Republic of Iraq
Ministry of Higher Education
And Scientific Research
University of Diyala
College of Science
Computer Science Department

Generation of Unique Verification from Human Palm Based on Elliptic Curves

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

Murooj Mohammed Abood

Supervised by

Prof. Dr. Ziyad Tariq Mustafa *Prof. Naji M. Sahib*

2020 A.C. 1440 A.H

بسم الله الرحمن الرحيم

يَرۡفَعِ ٱللَّهُ ٱلَّذِينَ ءَامَنُواْ مِنكُمۡ وَٱلَّذِينَ أُوتُواْ ٱلۡعِلۡمَ
دَرَجَٰتٖۚ وَٱللَّهُ بِمَا تَعۡمَلُونَ خَبِيرٞ ١١

صدق الله العظيم

سورة المجادلة (١١)

Acknowledgment

First of all, praise is to GOD, the lord of the whole creation, on all the blessing was the help in achieving this research to its end.

I wish to express my thanks to my supervisors, Assist. Prof Dr. Ziyad Tariq Mustafa and prof. Naji Mutar Sahib for supervising this research and for the generosity, patience and continuous guidance throughout the work. It has been my good fortune to have the advice and guidance from them. My thanks to the academic and administrative staff at the Department of the computer sciences.

I would like to express my gratitude to my father, my mother, my sisters and my brothers.

Murooj mohammed

Dedication to

This work is dedicated to my family, whose assistance, forbearance, and continues encouragement during the whole period of time, made it possible to finish this work. Also dedicated to giving the effort to my parents, I wish to express my love and gratitude to my beloved family members

With My love
Murooj

Supervisor's Certification

We certify that this research entitled **"Generation of Unique Verification from Human Palm Based on Elliptic Curves"** *was prepared by* ***Murooj Mohammed Abood*** *under our supervision at the University of Diyala Faculty of Science Department of Computer Science, as a partial fulfillment of the requirements needed to award the degree* ***of Master of Science in Computer Science.***

(Supervisor)

Signature:

Name: Prof. Dr. Ziyad Tariq Mustafa

Date: / / 2020

(Supervisor)

Signature:

Name: Prof. Naji M. Sahib

Date: / / 2020

Approved by University of a Diyala Faculty of Science Department of Computer Science.

Signature:

Name: Assist. Prof. Dr. Taha M. Hassan

Date: 22/2/2020

(Head of Computer Science Department)

Linguistic Certification

I certify that this research entitled **"Generation of Unique Verification from Human Palm Based on Elliptic Curves"** *was prepared by* ***Murooj Mohammed Abood*** *and was reviewed linguistically. Its language was amended to meet the style of English language.*

Signature :

Name : Amthal Mohammed Abbas

Date : 22 / 2 / **2020**

Examination Committee Certification

We certify that we have read this research entitled **"Generation of Unique Verification from Human Palm Based on Elliptic Curves"**, *and as an examining committee, examined the student* ***"Murooj Mohammed Abood"*** *in its contents and that in our opinion, it is adequate as fulfill the requirements for the Degree of Master in Computer Science at the Computer Science Department, University of Diyala.*

(Chairman)

Signature:
Name: Prof. Dr. Ali makki Sagheer
Date: 22/2/2020

(Member)

Signature:
Name: Assist. Prof. Dr. Jamal M. Abbas
Date: 22/2/2020

(Member)

Signature:
Name: Assist. Prof. Dr. Salam A. Noaman
Date: 22/2/2020

(Member / Supervisor)

Signature:
Name: Prof. Dr. Ziyad Tariq Mustafa
Date: 22/2/2020

(Member / Supervisor)

Signature:
Name: Prof. Naji M. Sahib
Date: 22/2/2020

Approved by the Dean of College of Science, University of Diyala.

(The Dean)

Signature:
Name: Prof. Dr. Tahseen Hussein Mubarak
Date: 8/3/2020

Abstract

A Human palm biometric is one of the fastest, accurate, reliable and secure biometric techniques for identification and verification, because it provides automatic authentication of an individual based on unique features in palm structure. Palm print contain distinctive features such as principal line, wrinkles, ridges and valleys on the surface of the palm. Unlike palm print identification that matches one feature to many features in the database, palm print verifies the persons claimed identity to the stored pattern in the system.

In this thesis, an efficient unique verification system is proposed by using human palm. Human palm can give unique features which can be used in generating unique verification. Therefore, this system consists of three stage (1) image preprocessing stage:(color to gray scale and histogram equalization).(2) feature extraction stage:(GLCM (Haralick) algorithm). (3) Generating unique verification stage :(Elliptic Curve and Cubic Spline function with MD5 algorithm).

The performance test results show that the MD5_B coefficients has lowest convergence ratio in terms of users signatures than the coefficients of MD5_A.

List of Contents

Contents	Page No
Chapter One: General Introduction	
1.1 Introduction	1
1.2 Related Works	2
1.3 Aim of the thesis	4
1.4 Contribution	4
1.5 Outline of the Thesis	5
Chapter Two: Theoretical Background	
2.1 Introduction	6
2.2 Biometric	6
2.2.1 Biometric Types	7
2.2.2 Biometric Recognition	9
2.2.3 Biometric System	10
2.2.4 Basic Steps of Biometric System	11
2.3 Preprocessing of an Image	12
2.3.1 Converting Image to Grayscale	13
2.3.2 Image Enhancement with Histogram Equalization	13
2.4 Feature Extraction	14
2.4.1 Texture Features	15

2.4.2 Gray Level Co-occurrence Matrice	15
2.4.3 Features Extracted from GLCM	17
2.5 Elliptic Curve Cryptography	18
2.5.1 Finite Field	19
2.6 MD5 Algorithm	20
2.7 Interpolation	21
2.8 Longest Common Subsequence	23
Chapter Three :The Proposed System	
3.1 Introduction	25
3.2 The Proposed system	25
3.2.1 Input Stage or (Load Palm Image)	26
3.2.2 Image Pre-Processing Stage	27
3.2.3 Feature Extraction stage	28
3.2.4 Generate Digital Signature Stage	32
Chapter Four :Results and analysis	
4.1 Introduction	37
4.2 Initialization	37
4.3 Results of the Proposed Model	37
4.3.1 Result of Palm Image Preprocessing	37
4.3.2 Result of Haralick Algorithm	42
4.3.3 Result of Elliptical Curve	45
4.3.4 Result of Spline function	47

4.3.5 Result of MD5	50
4.4 Performance Test	51
Chapter Five: Conclusions and suggestions for Future Works	
5.1 Conclusions	54
5.2 Suggestions for future works	55
References	56

List of Abbreviations

Abbreviation	Description
GLCM	Gray level co-accurence matrice
ECC	Elliptic Curve Cryptography
FF	Finite Field
MD5	Message- Digest
GF	Galois Field
PINS	Personal Identification Numbers
RSA	Rivest-Shamir-Adleman
RGB	Red- Green- Blue
PDF	Probability Density Function
IDM	Inverse Difference Moment

List of Figures

Figure No.	Figure title	Page No.
2.1	Different features of palm print (a) inked palm print (b) inkedless palm print	8
2.2	Offline Palm Print Acquisition Method	9
2.3	Histogram Equalization	14
2.4	Directions used for computing isotropic GLCM	16

2.5	Calculating a GLCM for an image of size 4×4	16
2.6	Calculating a GLCM for an image of size 3×3	16
2.7	Elliptic Curve	19
3.1	Block Diagram of the proposed system	26
3.2	Direction angles for the GLCM	30
3.3	Apply the direction of the GLCM angles on palm	30
3.4	Example of the Haralick Feature Algorithm	31
4.1	Original Images of Palm Data Set	38
4.2	Images of Converted to Gray Scale Images	39
4.3	Images after Enhancement with Histogram Equalization	41
4.4	Intersection points of Haralick Algorithm	43
4.5	Details of the intersection points in all Dataset	44
4.6	Results of Elliptic curve	45
4.7	spline function	47
4.8	sults of MD5 algorithm	50
4.9	Results of Performance Test of the MD5 user using coefficient MD5 -A and coefficient MD5 -B	51
4.10	Performance Test results of the MD5 user using coefficient	52

	MD5 -A and coefficient MD5 -B.	
4.11	Result of MD5 algorithm using Coefficient MD5-B	52

List of Algorithms

Algorithm No.	Algorithm Title	Page No.
3.1	Converting to Gray Scale Image	27
3.2	Image Histogram Equalization	28
3.3	Haralick Feature	32
3.4	Elliptic Curve	33
3.5	Cubic Spline function	35
3.6	MD5 Hashing	36

Chapter One

Introduction

Chapter one

Introduction

1.1 Introduction

Biometric systems are the most important systems used in our everyday life. Because of the large number of threats, fraud and identity theft, it is important to secure and maintain data accurately. However, theft and impersonation still hinder data security by stealing passwords, PINs, and IDs. [1]

Biometric systems can be used in many applications such as security, personal data, commercial and legal applications, personal data, and so forth. Biometric patterns are used as data for biometric identification systems, meaning "life measurement", which can identify any person based on characteristics because they vary from person to person. [2]

Biometric patterns can be divided depending on their characteristics into two categories: behavioral and physiological. The Physiological characteristics can be divided into five parts:

1. Fingerprint: It is very important and wide-ranging, depends on the surface of the fingertips.

2. Face recognition: Its work is mainly focused on the characteristics of video or fixed images of the face.

3 - Vein patterns: This pattern is variable with time and unique between the persons.

4 - Iris examination: This pattern is not variable with time and unique between people.

5 - DNA: In every human cell, there is an acronym for deoxyribonucleic acid. [3]

The Behavioral characteristics can be divided into three parts:

1 - Keystroke: depends on the correlation between the dynamics of keystrokes and the way people write.

2 - Signature: The handwriting of a particular person can represent its characteristics.

3. Sound: It depends on the channels of voice, lips, mouth and nose, as well as the physical and emotional state of the speaker [3].

1.2 Related Works

Related recent studies, which have proposed several algorithms on digital signature and palm print on texture feature, are discussed in this section:

In 2016 K. Tamilsevan, et. al.[4] proposed a hybrid approach of using finger and palm vein for the design of biometric system has been proposed. The proposed system approach simultaneously acquires the finger, palm vein database, and combines these two evidences using a hybrid comparison strategy in order to increase the accuracy and sensitivity of the system while reducing the time complexity and harmfulness to human being.

In 2017 J. A .Shaikh and U. D. Kolekar [5], a system has been developed to identify the printing of palm based on a gray text matrix feature. Using the Euclidean distance tool, the Harlick feature of the sub-

images of each area of interest (ROI) was extracted to create a very small vector of fetures, however better accuracy is obtained, also there is an improvement on performance parameter, the False Acceptance Ratio (FAR) and False Rejection Ratio (FRR).

In 2017 K.J Archana, et. al.[6], through the focus of (ROI), which is very important in palm printing and based on (GLCM), a new algorithm was discussed to define palm printing. Compared to the recovery of (ROI) dynamic, the palm area of recognition is few when using fixed size (ROI). The proposed algorithm focused on extraction of maximum possible ROI. Texture features are extracted using GLCM from dynamic ROI image. The experimentations are performed on the Poly U database to validate the proposed algorithm.

In 2017 P. T. Selvyp, et. al. [7] proposed a palm print recognition system using Gray level co-occurrence matrix (GLCM) in feature extraction and Support vector machine (SVM) in classification. The proposed method not only uses the orientation features and also includes second order features like energy, correlation, contrast and homogeneity for recognition and comparison. The proposed system had a simple and effective balancing scheme to improve the precision of the orientation feature of the palm print. Experiments conducted on dataset demonstrated that proposed method give better results than existing orientation methods. The proposed method enhanced the accuracy and also it reduced the average error rate in classification.

In 2018 A. Alhayajneh, et. al. [8] seek to analyze and evaluate the most prominent biometric authentication techniques based on accuracy, cost, and feasibility of implementation. They suggest several authentication schemes which incorporate multiple biometric properties.

In 2018 D. Rachmawati1, et. al. [9] the research results obtained from the complexity of the Algorithms MD5 and SHA256 is the same, i.e., Θ (N), but regarding the speed is obtained that MD5 is better compared to SHA256.

In 2019 S. Samreen, et. al. [10] AC2 spline technique QTS is proposed and built with the eagerness of the object modeling using quadratic trigonometric functions. The curve model built through the proposed method owns the best suitable geometric properties such as partition of unity, CHP, AIP and VDP. The proposed scheme is more advantageous over the traditional CPS method. It is smoother, more flexible, faster and more accurate alternate to CPS. Furthermore, the built curve method is modest overall and is ideal for curve modeling. The comparison analysis of QTS and CPS verifies the QTS as better alternate to CPS. Also, the time analysis proves QTS computationally efficient than CPS.

In 2020 K. Bharathi and V. Sangeetha [11] suggested an increased security model of OTP system using IRIS Biometric with ELLIPTIC CURVE CRYPTOGRAPHY. This model provides to higher security with lesser key size than prevailing public key crypto-model.

1.3 Aims of the Thesis

The goal of this thesis is to design an unique verification based on elliptic curve technique. The proposed elliptic curve signature is secured by biometric features of the palm.

1.4 Contribution

The main contribution of this work is the linking between an elliptic curve and biometric palm features.

1.5 Outline of the Thesis

Beside the current chapter, this thesis contains the following chapters**:**

- **Chapter Two: Theoretical Background**
  Presents the theoretical background and the biometric parameters which contains the biometric image, GLCM, Haralick, EC, Splines, and MD5 algorithms.
- **Chapter Three: Design and Implementation of Proposed System**
  Describes the development of the proposed system, which introduces the main stages; extraction features, exploring edges, estimation dummy features and comparing for human hand image.
- **Chapter Four: Results and Analysis**
  Illustrates, investigates and analyzes the experimental results.
- **Chapter Five: Conclusions and Suggestions for future works**
  Presents the conclusions from this work and the suggestions for the future work.

Chapter Two

Theoretical Background

Chapter Two

Theoretical Background

2.1 Introduction

Biometric technology analyzes a person by his\ her unique features as their signature, fingerprint, smell, voice, eyes, face and others. A good biometric is a system that allow people to securely authenticate themselves because data is safe and could not be shared, stolen, lost or duplicated. The biometric technology enables people to perform authentication with simple process, and individuals are not required to remember words or numbers if they would wish to digitally verify themselves [12].

This chapter gives a theoretical background to this thesis. Biometrics are presented in section (2.2). Preprocessing of images is introduced in section (2.3). Section (2.4) explains feature extraction. Elliptic curve cryptography, MD5 algorithm, interpolation, longest common subsequence are given in sections (2.5, 2.6, 2.7 and 2.8) sequentially.

2.2 Biometric

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). Biometric verification refers to an automatic verification of the person based on some specific biometric features derived from his/her physiological and/or behavioral characteristics. A biometric verification system has more capability to reliably distinguish between an authorized person and an impostor than the traditional systems that use a card or a password [13]. The Biometric system is essentially a pattern recognition system that acquires biometric data from

an individual, then extracts a feature set from the data, compares this feature set against the feature sets (templates) stores in the database, and executes an action based on the result of the comparison [14].

2.2.1 Biometric Types

There are many biometric types such as: fingerprint [15], Iris [14,16], face [17,18] hand vein [19], signature [20], voice [16], and palm print (subject of this thesis) which can be described as:

The palm is refers to the inner surface of human's hand from the wrist to the root of fingers. A print is the impression created in or on a surface by pressure. A palm print is defined as the patterns of skin of a palm, composed of the physical characteristics such as texture, points and lines. Palm prints may exist on the object surface, mainly due to the perspiration. Less observable "prints" are generated for a dryer hand. The study of palm prints can be divided into two main streams, non-forensic and forensic. The "actual" palm prints observed on a crime scene are useful for forensic investigation, while the non-forensic study may use imaging techniques to obtain observable human "palm prints" of a palm. Palm print authentication is a means of personal authentication that uses unique palm print features, which may or may not be observable to the naked eye. It can be achieved by designing an appropriate algorithm capable of separating two persons by their palm print features. Palm prints are rich in features: principal lines, winkles, ridges, singular points and minutiae points, as shown in figure (2.1). Palm prints have a surface area much larger than a fingertip but are covered with the same kind of skin of a finger [20]. The data set is palm dataset version 1-0 of 100 subjects [21].

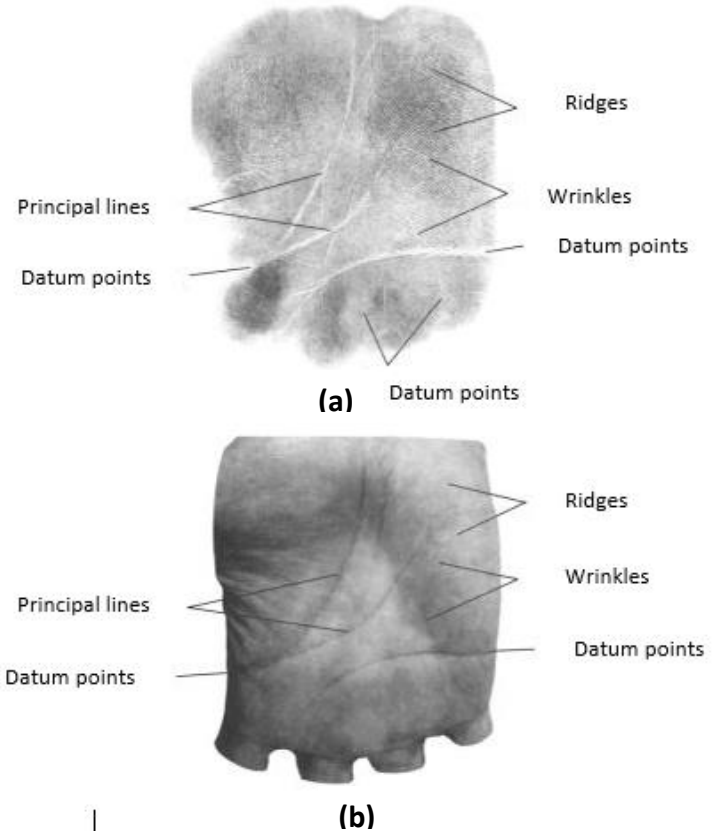


Figure 2.1: Different features of palm print (a) inked palm print (b) inkedless palm print [22]

There are two acquisition methods for palm prints [22]:

a. **Offline Palm Print**: in 1996 the offline palm print started using inked images, as shown in Figure 2.2. The offline method involves the process of collecting samples though pressing a user's palm onto a sheet of white paper after inking it. After the ink has dried, the image of palm print on the paper is digitized with a scanner and stored on personal computer. Clearly, for real-time application such as physical access control this method proved to be unsuitable. In addition to the number of steps involved, the palm print has an unsatisfactory quality because it may be affected by the how much ink has been used. Too little or too much ink can produce low quality palm prints.

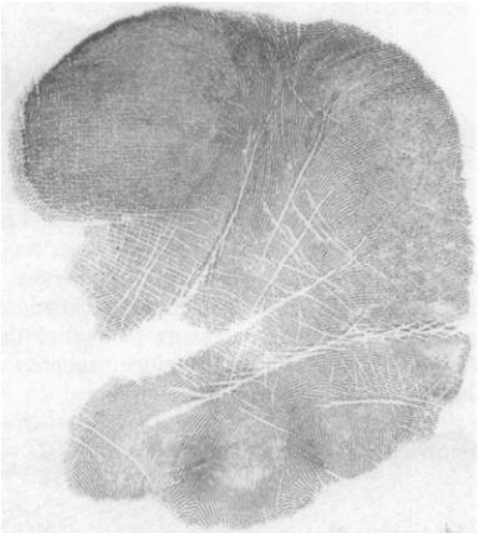


Figure 2.2: Offline Palm Print Acquisition Method [22].

b. **Online Palm Print Acquisition:** is the most direct method for digitizing data of palm print, makes the need for a third medium like paper unnecessary. It can 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.

2.2.2 Biometric Recognition

A number of biometric characteristics have been use in various applications. Each biometric has its strengths and weaknesses, in other words, no biometric is ideal. The relevance of a specific biometric to an application is establish depending upon the nature and requirements of the application, and the properties of the biometric characteristic. Biometric characteristics can be divided in two main classes [16,23].

1- **Physiological:** which are related to the shape of the body and thus it varies from person to person. Fingerprints, face, hand geometry and iris are examples of this type of biometric.
2- **Behavioral:** which are related to the behavior of a person. Some examples in this case are signature, keystroke dynamics and voice.

2.2.3 Biometric System

A biometric system measures one or more behavioral or physical characteristics: (face, iris, palm print, fingerprint, odor, hand vein, retina, signature, ear, voice, gait or the DNA) of an individual to verify or determine his identity. Two main phases are followed in order to access the system of biometric recognition for an individual's identification depending on his/her behavioral and/or physical features, namely: enrollment phase and recognition phase [24].

i. Enrollment Phase

It's also named registration process; in which the raw biometric data of a given individual is captured by biometric device for sensing and processing. Unique characteristics that can distinguish each individual are extracted from this biometric data, then transferred into a biometric template stored in database under the identity of each person. The use of template is to compare for the purpose of identifying a specific authentication user [25].

ii. Recognition Phase

In the recognition phase, the raw biometric data is re-acquired from the user also pass through the same stage of pre-processing and feature extraction to generate template, compared with corresponding reference samples that stored in database, in order to determine the person identity. There are two types of identity management functionalities: identification and verification [24].

1- Identification

The identification task is similar to the verification task. It is a one-to-many matching process, in which the person identifies himself to

the system without claiming an identity by submitting to a biometric system to extract his biometric data and generate a template, that compared to all templates that stored in reference database during enrollment step in order to identify person identity [24].

2- Verification

The verification is a one-to-one matching process, in which a person claims an identity and the system checks whether this claim is genuine or not by generating a query template according to the mechanism of the system which had been prepared in advance, and comparing this query to the only template corresponding usually claimed through the use of a personal identification number, a user name, or a token (e.g., smart card), and the claim is accepted or rejected depending on the degree of similarity between this two templates [26].

2.2.4 Basic Steps of Biometric System

Typically, the biometric system mainly is a system of pattern recognition consists of the essential following blocks: sensor module, feature extractor module, matching module, decision-making module and a database module [27]:

a. **Sensor Module:** the quality of a captured image depends on the selected sensor form several. Where each biometric pattern has an equivalent radar sensor that easy, intuitive, and comfortable to use interface may facilitate a fast user habituation and enable acquiring biometric samples of a good quality from the person or it can be self-contained to achieve the whole process of biometric verification within itself.

b. **Feature Extraction Module:** it is a process of extracting a certain interesting feature that represents the underlying trait of the biometrics pattern, called a template. This process is of an important function in the recognition system since that the result is being used as an input data in a recognition process, thus, affect the output of matching process in a significant manner.
c. **Database Module:** is a warehouse build during the enrollment process. The database holds the features set which have been taken out from the raw biometric sample (i.e., the template) and some personal identity information (as address, name or PINS, etc.) describing the users. The biometric information warehouse is represented by the biometric system.
d. **Matching Module:** the biometric matching is a process of match score generating through calculating the similarity between the query features and the templates in database. Greater similarity result from smaller distance score. A decision making module is encapsulated by the matcher module, where scores of matching are used to either ratification a claimed identity or provides the enrolled identities in order to identify a person.
e. **Decision Making Module:** this module is responsible of making the decision on the person's identity depending on the matching target.

2.3 Preprocessing of an Image

Image enhancement techniques improve the quality of an image as perceived by human. Generally, image enhancement techniques are used to get detail that is obscured, or to highlight certain features of interest in image. In image enhancement process one or more attributes of image are modified. The main purpose of image

enhancement is to bring out detail that is hidden in an image or to increase contrast in a low contrast image. Whenever an image is converted from one form to other such as digitizing the image some form of degradation occurs at output [28]. The most interest preprocessing methods are as follows:

2.3.1 Converting Image to Grayscale

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 grayscale domain rather than three as in RGB domain [29].

Three principles for converting color to grayscale are such as [30]:

1- The **lightness** method averages the most prominent and least prominent colors as in equation (2.1):

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

2- The **average** method averages the color values as in equation (2.2):

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

3- The **luminosity** method is a more developed version of the average method. It also averages the values, but it forms a weighted average to account for human perception. The most heavily is the green because they are more sensitive to it. The luminosity formula is shown in equation (2.3):

$$Grayscale(i,j) = (0.2989 * R) + (0.5870 * G) + (0.1140 * B) \qquad (\mathbf{2.3})$$

2.3.2 Image Enhancement with Histogram Equalization

Histogram equalization is a technique in image processing of contrast-adjustment using the image's histogram. This method usually increases the global contrast of several images, especially when the usable data of the image is represented by close contrast values. Through

this correction, the intensities can be better distributed on the histogram. This allows for areas of lower local contrast to gain a higher contrast. Histogram equalization performs this by effectively spreading out the most frequent intensity values. Consider a discrete gray scale image {x} and let ni be the number of occurrences of gray level i. The probability of an occurrence of a pixel level I in the image is [31]:

$$Px(i) = p(x = i) = \frac{n_i}{n}, 0 \leq i < L \qquad (\mathbf{2.4})$$

L is the total number of gray levels in the image (typically 256), n is the total number of (pixels) in the image, as shown in Figure (2.3).

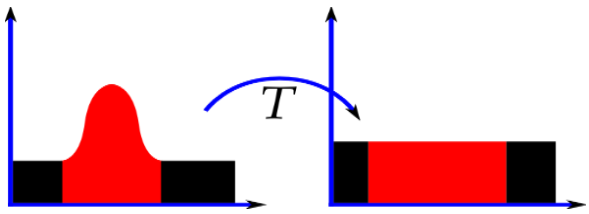


Figure 2.3: Histogram Equalization [31].

2.4 Feature Extraction

Features, characteristics of the objects of interest, if selected carefully are representative of the maximum relevant information that the image has to offer for a complete characterization a lesion. Feature extraction methodologies analyze objects and images to extract the most prominent features that are representative of the various classes of objects. Features are used as inputs to classifiers that assign them to the class that they represent [32].

Feature extraction is the indexing of an image database; mathematically, a feature is an n-dimensional vector, with its components computed by some image analysis. The three feature descriptors mainly

used most frequently during feature extraction are shape, color and texture [33].

2.4.1 Texture Features

In a large number of applications, texture plays the role of an important feature in image analysis. Texture analysis attempts to quantify intuitive qualities described by terms such as rough, silky, bumpy or smooth as a function of the spatial variation in pixel intensities. The choice of the textural features should be as compact as possible and yet as discriminating as possible. It is important to find a set of texture features with good discriminating power. Texture features can be found using methods as Gabor Filter, Haar Wavelet Decomposition and Wavelet GLCM etc. [34].

2.4.2 Gray Level Co-occurrence Matrice

GLCM is one of the most known texture analysis methods, it estimates image properties related to second-order statistics [35]. GLCM also known as the gray-level spatial dependence matrix. The information on the texture image is assumed by GLCM method to be adequately provided by a certain matrix. The technique depends on manipulating the levels of gray of an image [36].

By default, the spatial relationship is defined as the pixel of interest and the pixel to its immediate right (horizontally adjacent), but other spatial relationships can be specified between two pixels. X number of times that the pixel with value I occurring in the specified spatial relationship to a pixel with value Jin the input image [37]. The GLCM can be computed for eight directions around the pixel of interest (see Figure 2.4).

135^0	**90^0**	**45^0**
180^0	**X**	**0^0**
225^0	**270°**	**315^0**

Figure 2.4: Directions used for computing isotropic GLCM [36].

1- For example, figure (2.5) depicts a GLCM for an image of size 4×4 where number of gray level (*Ng)* = 4 and where d= 1 and where θ = 0.

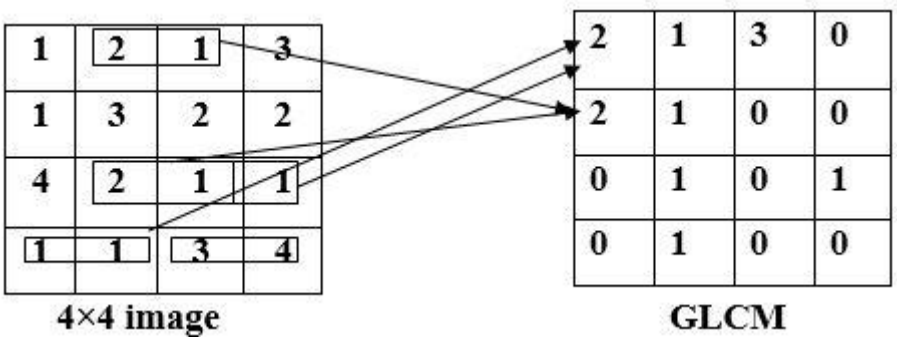


Figure 2.5: Calculating a GLCM for an image of size 4×4 [37].

2- For example figure (2.6) depicts a GLCM for an image of size 3×3where d= 1 and where θ = 45.

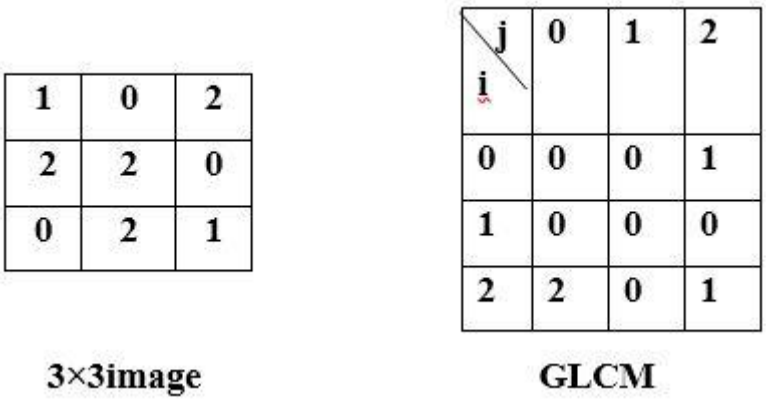


Figure 2.6: Calculating a GLCM for an image of size 3×3, with *d* = 1 and direction θ = 45 [37].

2.4.3 Features Extracted from GLCM

Haralick et al [38], have proposed a number of useful texture features that can be computed from the co-occurrence, based on the GLCM, various texture feature measures are defined. such as Entropy, Energy, Contrast, Homogeneity, Inverse Difference Moment(IDM), Mean.

1- **Entropy [**39]**:** Entropy shows the amount of information of the image that is needed for the image compression. Entropy measures the loss of information or message in a transmitted signal and also measures the image information as in Eq (2.5).

$$\textbf{Entropy} = -\sum_{i,j=0}^{n} p(i,j) log p(i,j) \qquad \textbf{(2.5)}$$

2- **Energy [40]:** Angular Second Moment is also known as Uniformity or Energy. It is the sum of squares of entries in the GLCM Angular Second Moment measures the image homogeneity as in Eq.(2.6). Angular Second Moment is high when image has very good homogeneity or when pixels are very similar

$$\textbf{Energy} = \sum_{i,j=0}^{n} \{p(i,j)\},^{2} \qquad \textbf{(2.6)}$$

Where i, j are the spatial coordinates of the function p (i, j), Ng is gray tone.

3- **Contrast** [40]**:** This statistic measures the spatial frequency of an image and is difference moment of GLCM. It is the difference between the highest and the lowest values of a contiguous set of pixels. It measures the amount of local variations present in the image as in Eq.(2.7). A low contrast image presents GLCM concentration term around the principal diagonal and features low spatial frequencies.

$$\textbf{Contrast} = \sum_{i=0} \sum_{j=0} P(i-j)^2 P(i,j) \qquad \textbf{(2.7)}$$

4- **Inverse Difference Moment** [40]**:** It measures image homogeneity as in Eq.(2.8). This parameter achieves its largest value when most of the occurrences in GLCM are concentrated near the main diagonal [36].

$$\textbf{IDM}= \sum_i \sum_j \frac{1}{1+(i-j)^2} P(i,j) \qquad \textbf{(2.8)}$$

2.5 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) was first introduced by victor Miller, who was then at IBM, and Neil Koblitz from the university of Washington independently in 1985. The principal attraction of ECC compared to RSA is that it offers equal security for a far smaller key size, theory reducing processing overhead. ECC is based on Discrete Logarithmic problem over the points on an elliptic curve [41].

ECC is a relative of discrete logarithm cryptography. An elliptic curve E over Zp as illustrated in Figure 2.10 is defined in the Cartesian coordinate system by an equation of the form [42]:

$$y\text{^}2 = x\text{^}3 + ax + b \qquad (\mathbf{2.9})$$

Where a, b ε Zp, and $4a\text{^}3 + 27b\text{^}2 \neq 0$ (mod p), together with a special point O, referred as the point at infinity. The set E (Zp) is made of all points (x, y), x ε Zp, y ε Zp, this satisfies the defining equation, together with O.

Each value of a, and b provide a various elliptic curve. The point on the curve is the public key while the random number is the private key. The process of multiplying the private key with a generator point G in the curve will result in the public key [41].

The nest subsections include a discussion of the definitions of finite fields and groups which are essential for constructing the elliptic curve cryptosystem [41].

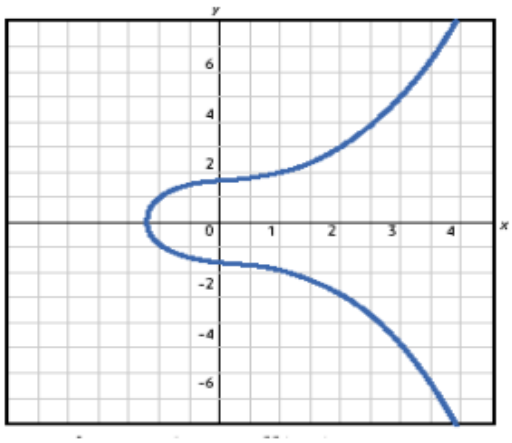


Figure 2.7: Elliptic Curve [41].

2.5.1 Finite Field

A finite field is made of a finite set of elements and two binary operations: multiplication and addition, which meet particular arithmetic properties. The number of elements in each field is the order of the finite field. A finite field of order q exists if and only if q is a prime power, if that; then basically there is only a single finite field of order q; which is denoted by Fq. However, there are lots of ways to represent the Fq elements. Some of these ways may result in better implementations of the field arithmetic in software or hardware. If (q = pm) where: q is a prime number and m is a positive integer, then p is referred as the characteristic of Fq and m is called the extension degree of Fq [42].

- Prime Field Fp

Assuming that p is a prime number, the finite field Fp is referred as a prime field, which consist of the set of integers {0,1,2,….,p-1} with the following arithmetic operations[42]:

Addition: $\boldsymbol{If}\ a\ b\ \varepsilon\ Fp\ then\ a + b = r$

Where r is the remainder when a+b is divided by p and $0 \leq r \leq p-1$ known as addition modulo p.

Multiplication: If a, b ε Fp then a.b=s, where s is the remainder when a.b is divided by p and $0 \leq s \leq p-1$ known as multiplication modulo p **Inversion:** If is a non-zero element in Fp, the inverse of modulo a modulo p_, denoted by a-1, is the unique integer c ε Fp for which a.c=1

Discriminant :

- The discriminant of an elliptic curve is similar the discriminant of a quadratic equation. If and only if the discriminant $\neq 0$ the get the proposed system has elliptic curve. For curves of the characteristic is at least 5, the condition is $4a^3+27b^2$.

2.6 MD5 Algorithm

MD5 refers to Message-Digest Algorithm 5. MD5 algorithm is co-invented by Rivets in MIT Computer Science Laboratory and RSA Security Company. The algorithm of MD5 is a non-reversible encryption. It is applied widely in large number of aspects, including encryption of information in a database, digital signature and encryption of communication information. The function of MD5 is creating large amounts of information to be compressed into a confidential format and then the private key is signed by digital signature soft (that is, any length byte string is transformed into a certain length of big integer). Following a brief explanation about the MD algorithm: it divides the input of plaintext into 512-bit blocks, each of which is subdivided into sixteen message words has 32 bit. After a number of processing tasks, the outputs of this algorithm will be made of four 32-bit message words. These four message words then are cascaded, a 128-bit hash value is generated by the algorithm and this is the required cipher text [43].

2.7 Interpolation

Interpolation schemes must model a function beyond, or between the known points, by some plausible functional form. The form should be sufficiently general so as to be able to approximate larger classes of function that might arise in practice. There is an extensive mathematical literature devoted to theorems about what sort of function can be approximation. The task is made of finding an approximate function to replace a more sophisticated one. In the case of interpolation, the function f is given at a point that is chosen randomly. For the case of function approximation, it is allowed to compute the function f at any desired point in order to enhance the approximation. The task, then, is to estimate $f(x)$ for arbitrary x by, in some sense, drawing a smooth curve through the value of $f(x_i)$. Interpolation methods can divided into two main categories [44]:

1- $Global\ interpolation.$ These methods depend on the construction of single equation that fits all points of data. Usually, this equation is a high degree polynomial one. Although the output of these methods is a smooth curve, they are prone to severe oscillation and overshoot at intermediate point.
2- $Piecewise\ interpolation.$ These methods depend on the construction of a polynomial of low degree between each pair of known data points. Polynomials have the general from:

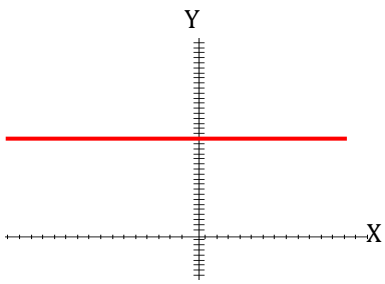
$$y = a + bx + cx^2 + dx^3 + \cdots \qquad \textbf{(2.10)}$$

The $degree$ of a polynomial shows a correspondence to the highest non-zero coefficient. For example if c is non-zero but coefficients d and higher are all zero, the polynomial is of degree 2. Following are the shapes that can be made by polynomials:

degree 0: $Constant, only\ a\ is$ non-zero.

Example: y=13

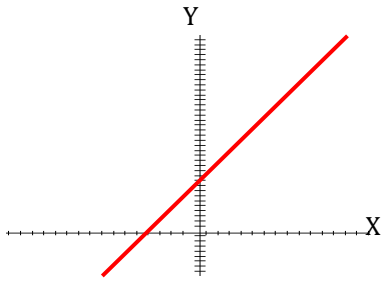
A Constant, uniquely defined by one point.



degree 1: $Linear, b$ is highest non-zero coefficient.

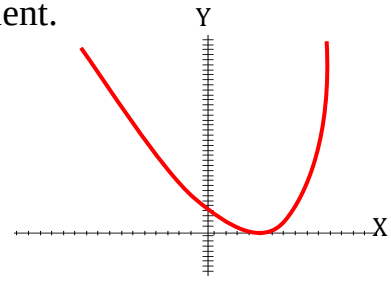
Example: $y = 3 - 12x$

A line, uniquely defined by two points.



degree 2: $Quadratic\ , c$ is highest non-zero coefficient.

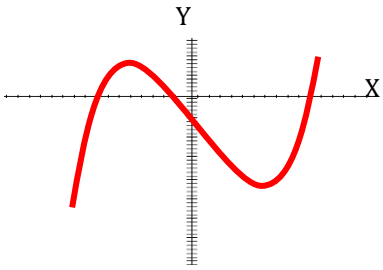
Example: $y = 3 - 12x + x^2$



A parabola, uniquely defined by two points.

degree 3: $Cubic\ , d$ is highest non-zero coefficient.

Example: $y = 3 - \frac{17}{12x} + \frac{4}{x^3}$

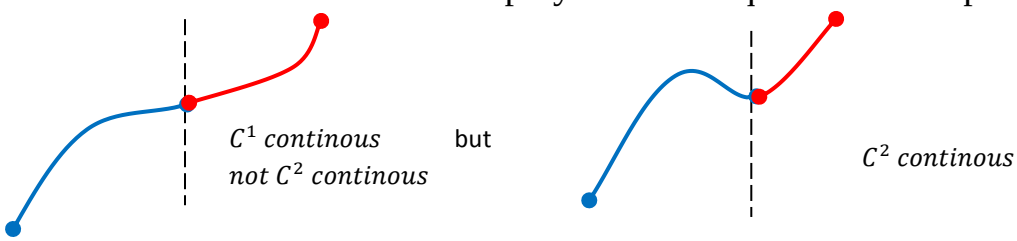


A cubic curve (which can have an inflection, at $x = 0$ in this example), uniquely defined by for points. Our spline will require to conform to the stipulations:

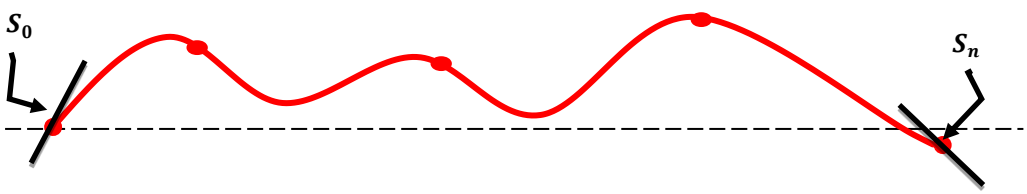
1- The value of each polynomial is equal at control points.

2- The first differential of each polynomial is equal at control points.

3- The second differential of each polynomial is equal at control points.



4- The second differential of each polynomial is continuous between control points.



Now we are almost done, but it should be noted that at the left end of the curve the C^1 and C^2equations are missed, since there is no polynomial on the left. So, necessary equations to solve the entire system are missed. We can obtain them having the user supply the slopes at the two ends. Let us call these slopes S_n and S_n [44].

2.8 Longest common subsequence

The longest common subsequence (LCS) problem has been extensively studied for several decades [45]. Finding the LCS between two strings

(sequences) can be used to measure their similarity. In the LCS problem, A = a1a2⋯am and B = b1b2⋯bn denote input sequences where ai in A, 1 ≤ i ≤ m, and bj, 1 ≤ j ≤ m, in B are characters or symbols, instead of real numbers in the time series. By deleting the characters from a sequence without changing the order of the remaining characters, we can get a subsequence. The LCS is the common subsequence of both A and B with the maximum length. For example, suppose A = BABCADAB and B = ACCEDABC. Then, the LCS of A and B is ACDAB with length 5. The LCS problem can be solved by the dynamic programming approach. Let LCS(i,j) denote the LCS length of A1..i and B1..j, where A1..i and B1..j are the prefix substrings of A and B, respectively, and 1 ≤ i ≤ m and 1 ≤ j ≤ n. LCS(i,j) can be calculated by Equation 17 [46].

$$LCS = \begin{cases} 0 & if\ i = 0\ or\ j = o, \\ LCS\ (i-1, j-1) + 1 & if\ a_i\ = b_j \\ \max[LCS\ (i-1, j), LCS(i, i.j-1] & if\ a_i\ \neq b_j \end{cases} \quad (\mathbf{2.11})$$

Chapter Three

Design and Implementation of Proposed System

Chapter Three

Design and Implementation of Proposed System

3.1 Introduction

This chapter is concerned with the implementation requirements and design considerations of the proposed system. The proposed system: (Generation of Unique Verification from Human Palm Based on Elliptic Curves) is related to various techniques which are relies on extracting palm print features as keys using security approaches. These keys are used as unique verification. Section (3.2) explains the proposed system.

3.2 The Proposed system

The main block diagram of the proposed system is shown in Figure (3.1).

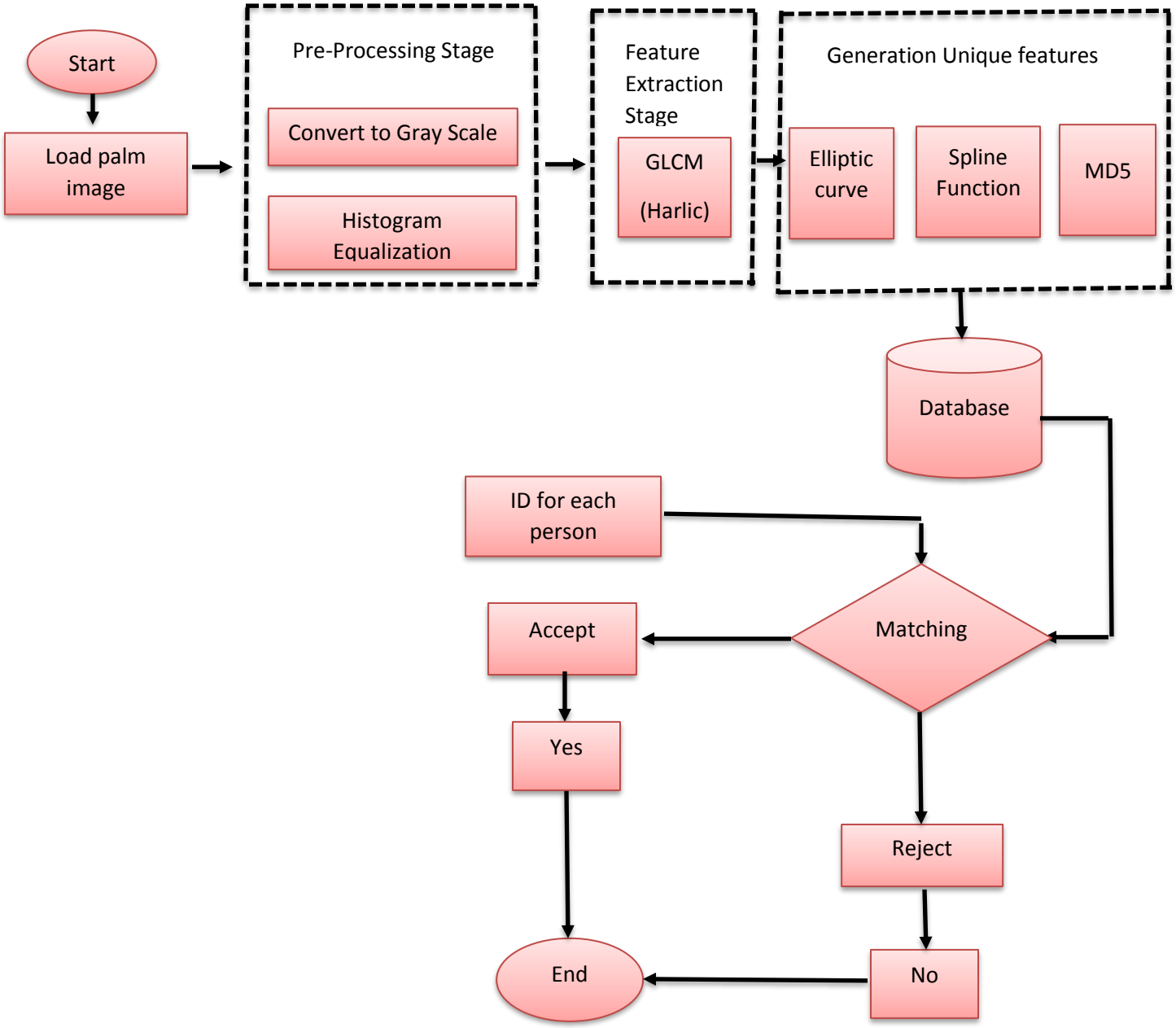


Figure (3.1): Block Diagram of the proposed system.

3.2.1 Input Stage or (Load Palm Image)

In this work, a specific class of palm images dataset is adopted which is (palm dataset) [25].

3.2.2 Image Pre-Processing Stage

The pre-processing stage is necessary to prepare the palm image for further processing. In this work, the image preprocessing consists of two steps: convert the colored image to the gray scale image and using histogram equalization as shown in subsection (i and ii).

i. Image Transformation (Gray scale Image)

In this step, each palm image in (RGB) format should be converted into gray scale image by using "luminance method" as explained in section (2.3.1). This process is described in algorithm (3.1).

Algorithm (3.1): Converting to Gray Scale Image

Inputs: Colored palm image.
Output: Gray scale palm Image

Begin
Step1: read palm image from database pixel by pixel.
Step2: apply equation (2.3) on each pixel of palm image.
Step3: return gray scale image.
End

ii. Image Histogram Equalization Method

The histogram equalization is employed in this work in order to enhance the palm image. This step is necessary to overcome the low contrast and non-uniform illumination problems, which influence the feature extraction and authentication stage. This process is described in algorithm (3.2).

Algorithm (3.2) Image Histogram Equalization Algorithm

Input: gray scale palm image
Output: Enhanced palm image (histogram equalized palm image)

```
Begin
Step1: read of grayscale palm image pixel by pixel.
Step1: get histogram from image call GrayHistogram
Step2: GraySum[0] = GrayHistogram[0];
       xmax = GraySum[0];
       for ( level = 0; level <= 254; level++)
         GraySum[level + 1] = GrayHistogram[level] +
GrayHistogram[level + 1]
          if (GraySum[level + 1] >= xmax)    xmax = GraySum[level +
1];
       end for
Step3: for (i = 0; i <= 255; i++)
          Calculate [i] =  (Graysum[i]/MAX)*255;
       End for
Step 4: for(i=0,j=0; i< Width,j< Height;i++,j++)
            Color  clr = bmp.GetPixel(i, j)
             Red1 =  calculate[clr.Red])
             b2.SetPixel(i, j, Red)
       endfor
Step5: Return the enhanced palm image.

End.
```

3.2.3 Feature Extraction stage

The aim of this stage is to extract palm code from palm image. In the proposed system the GLCM (Haralick) algorithm is used in order to extract features. The goal of the features extraction is reducing the immaterial features and extracts only the benefit features in order to generate compact but expressive digital representation of the underlying biometric trait, called

a template. The template contains only the salient discriminatory information that is essential for recognizing the person. Haralick algorithm describes the correlation in intensity of pixels that are next to each other in space. Haralick are derived from the co-occurrence matrix (a well-known statistical technique for texture feature extraction). It contains information about how image intensities in pixels with a certain position in relation to each other occur together.

In Haralick algorithm the edges of the palm image are taken. In the GLCM the inner points of the hand palm image are taken at any angle any angle as shown in figure (3.2). The inputs to Haralick feature algorithm are all image samples for each person in database. For example, if each person has 4 samples image [*w*,*h*] for his palm image then apply on its samples Haralick equations which is discussion in section (2.4.3) to produced 4 images ($HI_1[w,h]$, $HI_2[w,h]$, $HI_3[w,h]$,$HI_4[w,h]$) ,these image consists from two value ('0' represents black pixel or 255 represents white pixel) .Interrupted the (,$HI_2[w,h]$,$HI_3[w,h]$,$HI_4[w,h]$) images by placing these images in the order of one over the other to produced set of pixels called Haralick feature pixels HFP, the HFP value =0 if any of interrupted pixels = 0 and in other wise HFP value =255 if all interrupted pixels =255. For example, if the $HI_1[0,2]$= 0,$HI_2[0,2]$=255 ,$HI_3[0,2]$=255,$HI_4[0,2]$=255 then result pixel =0 and if $HI_1[1,2]$=255,$HI_2[1,2]$=255 ,$HI_3[1,2]$=255,$HI_4[1,2]$= 255then result pixel =255 .The HFPs are set of randomly pixels represented as one image called sample haralick image (SHI[*w*,*h*]) ,the SHI must be unique doesn't similar no one of other sample images for all personal that are stored in data based. Algorithm (3.3) describes the Haralick feature algorithm, and figure (3.3) represents an example of Haralick Feature algorithm.

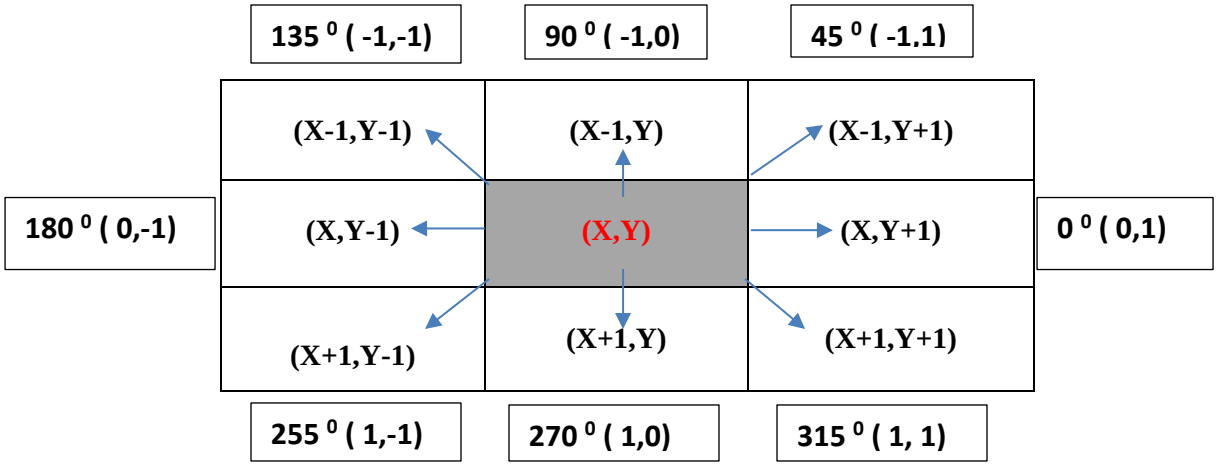


Figure (3.2): Direction angles for the GLCM

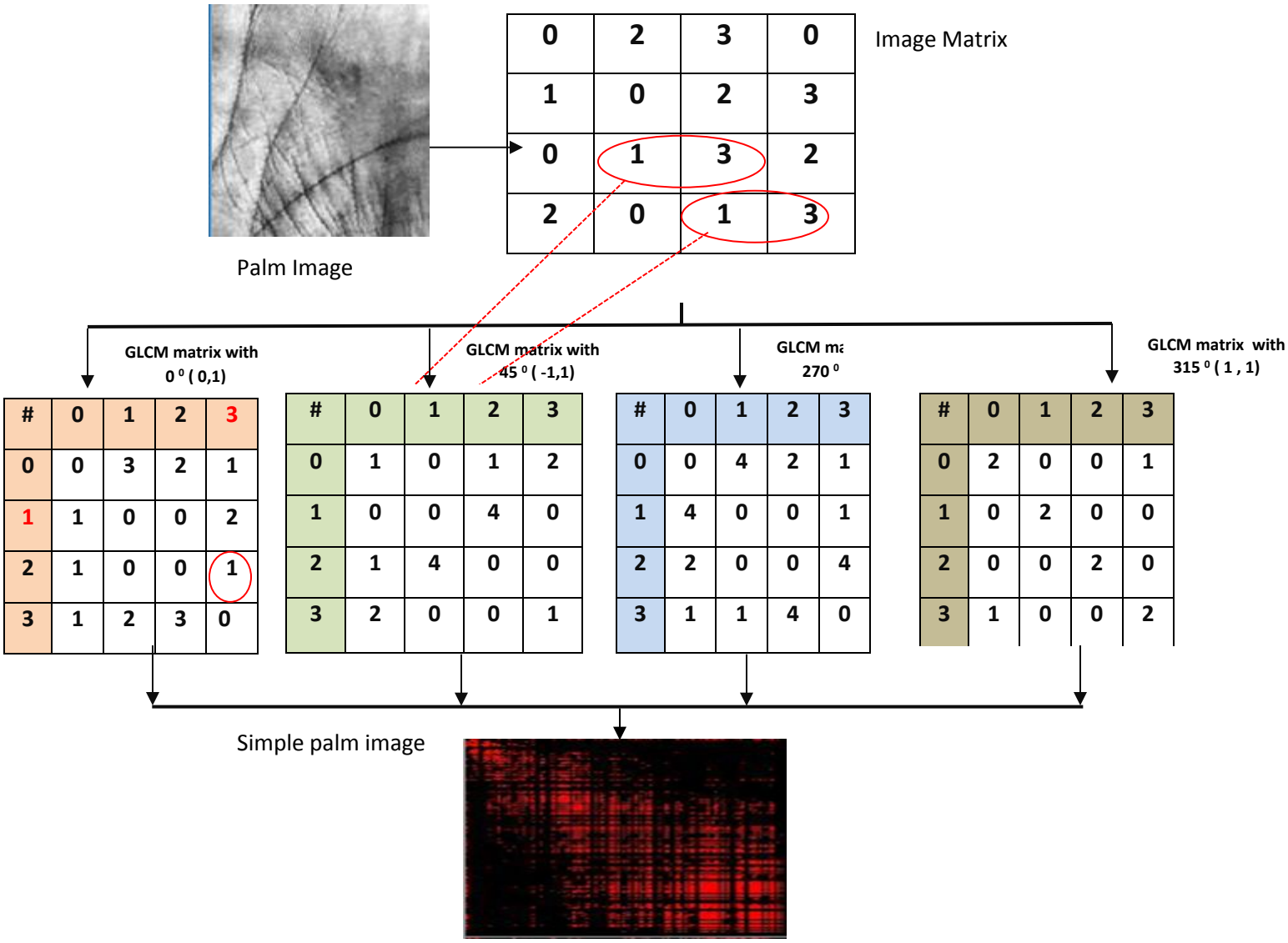


Figure (3.3): Apply the direction of the GLCM angles on palm

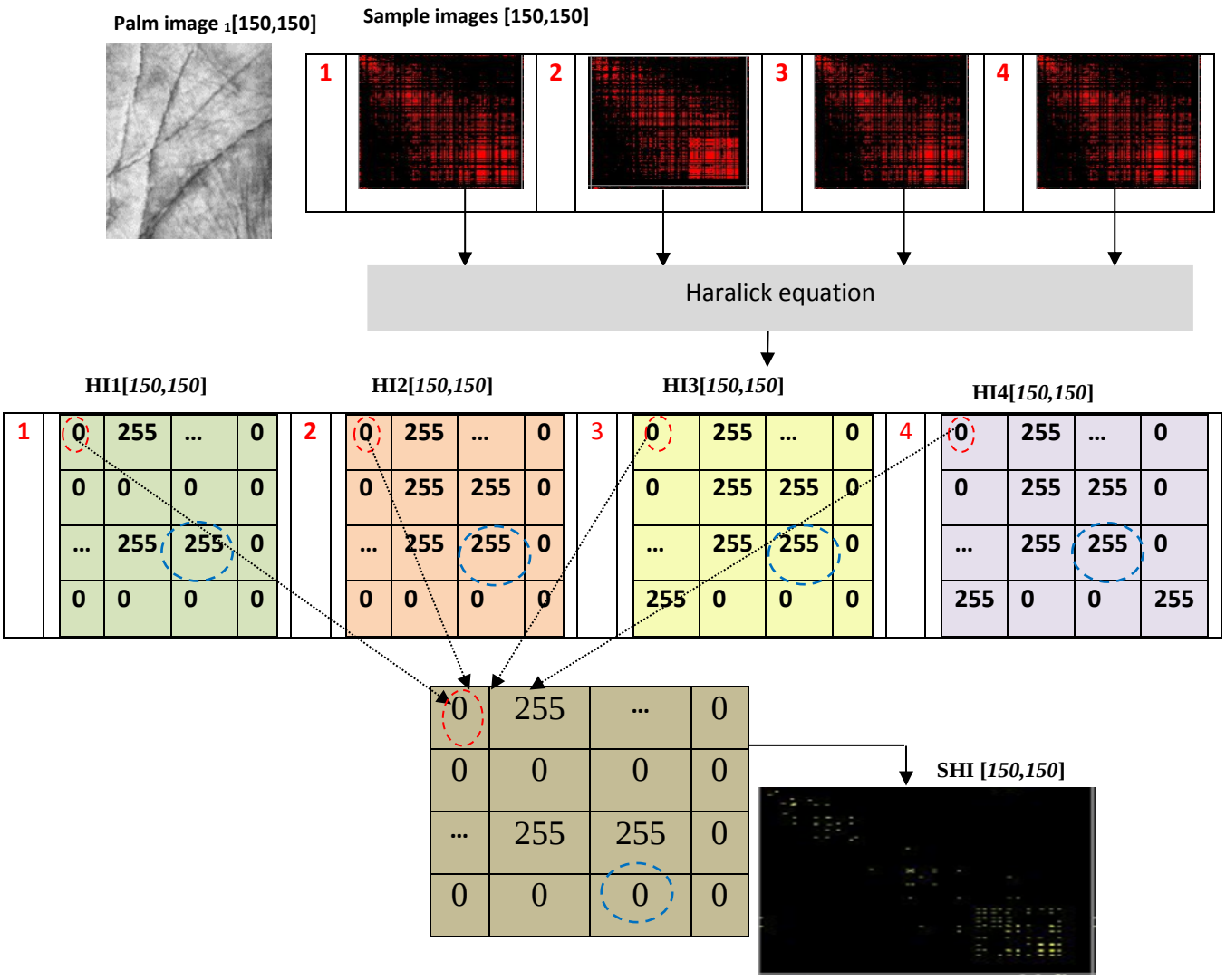


Figure (3.4): Example of the Haralick Feature Algorithm

Algorithm (3.3): Haralick Feature Algorithm

Input: All image samples for each person in database
Output: Point coordination for each person (unique Coordinates)

Begin

```
Step1: Put image samples of all Persons in data base
       i=0
        While ( all image Person samples in database not null) do
       {
         Sample1, sample 2 ,sample 3, sample 4
         Apply Equations (2.7 , 2.8 , 2.9 , 2.10)
        Intersection-array(i) = Intersection Coordinates (Smple1, Smple2,
                                                          Smple3, Smple4)
          i = i+1
         }
Step2: Detetrmain unique Coordinates extraction Intersection_array
          While (each Coordinates in Intersection_array from each sample) do
           {
             match =false
             get x_Coordinates
            While (each Coordinates in Intersection_array)) do
              {
                 get y_ Coordinates
                 if  x_ Coordinates = y_ Coordinates then  match=true
              }
             If match =flase  then
             unique_Coordinates [i].add(x_Coordinates)
          } }
end
```

3.2.4 Generate Digital Signature Stage

In this stage digital signature is generated using (elliptic curve, cubic spline function, and MD5).

i- Elliptic Curve

The points obtained from an Haralick algorithm are considered as input to the elliptic curve. The elliptic curve points must be belong to specific field called Galois field or (GF) ,these points are denoted as

(a,b,p) ,where p is prime number and the other point (a,b) must be satisfy the four condition as illustrated in algorithm (3.4).

Algorithm (3.4) Elliptic Curve Algorithm

Input: unique -Coordinates for each Person
Output: Determination fields for each Person call fields_ Person_ Coordinates

```
Begin
Step 1:  Get unique coordinates from Algorithm (3.3)
Step 2:  While (each Coordinates in unique -Coordinates ) do
         {
           Generation random (n)
            p = get max value from Coordinates
            a= select first Coordinates. x
            b= select first Coordinates. y
            Find composite  (p,n)
           If composite (p,n) then end  // *p is not prime
           Find discriminant All elliptic curves over a finite field
            If   discriminant(a,b,p) =0 then End // * the points not an elliptic
curves
          Get square root mod prime
           x=1
             while (y==0)
               Get using Weierstrass function (a,b,x)
               If y=0  then x=x+1
           End while
          Get x,y in elliptic curves using  Multiplication
           k=1
           do
           set point (x=0,y=1)
          set point (xx=0,yy=1)
          If Bitwise-AND (k,1) then
            xx=x
            yy=y
          End if
           k>>=1    //* >>= represent half  of value
           while (k<>0)
             xx.x=Addition(a,xx,yy)    // point addition
             xx.y=Addition2(a,xx,yy)  // point doubling
             If Bitwise-AND (k,1) then
```

```
            x= Addition((x,y),(xx,yy))  : y= Addition1((x,y),(xx,yy))
          End if
         k>>=1
         End while
        IspointAt (x,y)  :  k=k+1
        while (not(x=0 and y=1))
Step 3: End Algorithm
```

In algorithm (3.4), step 2 after get all unique point from Haralick which are denoted (a, b, p) .Firstly, check the parameter p if its prime number or not by follow two steps :

I- generate random number (n), where the random number using as seed in composite function.

II- apply the composite function. The composite number n is a positive integer n>1 with condition is not a prime number so can be formed the composite number as multiplying two smaller positive.

After check the parameter p is prime then must be testing the parameters (a,b) if are discriminant then they are elliptic curve , can be diriffion the discriminant which is define $4a^3 + 27b^2 \neq 0$.

The Weierstrass function is using to find relationship between points of solution which are extracted from the discriminant function based on square root mod prime. The aims to create a function that is not differentiable anywhere, without sacrificing continuity at even a single point, so the Weierstrass function is perfect example of the continue elliptic function.

A modular square root **r** of an integer number **a** modulo an integer **m** greater than 1 is an integer, in this work the modulus is prime

$$r^2 \equiv a \pmod{m} \qquad (3.1)$$

Multiplication operation of the elliptic curve point is the process of successively adding a point along an elliptic curve to itself repeatedly. It is used in elliptic curve cryptography (ECC) as a means of producing a one-way function. In this step using bitwise-and operation to perform manipulation of individual bits of a number.

ii- Cubic Spline Function

After extracting points from elliptic curve , this is considered control point through which coefficient (a,b) are obtained. In this step using a cubic spline function to obtain values between the points (which are practically specific) and the cuboid interpolation is a special case for the key interpolation and has a feature that is more smooth and characterized by flexibility, derivation, simple curve and control point. This process is shown in algorithm (3.5).

Algorithm (3.5) Cubic Spline function

Input: fields_ Person_Coordinates
Output: coffiction A,B for each Person call spline coffiction A, B.

```
Begin
Step1: get keypointfrom  Person_Coordinates
        While (each Coordinates in fields_ Person_Coordinates)) do
        {
          Control point.add(Coordinates)
        }
  Step2: determine coffiction base on spline function  call algorithm in equation 2-16

end
```

iii- MD5 Hashing

The input of the MD5 Hash is the coefficients that extract from algorithm (3.5). The idea of the MD5 hash is that it is a hash of the entire file will be different if any bit is changed. When you download a file, you can get the MD5 hash of it on your own machine, and comparing that to the MD5 stored previously, so you can reassure yourself you have the correct unmodified file. Algorithm (3.6) describe the MD5 Hashing algorithm.

Algorithm (3.6) MD5 Hashing

Input:coefficients A,B for each Person (spline coefficients A, B).
Output: MD5 coefficients A,B coefficients for each person

Begin

Step1: read all persons coefficients A and B

While (each coefficients A and B in spline coefficients A and B).

{

MD5- A= apply steps of MD5 algorithm in section (2-10), on coefficient A.
MD5- B= apply steps of MD5 algorithm in section (2-10), on coefficient B.

Step2: save MD5 coefficients A,B for each person in data base .

end

Chapter Four

Results and Analysis

Chapter Four

Results and Analysis

4.1 Introduction

This chapter is dedicated to present the results and tests that evaluate the proposed model: (embedding and extracting) stages. An initialization is given in section (4.2). The details of the results are presented in section (4.3).

4.2 Initialization

The proposed system is implemented using Microsoft visual studio (2013) by the C# programming language with a laptop computer (core i5) and (windows 10) as an operating system. The data set is palm dataset of 100 subjects, with at least 12 images per subject. The palm dataset contains Gray scale images.

4.3 Results of the proposed system

The results of the proposed model will shown sequentially in subsections: (4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.5, 4.4 and 4.5).

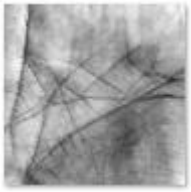
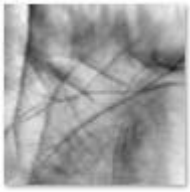
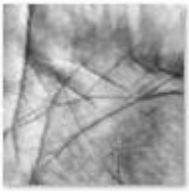
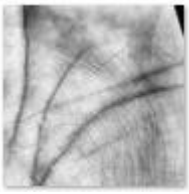
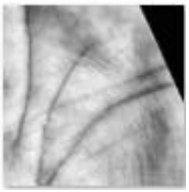
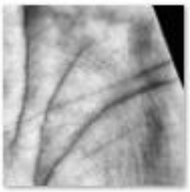
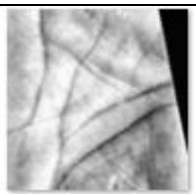
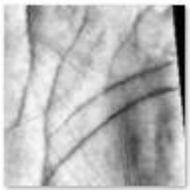
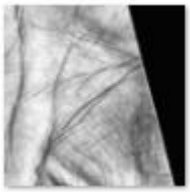
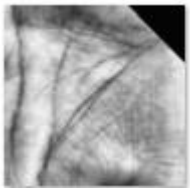
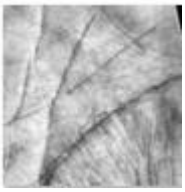
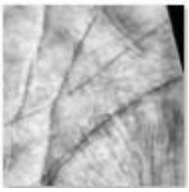
4.3.1 Results of Palm Image Preprocessing

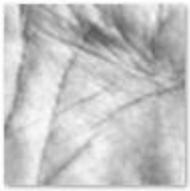
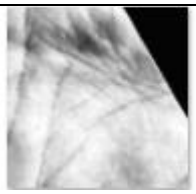
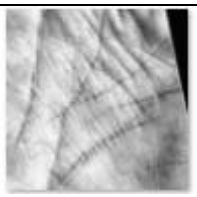
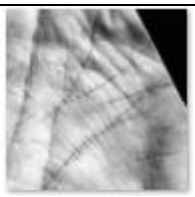
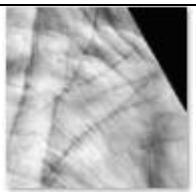
The image preprocessing steps includes (RGB to Gray scale conversion, image enhancement (histogram equalization)).

i- Loading Original Images

In this step, the number of loading original images are ten as shown in figure (4.1).

Figure (4.1): Original Images of Palm Data Set.

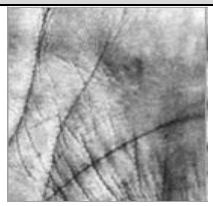
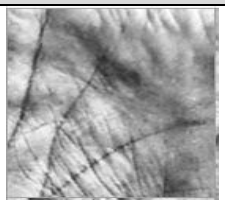
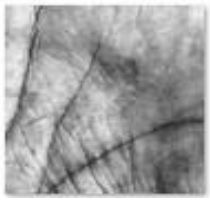
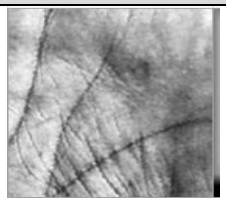
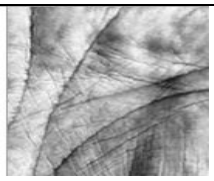
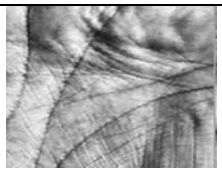
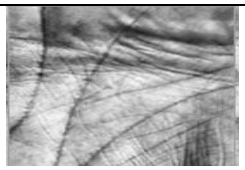
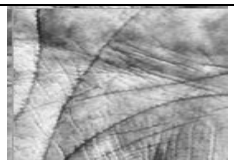
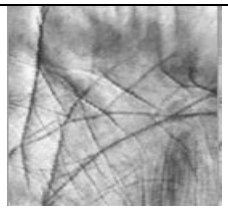
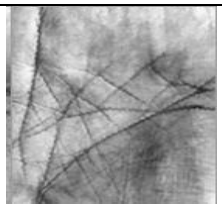
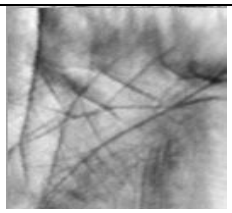
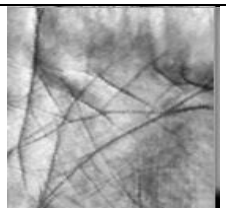
Person	Sample1	Sample 2	Sample 3	Sample 4
1				
2				
3				
4				
5				
6				
7				

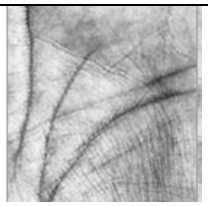
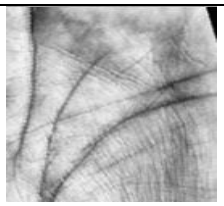
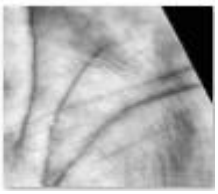
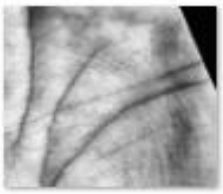
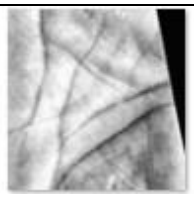
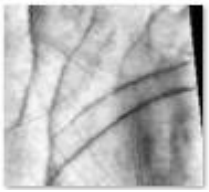
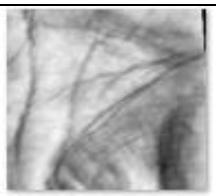
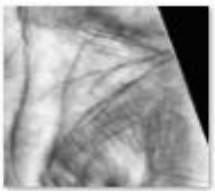
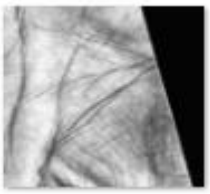
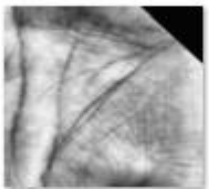
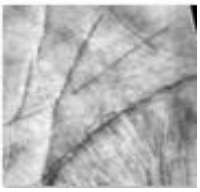
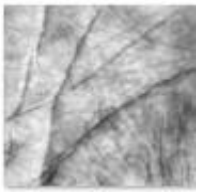
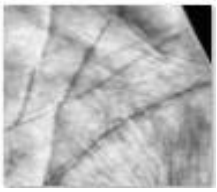
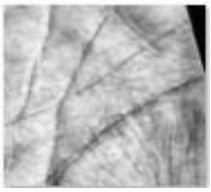
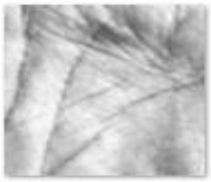
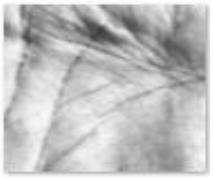
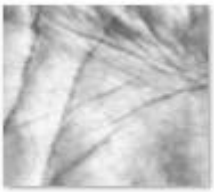
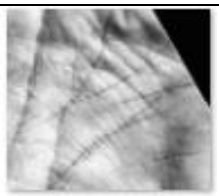
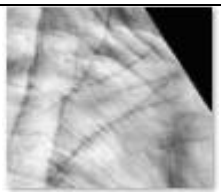
8				
9				
10				

ii- RGB to Gray Scale Conversion

Converting the color format of the palm image from RGB to Grayscale is shown in figure (4.2).

Figure (4.2): Images of Converted to Gray Scale Images.

Person	Sample1	Sample 2	Sample 3	Sample 4
1				
2				
3				

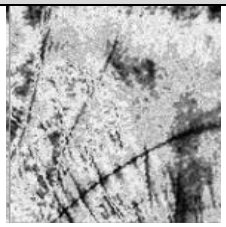
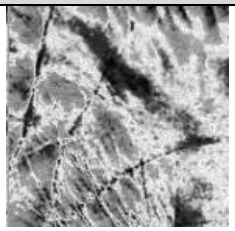
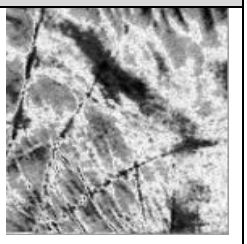
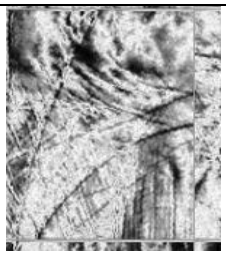
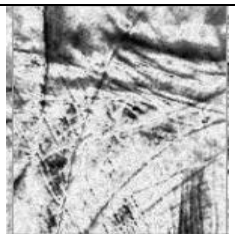
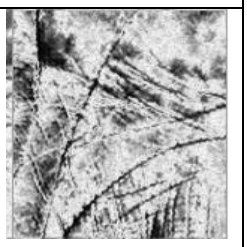
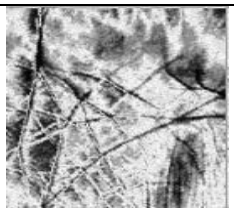
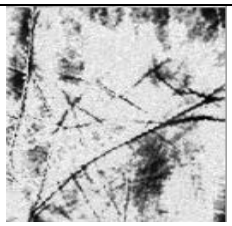
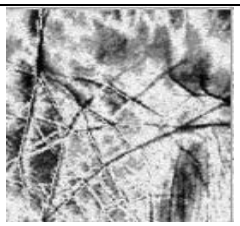
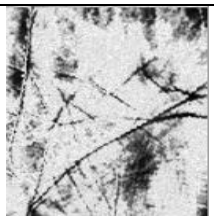
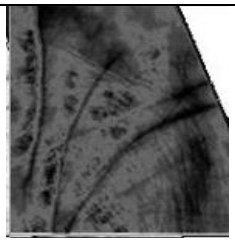
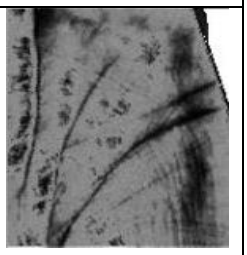
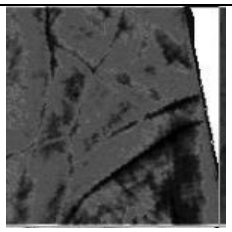
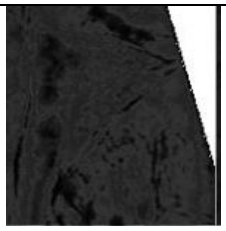
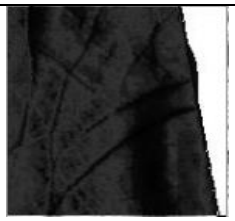
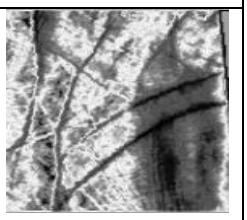
4				
5				
6				
7				
8				
9				
10				

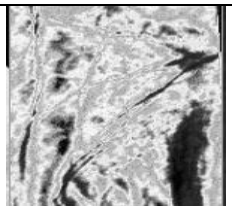
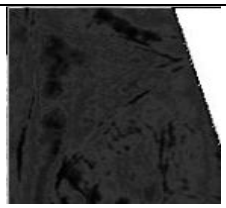
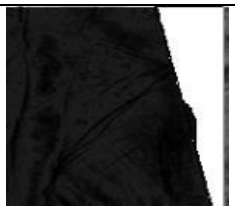
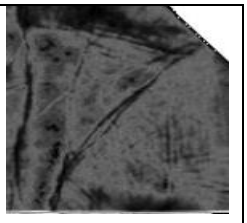
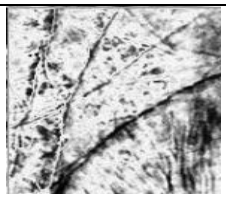
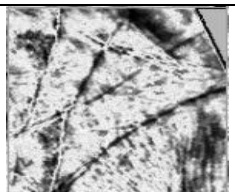
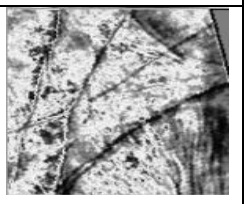
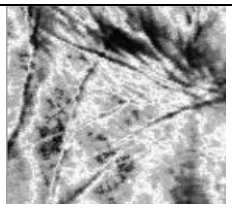
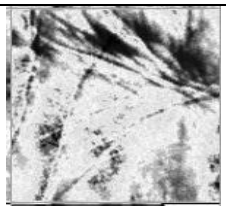
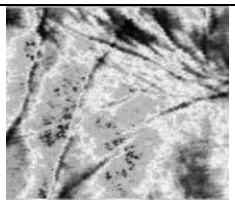
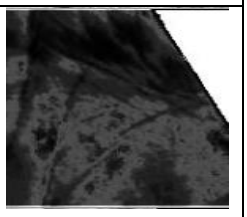
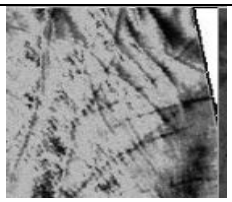
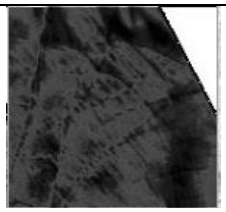
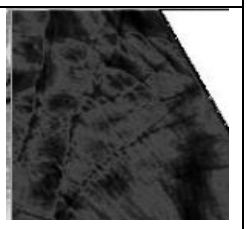
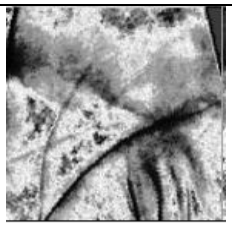
iii- Enhancement with Histogram Equalization

In this step, because most of the palm images have low contrasts and also may have non-uniform brightness due to the changes in lights

sources positions, the proposed enhancement method (histogram equalization) of palm image is very important. This process is presented in figure (4.3).

Figure (4.3): Images after Enhancement with Histogram Equalization.

Person	Sample1	Sample 2	Sample 3	Sample 4
1				
2				
3				
4				
5				

6				
7				
8				
9				
10				

4.3.2 Results of Haralick Algorithm

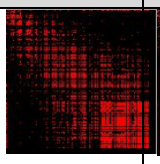
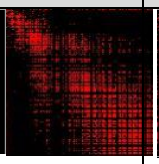
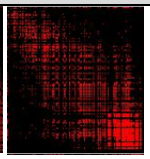
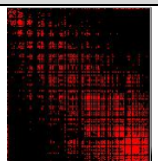
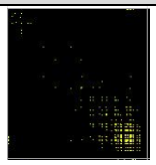
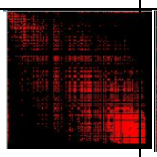
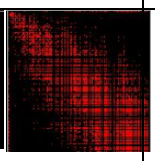
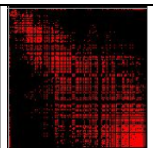
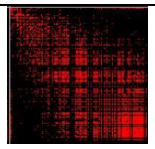
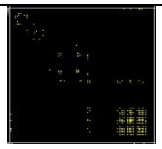
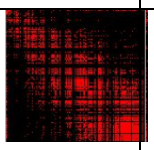
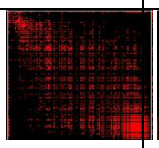
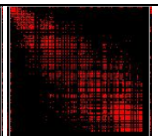
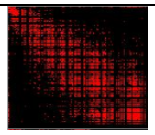
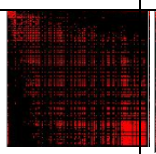
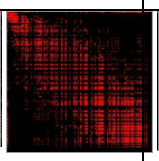
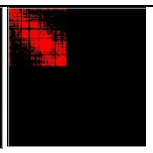
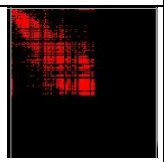
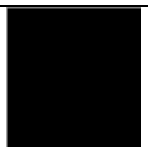
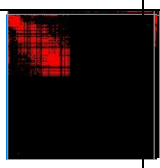
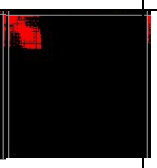
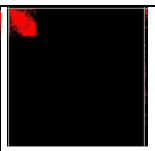
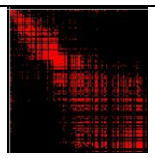
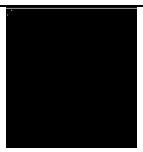
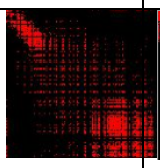
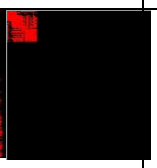
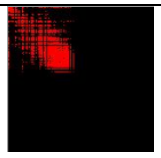
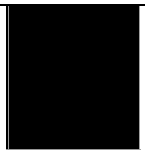
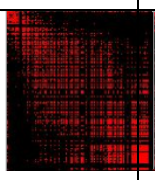
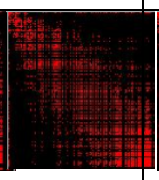
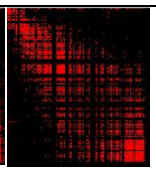
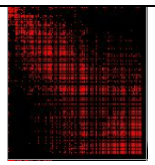
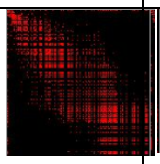
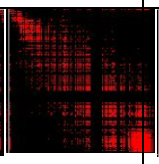
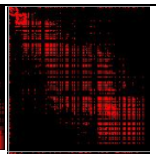
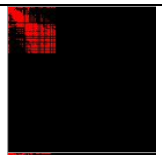
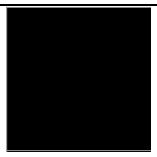
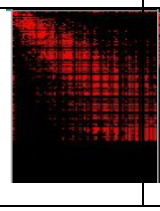
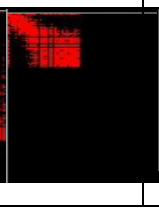
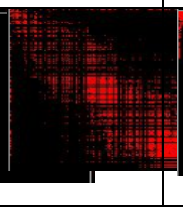
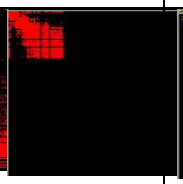
The intersection points are found in two steps:

1. Cross the points between the samples.

2 - Cross the points between the Data Set.

The images of intersection points are shown in figure (4.4).

Figure (4.4): Intersection points of Haralick Algorithm.

Person	Sample1	Sample2	Sample3	Sample4	Intersection for all samples	Intersection for all data set
1						
2						
3						
4						
5						
6						
7						
8						
9						

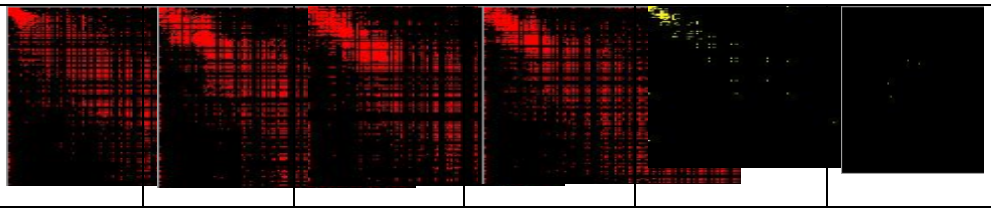
10	

Figure (4.5): Details of the intersection points in all Dataset

Person	No. of point	Coordinates of Point
1	108	(0,106)_(0,113)_(11,22)_(15,30)_(22,11)_(25,30)_(25,31)_(25,41)_(30,15)_(30,25)_(30,35)_(31,25)_(31,31)_(35,30)_(41,25)_(41,43)_(43,41)_(50,67)_(67,50)_(67,79)_(68,68)_(68,90)_(69,79)_(73,113)_(79,67)_(79,69)_(79,79)_(90,68)_(90,90)_.....
2	180	(0,126)_(0,135)_(0,136)_(0,138)_(7,14)_(14,7)_(25,27)_(27,25)_(30,34)_(34,30)_(41,69)_(50,50)_(50,53)_(50,70)_(50,71)_(52,52)_(52,73)_(52,81)_(53,50)_(53,70)_(53,71)_(53,81)_(56,81)_(69,41)_(69,71)_(70,50)_(70,53)_(70,71)_(71,50)_(71,53)_(71,69)_(71,70)_(73,52)_(73,81)_(74,81)_(81,52)_(81,53)_(81,56)_(81,73)_(81,74)_(81,112)_(81,117)_.....
3	96	(0,130)_(0,140)_(15,23)_(23,15)_(23,29)_(29,23)_(29,29)_(29,33)_(33,29)_(67,80)_(76,80)_(76,89)_(80,67)_(80,76)_(80,80)_(80,86)_(80,89)_(80,96)_(80,100)_(86,80)_(86,89)_(87,87)_(89,76)_(89,80)_.....
4	8	(6,15)_(10,15)_(15,6)_(15,10)_(20,33)_(28,33)_(33,20)_(33,28)_
5	50	(0,5)_(1,6)_(3,8)_(5,0)_(6,1)_(6,6)_(6,9)_(6,11)_(6,14)_(8,3)_(8,21)_(8,24)_(9,6)_(10,13)_(11,6)_(11,21)_(11,24)_(13,10)_(13,18)_(14,6)_(14,21)_(14,23)_(14,24)_(18,13)_(18,24)_(21,8)_(21,11)_(21,14)_(21,24)_(21,25)_(21,26)_(23,14)_(23,24)_(23,26)_.....
6	8	(4,11)_(11,4)_(11,16)_(13,15)_(13,16)_(15,13)_(16,11)_(16,13)_
7	125	(0,7)_(0,47)_(1,7)_(3,7)_(7,0)_(7,1)_(7,3)_(8,30)_(15,33)_(16,21)_(1

		6,33)_(17,33)_(21,16)_(21,33)_(27,33)_(27,35)_(27,53)_(30,8)_(30,38)_(30,58)_(33,15)_(33,16)_(33,17)_(33,21)_(33,27)_(33,35)_.....
8	18	(5,9)_(9,5)_(9,13)_(13,9)_(14,20)_(17,28)_(18,28)_(18,40)_(20,14)_(28,17)_(28,18)_(28,40)_(40,18)_(40,28)_(40,40)_(40,44)_(43,43)_(44,40)_
9	28	(5,13)_(7,12)_(8,13)_(12,7)_(12,19)_(12,24)_(12,28)_(13,5)_(13,8)_(13,17)_(17,13)_(17,19)_(17,35)_(19,12)_(19,17)_(19,19)_(19,28)_(21,35)_(24,12)_(24,35)_(28,12)_(28,19)_(35,17)_(35,21)_(35,24)_(35,37)_(37,35)_(42,42)_
10	41	(0,81)_(0,125)_(2,10)_(6,7)_(7,6)_(7,9)_(9,7)_(10,2)_(12,15)_(14,28)_(15,12)_(15,28)_(16,28)_(23,28)_(23,30)_(25,28)_(28,14)_(28,15)_(28,16)_(28,23)_(28,25)_(28,35)_(30,23)_(35,28)_(35,38)_(35,48)_(35,51)_(38,35)_(48,35)_(48,48)_(48,51)_(48,69)_(51,35)_(51,48)_(51,69)_(51,81)_(69,48)_(69,51)_(81,0)_(81,51)_(125,0)_

4.3.3- Results of Elliptic Curve

In this stage algorithm (3.4) is applied where all the points that belong to the Galois Field are extracted using (a, b, q) coefficients. These coefficients are selected for every person in dataset.

Figure (4.6): Results of Elliptic curve.

Sample	Max x	Max y	prime	a	b	Coordinates of points	No. of Point
1	127	127	127	0	113	1,34|69,90|88,111|111,19|94,123|104,75|71,75|76,40|75,82|103,44|13,47|108,30|79,52|20,30|29,12|119,95|89,125,.....	127
2	139	139	139	0	135	1,54|32,88|56,74|11	133

						2,32|33,40|8,62|15,69|105,53|49,32|102,56|103,105|70,120|117,107|92,59|,…… ……	
3	127	127	127	0	140	1,34|69,90|88,111|111,19|94,123|104,75|71,75|76,40|75,82|103,44|13,47|108,30|79,52|20,30|,…… …	127
4	23	23	23	1	6	1,13|10,21|2,4|9,13|13,10|22,21|16,1|14,2|3,17|0,12|0,11|3,6|14,21|16,22|22,2|13,13|9,10|2,19|10,2|1,10|0,1|	21
5	13	13	13	11	4	1,9|10,10|11,0|10,3|1,4|0,1|	6
6	137	137	137	0	47	3,38|133,42|88,128|95,58|117,104|105,76|54,80|20,85|106,56|6,20|,…….	138
7	43	43	43	9	5	3,69|17,40|45,18|41,71|47,67|50,36|12,1|52,66|26,65|53,0|26,8|,……..	47
8	37	37	37	7	12	2,16|6,14|20,30|22,26|4,20|35,29|36,2|29,6|7,16|28,21|28,16|7,21|29,31|36,35|35,8|4,17|22,11|20,7|6,23|2,21|0,1|.	21

9	23	23	23	0	125	1,9|14,8|11,13|13,0|11,10|14,15|1,14|0,1|	8
10	73	73	73	4	18	3,69|17,40|45,18|41,71|47,67|50,36|12,1|52,66|26,65|53,0|26,8|52,7|12,72|50,37|47,6|41,2|45,55|17,33|3,4|0,1|	20

4.3.4 Results of Spline function

The extracted points from elliptic curve are considered control points. In this step, using a cubic spline function to obtain values between the points (which are practically specific). As shown in figure (4.7).

Figure (4.7): spline function.

person	No. of point	a	b
1	127	-14.18605, 6.124083, 106.5779, -104.5593, 27.31482, -10.57935, 13.07813, -44.42384, 59.68615, -86.92306, 20.44698, -6.366536, 48.28447, -0.7883043, -167.1979, 18.05268, 68.01254,……	-28.37208, 16.64657, -91.49664, 148.4581, -32.28146, 20.46145, -32.96021, 22.69822, 5.990127, -0.2162808,…..

2	133	17.84187, 12.98322, -9.514316, -34.69373, -4.341859, 0.3689356, 72.81547, -10.82032, -26.51935,…	35.68375, 6.447422, -18.46768, -34.10386, -2.788875, 0.847086, 32.6345, -18.41019, -28.43421,….
3	127	40.21375, 63.31116, -26.17256, -82.75325, 0.4329845, 20.76304, 11.13592, -1.101266,….	80.42748, 28.78274, -49.52773, 50.84243, 0.2798104, 23.07648, 13.10743, -8.234118,….
4	21	6.102664, 10.4385, -4.938031, 1.939002, -15.36695, 23.54535, -0.6631657, -2.310248,….	12.20533, -23.69348, 11.41945, -1.463712, 8.586807, -23.14539,……
5	6	4.501919, 1.117156, -1.615244, 8.358788, 0.6003506	9.003839, -14.40082, -0.26823, 7.871548, 0.3001751.
6	138	-67.21523, 17.30737, 25.84822, -28.91806, 23.18693, -46.76236, 6.981673, 28.08065, -33.38957,…..	-134.4305, 146.9169, -93.56727, 54.05629, -2.535564, -13.83586, 5.348114, 30.25381,….
7	47	-1.84634, -0.3256814, -	-3.692683, -0.1722087, -

		12.55647, -3.787863, 6.367307, -1.073861, 27.83784, -6.948482,…..	24.47067, 5.373386, -3.896813, 9.091763, -4.460224, -8.585071, 22.46942,
8	21	-0.8925412, -17.0217, 1.797429, -13.08818, 0.8526874, 7.681472, -3.406361, 4.886034, 7.032364,….	-1.785083, 26.47091, 0.4991274, -11.79125, 32.08057, -28.98942, -0.9662569, -3.4699, 23.5011, -0.7147685,…
9	8	6.263318, 0.1548679, 15.10294, -12.01496, 2.115808, 7.926384, 4.592462,	-12.52664, 4.067726, -10.4012, -2.445189, 1.902427, 7.407538, 2.29623,
10	20	1.996907, -14.48403, -31.66559, 2.220465, 7.573535, -22.12785, …….	3.993814, -36.29325, 66.11638, 1.424038, 3.439703, -42.34576, 28.24706, 14.2001, -61.05202, 4.209308, -6.360431,…..

The cubic spline curves for persons in figure (4.7) are described in figure (4.8).

4.3.5 Results of MD5

In this stage, the digital signature is being extracted through coefficient (a, b) for every person in dataset. Algorithm MD5 is applied for these coefficients as shown in figure (4.8).

Figure (4.8): Results of MD5 algorithm.

Personal	Massage coefficient A	Massage coefficient b
1	-14.18605, 6.124083, 106.5779, -104.5593, 27.31482, -10.57935, 13.07813, -44.42384, 59.68615, -86.92306, 20.44698, -6.366536,….	-28.37208, 16.64657, -91.49664, 148.4581, -32.28146, 20.46145, -32.96021, 22.69822, 5.990127,…..
2	17.84187, 12.98322, -9.514316, -34.69373, -4.341859, 0.3689356, 72.81547, -10.82032, -26.51935, -4.830574,….	35.68375, 6.447422, -18.46768, -34.10386, -2.788875, 0.847086, 32.6345, -18.41019, -28.43421,,……
3	40.21375, 63.31116, -26.17256, -82.75325, 0.4329845, 20.76304, 11.13592, -1.101266, -69.87677,…..	80.42748, 28.78274, -49.52773, 50.84243, 0.2798104, 23.07648, 13.10743, -8.234118, 21.80098,….
4	6.102664, 10.4385, -4.938031, 1.939002, -15.36695, 23.54535, -0.6631657, -2.310248,,……	12.20533, -23.69348, 11.41945, -1.463712, 8.586807, -23.14539, -0.525458, 22.2118, 0.886226,,……..
5	4.501919, 1.117156, -1.615244, 8.358788, 0.6003506.	9.003839, -14.40082, -0.26823, 7.871548, 0.3001751
6	-67.21523, 17.30737, 25.84822, -28.91806, 23.18693, -46.76236, 6.981673, 28.08065,……	-134.4305, 146.9169, -93.56727, 54.05629, -2.535564, -13.83586, 5.348114, 30.25381, -111.2486,…..
7	-1.84634, -0.3256814, -12.55647, -3.787863, 6.367307, -1.073861, 27.83784, -6.948482,,…..	-3.692683, -0.1722087, -24.47067, 5.373386, -3.896813, 9.091763, -4.460224, -8.585071, 22.46942,,……
8	-0.8925412, -17.0217, 1.797429, -13.08818, 0.8526874, 7.681472, -3.406361, 4.886034, 7.032364,	-1.785083, 26.47091, 0.4991274, -11.79125, 32.08057, -28.98942, -0.9662569, -3.4699, 23.5011,,…..

	0.714767,,…..	
9	-6.263318, 0.1548679, 15.10294, -12.01496, 2.115808, 7.926384, 4.592462	-12.52664, 4.067726, -10.4012, -2.445189, 1.902427, 7.407538, 2.29623
10	1.996907, -14.48403, -31.66559, 2.220465, 7.573535, -22.12785, -54.14798, 13.52964, 23.88219, -9.579548, 4.502486,….	3.993814, -36.29325, 66.11638, 1.424038, 3.439703, -42.34576, 28.24706, 14.2001, -61.05202, 4.209308, -6.360431,……

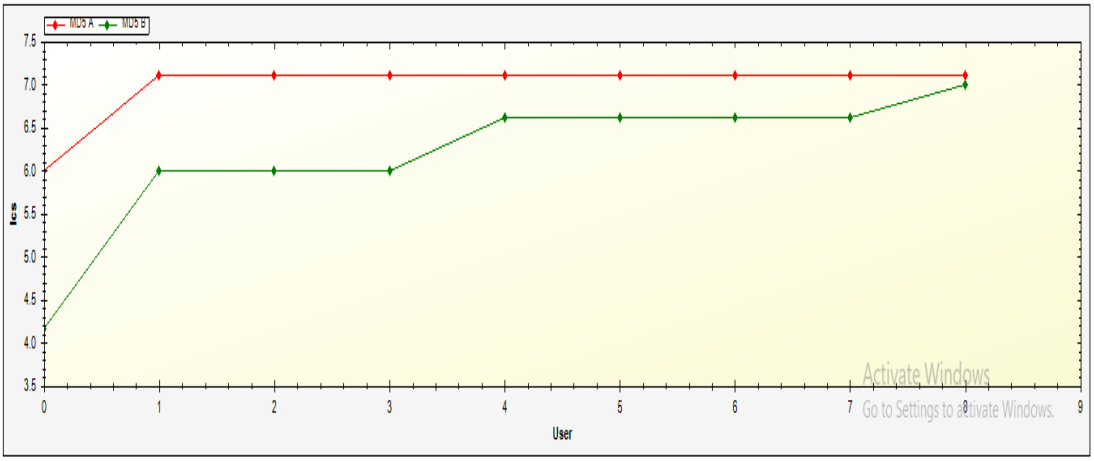
4.4 Performance Test

The performance test is evaluated strength of proposed system against plain text attack based on LCS algorithm. Figure (4.9) and figure illustrated results of performance test represents congruence ratio between MD5 for 10 users using coefficient MD5 -A and coefficient MD5 -B.

Figure (4.9): Results of Performance Test of the MD5 user using coefficient MD5 -A and coefficient MD5 -B.

	User [1]	User [2]	User [3]	User [4]	User [5]	User [6]	User [7]	User [8]	User [9]	User [10]
User[1]		4.1322	2.4793	1.5625	2.7778	0.8264	0.0000	6.0000	0.6944	0.000
User[2]	4.9587		1.2346	1.6529	7.1006	1.6529	2.9586	4.0000	2.4793	3.305
User[3]	4.1322	0.0000		4.9383	3.3058	1.0000	0.0000	0.8264	0.0000	0.826
User[4]	1.5625	0.8264	3.7037		0.0000	0.0000	1.6529	2.0000	0.0000	3.000
User[5]	2.0833	7.1006	4.1322	1.0000		0.0000	1.2346	1.7751	0.0000	2.777
User[6]	1.6529	1.6529	1.0000	0.0000	0.0000		0.0000	4.9587	2.0408	2.469
User[7]	1.0000	3.5503	0.6944	1.6529	0.0000	0.0000		4.1322	0.0000	1.388

User[8]	6.0000	4.0000	1.6529	2.0000	1.7751	5.7851	4.1322		1.3889	1.652
User[9]	0.6944	2.4793	0.0000	0.0000	2.0000	2.0408	0.0000	1.3889		3.472
User[10]	0.0000	3.3058	1.6529	3.0000	2.7778	3.7037	1.3889	1.6529	4.8611	



Figure(4.10): Performance Test results of the MD5 user using coefficient MD5 -A and coefficient MD5 -B.

Figure (4.11): Result of MD5 algorithm using Coefficient MD5-B**.**

id	Message on design
0	E63F157491DC01B45189B33945A28CC3
1	C3F76C2C999E039C55DFDC1D79092CA1
10	8E0D341B6AF731AF246B1759411E2D88
11	2CA2DEECC0A2E1F69F653D722FDF3D16
2	C2EB3F96646D41ECC3B49C75447D0525
4	97C8C2AB891A9E18AEC14351A8B08ABA
5	B1FA804D57628F3921EA8FDD170C62A4
6	B3329061341E30C6C25043AFAE06A9D0

7	401456033F452CD0A92D411639320427
8	45B6409C70EF79D3F0EB4C872AF415FA

Chapter Five

Conclusions and Suggestions for Future Works

Chapter Five

Conclusions and Suggestions for Future Works

5.1 Conclusions

Several conclusions have been deduced from the obtained results of the proposed model, such as:

1. The preprocessing stage in the proposed system gave an accurate results that made palm images more distinguishable.
2. The GLCM (Haralick) algorithm can extract important features from palm images.
3. Elliptic curve points can be used as good control points for cubic spline curves.
4. The cubic spline found the good choice of in-between points for spline curves.
5. The LCS algorithm shows that the coefficient MD5-B is less similarity ratio than coefficient MD5-A than the proposed system with coefficient MD5-B is more strength against the plain text attack.

5.2 Suggestions for Future Works

1. Adapting the proposed model for a large-scale iris database to make the system more reliable.
2. Use SHA- 256 algorithm in generating digital signature.
3. Use one of the methods of optimization algorithms to generate features.

References

References

[1] Basu and Mita, "Development of a human identification system from finger vein biometric," Digital Library, 2013.

[2] Assma Mohammed J., "Palm Vein Identification and Verification System," M.Sc. Thesis, Computer Science, University of Baghdad, Baghdad- Iraq, 2014.

[3] Abdul-Wahab S**.,** "Face Recognition Using Skin Color and Texture Features," Ph.D thesis, Computer Science, University of Technology, Baghdad- Iraq, (2005).

[4] M. N. Nabi, S. Mahmud and M. L. Rahman, "Implementation and Performance Analysis of Elliptic Curve Digital Signature Algorithm," Daffodil International University Journal of Science and Technology, Vol:2 (1), 2007.

[5] Luxton David D., R. A. Kayl, and M.C. Mishkind. "MHealth data security: The need for HIPAA-compliant standardization," Telemedicine and e-Health ,Vol: 18 (4), PP:284-288, 2012 .

[6] Stallings, William, "Cryptography and Network Security, 4/E," Pearson Education India, 2006.

[7] S. B. Sadkhan, and N. F. Hameed, “Proposed Developments of Elliptic Curve Digital Signature Algorithm”, International Journal of Mathematical and Computational Sciences Vol:4(2), 2010.

[8] G. Seshikala, U .Kulkarni, M.N. Giriprasad, "Biometric Parameters & Palm Print Recognition," International Journal of Computer Applications Volume 46(21) , PP: 0975 – 8887 May 2012.

[9] M. Behera and V.K. Govindan, " Palm print Authentication Using PCA Technique," (IJCSIT) International Journal of

Computer Science and Information Technologies, Vol. 5 (3) ,PP : 3638-3640, 2014.

[10] K. Tamilselvan, R. Krishnaraj , P. Sukumar, T. Jayakumar, "Security Method for Human Finger and Palm Image Identification ," International Journal of Emerging Technologies in Engineering Research (IJETER), Vol: 4 (6), 2016.

[11] J. A. Shaikh, U. D. Kolekar "Palm Print Recognition Using Textural Harlick Feature," International Journal of Applied Engineering Research ,Vol : 12, (11) , pp. 2922-2925, 2017.

[12] K.J Archana, V.S angeetha and Y. L. Malathi Latha, "Palmprint Identification based on texture features using GLCM through Dynamic ROI," International Journal of Computer Science and Engineering - (ICRTESTM) - Special Issue – April 2017.

[13] P. T. Selvy, A. Anjugam and P. A. Begum, “Authentication Using Palm Print Recognition System”, International Journal of Engineering Development and Research (IJEDR), Vol: 5(1), PP : 2321-9939, 2017.

[14] E. Rahmawati, M. Listyasari, A. S. Aziz, S. Sukaridhoto, F. A. Damastuti, M. M. Bachtiar and A. Sudarsono, "Digital Signature On File Using Biometric Fingerprint With Fingerprint Sensor On Smartphone," *IEEE*, pp. 234-238, 2017.

[15] S. R. A. H. MIR, Z. A. JHAT, "Biometrics Verification: a Literature Survey," Journal of Computing and ICT Research, vol. 5, p. 14, 2011.

[16] G. J. Mohammed, "Efficient Iris Segmentation Method For Recognition Based on New Projection Function " Doctor of Engineering School of Computer Science and Technology, Harbin Institute of Technology, 2011.

[17] M. E.-A. a. C. Charrier, "Evaluation of Biometric Systems," in New Trends and Developments in Biometrics, ed: InTech, 2012.

[18] A. A. Jarjes, "Improving Snake Models For Accurate And Efficient Iris Segmentation," Doctor of Engineering, School of Computer Science and Technology, Harbin Institute of Technology, 2011.

[19] F. P. Jain A. K., Ross A. A., Handbook of biometrics. New York: Springer Science, 2008.

[20] J. A. K. Li S. Z., Handbook of face recognition. New York: Springer Verlag, 2004.

[21] A. Nadort, "The Hand Vein Pattern Used as a Biometric Feature," Master, Science programme Physics of Life, Free University, Amsterdam, 2007.

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

[23] D. D. ZHANG, PALMPRINT AUTHENTICATION, United States of America: Springer, 2004.

[24] R. R. Debnath Bhattacharyya, Farkhod Alisherov A., and Minkyu Choi, "Biometric Authentication: A Review," International Journal of u- and eService, Science and Technology, vol. 2, p. 16, 2009.

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

[26] Anil K. Jain, Arun A. Ross and Karthik Nandakumar," Introduction to Biometrics", Springer, 2011.

[27] Mamta Kothavale, Robert Markworth, Parmajit Sandhu, "Computer Security SS3: Biometric Authentication", edocument, The University of Birmingham, Birming hamEngland, 2004.

[28] Assma Mohammed J., “Palm Vein Identification and Verification System”, M.Sc. Thesis, Computer Science, University of Baghdad, Baghdad- Iraq, 2014.

[29] Joseph N. Pato and Lynette I., “Biometric Recognition: Challenges and Opportunities”, National Academy of Sciences, 2010.

[30] Mark Stamp and Peter Stavroulakis, “Handbook of Information and Communication Security”, Springer Science & Business Media, 2010.

[31] 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.

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

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

[34] R. . P. Singh and . M. Dixit, "Histogram Equalization: A Strong Technique for Image Enhancement," *International Journal of Signal Processing*, vol. 8, no. 8, pp. 345-352, 2015

[35] A. K. Mohanty et al., "Image Mining for Mammogram Classification by Association Rule Using Statistical and GLCM Features" Journal: International Journal of Computer Science Issues ISSN: 16940784 , 2011.

[36] I. N. Ibraheem ," Color Models Indexing for Content Based Image Retrieval System", Ph.D. Thesis, department of computer Science, University of Technology, IRAQ, 2009.

[37] A. Tiwari, A. K. Goswami and M. Saraswat, "Feature Extraction for Object Recognition and Image Classification," International

Journal of Engineering Research & Technology , vol. 2, no. 10, pp. 1238-1246, 2013.

[38] M. Partio, B. Cramariuc and M.Gabbouj, "Rock Texture Retrieval Using Gray Level Co_occurence Matrix ",Tampere University of Technology, Finland ,2010 .

[39] S. Asadollah, et al., "Parallel Implementation of Gray Level Co-occurrence Matrices and Haralick Texture Features on Cell Architecture" **Journal**: The Journal of Supercomputing **ISSN**: 0920-8542**,** 2012 .

[40] K. Li, M. Nannan, K. Yan , "Mass Computer-Aided Diagnosis Method in Mammogram Based on Texture Features", Biomedical Engineering and Informatics (BMEI), 3rd International Conference, IEEE Explore, pp.146 – 149, 2010.

[41] T. Ojala, M. Pietikaine ," Texture Classification", M.Sc thesis, Machine Vision and Media Processing Unit, University of Oulu, Finland, 2010.

[42] P. Mohanaiah, P. Sathyanarayana and L. GuruKumar, "Image Texture Feature Extraction Using GLCM Approach," *International Journal of Scientific and Research Publications*, vol. 3, no. 5, pp. 1-5, 2013.

[43] D. Gadkari, "Image Quality Analysis Using Glcm", electronic thesis, University of Central Florida, 2004.

[44] J. Thangavel, "Digital Signature Comparative study of its usage in developed and developing countries", Thesis for the Degree of Master in Information Systems Sciences, Uppsala University.

[45] Nurhaida, D. Ramayanti and R. Riesaputra, "Digital Signature & Encryption Implementation For Increasing Authentication, Integrity, Security And Data Non-Repudiation," *International*

Research Journal of Computer Science (IRJCS), vol. 11, no. 4, pp. 4-14, 2017.

[46] Thangarasu.N and A. L. Selvakumar, "Implementation and Secured Authentication Key using Elliptic Curve Cryptography," International Journal of Innovative Research in Information Security (IJIRIS), vol. 1, no. 2, pp. 66-71, 2014.

[47] A. Khalique, K. Singh , K. Singh, " Implementation of Elliptic Curve Digital Signature Algorithm," International Journal of Computer Applications, PP 0975 – 8887 ,Vol. 2 , No.2, May 2010.

[48] A. K. Kasgar and M. K. Dhariwal, "A Review Paper of Message Digest 5 (MD5)," *International Journal of Modern Engineering & Management Research*, vol. 1, no. 4, pp. 29-35, 2013.

[49] D. Rachmawati, J. T. Tarigan and A. B. C Ginting, "A comparative study of Message Digest 5(MD5) and SHA256 algorithm," *IOP Publishing*, 2017.

[50] A. H. Fadel , S.B.Sadlkhan, "Modifid Digitral Signature Based on Cubic Splin Function," M.S.C University of Babylon , 2013.

[51] A.Kumar Kendhe and H. Agrawal, "A Survey Report on Various Cryptanalysis Techniques," International Journal of Soft Computing and Engineering (IJSCE), Vol-3, Issue-2, May 2013.

[52] Y. H. Peng, C. B. Yang, K.S. Huang, C. T. Tseng, and C. Y. Hor, “Efficient sparse dynamic programming for the merged LCS problem with block constraints,” International Journal of Innovative Computing, Information and Control, vol. 6, pp. 1935–1947, 2010.

[53] T. G´orecki, "Using derivatives in a longest common subsequence dissimilarity measure for time series classification," Pattern Recognition Letters, vol. 45, no. 0, pp. 99–105, 2014.

الخلاصة

تحظى الأنظمة البيومترية بمزيد من الاهتمام في مجال الأمن. تعد المقاييس الحيوية لخطوط كف الإنسان واحدة من أسرع التقنيات البيومترية دقة وموثوقية وآمنة لتحديد الهوية والتحقق منها ، لأنها توفر المصادقة التلقائية للفرد استنادًا إلى الميزات الفريدة في بنية الكف البشري .راحة اليد تتضمن ميزات مميزة مثل الخط الرئيسي, التجاعيد, التلال والوديان على سطح راحة اليد. على خلاف تحديد راحة اليد الذي يطابق الميزات بالعديد من الميزات في قاعدة البيانات, راحة اليد تتحقق من هوية الاشخاص المدعين مع الانماط المخزونة في النظام.

في هذه الرسالة ، يتم اقتراح نموذج تحقق فريد من نوعه فعال للوثيقة باستخدام خطوط اليد البشرية. يمكن أن يوفر خطوط اليد البشرية ميزات فريدة يمكن استخدامها في توليد توقيع رقمي آمن. لذلك ، يتكون هذا النموذج من جانبين: جانب التضمين وجانب الاستخراج. يتضمن جانب التضمين: (1) مرحلة ما قبل معالجة الصورة: (تحويل الصورة الملونة إلى اللون الرمادي ومعادلة الرسم البياني). (2) مرحلة استخراج الميزة: استخدام خوارزمية(GLCM (Haralick). اما المرحلة (3): توليد مرحلة التوقيع الرقمي:(Elliptic Curve and Cubic Spline function with MD5)بينما يحتوي جانب الاستخراج على مرحلة استخراج التوقيع ومرحلة المطابقة.

بينت نتائج اختبار الاداء ان معاملات ال MD5_B تمتلك نسبة تقارب اقل من معاملات ال MD5_A من ناحية تواقيع المستخدمين.

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة ديالى

توليد التحقق الفريد من نوعه من كف اليد بأستخدام المنحنيات الأهليجية

رسالة

مقدمة الى قسم علوم الحاسوب / كلية العلوم/ جامعة ديالى وهي جزء من متطلبات نيل درجة الماجستير في علوم الحاسوب

من قبل

مروج محمد عبود

بإشراف

أ.د. زياد طارق مصطفى **أ. ناجي مطر سحيب**

1440 هـ **2020م**