــل الأمثـــل باســـتخدام خوارزميـــات التحســـين لرائحـــة أســـماك القـــرش ESSOاســـتنادًا إلـــى الوظيفـــة الفوضـــوية Chaotic Logistic Mapواســـتخدم هـــذه الميـــزات لتوليـــد مفتـــاح دفـــق بطـــول متغيـــر باســـتخدام خوارزميـــة MD5 ، وأخيـــرا النظـــام المقتـــرح يســـتخدم مفتـــاح الـــدفق فـــي توقيـــع الوثيقـــة لحمايـــة الشخصـــية و المعلومـــات بطريقـــة آمنـــة تمامًـــا.
التحســـينات المقترحـــة علـــى تحســـين خوارزميـــة ســـمك القـــرش تســـتخدم وظيفـــة الفوضـــى اللوجيســـتية ثلاثيـــة الأبعـــاد لتوليـــد مجموعـــة مـــن الأرقـــام العشـــوائية التـــي

تغـــذي المعلمـــات العشـــوائية للخوارزميـــة ، وســـلوكيات أكثـــر عشـــوائية وســـرعة الوصـــــــــــــــــول إلـــــــــــــــــى أفضـــــــــــــــــل حـــــــــــــــــل.

أظهـر تنفيـذ النظـام المقتـرح ونتـائج اختبـارات إنشـاء الأرقـام العشـوائية (National Institute of Standards Technology (NIST))المعهـد الـوطني للمعـايير والتكنولوجيـــا أن النظـــام المقتـــرح لديـــه القـــدرة علـــى توليـــد مفتـــاح دفـــق لمضـــاعفة المسـتخدمين الـذين يمتلكـون العديـد مـن حيـث تكـون مواصـفاته فريـد مـن نوعـه ,غيـر متوقع عشوائي , قوي ومتنوع الطول.

وزارة التعليم العالي والبحث العلمي

جامعة ديالى - كلية العلوم

قسم علوم الحاسوب

توقيع المستند باستخدام تحسين خوارزمية سمك القرش

من قبل

اسراء نزيه

بإشراف

أ.م. د. جمال مصطفى عباس

أطروحة مقدمة الى قسم علوم الحاسوب في كلية العلوم/ جامعة ديالى

وهي جزء من متطلبات نيل درجة الماجستير في علوم الحاسوب

2020