Ministry of Higher

Education and Scientific

Research

University of Diyala

Multi level biometric to generate stream key using swarm intelligence algorithms

Prepared By

Hussein Ali Ismail

Supervised By

Asst. Prof Jamal Mustafa Abbas

A Thesis Submitted in Partial Fulfillment of the Requirements for the Master Degree in Computer Science at the Department of Computer Science/ College of Science/ University of Diyala

Iraq / Diyala

2020

بسَم الله الرحمن الرحَيم

((أَفَلَا يَنظُرُونَ إِلَى الْإِبِلِ كَيْفَ خُلِقَتْ))

صدق الله العظيم

الغاشية (17)

Dedication

To . . .

My family

My dear parents

All our distinguished teachers those who paved the way for

our science and knowledge . . .

Acknowledgements

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

Finally, I express my profound gratitude to my friends and my colleagues for supporting me. I am grateful to my mother and to my father for providing me with support and continuous encouragement throughout my years of study and the process of researching and writing this thesis. This accomplishment would not have been possible without them.

Abstract

New techniques are used to keep personal information secure. The encryption key is a technique that is derived from the biometric data of the user indirectly. The fingerprint is a unique biometric feature used to verify the identity of each person. The systems of fingerprint extraction are based on the universal and detailed features of fingerprints.

The stages of implementation of this work include preparing the image depending on the Otsu method. This method is used to extract the value of the threshold of the image by converting the image grayscale to a binary image represented by (0, 1) to be suitable for the computer system.

In addition, the convolution techniques are used to extract features from the fingerprints biometric image and to get fast access to the important regions inside the fingerprints biometric image. These features are used to find the optimal solution by using Hybrid optimization algorithms.

The hybrid system consists of two algorithms: fireworks and camel herd algorithms. Fireworks algorithm is based on three-dimension chaotic maps to enhance the performance of fireworks to generate a stream cipher key used for many purposes depending on the fingerprint biometric image.

The QRcode is activiated by using a secrete text, then dropping the best coordinates position feature which come from hybrid optimization to QRcode leading to generate a variable size key which is called stream cipher key.

The advantages of this key is unique, unpredictable, and suited for cryptography because the stream cipher key is checked by several parameters of “Random Number Generation Tests” to measure the strength of the key with a focus on a variety of different types of non-randomness that could exist in a sequence. The random number generation tests are performed in two cases: fireworks without hybrid and fireworks with hybrid based on the length key 512

and 1024. The results of these tests show that the resulting key is strong, active, and not broken and the stream cipher key is used for the following purposes:

1. Generating a prime key which is used for multiple users. The prime key also is checked by using the “Miller Rabin test” to get the strength of the prime key. This key can be employed in many places such as banks, security companies, and QI cards.

2. Generating a key that is used to hide text inside the images by steganography method depending on universal images.

Linguistic Certification

This is to certify that this thesis entitled **"Multi level biometric to generate stream key using swarm intelligence algorithms"** was prepared under my linguistic supervision. It was modified to meet the style of English language

Signature:

Name:

Date: **/ /2020**

Computer Science Department

Supervisor's Certification

I certify that this thesis entitled **"Multi level biometric to generate stream key using swarm intelligence algorithms"** was prepared under my supervision at Department of Computer Science\ College of Sciences\ University of Diyala in a partial fulfillment of the requirements for the degree of Master of Science in Computer Science.

Signature:

Name: **Asst. Prof. Dr. Taha M. Hassan**

Date : **/ / 2020**

Signature:

Name: **Asst. Prof. Dr. Jamal Mustafa Al-Tuwaijari**

Date: **/ / 2020**

Examination Committee Certification

We certify that we have read the thesis entitled **" Multi level biometric to generate stream key using swarm intelligence algorithms "** and as examination committee, examined the student **" Hussein Ali Ismael "** in the thesis content and that in our opinion, it is adequate to fulfill the requirement for the Degree of Master in Computer Science at the Computer Science Department, University of Diyala.

Signature:

Name: **Prof. Dr. Dahir Abdulhade Abdulah** (Chairman)

Date: **/ / 2020**

Signature:

Name: **Asst. Prof. Dr. Boshra F. Zopon Al_bayaty** (Member)

Date: **/ / 2020**

Signature:

Name: **Asst. Dr. Bashar Talib Al-Nuaimi** (Member)

Date: **/ / 2020**

Signature:

Name: **Asst. Prof. Dr. Jamal Mustafa Al-Tuwaijari** (Supervisor)

Date: **/ / 2020**

Approved by the Department of Computer Science at the University of Diyala

Signature:

Name: **Prof. Dr. Tahseen Hussein Mubarak** (The dean)

Date: **/ / 2020**

Head of Computer Science Department

Chapter One

General Introduction

Chapter Two

Theoretical Background

Chapter three

The Proposed System

Chapter Four

Implementation of the Proposed System

Chapter five

Conclusions and Future Work

Reference

List of Figures

List of Tables

List of Algorithms

Symbols

No.	Symbol	Meaning
A.	*	Multiplication operation
B.	+	Addition operation
C.	/	Division operation
D.	-	Subtraction operation
E.	=	Equality sign
F.	μ	Mean value
G.	σ	Standard deviation
H.	Δ	Delta
I.	Σ	Sigma
J.	%	Percent sign
K.	(a,b)	Ordered pair, collection of 2 elements
L.	( )	Parentheses, calculate expression inside first
M.	Xi	The random neighbor

CHAPTER ONE

GENERAL INTRODUCTION

Chapter One

General Introduction

1.1 Introduction

Development in the field of information technology makes the system of authentications an integral part of life people. Authentication in the biometric field has become the first work important to be performed in ensuring security. To determine the identity of a person, the system needs some physiological or behavioral characteristics as parameters to verify the identity. The identification process requires a set of reliable systems for personal recognition to confirm or identify the individual who requests his services. Information security is concerned with the assurance of integrity, confidentiality, and the information available on a network in all its forms [1].

Some systems and techniques are used for managing the system of authentication. One of the systems is biometric. Biometric authentication has developed in popularity as a way of supporting personal identification depending on individual characteristics. A person's identification is significant in many applications, whereas the biometric authentication process can be individual communication that cannot be interrupted by attacks. In biometrics, the user does not need to remember the series of passwords. Some normal alphanumeric password expires after a certain interval of time and needs to assign [2].

In many places, such as computer applications, research institutes, and all kinds of applications and systems, there may be a series of passwords. Because of ease of use with a high-level user, the security system can be the solution in such cases. Recently, most of the old methods in the authentication system, such as personal identification numbers (PINs) are increasingly being replaced by biometric systems. Passwords have some obvious disadvantages. They possibly will be taken, lost, or forgotten. Recently, biometrics proposal another solution to the process of personal authentication or identification depending on biometric characters [3].

1.2 Biometric Overview

Biometrics is one of the systems that measure a physical or behavioral attribute of a person it is used to identify or confirm the personality that claims it. The measurable tools depend on the characteristics or traits of a person. It can be configured and presented to a sensor and then converted to a measurable digital system. This procedure allows for programmatic matching and can occur in a few seconds. The strength of biometrics depends on the extent to which physical or personality characteristics undergo change over time [4].

Such change can occur because of exposure to a person's harmful substances, aging, or injury. Biometrics is not subject to major changes over time. The low degree of durability indicates a biometric that can change over time. For example, the iris form can change very little over the ages, so the iris is more powerful than the sounds. The highest degree of discrimination is unique, while the low degree of discrimination indicates a significant biometric form among the general people [5].

Biometrics refers to measurements associated with human characteristics. It represents measurable behavioral and physiological traits of persons for identification and authentication. Physiological and behavioral traits are the two most important tasks in biometrics. Physiological includes a set of measurements such as hand, palm, deoxyribonucleic acid (DNA), face, iris and fingerprints, while behavioral traits include rhythm, walking, and writing. Biometrics applications include border security, fraud prevention, crime detection, security issues, payment systems, bank overdrafts, employee attendance recording, and other uses [6].

1. Unimodal biometric systems

The unimodal biometric system is using one of the biometric characteristics of the individual to identify and verify identity such as fingerprint, face, iris, voice, retina, etc. In addition, the system leads to a decrease in the level of accuracy due to the noisy data, that to occurs during a match, such as inter-

class similarities. This system registers a very high false acceptance rate (FAR) and a false rejection rate (FRR) [7].

2. Multimodal biometric system

Biometrics has the ability to use two or more multiple biometric systems characteristics to identify a person. Multimodal biometric systems are more reliable than a uni-modal biometric system because some independent biometric modalities are used. The use of the multimodal biometric system may be the result of a greatly accurate and protected biometric identification system. It can overcome the greatest of the gaps such as inter-class variations, noise in collected data, a spoof of attacks, non-universality etc. [5, 6].

1.3 Classification of multi-biometric

There are many types of biometrics systems that are used to design authentication systems. However, the multiple biometrics have been designed to use one of the forms of combination as described below:

1. Multi-sensor systems

The sharing of similar information biometric system is used in various sensors. Compared information corresponding to a fingerprint is acquired by using different kinds of sensors. Then the information obtained is integrated using a certain technique [7].

2. Multi-modal systems

More than one of the biometric traits can be used for user identification. The information got by using retina and face is integrated in order to build the identity of the user. This system has a high cost because it needs several sensors with different biometric features. [8].

3. Multi-instance systems

Multiple samples of a specific biometric trait are taken. For example, images of the right and left irises can be employed for recognizing iris. Fingerprints taken from two or more fingers of a person are combined. If a single sensor is used to get the images in a sequence manner, the system will be made actually cost-effective because it does not need multiple sensors. In addition, it does not combine further feature extraction and similar modules [8].

4. Multi-sample systems

Multiple models of a similar biometric trait can be used for recognition and enrollment. For instance, along with the frontal face, the right and left profiles are taken. Multiple impressions of a similar face and multiple models of a retina can be linked. Multiple models may overcome reduced performance. However, it needs multiple sensors or the user has to wait a long time to be recognized [9].

5. Multi-algorithm systems

Multiple various methods of feature extraction and identical algorithms are applied to one biometric trait. The result is achieved if any of the matching fusion techniques can be applied to the results by using different algorithms. These systems are more complex and economical because of using different algorithms [10].

6. Hybrid systems

The hybrid system is that combines more than one of the mentioned multi-biometric systems. For instance, two iris recognition algorithms can be linked with two retina recognition algorithms. The structure of such a system is multi-algorithmic and multi-modal. If multiple sensors are used to get the images, it will be multi-sensory. If multiple instances of the face are used, it will be a multi-instance system [10].

1.4 Related Works

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

No.	Name &Year	Algorithms	Methodology	Biometric	Database
[11]	Chaos Encryption Algorithm using Key Generation from Biometric Images **(2016)**	Stream cipher algorithm	1-Logistic Map 2-Tent map	Iris	Chinese Academy of science and institute of Automation (CASIA)
[12]	RSA Key Generation From Cancelable Fingerprint Biometrics **(2017)**	RSA Algorithm (Rivest Shamir Adleman) algorithm	Shuffling method based transformation method	Fingerprint	Fingerprint Verification Competition (FVC) 2002
[13]	A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security **(2018)**	Binary Reed–Solomon coding (BRS) algorithm	1-Support vector machine (SVM) Ranking. 2-Thermal Sweeping Sensor (TSS).	Fingerprint	1- Fingerprint Verification Competition (FVC) 2004 2- NIST Special Database.
[14]	Retina Random Number Generator for Stream Cipher	1-The Acute Coronary Syndromes	1-Dimension logistic chaotic map.	Retina	DRIONS database

	Cryptography **(2019)**	(ACED) algorithm *2*-Entropy algorithm			
[15]	Design and Implementation of a new DNA based stream cipher algorithm using Python **(2020)**	Stream cipher algorithm	Steganography	Deoxyribose Nucleic Acid (DNA)	Online database National Center For Biotechnology Information (NCBI)

1.5 The Statement of Problem

Biometrics is one of the most promising technologies for providing secure authentication. There are many problems with the identity verification process in the personal authentication system such as attacks, spoof, authorization etc. In this work multilevel algorithms are presented through a process that is based on fireworks algorithm and camel herd algorithm by using hybrid techniques to generate stream cipher key. It is used for many purposes in order to overcome many difficulties in individual biometrics and this enhanced authentication, and accuracy.

1.6 Aims of the thesis

The aim of the thesis is to build a strong identification system based on a hybrid technique by using two algorithms fireworks algorithm (FWA) and camel herd's algorithms (CHA). Fireworks algorithms based on the 3-dimension logistic chaotic map to enhance the performance of fireworks algorithms to generate stream cipher key. It is used for many purposes and make the system more secure and authentication.

1.7 Thesis organization

The thesis is segmented into five chapters; a brief description of their contents is given below:

Chapter One: This chapter introduces an overview of the work and related works

Chapter Two: This chapter includes theoretical background. It presents fireworks and Camel algorithms, their characteristics, behaviors, and parameters for finding the optimal solution.

Chapter Three: This chapter describes the proposed systems with their design and implementation includes a hybrid optimization algorithm.

Chapter Four: This chapter presents the tests and the results of implementation.

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

CHAPTER TWO

THEORETICAL BACKGROUND

Chapter Two
Theoretical Background

2.1 Introduction

This chapter addresses a range of important topics including the use of biometrics to protect information and its importance in confirming people's identity and verifying vital data by using innumerable special features that can make each of us unique, such as our physical attributes that make our identity unique. In addition, it provides an overview of some of the benefits of biometrics. It also presents the methods used for identity verification. Swarm intelligence (SI) with different forms by observing the collective behavior of creatures as an idea of the algorithms used.

Biometric systems are based on several separate processes, including direct recording and extraction of features for the identical purpose. This chapter presents some of the methods used in biometrics, including the fireworks (FWA) and the camel herd (CHA) algorithms with explaining for each algorithm, its behavior, characteristics, and the technique that joins the two of the algorithms.

2.2 Biometrics

The term biometrics comes from the Greek words “bio” which means life and “metrics” which means measure. Biometrics refers to the identification or verification of a person based on his/her physiological and/or behavioral characteristics. Biometrics has developed depending on various unique aspects of the human body, ease of acquiring the biometric, public acceptance and the degree of security required. A biometric system is used as a favorable technique for security applications because the traditional techniques are based on something that people are familiar with such as, personal identification

number (PIN), password etc. or something you own such as card, key, etc. [16].

An authentication system involves the verification of any confirmation or rejection of the false identity of the person. The identity of the person must be proved; the vital systems that are used in authentication broadly divided into hand geometry, vein pattern, sound pattern, signature forms, Deoxyribose Nucleic Acid (DNA), fingerprints, iris pattern, and facial detection. These tools are working based on the average range of testing, the accuracy required, and the high speed required. These tools have advantages and disadvantages. Computers become more useful as IT (internet information) tools, so it is necessary to restrict or stop access to unauthorized persons or false use [17].

Biometrics is used in several places, including law enforcement, health care, trade, travel, financial and banking, and so on. Government applications include national identity cards, driver's licenses, social security cards, passports, voter registration and so on, where techniques are used to reinforce or replace some of these important documents or processes. Multiple biometrics, combined in multi-module frameworks, are used to provide much better accuracy and durability to secure restricted areas at airports, national security facilities, etc. [18].

Categories of biometrics

The biometric system is an advanced way of identifying a person based on some physiological or behavioral characteristics. Biometrics systems is a more reliable solution to protect the identity and rights of persons because they recognize the unique characteristics of people. Biometric is divided into two basic categories [19]:

1. Physiological

The following are examples of physical characteristics used in biometrics:

1. Features of the Face

2. Retina

3. Iris
4. Palm geometry
5. Fingerprints
6. DNA
7. Odor/scent [19].

2. Behavioral

The following are examples of behavioral characteristics used in biometrics:

1. Keystrokes/Typing patterns
2. Voiceprint
3. Typing rhythm
4. Gait
5. Handwritten signature [19].

2.3 The basics of biometric system

This field of work will attempt to answer the question "Why is biometrics required?" The growing use of information technology in the fields of science, driver's licenses, etc. is a real and significant need to protect data from unauthorized users by using biometrics to authenticate a person and allow access. Biometrics involves the following processes [20]:

1. Verification (one-to-one)

This an individual matching process where the direct sample entered by the nominated person is matched to the previously stored template in the database If both match more than 80% of the similarity so it is considered acceptable and the process is successfully verified [20].

2. Authentication (one-to-many)

The one-to-many step has such good features; For example, no identity is needed from the user since the automatic system determines who the user is and whether he belongs to a pre-defined group of known users or not. This process can answer the question: "Are you really the person you claim to be?",

Or “Do I know you?" These are identical to each other. The system compares the biometrics of the person with the entire database [20].

3. Authorization

Authorization is the process of allowing access to authorized and authenticated users trying to figure out the answer to the question "Are you eligible for certain rights to access this resource or location?” [20].

2.4 Requirements of biometric characteristics

There are some requirements that should be available for using physical and behavioral characteristics. These requirements include the following [21]:

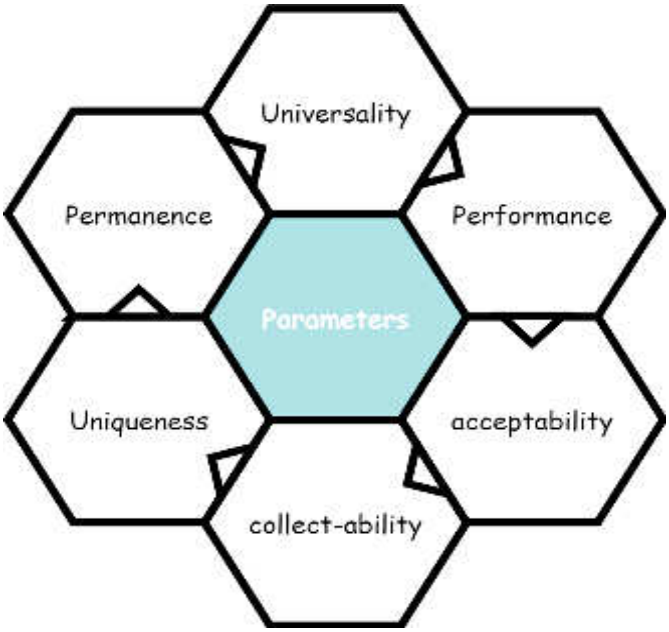


Figure (2.1): Biometrics requirements [21]

1. Universality

Every person has own biometric characteristics. There are some people is lose some features such as, persons with no fingers, or with hurt eyes. It is so challenging to get 100% coverage [21].

2. Uniqueness

In biometrics, no two individuals are similar in terms of biometric characteristics. The biometric system is able to identify every user among the collections of users [21].

3. Collect-ability

Each feature that is recorded in the system database must be constant for a period [21].

4. Permanence

It is required for every single characteristic or trait which is recorded in the database of the system and needs to be constant for a certain period of time period. This means that the characteristics should be invariant with time [21].

5. Acceptability

It is very important that the biometric system selected for check testing is acceptable [21].

6. Performance

This refers to the achievable identification/verification accuracy, the resources, and working or environmental conditions needed to achieve an acceptable accuracy [21].

2.5 Swarm intelligence optimization

SI algorithm is defined to be the cooperative performance of decentralization, self-regulation systems, and natural. SI algorithms are made up of individuals of causes collaborating locally with one another and with their environments. The swarm intelligence algorithm includes bird flocking, ant colonies, fish schooling, and animal herding [22].

Optimization is the act obtaining the best result under given circumstances. The optimization is inspired by swarm intelligence. Optimization means the process of searching in order to find the optimal solution in given circumstances [23, 24].

2.6 Fireworks Algorithm (FWA)

The FWA is a comparatively new SI algorithm. The basic idea of the fireworks algorithm comes from the explosion of fireworks in the sky at night. The explosion of fireworks like a single search for the ideal solution in

optimization algorithms. The work of FWA depends on iterative search which is similar to the optimization algorithm. FWA which has different specifications and diverse prices produces many forms. For example, FWA of lesser price introduces, fewer sparks of greater amplitude, and vice versa. FWA simulates the explosion of FWA based on each FWA analysis. The fireworks algorithm involves four strategies [25]:

1. The explosion operator
2. Mutation operator
3. Mapping rule
4. Selection strategy [25].

The outcome of the explosion operator leads to producing a number of sparks. The explosion operator governs the amplitude and number of the sparks. The mutation operator also produces some sparks. The mutation operator uses a Gaussian operator to produce sparks by helping Gaussian distribution. To identify sparks the next step a selection strategy should be employed [26].

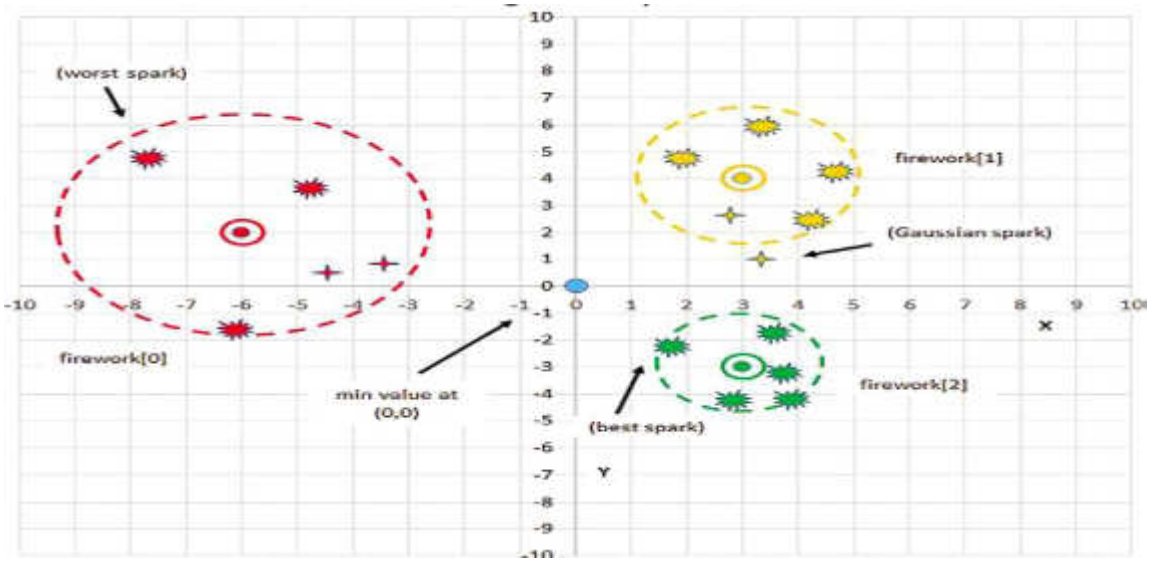


Figure (2.2): Fireworks optimization algorithm [26]

2.6.1 The Explosion Operator

The fireworks produce a number of sparks (N) by the explosion operations random. The explosion operator represents a key to solve in FWA and it plays an active role in the FWA. The explosion operator contains the following [27]:

1. Explosion Strength

It is a major process in the explosion operator phase. That is the process simulates the method of the explosion of FWA. When firework explosions, the fireworks disappear within seconds, and then generate many small explosions around them. The number of sparks is determined by equation (2.1) [28]:

$$S_i = m * \frac{Ymax - f(xi) + \varepsilon}{\sum_{i=1}^{N}(Ymax - f(xi) + \varepsilon} \quad (2.1)$$

S_i**:** The N of sparks for every individual.

M: Total of sparks

Y max: suitability value of the worst individual between the N individuals in the populace.

F (xi): fitness for an individual xi.

ε: constant: used to avoid the denominator from fetching zero. Limit the number of sparks calculated through by equation (2.2) [28,29]:

$$\hat{s}i = \begin{cases} round(a \cdot m). if\, S_i < am \\ round(b \cdot m). if\ S_i > bm.\ a < b < 1. \\ round(a \cdot m). otherwise. \end{cases} \quad (2.2)$$

A and B are invariable

$\hat{s}i$: The limit of the number of sparks.

2. Explosion Amplitude

The explosion amplitude is calculated through by equ (2.3) [29]:

$$Ai = \hat{A} * \frac{f(xi) - Ymin + \varepsilon}{\sum_{i=1}^{N}(f(xi) - Ymin) + \varepsilon} \quad (2.3)$$

Ai: The amplitude of every individual

$\hat{A}$: The totality of all amplitudes

3. Displacement Operation

FWA produces different random displacements within every amplitude to make sure of the variety of spark. Through the explosion operator, every firework produces a number of sparks that are used to help to discover the global optimal category of the optimization. The displacement operation helps

to make displacement on all the dimensions of a firework and it is calculated by equation (2.4) and shown by the algorithm (2.1) [29].

$$X_i^k = X_i^k + U(-Ai, Ai) \quad (2.4)$$

U (−Ai, Ai): The uniform random N within the intervals of the amplitude Ai.

Algorithm (2.1): General explosion operator [29]

Input: initial point (spark, initial)
Output: initial solution

Calculate the fitness value f (xi) for each firework. (2.1)
Calculate the N of sparks Si. (2.2)
Calculate the amplitude of sparks Ai. (2.3)
z = rand (1, dimension) //randomly choose z dimensions
for k = 1 → dimension **do**
if k ∈ z **then**
$X_i^k = X_i^k + U(-Ai, Ai)$
end

2. Mutation operator

The original spark location is defined by (X_i^k), where (i) differs from (1 to N).

K: Dimension of spark.

The new sparks produced by the Gaussian explosion are calculated by the following [28].

$$X_i^k = X_i^k * g \quad (2.5)$$

G: The Gaussian distribution of random number, which has mean 1 old and the new spark by 1 New such as:

$$g = N(1 \text{ old}, 1 \text{ New}) \quad (2.6)$$

Algorithm (2.2): Gaussian mutation [28]

Input: generate new spark by gaussian
Output: Best coordinate position

Calculate the fitness value f (xi) for each firework. (2.1)
Calculate the coefficient g = N (1 (old), 1 (new)). (2.6)
z = rand (1, dimension) //randomly select z dimensions
for k = 1 → dimension **do**
if k ∈ z **then** $X_i^k = X_i^k * g$
end

3. Mapping rule

Mapping Rule is to make sure that the mapping rule for all sparks is within the possible space. When several sparks are outside boundaries, they are mapped back to their specified and allowed ranges. The mapping rule uses a standard process and is stated shown by equation (2.7) [28, 29]:

$$X_i^k = X_{LB.K} + X_i^k \%(X_{LB.K} - X_{UB.K}) \quad (2.7)$$

X_i^k: The locations of out the bounds sparks.

$X_{LB.K}$ and $X_{LB.K}$: Represent minimum and maximum borders of a spark location.

3. Selection Strategy

It is used for measuring conventional distance, where d (Xi, Xj) defines the conventional distance between whichever two individuals Xi and Xj as given in equation (2.8)

$$R\langle x_i \rangle = \sum_{j=1}^{k} d(x_{i.}\ x_j) = \sum_{j=1}^{k} \|x_i - j_i\| \quad (2.8)$$

D: Distance

R (xi): The totality of distances between spark Xi and the others

j ∈ K: location j of the set K.

K: sparks produced by a mutation operator and explosion operator. The roulette method selects entities to the next product, similar to the probability for nominated the specific xi and P (xi), which intrudes in (2.3) [28, 29].

$$P(xi) = \frac{R(Xi)}{\sum_{j \in k} R(xi)} \quad (2.9)$$

Algorithm (2.3): General of FWA [29]

Input: Best region of fireworks
Output: Best coordinate position

Randomly select N locations for fireworks
while a terminal condition is not met **do**
Set off N fireworks, respectively, at the N locations:
for all fireworks xi **do**
Calculate the number of sparks as Si (2.1)
Calculate the amplitude of sparks as Ai (2.3)
end for
// $\widehat{m}$ is the number of sparks generated by Gaussian mutation
for k = 1→ $\widehat{m}$ **do**
Randomly select a firework xi and generate a spark
end for
Select the best spark and the other sparks according to the selection strategy
end

2.7 Camels Overview (Diet in the Wild)

The camels have an upper lip separated from the other, which helps camels to eat leaves, shrubs and some thorns. The presence of camels in desert and arid areas due to its different physiological systems may encourage researchers to study the behavior of camels in the desert and focus on its characteristics to increase its potential. The most common feature of a camel is walking in groups called a herd. It is rare for a camel to go alone in the desert. Each herd has a leader and other camels follow that leader [30].

The nose of the camel is characterized by its ability to feel and smell from long distances. Camels also have the capability to detect the route without any human intervention, and thus, they can detect the location of water and food

depending on the humidity ratio factor in the atmosphere. The camels can feel the humidity factor. This an important element to help it detect the location of the water in the desert [31].

1. Performance of the camel herds algorithm (CHA)

The Camel Herd algorithm (CHA) belongs to the (SI) which proposed in this work in order to find the best solution to increase the reliability of the identity confirmation. The camel herd algorithm is based on camels' behavior in nature, taking into consideration the existence of a specific leader for each group of camels. The camels in the desert are looking for food and water by relying on the humidity ratio factor present in the atmosphere. In terms of its natural habitat. In addition, that their typical consumer behavior is to accelerate and research large areas where the humidity ratio factor is high such as (day - dawn / dusk). Where camels tend to rest in a form period they maintain a constant temperature of the body and to decrease the loss of water and energy consumption, making them endure days and weeks without food and water [31].

2. Parameters of the camel herds algorithm (CHA)

CHA is based on the behavior of the camel, its parameters, and activities of this parameter on the performance of the algorithm. The Humidity Ratio factor (Hum) is the major parameter and it is set randomly for each herd in the desert. In addition, the factor (Hum) is important terms because it helps herds to directions search on the aim in the desert. Then delivers ways to estimate the best neighbor that can lead to the aim and that presents a location that can decrease/ increase according to the problem need in each step to rich aim. In addition, the parameters in the algorithm are, n denote the camel number, the total of herds Hc, and d refers to the neighbor number [32].

3. Strategies of Camel Herd Algorithm (CHA)

The algorithm is the first step determines the herd number. The Herd Number symbolizes (Hc). The (Hc) for each group of camel herd represents

one solution. Within each group, the number of camels is referred to as (n). One of the camel herds is selected by the algorithm, which is called a leader and symbolizes it Leader Herd Camel (LHc). Each LHc stores the starting state of the algorithm and is randomly selected and then the algorithm distributes the herd in the desert. The Leader (LHc) distributes tasks to determine the solution in the problem space. Leaders begin the process of search with different points in the problem space. This method offers diversity to discover more than one solution. The algorithm begins with each (HCK) herd. Neighbors are randomly generated for LHck. All adjacent space is verified to find the best solution according to the equations (2.10, 2.11) [32].

$$X_{i'} = X_i / \text{Hum} \quad (2.10)$$

$$X_{i'} + 1 = (X\ \text{Led} - X_{i'}) / \text{dis}(X\ \text{Led}, Xi') \quad (2.11)$$

$X_{i'}$: The random neighbor

X Led: a leader herd

The best neighbor is added to the list of (LHCK).

Note: (K) denotes the number of neighbors after selecting one of them as a leader.

Hum value is always updated. These phases are recurring for every herd until scope the aim. The group of CHA parameters affects the performance of the algorithm. (n) Denotes the camel's number and it represents the first parameter that identifies the size of the herd. (n) Must be carefully select, because if it selected with the small value it will provide limited solutions, on the other hand, if it selected with a large value, it may lead to increasing the needed time to attain the aim [32].

Algorithm (2.4): Camel Herds [32]

Input: n no. of the camel in a herd Hc no. of herds The max_Hum maximum value of Humidity m length of list LHC
Output: The best Hc (best solution)

```
Begin
    For each herd (HCK) Do
            Select one of HCK as a leader LHCK using selection method;
            Select starting state and insert into the list of LHCK;
End for
Repeat
 initialize (Hum);
            For each HCK Do /* k=1 to no. of Hc */
                 For y=2 to m
                       Generate neighbors (d) randomly for LHCK;
                       For z=1 to d Do /* for each neighbor (NC) */
                              NCZ= NCZ /Hum                          (2.10)
                              NCZ= LHCk - NCZ / dis (LHCk, NCZ)      (2.11)
                        End for
                       LHCK [y] = LHCK [y-1] + Best Neighbors (NCZ)
                       Insert the best neighbor to the path LHCK[Y]
                  End for
                        Update Hum
                   End for
 Until reaching the goal or max Humidity
End
```

2.8 Thresholding Techniques

A threshold is a technique used in image segmentation. It conversions the image from grayscale to binary (0,1). The binary image represents a set of color images coming from the process of segmentation. The segmentation technique is a method in which each pixel of the original source of the image is assigning to two or more categories. If there are more than two categories, the usual result is a set of binary images [34].

In the image-processing, the threshold is used to divide the image into small pieces at least one color or grayscale value is used to determine its boundaries. The main benefit of finding the first binary image is to reduces the data complexity and to simplifies the process of classification and identification.

Thresholding is a binary image coming from conversion to the grey-level ones by turning some pixels threshold to (0) and all other pixels around that

threshold to (1). If g(x, y) is a type of threshold of the f(x, y) at global threshold T by equation (2.12) [35].

$$g(x,y) = \begin{cases} 1 \text{ if } f(x,y) \geq T \\ 0 \text{ otherwise} \end{cases} \quad (2.12)$$

Thresholding process as T = M [x, y, p(x, y), f (x, y)]

T: Threshold, F (x, y) is a gray value of the point (x, y).

P(x, y): Means some local characteristics such as the average gray value centered on the position (x, y).

The method work the threshold is the input a grayscale or color image. The output is a binary image that means the segmentation image. The black pixels correspond to the background and white pixels correspond to the foreground. This technique of segmentation applies a single static criterion to all pixels in the image instantaneously [34].

Image Segmentation means the image is segmentation into regions or sets of pixels. These pixels are divided according to their "intensity" value. The image is divided into two categories, namely the foreground and the background. g (x, y) = 1 if f (x, y) in the foreground of pixels = 0 if f (x, y) is a pixel in the background. Since there are many peaks and valleys that are not clear, it is not always easy to determine the value of T [35].

2.8.1 Types of Thresholding

There are three major types of thresholding techniques:

1. Global Thresholding: This type of threshold (T) accredits only on a single threshold for all image pixels is used. It is .decide the conversion from gray-level pixels into black or white pixels [34].

2. Local Thresholding: The adaptive threshold means that images are divided into several regions. Every region performs a thresholding process based on a threshold value that is calculated accrediting on the specific region components [35].

3. Hybrid Thresholding: Hybrid approaches combine the global and the local material to label a pixel as an object or background [35].

2.8.2 Classification of Thresholding Techniques

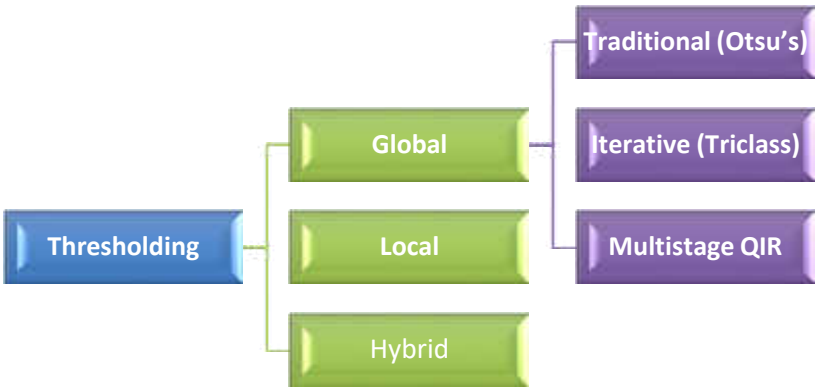


Figure (2.3): The Classified of thresholding techniques [35]

2.9 Otsu's Method

The Otsu method is usually used as a pre-processing image for image segmentation. The purpose of the Otsu method is obtaining more features and quantification. The aim of the Otsu method is to detect a threshold that minimizes differences within the divided image and provides satisfactory results. The graphic layout of the initial image has two distinct peaks, one belongs to the background pattern and the other to the foreground pattern. The Otsu threshold is determined by the process of detecting all kinds of pixel locations within the image so that the differences between layers are minimized [37].

The Otsu method is also used to determine the threshold more precisely and deeper by category with a greater contrast ratio. Both in background and foreground mode. Otsu method formulation, the Otsu method needs calculating a gray level histogram before running because of the availability one-dimensional which only the gray-level information, it does not give better segmentation effect, The lighting is required to be uniform [37].

The given image pixels are defined in L gray levels [1, 2. L]. The pixels number at level i is signified by ni and the total number of pixels by N = n1 + n2 +…, the gray-level histogram is standardized and regarded as a likelihood distribution by the equation (2.16):

$$P_i = \text{ni} / \text{N},\ \text{pi} > 0\ \sum_{\text{i=1.}}^{\text{L}}\ \text{pi} = 1 \quad (2.16)$$

The pixels are divided into two categories C0 and C1 (foreground and background) by a threshold at level k; C0 means pixels with levels [1, k] and C1 means pixels with levels [k +1, L]. Then the probabilities of category occurrence and the category mean give levels be equation below [38]:

$$W_0 = P_r\ (c_0) = \sum_{\text{i=1}}^{\text{k}} P_i = \text{W(k)} \quad (2.17)$$

$$W_1 = P_r\ (\text{Co}) = \sum_{\text{i=k+1}}^{\text{L}} \text{pi} = 1 - \text{W(k)} \quad (2.18)$$

$$\mu_0 = \sum_{\text{i=1}}^{\text{k}} \text{i}P_r(\text{i}|C_0) = \frac{\mu(\text{k})}{\text{w(k)}} \quad (2.19)$$

$$\mu_1 = \sum_{\text{i=k+1}}^{\text{l}} \text{ipr(i|C1)} = \mu_{\text{T}-} \frac{\mu(\text{k})}{1} - \text{w(k)} \quad (2.20)$$

$$\text{W(k)} = \sum_{\text{i=1}}^{\text{k}} P_i \quad (2.21)$$

$$\mu(\text{k}) = \sum_{\text{i=1}}^{\text{k}} \text{i}P_i \quad (2.22)$$

2.10 Feature Extraction

Feature extraction is the most important stage in the building of any pattern classification. The purpose of feature extraction is to extract information that is characterized by each image. The features are extracted from the image in order to formations parameter vectors. Moreover. Classifiers the input unit with the target output unit and that develops easier for the classifier to organize between the different categories by watching at these features, as it allows easy to distinguish between patterns, use the feature vectors [39].

2.11 Convolution Technique

In the image-processing field, the convolution is used to perform a diversity of image processing tasks, for example edge detection, smoothing, and blurring. In some scientific applications, the image data comes by scans that are not collected under certain conditions well-controlled conditions. In some cases, the data is being brought together from several sources. So, before it can be analyzed, data must be aligned, calibrated, and altered [40].

Convolution is used in the field of filtering processes, for example high-pass, band pass, and low-pass filters, but some filter forms are possible to discover features, for example edge detection kernels tuned sensitive to edge orientation, or corner, contour detectors, and basic points. The kernel mask (center image) is intended to amplify the center pixel in relation to the neighboring pixels. Every pixel is multiplied by its kernel location, and the result then displays the center pixel the totality of the convolution, which better or amplified in relative to the neighboring pixels [41].

2.12 Chaotic Logistic Map

The Chaotic logistic map is considered one of the very important popular examples of chaos dynamics. The fundamental chaos theory creates a procedural structure and provides a distinctive device for exploring and knowing the complex behavior in the installation of dynamic systems [42].

The difficulty of identifying the chaotic system comes because of the sensitive requirements of the initial constraints. The result of very minor changes that have formed in the initial conditions where significant developmental effects appear. In general, chaotic systems seem non-linear and random, but they must. Some chaotic algorithms work in order to images encryption [43].

The vulnerabilities in the image-encoding field are very sensitive to some attacks resulting from the large size of data and the similarity of pixels in different images. Therefore, cryptographic logarithms necessity very complex so that analyses become difficult or even impossible. You must have less time to fast encrypt large images. 3D functions are harmless than encryption attacks in this work, the 3D Logistic Function is proposed in order to encrypt images [44].

The 3D Logistic Formulation logistic map is used to increase the security level of the encryption method. The 3D map is detailed in the formula as given in equation (2.24, 2.25, 2.26) follows [45]:

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

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

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

Three quadratic coupling constant features are obtainable to strengthen the difficulty and security of the 3D Logistic map. The system offers chaotic behavior for $3.53<\lambda<3.81$, $0<\beta<0.022$, $0<\alpha<0.015$ and generates chaotic sequences X and Z in the range [0, 1].

2.13 Random number generation tests

The National Institute of Standards and Technology (NIST) number of criteria that include 12 tests. These tests are important and updated in order to measure the randomness of complete (arbitrarily long) binary sequences either by software or hardware depending on cryptographic random or pseudo-random number generators. The 12 tests are explained as follows [46]:

1. Approximate entropy

The basic idea behind this assessment is the frequency of probable overlying m-bit forms across the full sequence. The real goal of the test is to compare the frequency of overlapping blocks of two consecutive/adjacent lengths (m and m 1) opposite the probable result for a random sequence [46].

2. Block frequency

The real aim of this test is to determine whether the frequency in an M-bit block is approximately from M/2, as would be likely a supposition of randomness [46]

3. Cumulative Sums (Cu sum) Test

The main purpose of this test is the maximal speed (from zero) of the random well defined by the accumulative totality of digits (-1, +1) in the sequence. The real goal of the test is to know whether the accumulative totality of the part sequences occurring in the tested sequence is too big or too small relative to the probable behavior of that accumulative totality for random

sequences. This implies, sum some be considered as random. For a random walk sequence, the trips of the random must be nearby zero [46].

4. Discrete Fourier transform

The major idea of this test is to examine the greatest heights in the Discrete Fourier Transform (DFT) of the sequence. The actual goal of this test is to discover periodic features (i.e., iterative forms that are near every other) this test indicates a deviation from the assumption of randomness. It is discovered the number of peaks exceeding the 95 % threshold is significantly different from 5 % [46].

5. Frequency

This test is aimed to know the ratio of the entire sequence for zeroes and ones. The main aim of this test is to decide whether the ones and zeros numbers of a sequence are roughly the same as the possible for accuracy of random sequence. In addition, the test produces the measures the segment of ones to ½, which determines the sequence of the ones and zeroes number must be similar [46].

6. Longest-run-of-ones

The idea of this test is to examine the longest run of ones within M-bit blocks. The primary purpose of this for the test is to know whether the length of the longest run of ones within the tested sequence is constant with the length of the longest run of ones that would be probable in a random sequence. An irregularity in the probable length of the longest run of ones involves that there is an irregularity in the probable length of the longest run of zeroes [46].

7. Non-periodic template

The basic idea of this test is to discover generators that produce some occurrences of given non-periodic patterns. The m-bit frame is found to search for a specific m-bit pattern. If the forms are not found, the frame slides are the

one-bit location. If the form is found, the frame is returned to the bit after the found form, and the search resuming [46].

8. Overlapping template in ones

Both Overlapping Template and the Non-overlapping Template are used as an m-bit frame to search for specific m-bit forms. If the form is not found, the frame slides a one-bit location. The frame slides are only one bit before resuming the search [46].

9. Rank

The basic idea of this test is to examine the rank of disassembled sub-matrices of the full sequence. The real aim of this test is to check for linear dependency between fixed-length sub-strings of the original sequence [26].

10. Runs

The idea of this test is based on the total number of runs in one sequence, where a run is a continuous sequence of identical bits. A run of length k contains exactly k identical bits and it is limited before and after with a bit of the conflicting value. The real goal of this test is to know the number of runs of zeros and ones of different lengths as probable for a random sequence. The test decides whether the oscillation among such zeros and ones is too fast or slow [46].

11. Serial test

The major goal of this test is to know whether the number of recurrences of the (2mm-bit) overlapping forms is approximately the similar as would be expected for a random sequence. That is, every m-bit forms have a similar chance of appearing as each other m-bit form [46].

CHAPTER THREE

THE PROPOSED SYSTEM

Chapter Three

The Proposed System

3.1 Introduction

This chapter presents the design of an authentication system based on a hybrid technique by using two algorithms fireworks algorithm (FWA) and camel herd's algorithms (CHA). Fireworks algorithms based on the 3-dimension logistic chaotic map to enhance the performance of the fireworks algorithms to generate stream cipher key. It is used for many purposes and make the system more secure and authentication.

3.2 The block diagram of the proposed system

The basic idea of the proposed system is generating a stream cipher key by using a fingerprint biometric image. The proposed system consists of four-stage is A, B, C, and D, each stage included several steps as shown in figure (3.1):

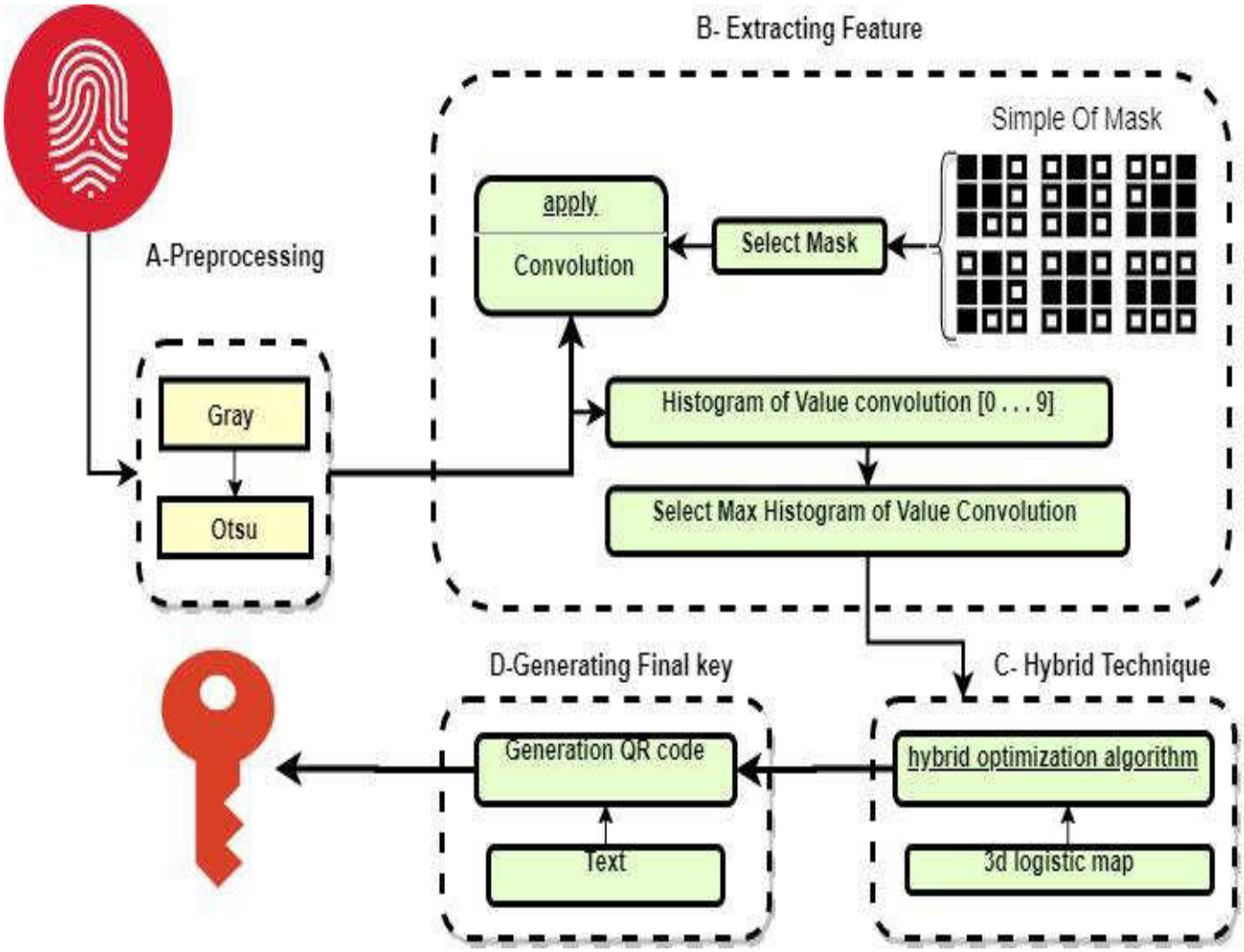


Figure (3.1): The Block diagram of the proposed system

3.3 Procedures of work

The major procedures of the thesis are summarized as follows:

A. **Preprocessing image:** Preparing images for further analysis, including uploading a fingerprint biometric image. Proposing a threshold algorithm in order to extract the value of the threshold of an image based on the Otsu method.

B. **Extracting Feature:** Extracting feature of the image by using the convolution technique depending on pattern mask.

C. **Proposing hybrid technique:** Proposing hybrid technique (fireworks and camel herd) algorithms to find the best coordinate position feature is used to generate stream cipher key used to secure the process of authentication.

D. **Generating Final the key:** Generating a stream cipher key, which is used in two cases:

1. Generating a prime key for multiple users.
2. Hiding a text inside an image by using steganography.

3.4 Fingerprint image dataset

The most important part of any test of a biometric system is the dataset. One of our aims is to test the effectiveness of the system and its strength based on a set of fingerprints images. The main use of the Fingerprint Verification Competition (FVC2004) organization is to provide a first overview of the evaluation. FVC2004 is a technology evaluation of fingerprint recognition algorithms which is open to companies, academic research groups and independent developers. Organization of FVC2004 started in April 2003 and the final evaluations were conducted in January-March 2004 at the University of Bologna, Italy.

3.5 Image Pre-Processing (Stage A)

The image pre-processing stage is the most important stage and as shown in figure (3.2). This stage represents the first task that must be implemented; it includes converting the fingerprint biometric image from the original image

(RGB) to grayscale image, then applying the Otsu method to extract the value of the threshold of the image by converting the image grayscale to a binary image. Furthermore, in order to extract the feature of the fingerprint biometric image we proposed convolution technique:

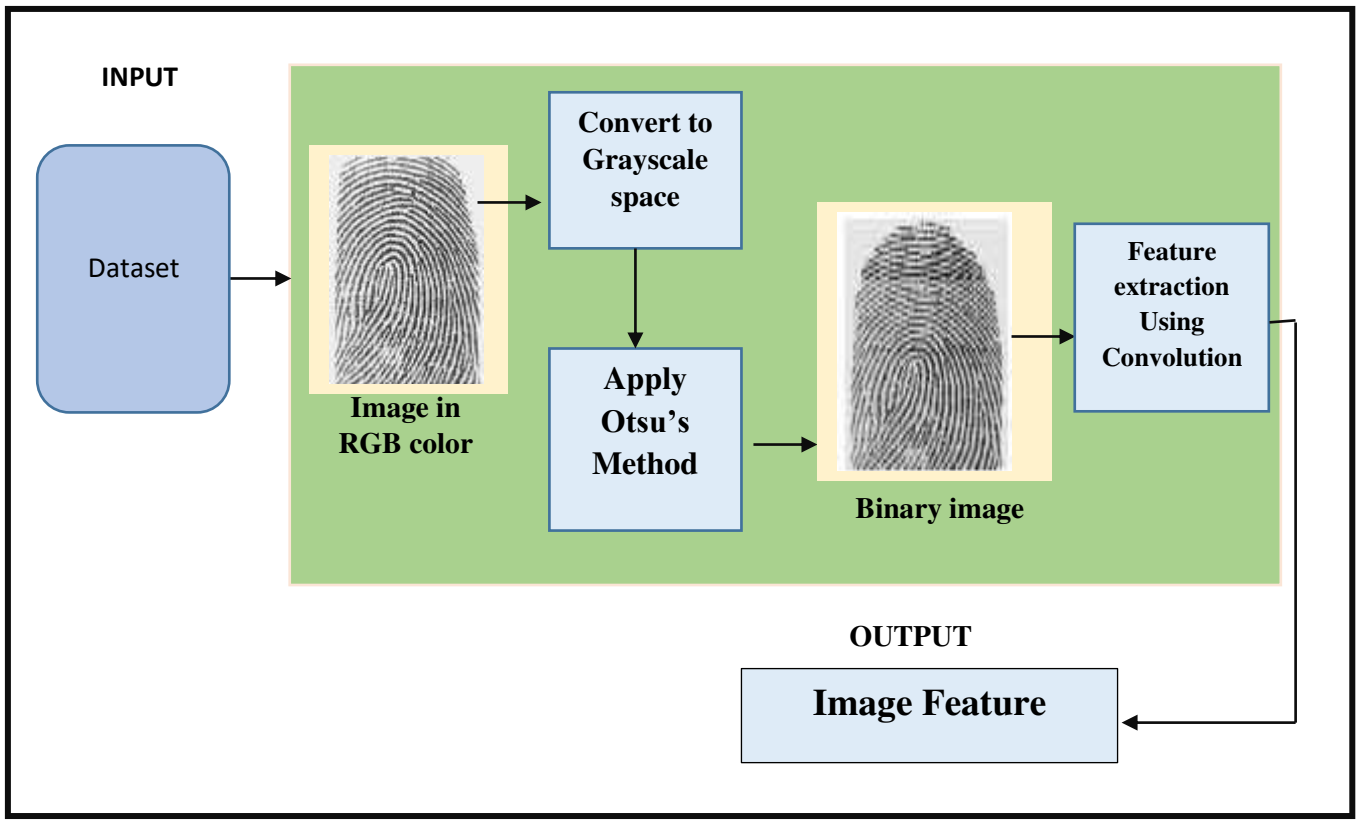


Figure (3.2): The block diagram of the pre-processing image

The pre-processing image consists of two-step; each step will be discussed in the following subsection: -

3.5.1 Conversion of the image from the original image (RGB) to grayscale

The conversion process is based on equation (3.1). The image biometric (fingerprint) is uploading from the dataset. The image contains a three-color band (R, G, and B) respectively. The intensity value can be obtained from each band and these values will be converted to grayscale value by equation (3.1) below:

$$\text{Grayscale image } (i, j) = 0.2989^{*} R + 0.5870^{*} G + 0.1140^{*} B \qquad (3.1)$$

3.5.2 Conversion of the image from grayscale to binary

The conversion process is based on the Otsu method. The purpose of this method is to find the value of the threshold for each fingerprint biometric image depending on the Otsu method. In the Otsu method, the optimal threshold is specified by maximizing the between-class variance (background and foreground) regions of the input image. Thus, this method will save the feature of the image without distorting it because the threshold that is determined by using the Otsu method is dynamic.

The figure (3.3) shows the fingerprint biometric image, each image has its own threshold, after calculating the threshold value of the grayscale image, the threshold binarization can be used to convert the image from the grayscale to a binary image, as shown in the algorithm (3.1).

Fingerprint Image (RGB)	**Grayscale Image (binarization)**	**Otsu Thresholding T=155**
		

Figure (3.3): Otsu thresholding method

Algorithm (3.1): Black and white by using Otsu thresholding

Input: Original image
Output: Image Black and white

Begin
Step1: // Calculate histogram
for (i = 0; i < xrow; i++)
for(j=0; j< x col ; j++)
h = get Pixel value(i,j)
histData[h] ++;
endfor
endfor
Step2:// Total number of pixels

```
            Total= xrow* xcol
            sum = 0,  sumB = 0, wB = 0, wF = 0, var Max = 0,threshold = 0
Step3: for (t = 0; t <  256; t++)
                sum += t * histData[t]
Step 4: for (t = 0; t < 256; t++)
               wB += histData[t];          // Weight Background
               if (wB == 0) continue;
               wF = total - wB;            // Weight Foreground
               if (wF == 0) break;
              sumB += (float) (t * histData[t]);
              mB = sumB / wB;          // implies Background          (2.20)
              mF = (sum - sumB) / wF;    // implies Foreground        (2.21)
Step4-1 // Calculate between class variance                          (2.22)
              var between =  wB *  wF * (mB - mF) * (mB - mF)
Step4-2 // Check new maximum
               if (varBetween > varMax) then
                 varMax = varBetween
                 threshold = t                                        (2.12)
              endif
            endfor
           endfor
Step5:// apply threshold for image
```

3.6 Feature extraction by using convolution technique (Stage B)

The convolution technique is used to extract the most important features of images by analyzing the parts of the image. The extraction of features depends on the Pattern mask, which takes a certain size then the pattern of the mask is applied to the image. The feature extraction by using convolution can be achieved by several steps: -

3.6.1 Dividing image

The fingerprint image is divided into blocks. The size of each block must be square = [k × k]. Where (k) represent prime number = [1,3,5,7,9].

For example, the binary of the image is [W, H] which represents the dimensions of space problem and k =5. The dividing process of the image is starting from left to right in order to generate Block1 [5 × 5],…,Block M [5×5] and get the

value of each block from the original image, and then store block value in order to find Feature array [W/ k, H/ k], as shown in figure (3.4):

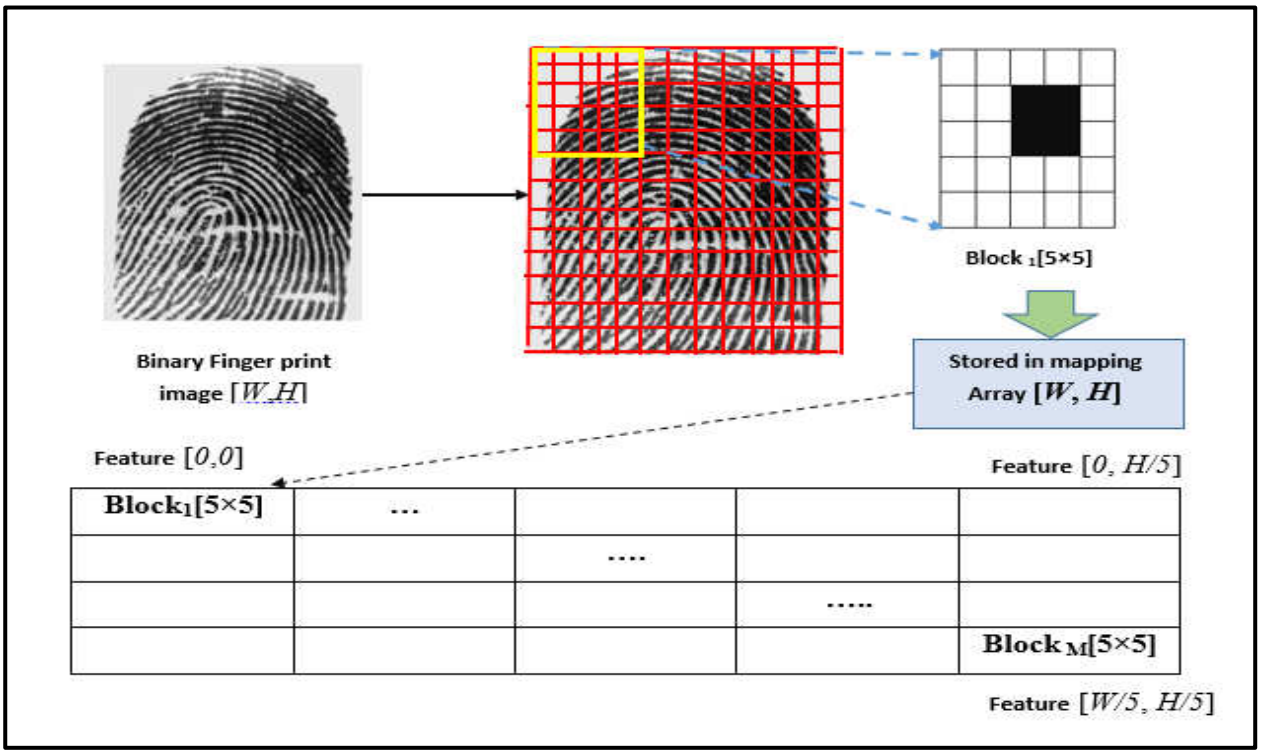


Figure (3.4): Representing the divided fingerprint image into a block

3.6.2 Mask construction

The building of the mask depends on various sizes and patterns. The mask size must satisfy certain conditions. The mask dimensions must be square as Mask [l × l], where l is a prime number ∈ [1,3,5,7,9] and Mask value takes two possible values (white '1'/ Black '0'). Figure (3.5) represents all possible patterns for the mask [l×l]

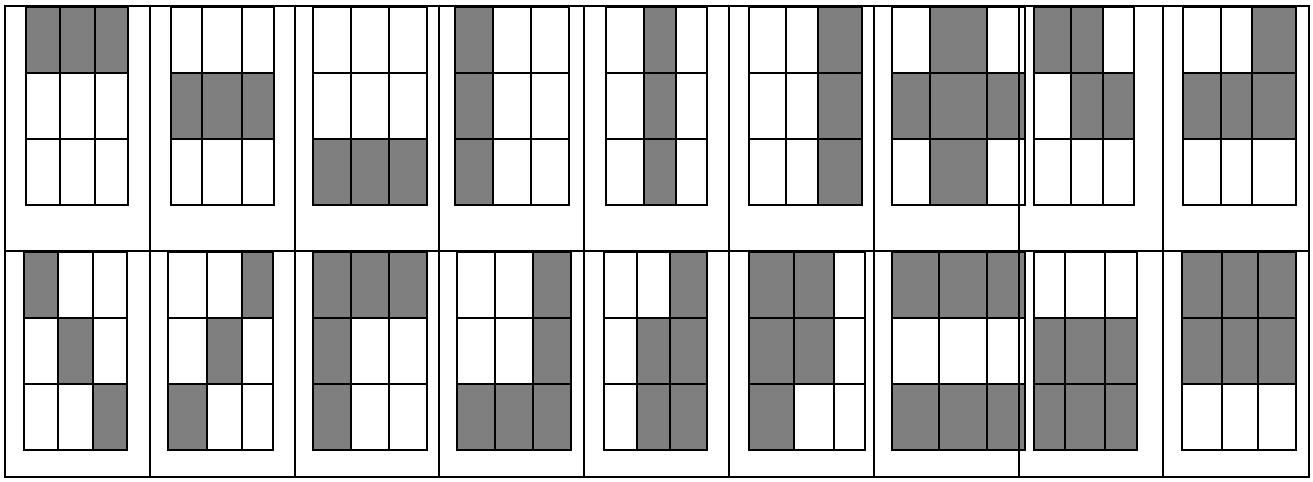


Figure (3.5): Representing all possible patterns for Mask [3×3].

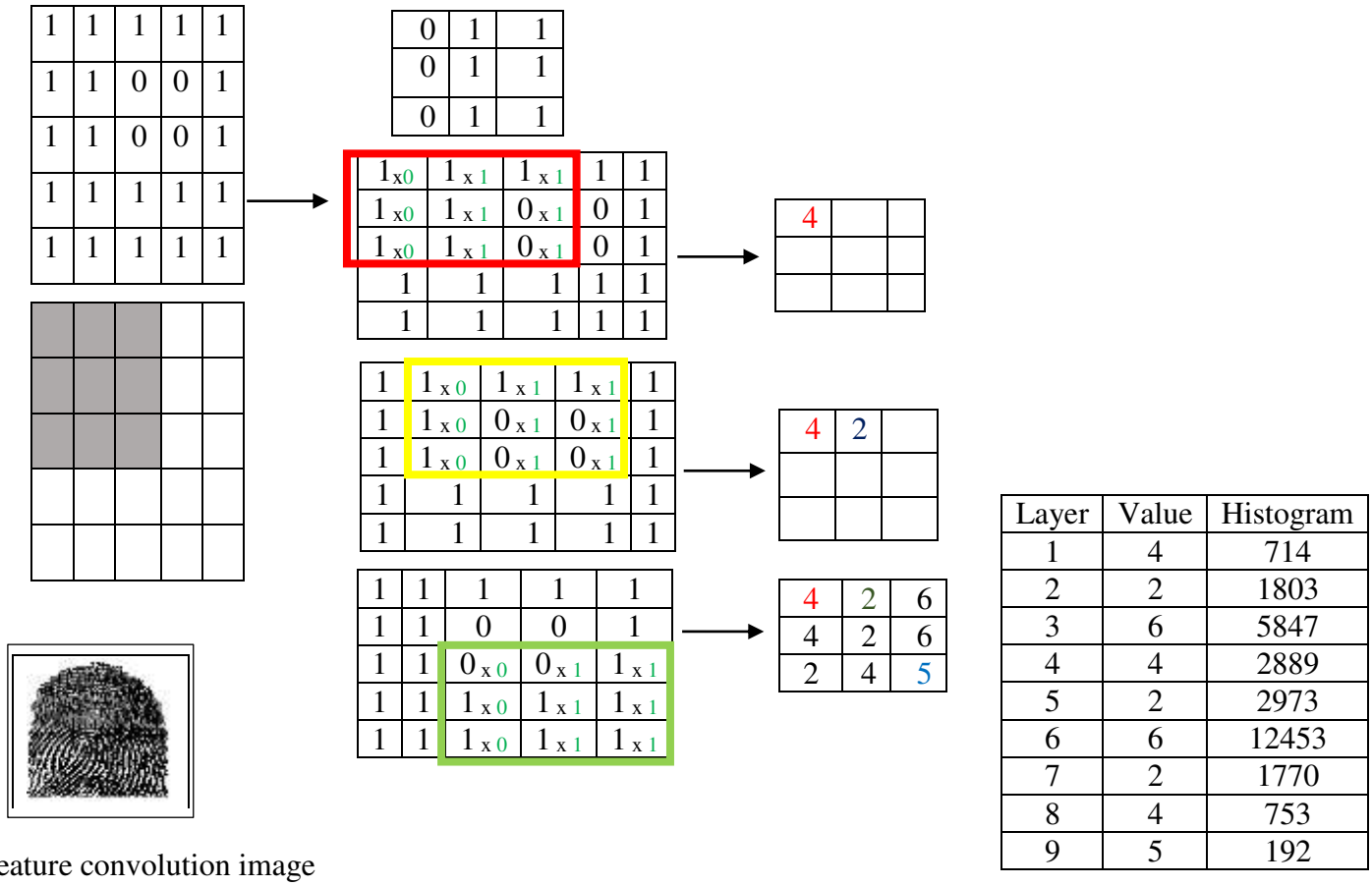
3.6.3 Convolution process

The mask is selected in order to apply to the matrix. For example, the mask [3x3] is selected. The following steps will be applied:

A. Getting the information of each block [k × k] from features [W/5, H/5] array. i.e. getting on the value of Block1 [5 ×5].

B. Applying the mask that is [3×3] at the same time. This mask represents a key of the matrix then applying it to the original block [5× 5] of the matrix, then it is moved from left to right, one element at a time. This process is repeated until the mask reaches the bottom-right corner.

C. At each step, the key [3 × 3] is applied to the original matrix [5 ×5]. The value of the mask is multiplied by the value of the mass covered by the window. These results represent all the values in that window of the image. Figure (3.6) illustrated an example for each step in the convolution process.



Layer	Value	Histogram
1	4	714
2	2	1803
3	6	5847
4	4	2889
5	2	2973
6	6	12453
7	2	1770
8	4	753
9	5	192

Figure (3.6): Steps of the convolution process

3.6.4 Finding max and min location by using histogram convolution

The hit-and-miss transform is a basic operation that is used in a binary image. The hit location in the fingerprint biometric image is represented as a white location and rest location or miss location is represented as a black location. The hit-and-miss operation is performed by translating the origin of the structuring element to all points in the image. The previous step produces into (9) images. The histogram convolution is applied for each image to find the maximum of miss location, where the miss location represents the match between the mask and the original block image as shown in an algorithm (3.2). Figure (3.7) illustrated the result of the histogram convolution algorithm.

Algorithm (3.2): Histogram convolution

Input: image Black and white

Output: Location Max Histogram Location

```
Begin
Step1: Initial parameters
          Smask = 3          (Key)
          Mmask = 5         (original block binary image)
Step2: Apply Convolution and get a result from array 2D    (2.17)
        CFe mask[][]=Convolution(Smask, Mmask, image Black and
   white)
Step3:   for (i = 0; i <  xrow; i++)
                for(j=0; j< xcol ; j++)
                    h = CFeMask[i][j]
                     histConv [h] +;
                endfor
            endfor
Step4: xxmax = histConv [0]                                    (2.18)
           Location =0
          for (t = 0; t <  10; t++)
            if (xxmax <= histConv [t]) then
               xxmax = histConv [t]
              Location = t
   END
```

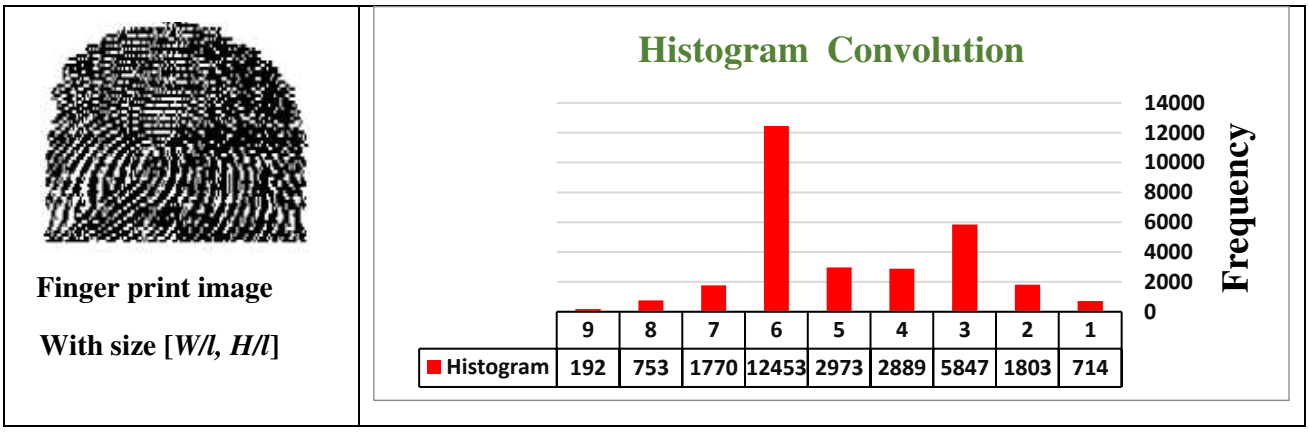


Figure (3.7): Histogram convolution algorithm

As shown in figure (3.7), the max frequency is represented miss location in layer (image) (6) is (12453) and the min frequency is represents hit location in layer (image) (9) is (192). The results of this step have two features of the map for the fingerprint image. The first feature map represents the max frequency of the hit location layer and the second feature map represents the min frequency of the miss location layer. The hit location in the fingerprint image is represented as a white location and miss location is represented as a black location as shown in figure (3.8).

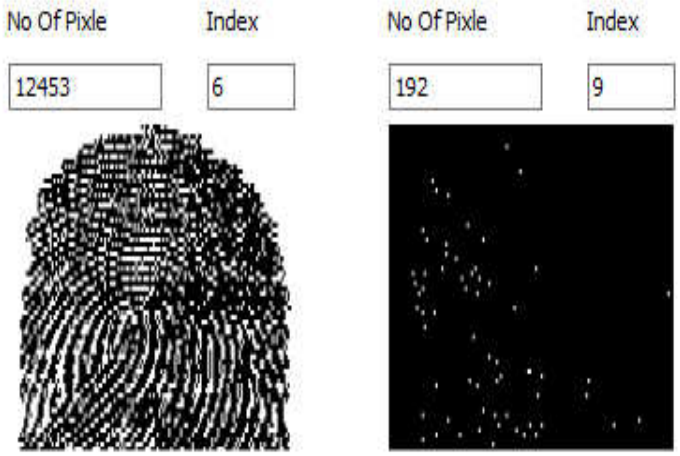
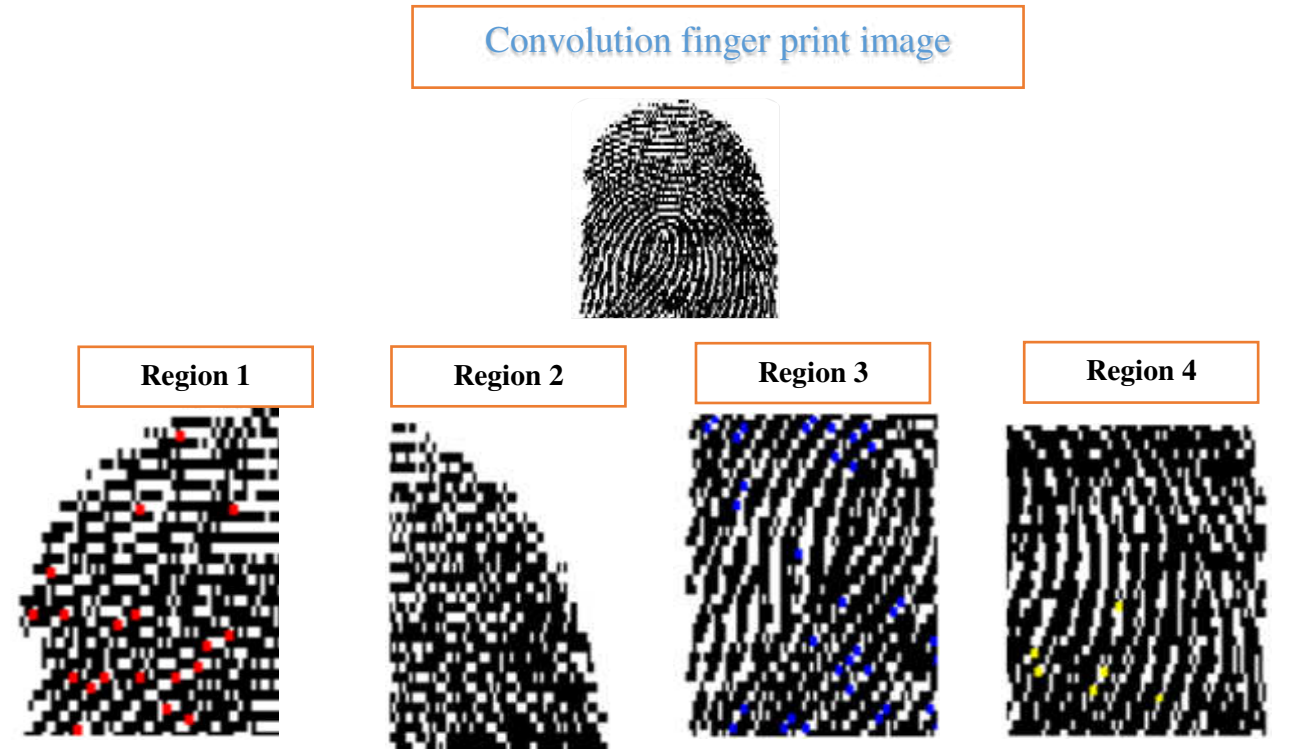


Figure (3.8): Feature of fingerprint image by using the histogram convolution

3.7 Proposing hybrid technique (Stage C)

The basics of hybrid optimization algorithm includes dropping the coordinates of the fingerprint image that is extracted by convolution from the previous step. This image is divided into four regions; each region has a min & max feature coordinates. Min & Max feature coordinates are used as sample

space to find an optimal solution from these coordinates. Inside the fingerprint image, there are important and unimportant regions as shown in figure (3.9)



Region 1 coordinate

#	x	y
1	9	63
2	9	64
3	9	65
4	11	99
..		
..		
62	69	26

Region 2 coordinate

#	x	y

Region 3 coordinate

#	x	y
1	9	2
2	9	3
3	9	4
4	11	0
..		
..		
103	72	97

Region 4 coordinate

#	x	y
1	7	71
2	7	72
3	7	73
4	8	77
..		
..		
18	41	88

Figure (3.9): Feature coordinate position of the optimization

Figure (3.9) shows four regions by using convolution in the fingerprint map, where region 3 consists of (103) locations which represent the maximum feature coordinates. (Max (x, y). The other part in region 4 represents the minimum coordinate (Min (x, y). Region 2 can be considered as a less important region because it has no coordinates, and so on for region 3 and region 4.

3.7.1 Fireworks algorithm (FWA)

Figure (3.10) shows the flowchart of the Firework algorithm (FWA), where the inputs of FWA are four convolution features regions (FW=R1 [x,y], FW=R2 [x,y], FW=R3 [x,y], FW=R4 [x,y]), where (x,y) is represent the Max and Min feature coordinate positions. FWA aims to find three optimal solutions for every four regions of the fingerprint image.

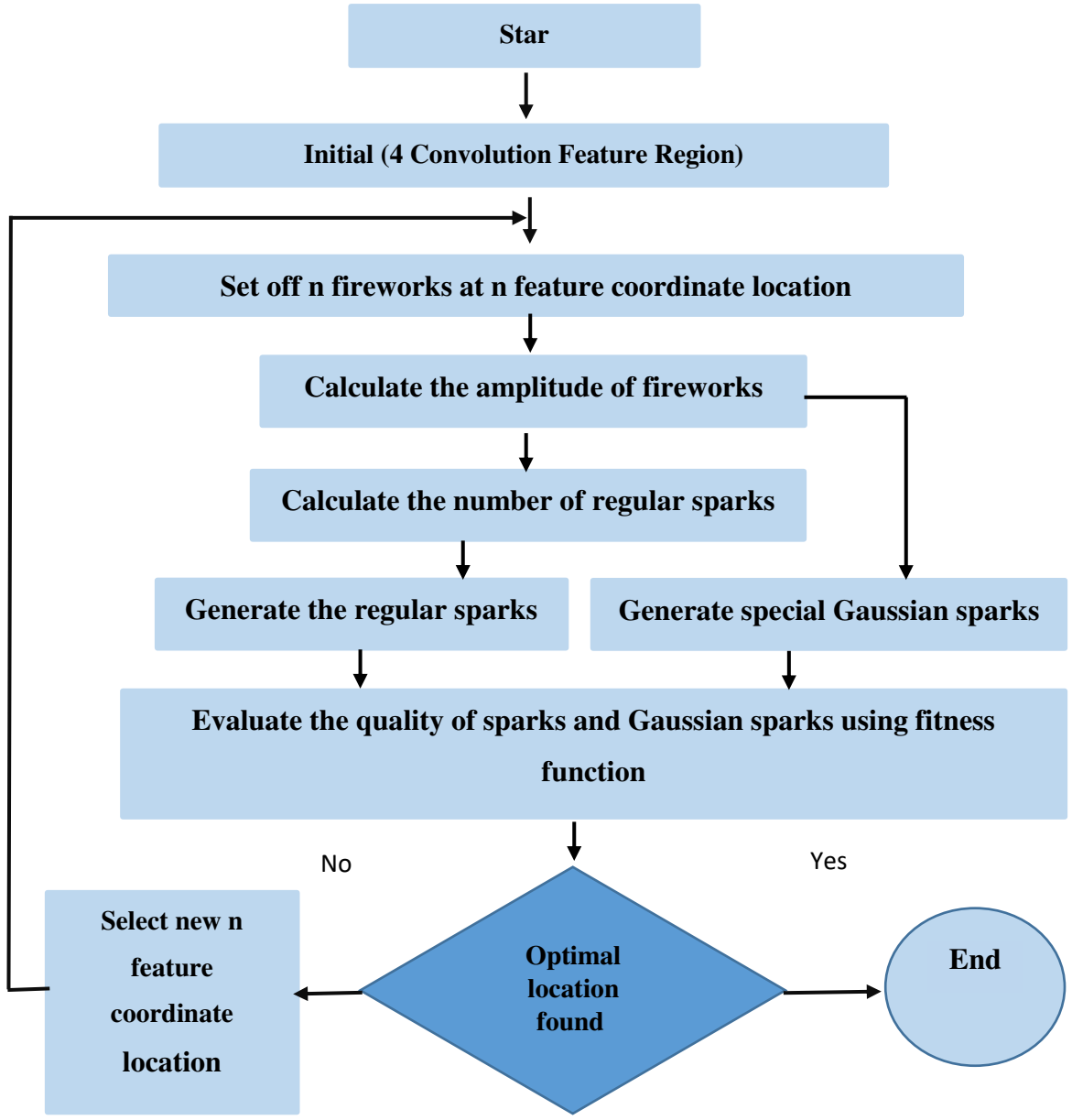


Figure (3.10): Flowchart of the Firework algorithm (FWA)

Figure (3.10) show a Flowchart of the Firework algorithm (FWA). FWA is working in four regions. The FWA takes from each region its feature

coordinates (Min coordinate as start and Max coordinate as a goal). The FWA generates three solutions, which are an initial, spark, and Gaussian amplitude, each one of the solutions must be evaluated based on a fitness function. The fitness function depends on the formula (3.2):

$$\mathbf{Fitness}^{n}_{\mathbf{spar}k} = \text{Max (number of black feature locations)} \quad (3.2)$$

$$\mathbf{Fitness}^{n}_{\mathbf{initial}} = \text{Max (number of black feature locations)} \quad (3.3)$$

$$\mathbf{Fitness}^{n}_{\mathbf{Gaussian}} = \text{Max (number of black feature locations)} \quad (3.4)$$

Where n is the feature coordinates location [x,y] in four regions. The best solution is the maximum number of black location and the worst solution is the less minimum number of white locations. The feature of the fingerprint image is extracted by convolution. The FWA always follows the edges of the fingerprint image. The initial solution is matching with an edge of a fingerprint image, so by default it is considered the optimal solution.

The spark and Gaussian amplitude solutions can be considered optimal solutions if they have a max number of the black locations. This means that they are on the edge of their fingerprints.

FWA outputs contain three solutions: The global solution, which represents one the best solution of initial capacitance, spark, and Gaussian in all four regions of the fingerprint image. The best solution represents the best solution for each region (initial, spark, and Gaussian amplitude) means the maximum number of black locations.

Finally, the worst solution represents the worst solution for each region (initial, spark, and Gaussian amplitude) means the maximum number of white locations. for each FWR. The algorithm (3.3) illustrated FWA in detail. Figure (3.11) shows an example of the output of FWA.

Algorithm (3.3): fireworks of algorithm

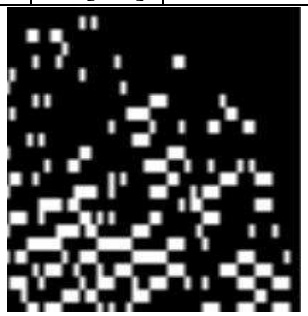
Input: Coordinates feature, image
Output: Global (initial, spark and gaussian)

Begin
Step 1: Initialize 4 fireworks to feature Coordinate position Split image to four regions each regain include fireworks to feature Coordinate position
Step 2:
loop until done
for each firework
calculate the amplitude of the firework (2.3)
calculate the number of regular sparks and generate the regular sparks
end for
Generate special Gaussian sparks
Evaluate each spark by check Coordinate positions on best positions
black convolution matrix from the list of sparks،
select 4: to act as feature Coordinate positions of new fireworks
create 4: new fireworks
end loop
return the feature Coordinates positions of the best spark found

FW1=R1	**FW2=R2**
FW3=R3	**FW4=R4**

#	R[X,Y]	Original Feature	New feature
1	R1[0.0]	1-6	0
2	R2[0.1]	1-45	41
3	R3[1.0]	1-15	8
4	R4[1.1]	1-41	38

#	X	Y
1	47	42
2	47	43
3	47	44
4	50	18
5	50	19
6	50	20



#	X	Y
1	4	39
2	4	40
3	4	41
-		
44	40	46
45	40	47

#	X	Y
1	25	6
2	25	7
3	25	8
-		
14	51	34
15	51	34

#	X	Y
1	0	45
2	0	46
3	0	47
-		
-		
41	43	4
41	43	5

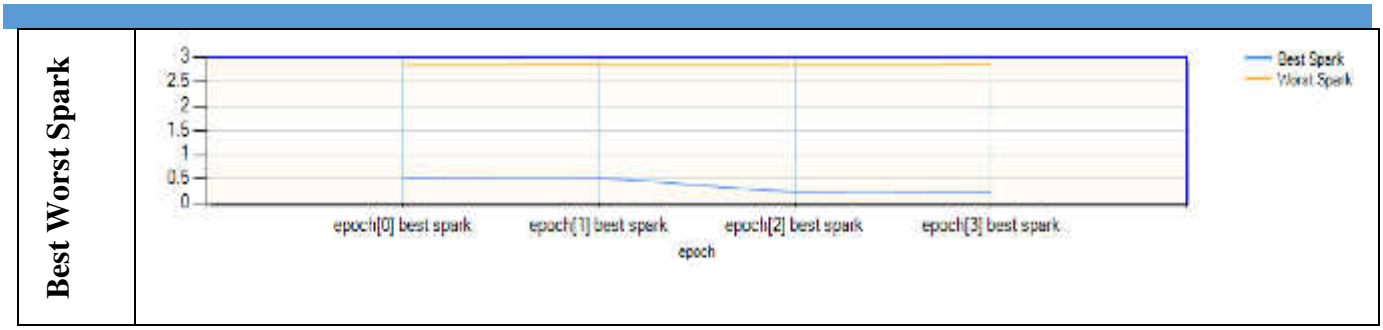


Figure (3.11): Output of the Firework algorithm (FWA)

3.7.2 Camel Herd Algorithm (CHA)

Figure (3.12) shows a flowchart of the Camel Herds Algorithm (CHA). The CHA relies on the behavior of camels in the desert, knowing that there is a leader for each herd, the major purpose of the herd searching for food and water depending on factor humidity value (Hum) is taking into consideration that there is a neighboring strategy.

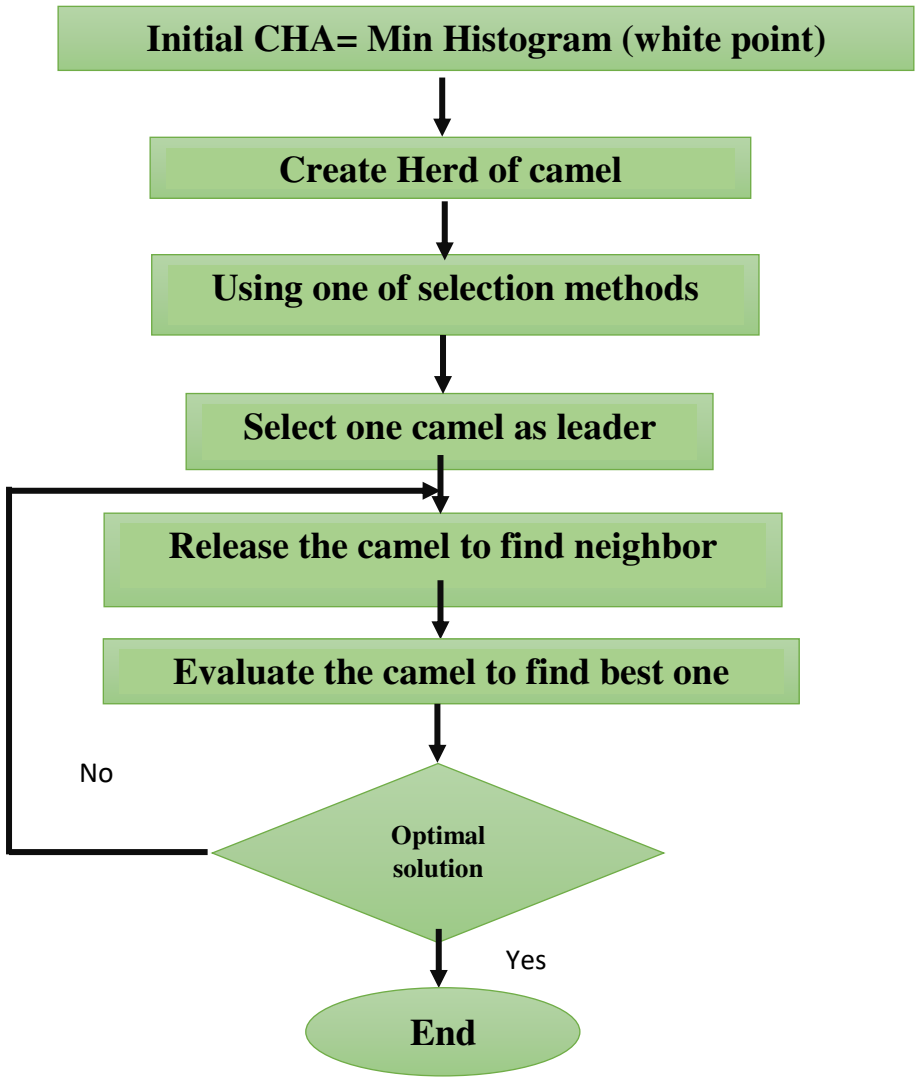


Figure (3.12): Flowchart of the Camel Herds Algorithm (CHA)

As shown in figure (3.12), CHA consists of several steps in order to find the optimal solution, which is described in detail in the algorithm (3.4).

Algorithm (3.4): Camel herds algorithm

Input: DataMax is Coordinates position **Max histogram convolution**
DataMin is Coordinates position **Min histogram convolution**
d is number neighbors
k is number neighbors space breeze

Output: The best Hc (best solution)

Step1: Select one of the herd based on coordinates min is called a leader
Step2: Generating the number of camel herd except for a leader
I_ leader**=1;**
For each Coordinates position herd (leader) Do
Generate neighbors (k) for leader **is call Element**_Coordinates
If Element_ Coordinates ∈ **dataMax then**
leader [**I_** leader]= Coordinates dataMax
I_ leader +=1
End
Step3 Initialize symbol space of Humidity
For each Coordinates position (**Datamax**) Do
Select one of Coordinates DataMax to call Select_Coordinates
If Select_ Coordinates∉ leader then
Select_ Coordinates add to list Sp_Hum
End for

Step4
loop until done
For each Coordinates leader (leader)Do
For each element Coordinates leader (Sp_Hum[leader])Do
Get P_Strat Coordinates (element .x, element.y).
Generate neighbors (K) randomly for the element. (2.10)
Find best_Hum by Calculate min Distance P_Strat with all (2.11)
neighbors and Insert the best Hc
End for
End for

```
        Update Sp_Hum
        Update leader
END
```

Step 1: The algorithm (3.4) classifies the number of herds where each herd produces one solution. The herds take a number of camels and the CHA selects one of there and makes it a leader for the herd. LHC denotes the leader of herds and it selects the position of LHC based on coordinates min histogram convolution. Each LHC starts from different points on the space problem. This approach gives a variety of solutions. For example, if the sample space = 7×7, selects one coordinate position [x,y] = min histogram convolution to be position of LHC. Each camel has sample space =3×3 to find the neighbors, max histogram convolution assigned for (Camels and Humidity (Hum)), where the Hum represents the goal that all the camels search in specific space to find it

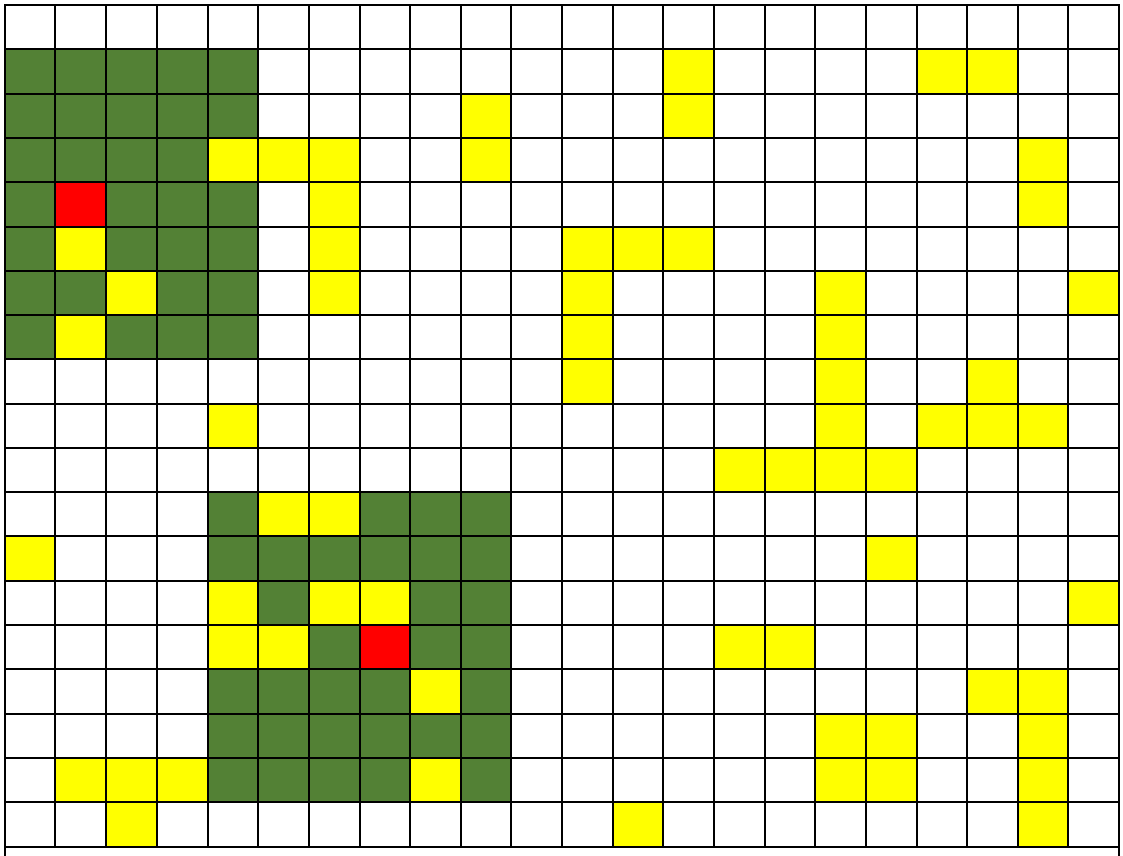
.

Step 2: After preparing the parameters, the CHA introduces the herds in the search space. The leader starts with its coordinate position [x,y], guide other camels to find food and water. A leader checks the neighbor of the camels, and fumbles high humidity. For example, any camel can reach Max -Hum in its search space 3×3 then this is camel replaced with current leader LHC of this area to be a new leader LHCs and start over again. The LHC (new and old) move represents the solution or the key and this solution, is saved in the dataset.

Step 3: When, each herd finishes its own action, the algorithm produced a number of solutions (neighbors). The distance between camel and Max-Hum, must be calculated to find the best neighbors. Therefore, the minimum distance represents the optimal solution (HC). The information is saved the location of HC in datasets. Figure (3.13) illustrates each step in the algorithm (3.4) to find the best solution by using a camel herd's algorithm.

Initial	
LHC	Camel

Get Location		Get Random Location	
#	(X,Y)	#	(X,Y)
1	3,1	4	44,5
2	15,7	5	10,49



LHC	Camel 1
{X=3,Y=2}	{X=15,Y=8}

Definition color is used in the example			
White color represents space solution	Green color represents space problem	Red color represents a leader of Herd	Yellow color represents the location of a solution

Figure (3.13): Camel Herds Algorithm (CHA)

3.7.3 Hybrid optimization algorithm

They propose of a hybrid optimization algorithm consists of firework and camel herd's algorithms. The goal of the proposed algorithm is to increase the speed of access to the best solution and thus reduce the access time that improves the performance of the optimization.

The principle of the hybrid optimization algorithm is enhancing the performance of the firework algorithm (FWA) by replacing the Gaussian sparks solution by the Camel herd's solution or (best_ HC). The Gaussian is used in FWA to generate new sparks that follow the Gaussian distribution. Gaussian works poorly in FWA.

On one hand, it only affects the fireworks, ignoring the sparks that are generated by the explosion operator and thus narrowing the interaction between the sparks. On the other hand, the sparks that are generated by gaussian can hardly be passed down to the next generation. In addition, when Gaussian generates a spark, it can close to the selected firework, or close to the best firework, or distance to both of them but on the line between the selected fireworks. The algorithm (3.5) illustrates each step in Hybrid optimization algorithms.

Algorithm (3.5): Hybrid optimization algorithms

Input: Coordinates feature, image d is number neighbors flock of camels k is number neighbors space breeze
Output: coordinate best spark
Begin Step 1: initializes 4 fireworks to feature Coordinates positions Split image to 4 reigns each reign includes fireworks of feature Coordinates positions Step 2: Datamax is Coordinates position max histogram convocation

dataMin is Coordinates position Min histogram convocation

step 3:

loop until done

for each firework

calculate the amplitude of the firework (3.2)

calculate the number of regular sparks (3.3)

generate the regular sparks

end for

Step3-1 Select a leader for herd depends on min and call leader

Step3-1Generation of camel herds except for the leader

I_ leader=1;

For each Coordinates position herd (leader) Do

Generate neighbors (k) for leader is call Element_ Coordinates

If Element_ Coordinates ∈dataMax then (2.10)

leader [I_ leader]= Coordinates dataMax (2.11)

I_ leader +=1

Endfor

Step3-3

initialize symbol space of Humidity

For each Coordinates position (Datamax) Do

Select one of Coordinates DataMax to call Select_Coordinates

If Select_ Coordinates∉ leader, then

Select_ Coordinates add to list Sp_Hum

End for

Step3 -4

loop until done

For each Coordinates leader (leader)Do

For each element Coordinates leader (Sp_Hum[leader]) Do

Get P_Strat Coordinates (element .x, element. y).

Generate neighbors (K) randomly for the element.

Find best_Hum by Calculate min Distance P_Strat with all neighbors and Insert the best Hc

End for

End for

Update Sp_Hum

Update leader

Steps3-5 evaluates each spark by check Coordinates positions on best positions black convolution matrix

from the list of sparks،

select 4 to act as feature Coordinates positions of new fireworks

create 4 new fireworks

end loop

return the feature Coordinates positions of the best spark found

END

3.7.4 Hybrid optimization based on chaotic maps (HOAC)

The proposed HOAC follows the same procedure of hybrid optimization algorithm as shown in the algorithm (3.5), but the proposed HOAC maps use 3D logistic chaotic maps to generate a random number to determine the domination in a random manner. HOAC maps consist of two steps:

First step: Generating random numbers using the 3D logistic chaotic map as shown in the algorithm (3.6).

Second step: Applying hybrid optimization algorithm (3.5)

Algorithm (3.6): Generating random number based on 3d logistic maps

The input set of the parameter of the 3d logistic maps

$\mu = 3.6$, where $3.53 < \mu < 3.81$

$\beta = 0.0001$, where $0 < \beta < 0.002$

a=0.0012 , where $0 < a < 0.002$

$x_0 = 0.5$ // initial value for x $y_0 = 0.001$ // initial value for y $z_0 = 0.8$ // initial value for z iteration =100 [] x array 1d of an integer number []y array 1d of double number
Output: dataset (Row Count, x, y, z, x)

Begin
Step1 for i = 0 to iteration
{
Logistic _ x_1 = apply equation (2.24)
Logistic _ y_1 = apply equation (2.25)
Logistic _ z_1 = apply equation (2.26)
Dataset .Add (Row Count, x_0, y_0, z_0, x_0)// for first element in dataset
x[i] = i
y[i] = x_0
x_0 = Logistic _ x_1
y_0 = Logistic _ y_1
z_0 = Logistic _ z_1
Dataset .Add (Row Count, x_0, y_0, z_0, x_0)
}
Return dataset (Row Count, x, y, z, x)
 	
END

3.6 Generating stream cipher key (Stage D)

An efficient algorithm is proposed to generate stream cipher key with variable length using the best coordinates position features. They are created by applying the proposed hybrid optimization algorithm. The algorithm (3.7) illustrates details to generate the key.

Algorithm (3.7): Key Generation

Input: Coordinates positions feature k is number neighbors
Output: bitstream cipher key
Step 1: Generation set points by using apply linear interpolation Between center point and all Coordinates positions feature

call set_Point

Step2: Calculating Mid-point

Step3: Generation QR code base on text

3-1 set initial QR code

QRCode Encode Mode = QRCodeEncoder.ENCODE_MODE.BYTE

QRCodeScale = 4 , QRCodeVersion = 2

3-2 get text

3-3 generation QRCode(text) call QR_T

3-4 Convert QR_T To Bitmap Call QR_T_Bitma

Step 3: Generation key Bit

For each element Coordinates positions (Set_Point)Do

Generate neighbors (K) from QR_T_Bitma image.

Calculate Count Black and White

If Count Black =k then bit=0

If Count White =k then bit=1

Else

Get a stream of bit by represents Black and White in

neighbors (K)

End for

return the stream of bit key Generation

Step 1: The algorithm (3.7), is calculating Mid-Point for all coordinates positions feature. For example, each P (x,y) point in Coordinates positions feature with start point (19,53) compute the sum of : sumx=x+19 and Sumy=y+53 and count x=count x+1 and count y=count y+1 , repeated for all P. find Mid x= sumx /countx , Mid y = Sumy /county .

Step 2: The liner interpolation between center point (Mid x, Mid y) and all coordinates positions feature P (x, y) to generate a set of points (x, y) is called set _Point. The interpolation is the process of finding points between two points on a line or curve.

For example, if P_1 (3,4) and P_2 (5,8), to find value y when x=4 by using interpolation formal given in equation (3.3) as follows:

$$\mathbf{y}\text{-}y_1 = \frac{y_2-y_1}{x_2-x_1}(x\text{-}x_1)$$

$$\mathbf{y}\text{-}4=\frac{8-4}{5-3}(4\text{-}3) \qquad (3.3)$$

$$\mathbf{y}\text{-}4= 2 \qquad y = 6$$

The new point $P_3 = (4, 6)$, where $3 < 4 < 5$ and $4 < 6 < 8$.

Step 3: QRcode is active by entering a random text For example "my computer" this represents a Bitmap format called QR_T_Bitma. The QRCode has various versions. The QRcode generates a stream key algorithm which is QRCode version=2 with cell size =4. Each character in input text converted to the binary square in QR code to produce a Binary image called QR_T_Bitma.

Step 4: To create the stream key, we drop points extracted from interpolation (Set_Point) on the QR_T_Bitma image, each P_i in Set_Point and it checks its neighbors based on mask size. Mask size represents sample space to find k_j neighbors of P. Check each neighbors k_j for P_i, if k_j=Black color then increment (count Black) by 1 in otherwise if k_j=White color then increments (count white) by 1, To find the stream key there are three cases:

Case1: If all neighbors k_j in sample space n×n = Black Pixels key bits=0 is selected.

Case2: if all neighbors k_j in sample space n×n = White pixels key bits=1is selected.

Case3: if the neighbors k_j in sample space n×n is mixed pixels (white and black), each k is checked. If they are black the bits=0 otherwise=1 (i.e.) bit= 110001110. Figure (3.14) illustrated an example of the generated stream key.

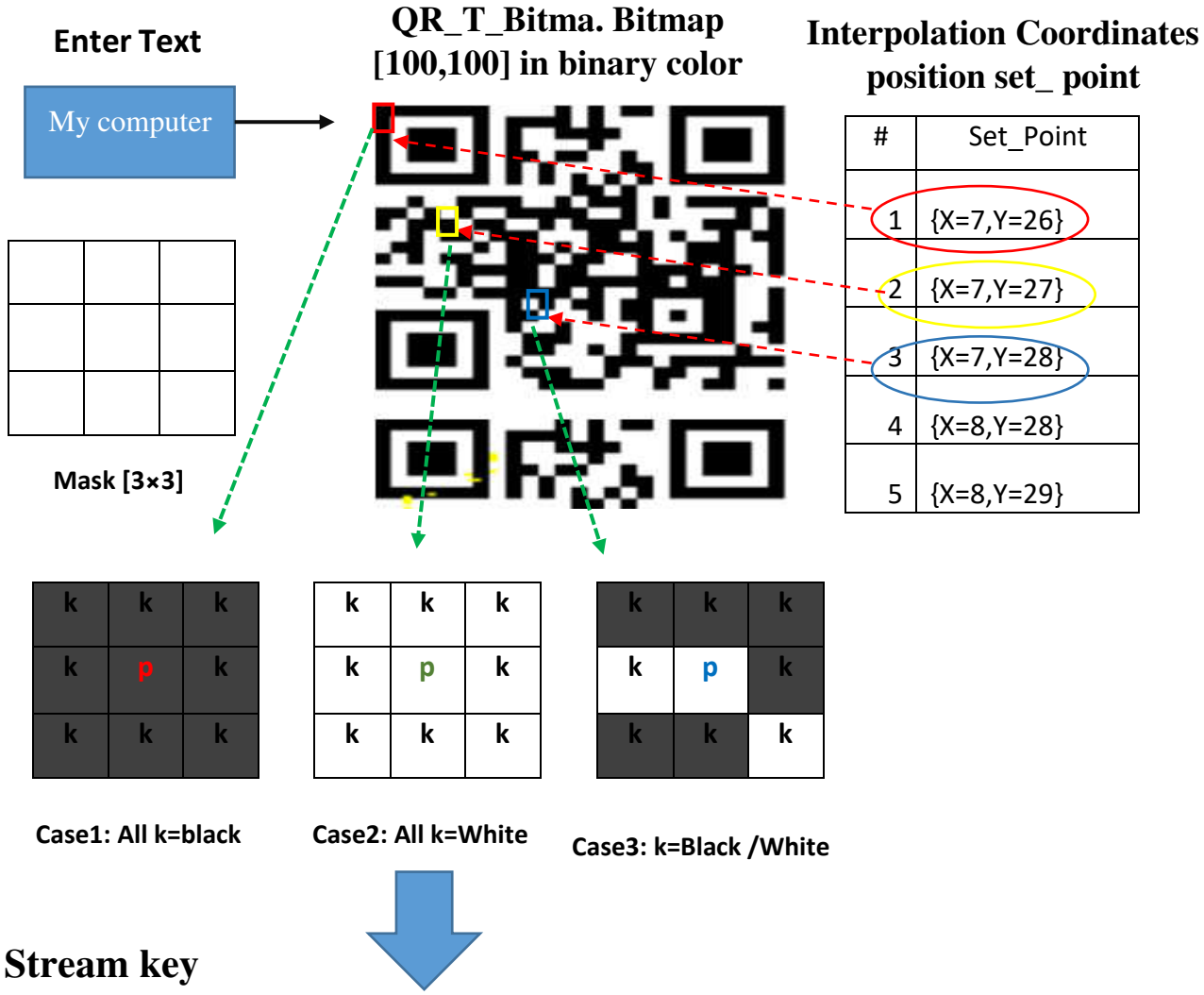


Figure (3.14): Generate the stream cipher key

3.8.1 Test random number key

The key is extracted it must be measuring the strength of randomness in two cases of tests of the random number test. First the random number generation test of fireworks with hybrid and second the random number generation test of fireworks out a hybrid. These tests are important and updated

in order to measure the randomness of complete binary sequences. It is applied by programming in a computer depending on random cryptographic.

3.8.2 Uses Key

The key extracted is used in two important cases:

1. Generating prime key used for multiple users
2. Generating key used to hide text inside the image

1. Prime Key

The stream cipher key is a variable-length arbitrary that is extracted using the best coordinate position feature based on the random text of QRcode. Which are founded through applying the hybrid optimization algorithm. It is checked by using the "Miller Rabin test" so as to get the highest percentage of the prime key.

2.Hidden Text

The system uses steganography to hide text inside the image by the following:

1. Inserting secret text in the still image by using one (LSB Technique) based on an image obtained from the histogram convolution technique.
2. Extracting the stego-text from many stego objects (images). The image is received by another side.

Finally, this technique will make it difficult to detect that there is a hidden message inside the image. Depending on some metrics are calculated results is the MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio), fidelity Image (FI), and Universal Image Quality Index (UIQI) morals of the stego image

CHAPTER FOUR

IMPLEMENATION OF PROPOSED SYSTEM

Chapter Four

Implementation of the Proposed System

4.1 Introduction

This chapter represents the implementation and results of the proposed system. The experimental tools are used in the proposed system, which contains Image preprocessing, different threshold, feature extraction, histogram value, and steps organization.

This chapter presents the results of the experiments by taking a set of biometric images based on the fingerprint to test the performance of the system through some improvements.

4.2 System Implementation

The algorithms are implemented by using the Hardware and Software environment with the following specifications:

4.2.1 Software environment

The proposed system is implemented by using a programming language (#C) that has certain and important tools compared to other languages. The proposed system is applied in windows ten (Win10) operating system. (#C) language deals with an easy path to access the image data of every digital image format. A software language first appeared in 2000 by Microsoft. The programming language (#C) is similar to Java language, as it is fast, and simple, and running on windows.

4.2.2 Hardware Environment

The proposed system is implemented on the computer (laptop) with the following specifications:

Table (4.1): Specification of computer

Major information about the computer	
Processor	Intel(R) Core(TM) i5-7200U, CPU @ 2.50 GHz 2.70 GHz
RAM	4.00 GB
System Type	64-bit operating System
Operating	Windows 10
Programming language	C #
Programming	Microsoft Visual Studio 2013 Visual
Microsoft office	2016

4.3 Fingerprint image database

The following Figure (4.1) contains (6) samples of the fingerprint images selected from the FVC2004 database to be applied in the system.

Figure (4.1): The forms of fingerprint image

F1	F2	F3	F4	F5	F6
					

4.4 Results of the proposed system

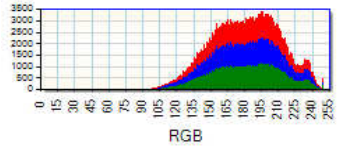
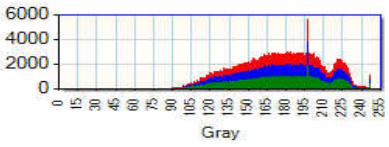
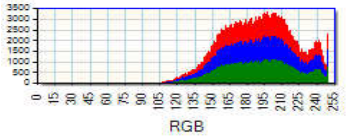
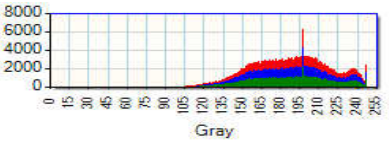
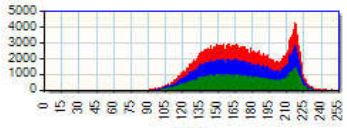
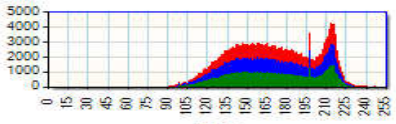
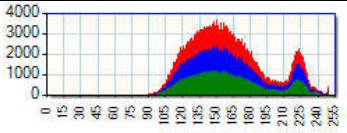
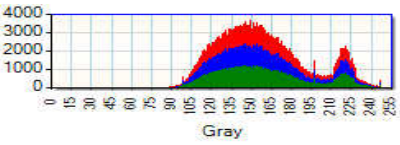
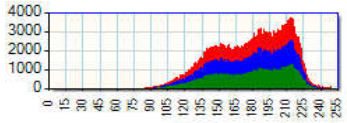
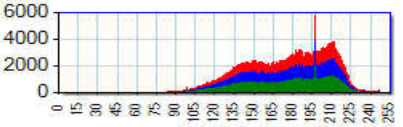
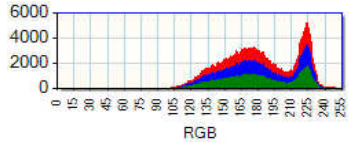
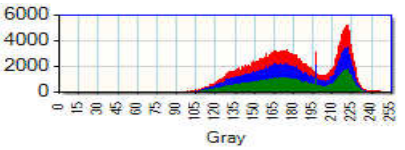
The experimental results gained from the proposed system are extracted by applying the algorithms, which are explained previously for each step used in the system. It has three stages executed gradually, starting with image uploading and ending with testing, as explained in the following steps:

4.4.1 Results of the image preprocessing

Table (4.2) Shows (6) samples of the original images of the fingerprint. The Pre-processing depends on the Otsu method. The table shows the effect of

the Otsu method on the image with finding the threshold of each image and the frequency before and after pre-processing.

Table (4.2): Pre-processing of the fingerprint image

#	Original Image	Frequency	Threshold By using Otsu	Results	Frequency
1			173		
2			187		
3			171		
4			169		
5			171		
6			182		

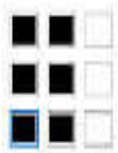
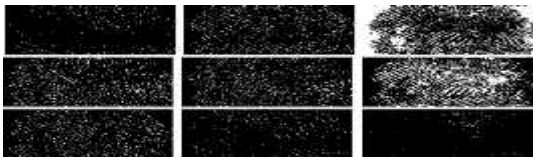
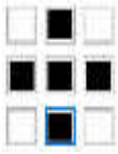
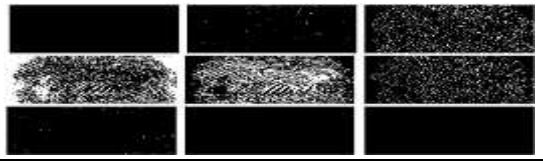
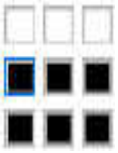
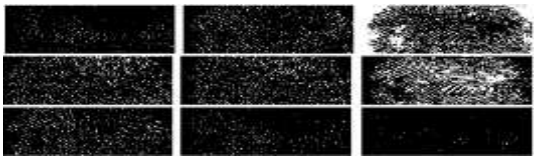
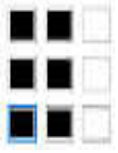
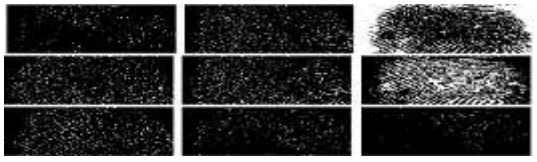
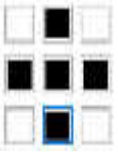
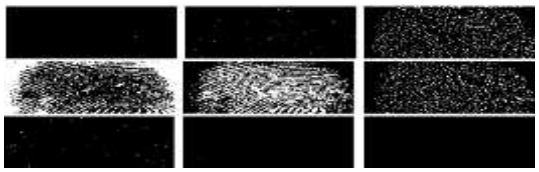
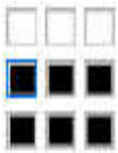
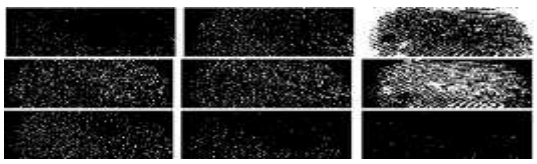
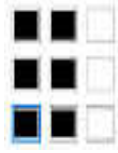
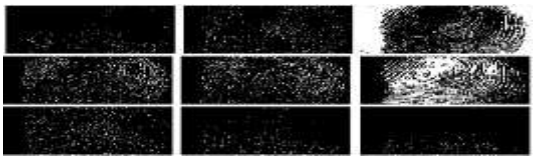
4.4.2 Results of feature extraction

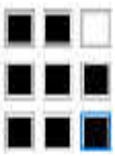
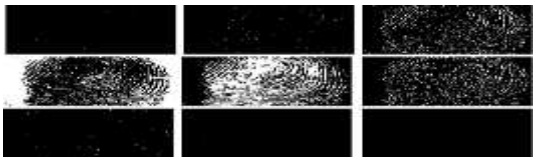
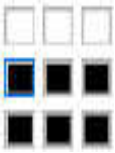
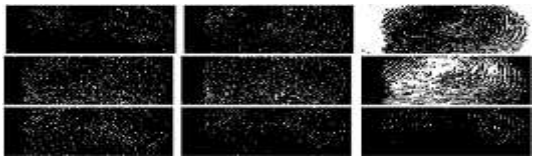
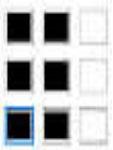
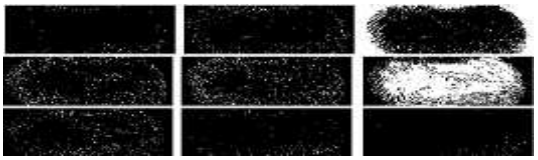
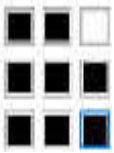
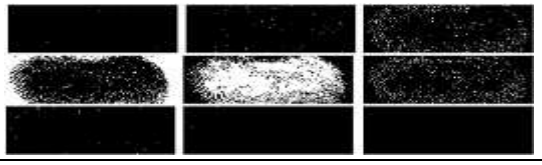
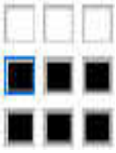
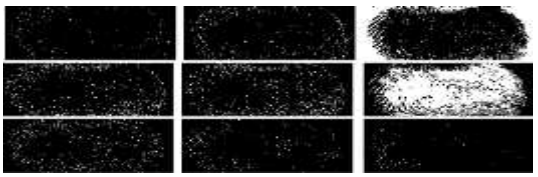
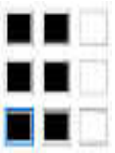
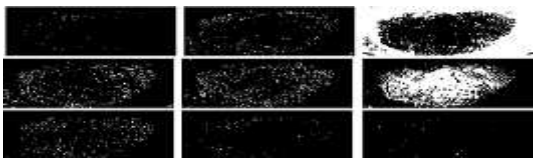
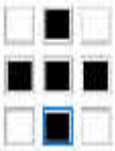
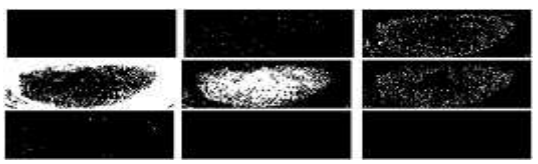
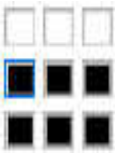
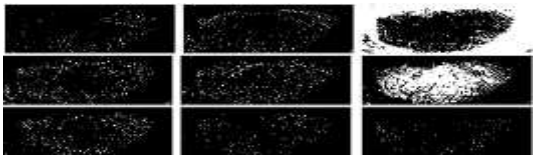
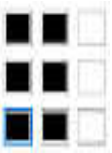
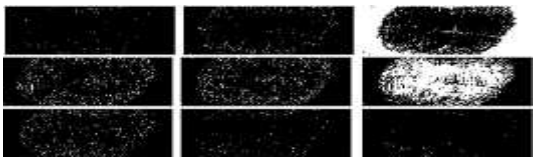
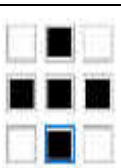
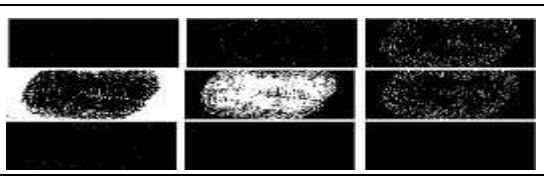
Feature extraction by using convolution techniques. These tables depend on (6) samples of fingerprint biometric images. The images in these tables are the results of the process Otsu methods.

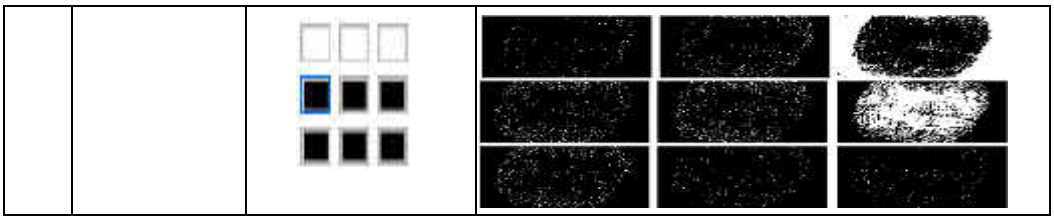
4.4.2.1 Effect of mask difference

Table (4.3) shows the effect of a different pattern mask on the image used in the process feature extraction by using the convolution technique. It is based on three different patterns of the mask with (6) samples of the fingerprint biometric images. After processing, the convolution process gives (9) images. Each image contains a set of features. The (feature) coordinates in the image are different depending on the pattern and strength of the selected mask.

Table (4.3): Effect mask difference

#	Image	Select mask	N.Value
1			
			
			
2			
			
			
3			

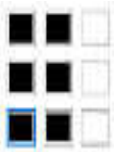
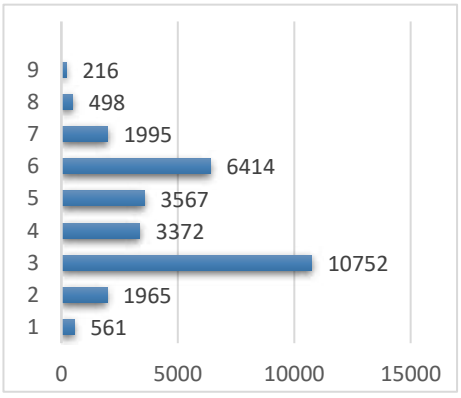
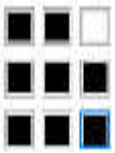
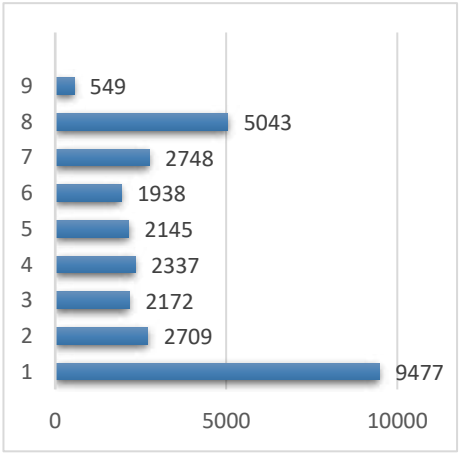
			
			
4			
			
			
5			
			
			
6			
			

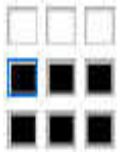
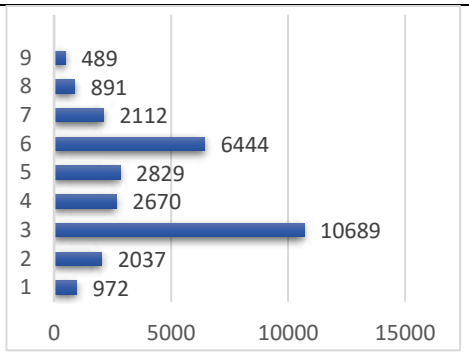
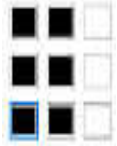
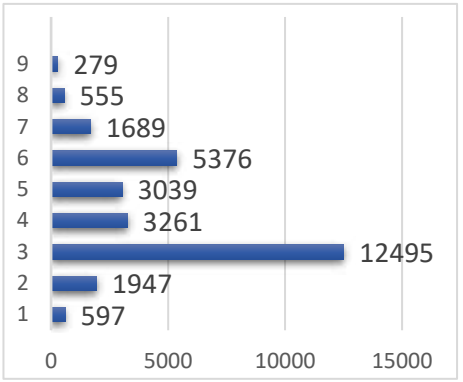
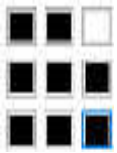
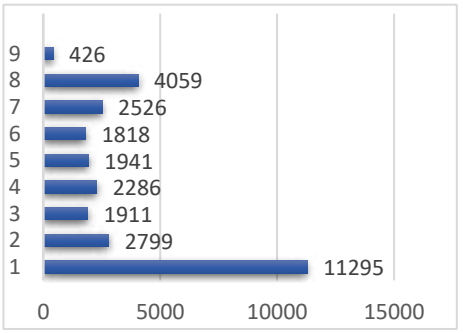
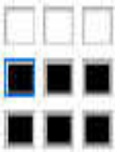
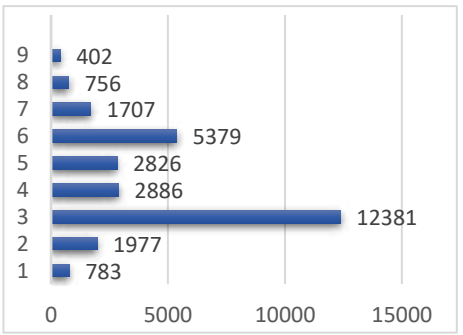
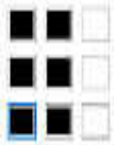
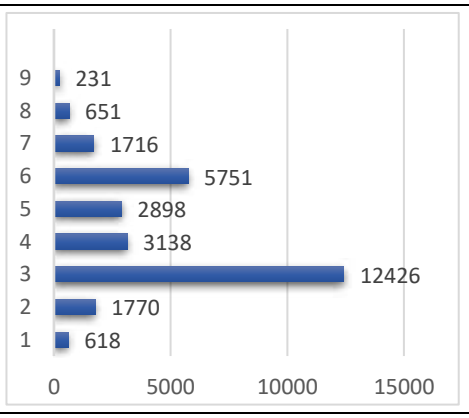


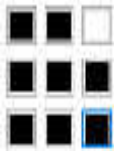
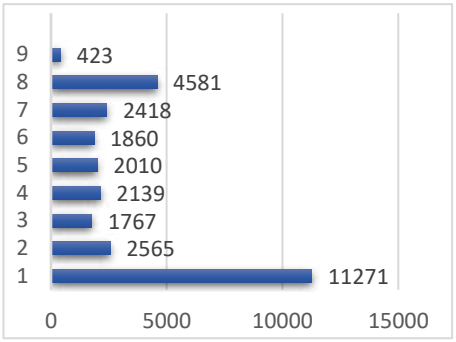
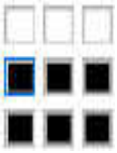
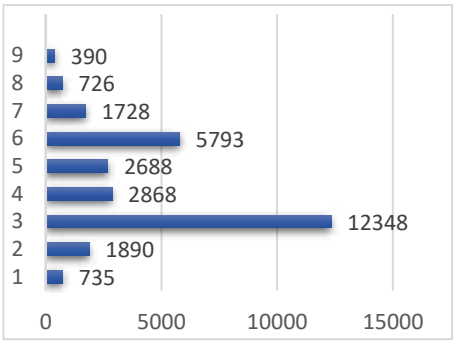
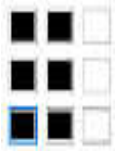
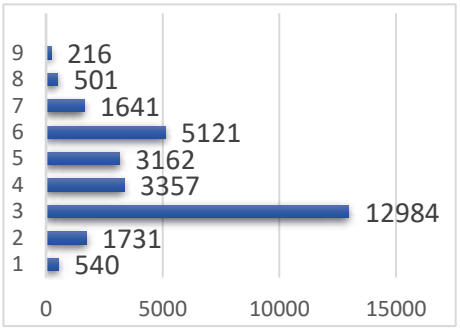
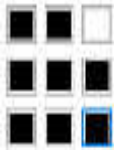
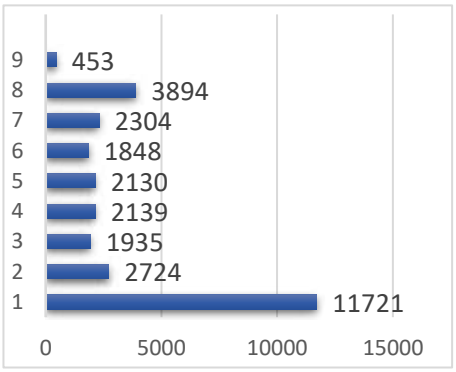
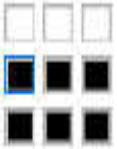
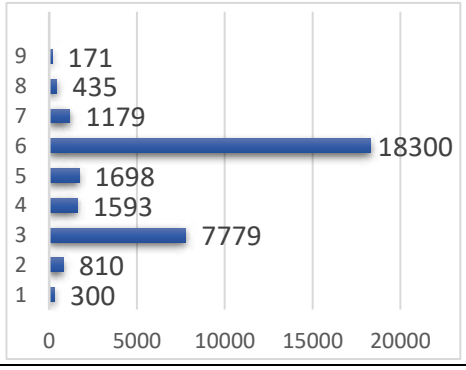
4.4.2.2 Results of finding max and min of histogram convolution

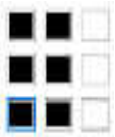
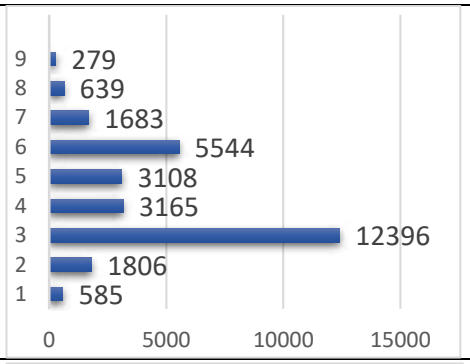
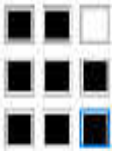
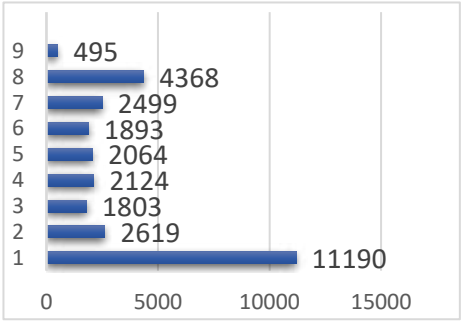
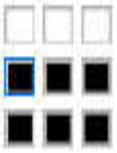
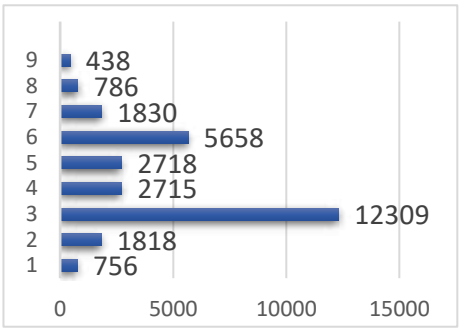
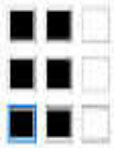
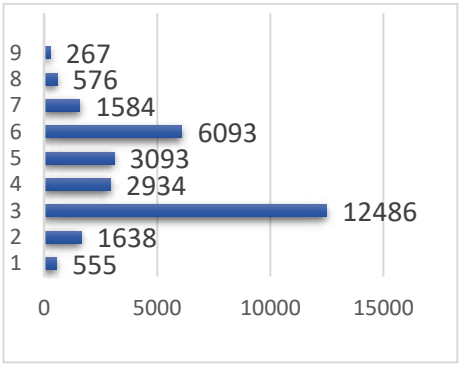
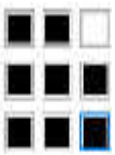
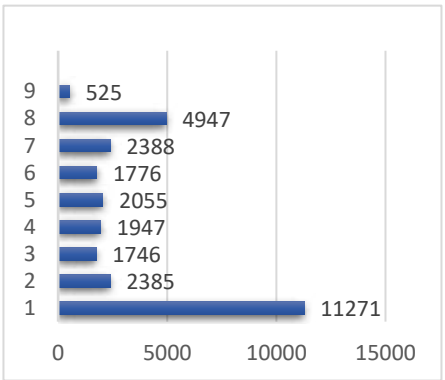
Table (4.4) shows histogram convolution based on three different patterns of the mask with (6) samples of the fingerprint biometric images. The first field in the table represents the resulting image of the convolution technique. Which is based on the patterns of the mask. It also shows the effect of different mask patterns on the results (max and min) value of the image.

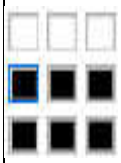
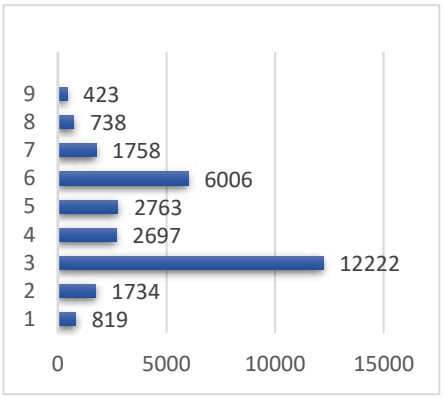
(Table 4.4): Max and min of histogram convolution

#	Image convolution	Select Mask	Histogram Convolution	No. of feature	
				Max	Min
1				10752	216
				9477	549

				10689 	489 
2				12495 	279 
				11295 	426 
				12381 	402 
3				12426 	231 

				**11271** 	**423** 
				**12348** 	**390** 
4				**12984** 	**216** 
				**12271** 	**420** 
				**18300** 	**171** 

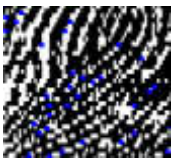
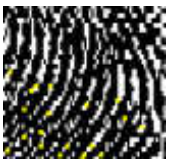
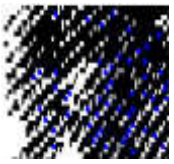
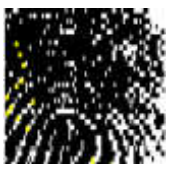
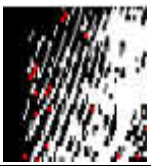
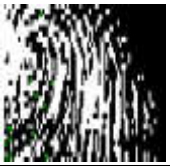
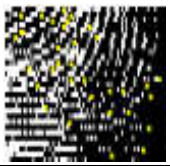
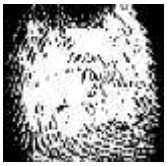
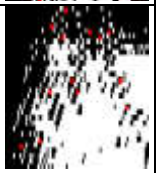
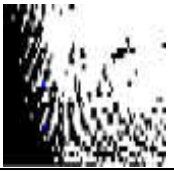
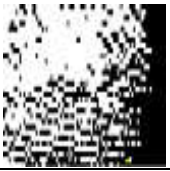
5				12396 	279 
				11190 	495 
				11290 	482 
6				12486 	267 
				1271 	252 

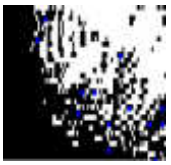
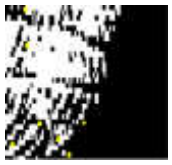
				1222	423
					

4.5 Proposing hybrid technique (coordinate of optimization)

Table (4.5) shows the best coordinate of the image. The resulting image of the convolution process is divided into four regions using the convolution technique. Each region contains a set of coordinates. Furthermore, each region contains max and min coordinates. In table (4.4) image convolution = four Region in FW [R00, R01, R10, R11]

Table (4.5): Coordinates of region

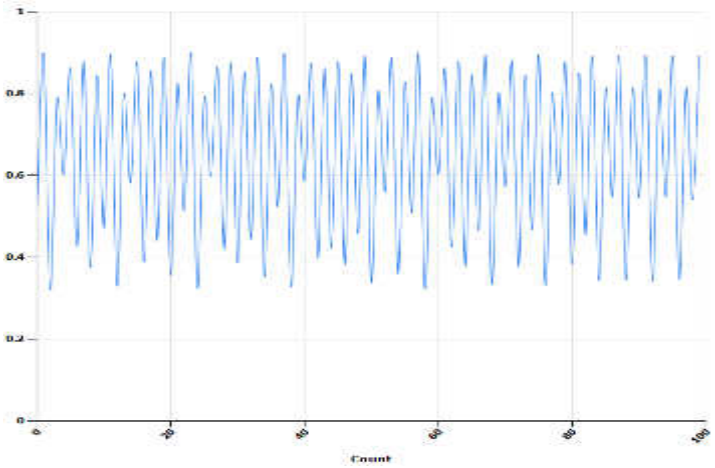
#	Image	Max	Min	Regions			
				R00	R01	R10	R11
1							
2							
3							
4							

5							

4.5.1 3D Logistic Map

Table (4.6) shows the fireworks algorithm based on 3d logistic chaotic maps to generate a random number in a random manner, similar to the key used by the same to the authorized person.

Table (4.6): 3D Logistic Map

Coordinate					3D Logistic Map
#	X	Y	Z	R	
1	0.5	0.001	0.8	0.5	
2	0.9006	0.0037	0.5760	0.9006	
3	0.9006	0.0037	0.5760	0.9006	
4	0.3224	0.0143	0.8792	0.3224	
5	0.3224	0.0143	0.8792	0.3224	
6	0.7873	0.0508	0.3822	0.7873	
7	0.7873	0.0508	0.3822	0.7873	
8	0.6028	0.1742	0.8501	0.6028	
9	0.6028	0.1742	0.8501	0.6028	
10	0.8626	0.5183	0.4587	0.8626	

4.5.2 Hybrid optimization algorithm

Table (4.7) shows the regions of firework algorithms. Each region has a set of coordinates. These coordinates are changeable (increase or decrease) when the number of iterations within the region is changing. Where (Fn) represents the number of images.

Table (4.7): Coordinates of optimization

Image	Region	No. of original Feature	Iteration	Fireworks with the 3D logistic map	Hybrid with the 3D logistic map

F1	R00	105	10	99	11
			30	103	69
			60	103	105
	R01	0	10	0	0
			30	0	0
			60	0	0
	R10	101	10	0	46
			30	98	97
			60	59	56
	R11	59	10	0	56
			30	0	57
			60	59	57
F2	R00	58	10	54	11
			30	56	58
			60	56	58
	R01	6	10	0	1
			30	4	4
			60	106	106
	R10	108	10	54	11
			30	0	66
			60	102	106
	R11	33	10	0	31
			30	102	106
			60	33	31
F3	R00	62	10	0	52
			30	51	62
			60	60	62
	R01	3	10	1	0
			30	1	0
			60	1	1
	R10	84	10	32	36
			30	76	82
			60	84	82
	R11	15	10	13	0
			30	13	11
			60	13	13
F4	R00	62	10	56	50
			30	60	62
			60	60	62
	R01	0	10	0	0
			30	0	0
			60	0	0

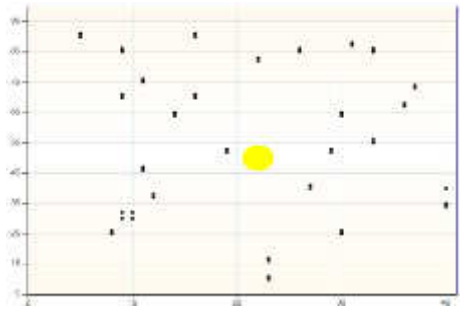
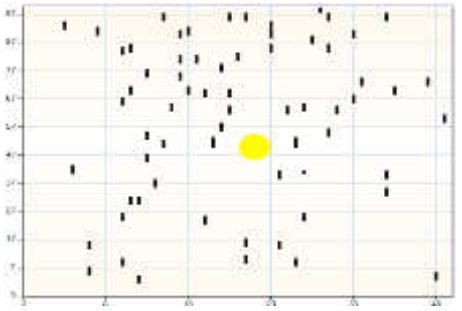
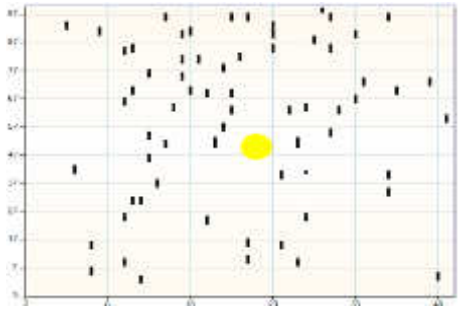
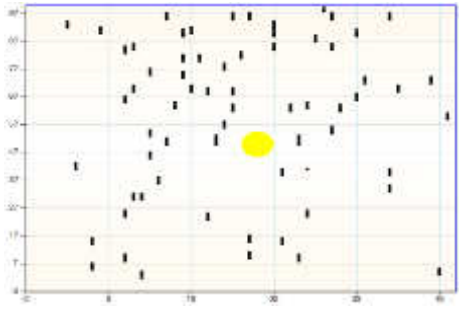
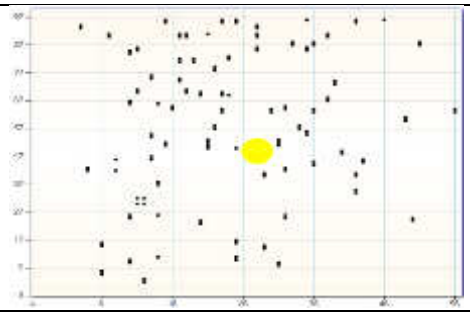
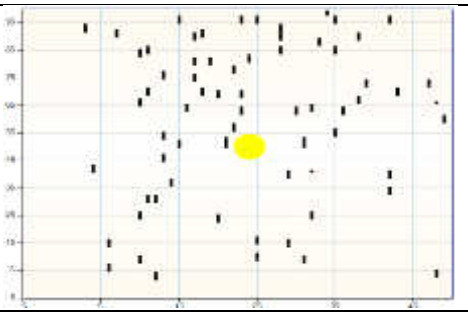
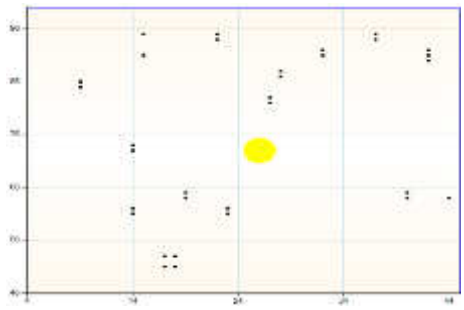
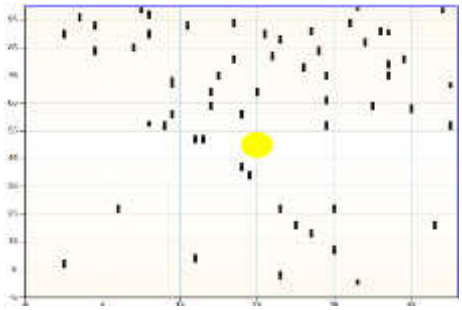
	R10	103	10	0	91
			30	95	101
			60	101	101
	R11	18	10	0	16
			30	0	16
			60	18	16
F5	R00	65	10	32	47
			30	64	65
			60	64	64
	R01	3	10	1	0
			30	1	1
			60	1	1
	R10	97	10	85	52
			30	91	95
			60	97	95
	R11	27	10	0	25
			30	27	25
			60	25	25
F6	R00	28	10	12	19
			30	24	28
			60	26	28
	R01	3	10	1	0
			30	1	0
			60	1	1
	R10	96	10	79	62
			30	94	93
			60	94	94
	R11	12	10	0	10
			30	0	10
			60	12	10

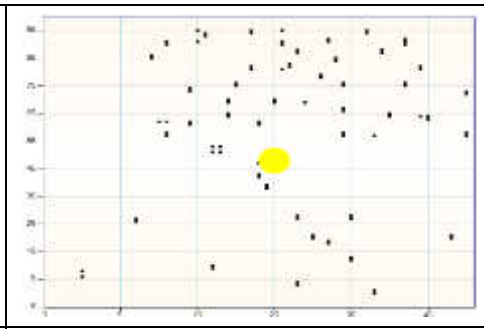
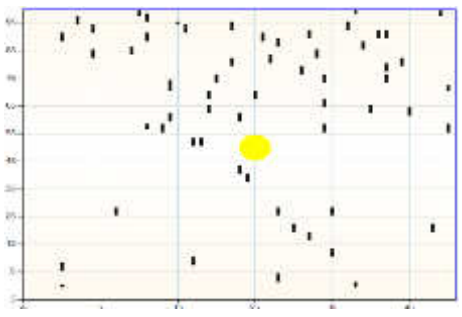
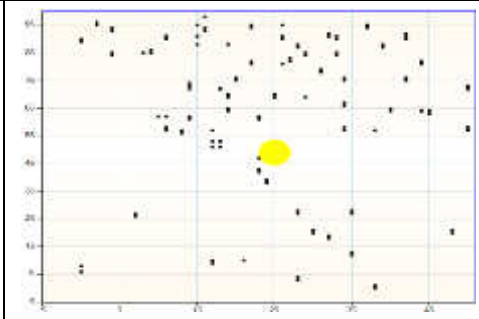
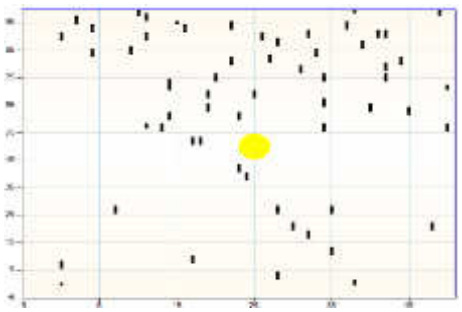
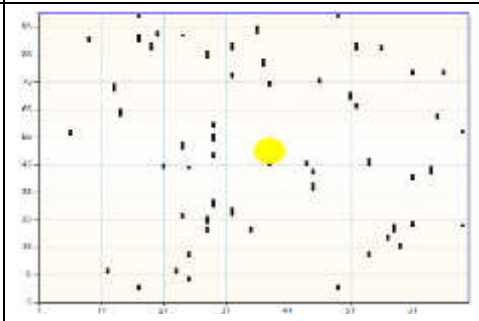
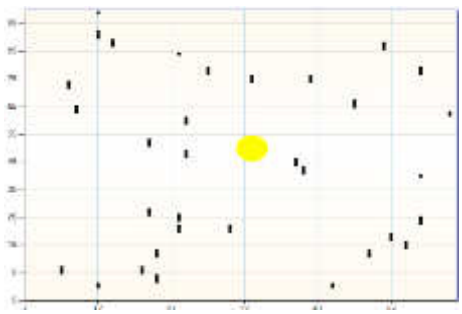
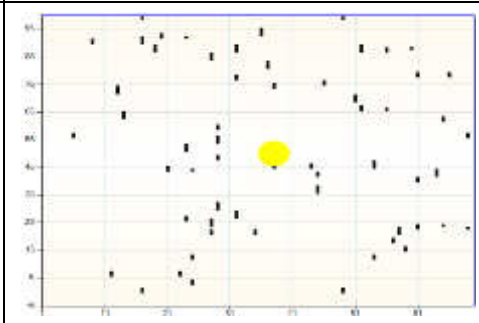
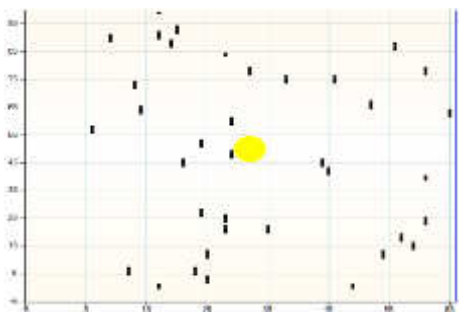
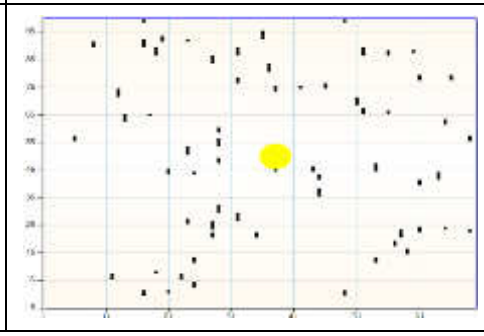
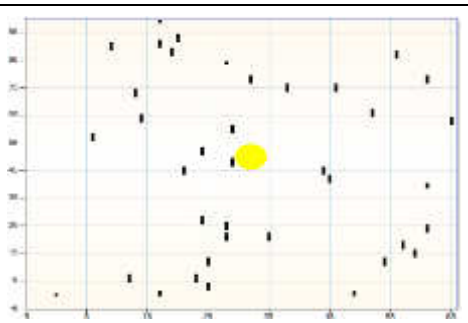
4.5.3 Optimization Based on 3D Logistic Map (All Points)

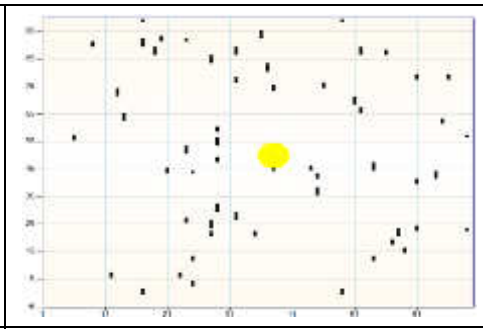
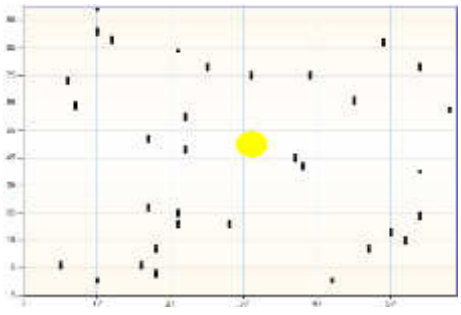
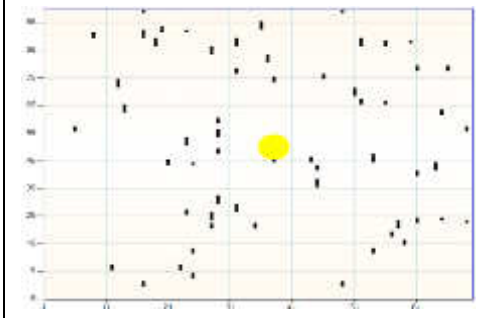
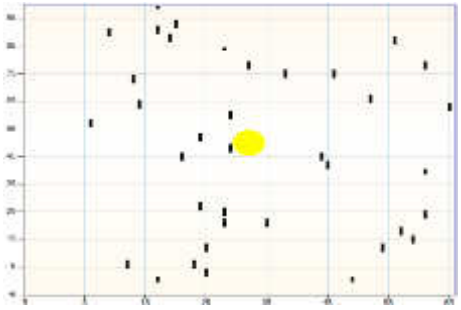
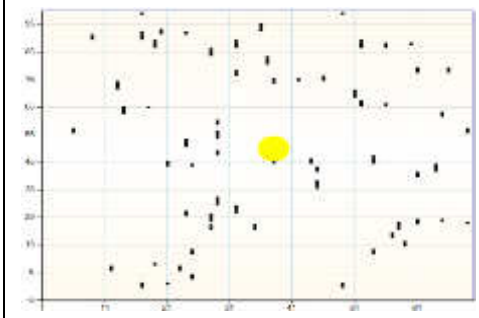
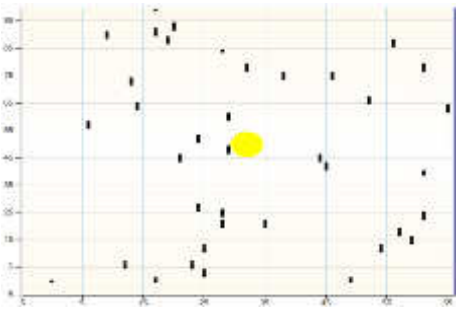
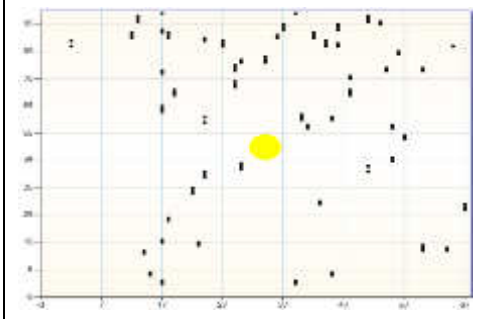
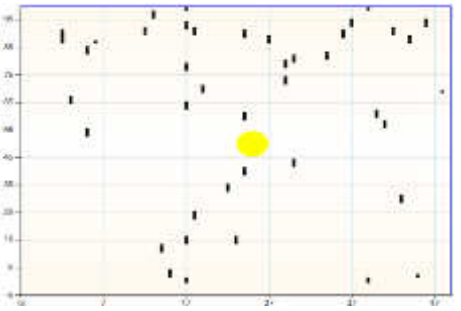
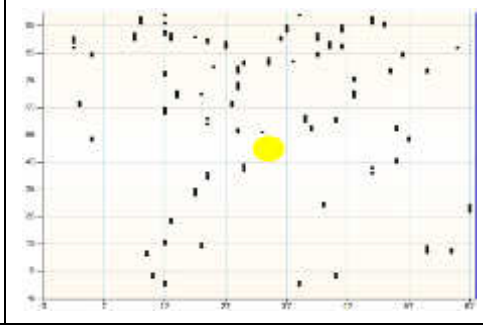
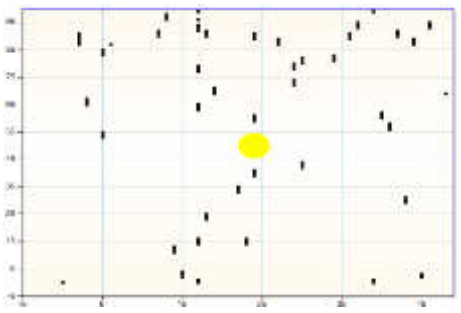
Table (4.8) Case all points coordinates, this table based on (6) samples of the fingerprint biometric images. Shows the optimal coordinates when using fireworks with the 3D logistic chaotic map and hybrid with the 3D logistic map to find the optimal solution. We find that the solutions with hybrid with the 3D logistic chaotic map are more than solutions without Hybrid due because the hybrid technique with the 3D logistic chaotic map is based on the number of

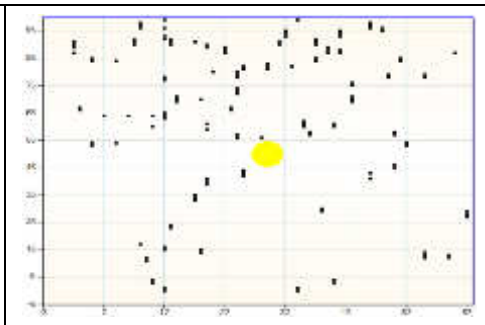
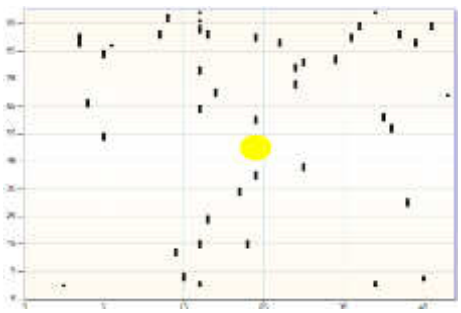
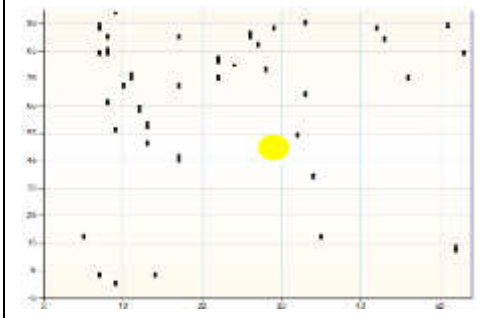
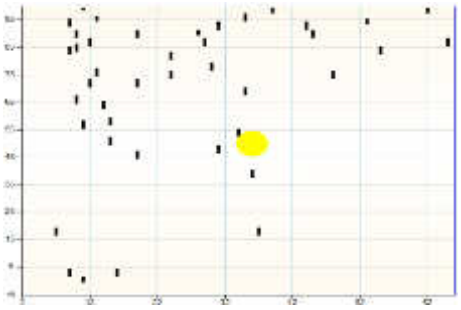
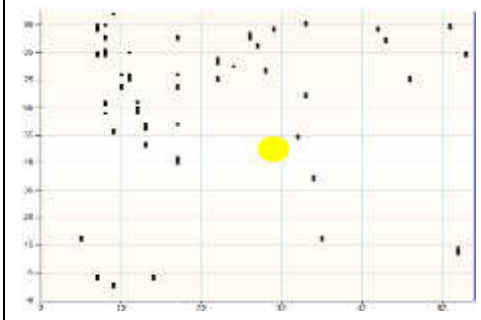
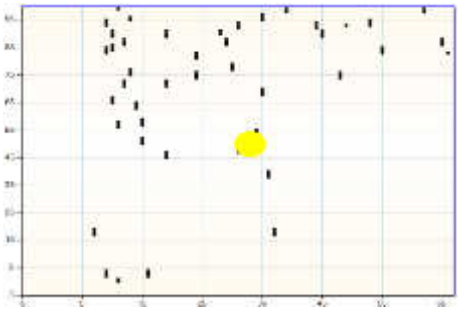
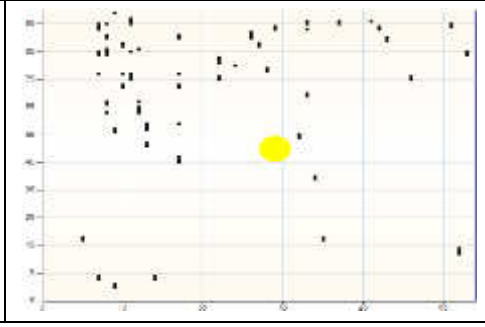
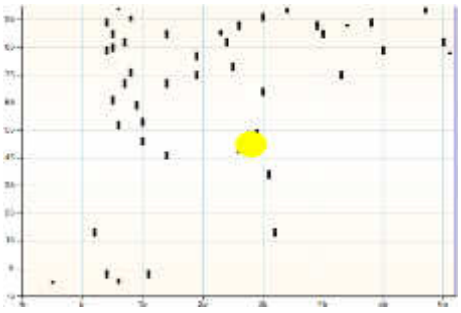
iterations all the greater the number the number of iteration increases arrival to the optimization. Where (Fn) in the table represents the number of the image is used, the point black represents all point coordinates, and Point Yellow represents Implying Mid-point.

Table (4.8): all points coordinates

All Points				
#	**Image**	**Iteration**	**Fireworks with the 3D logistic map**	**Hybrid with the 3D logistic map**
1	**F1**	**10**		
		30		
		60		
2	**F2**	**10**		

		30		
		60		
3	F3	10		
		30		
		60		

4	F4	10		
		30		
		60		
5	F5	10		
		30		

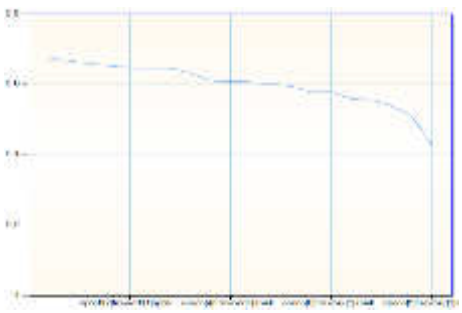
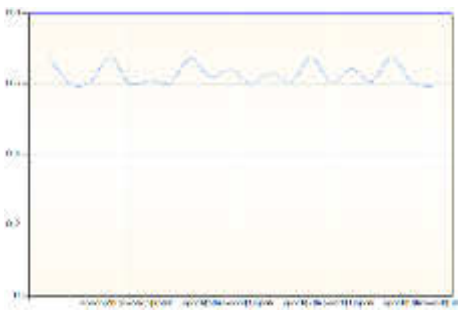
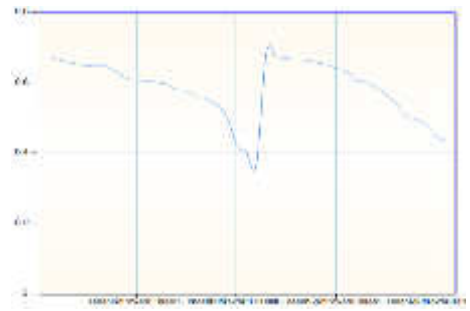
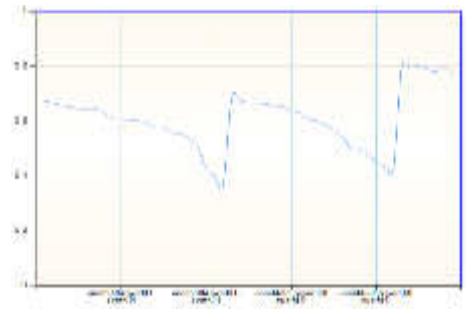
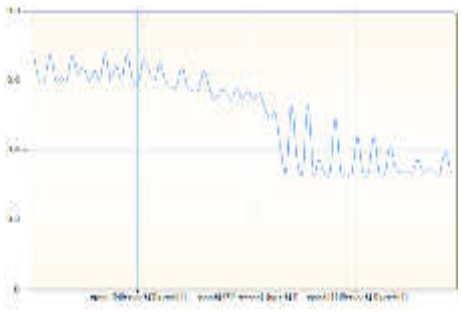
		60		
6	F6	10		
		30		
		60		

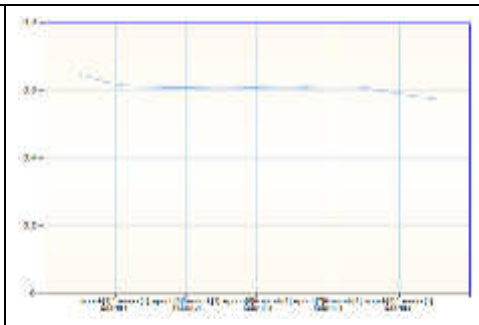
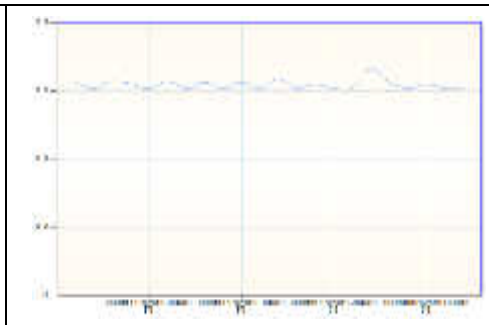
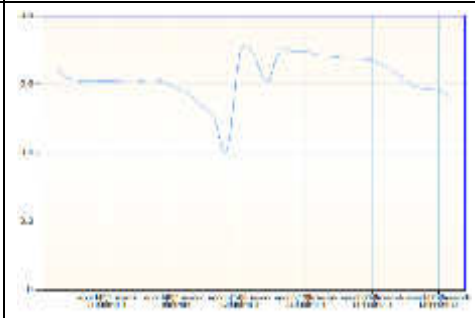
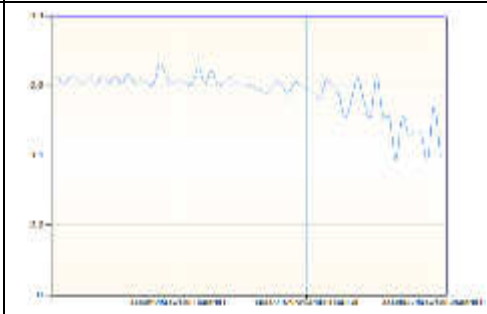
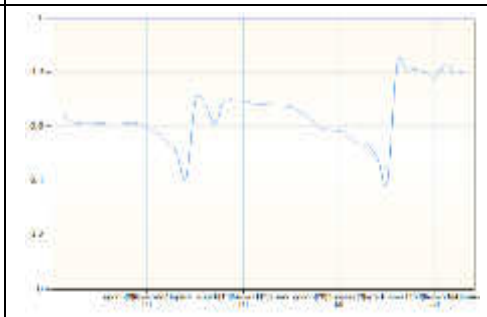
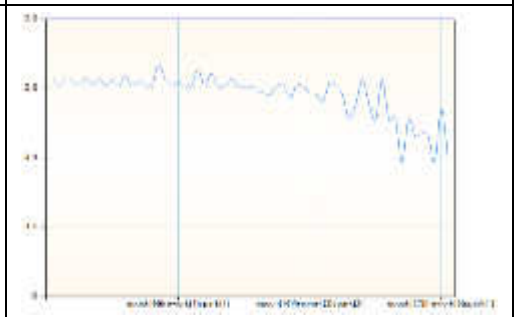
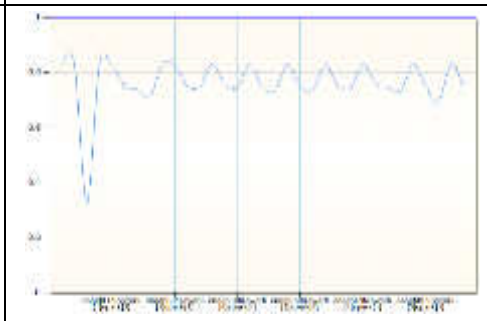
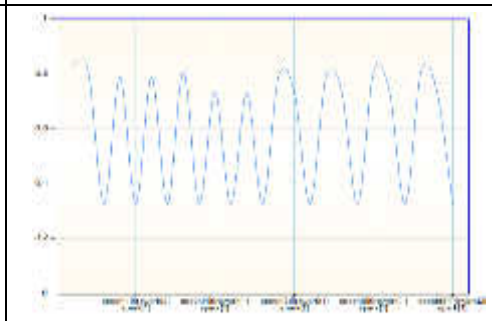
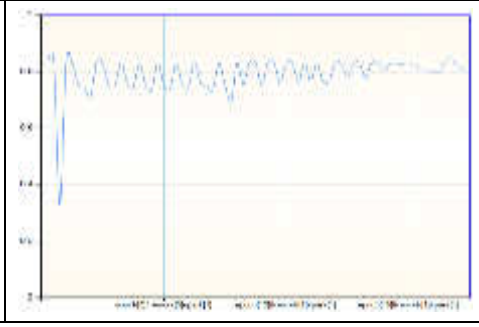
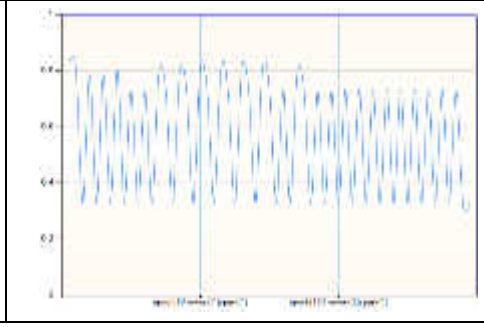
4.5.4 Optimization Based on 3D Logistic Map (Best Spark Global)

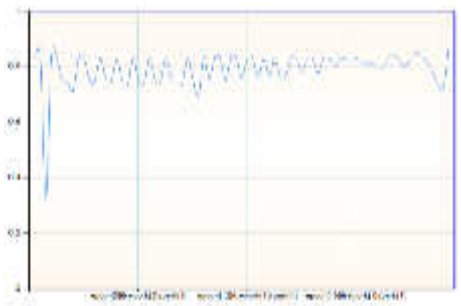
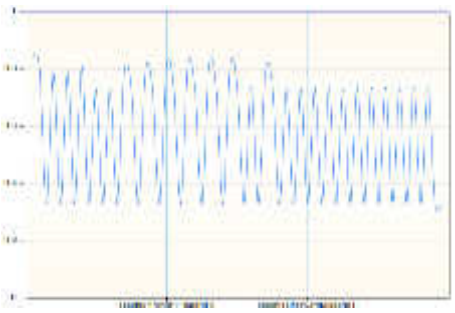
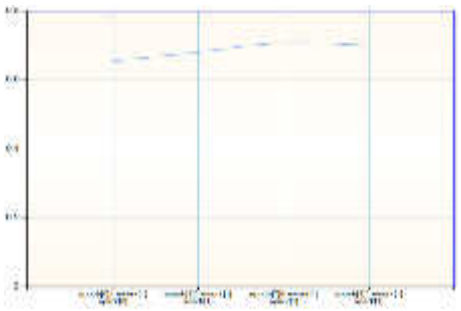
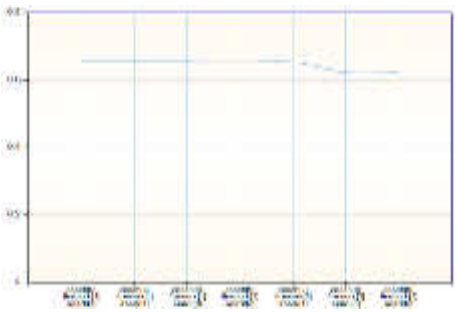
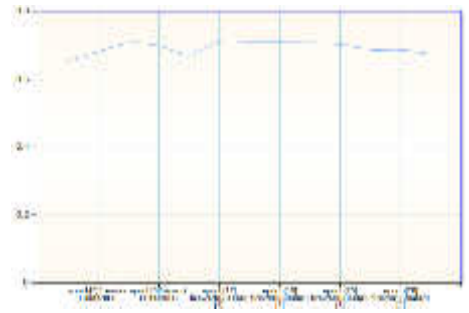
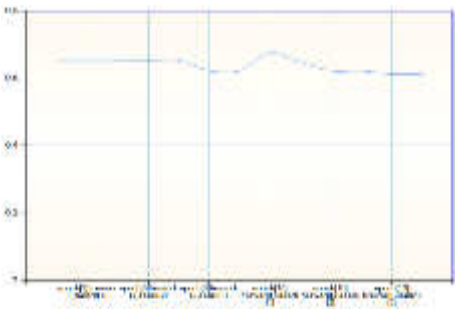
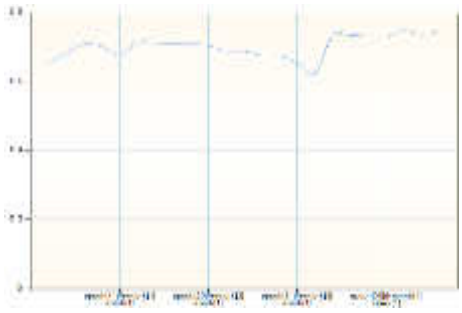
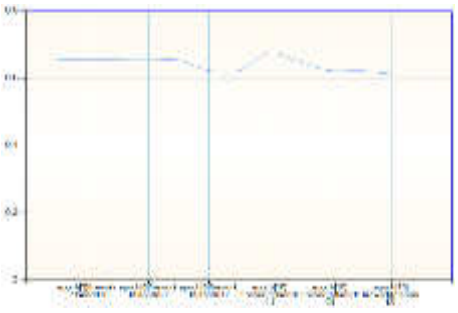
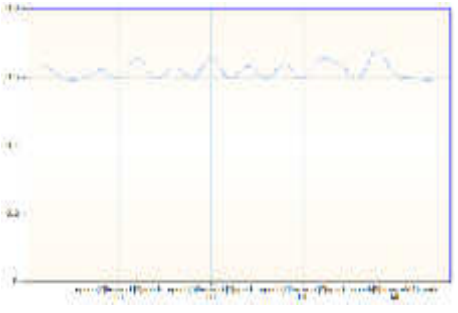
Table (4.9) Case best spark global, this table based on (6) samples of the fingerprint biometric images. Shows the optimal coordinates when using fireworks with the 3D logistic chaotic map and hybrid with the 3D logistic map to find the optimal solution. We find that the solutions with hybrid with the 3D

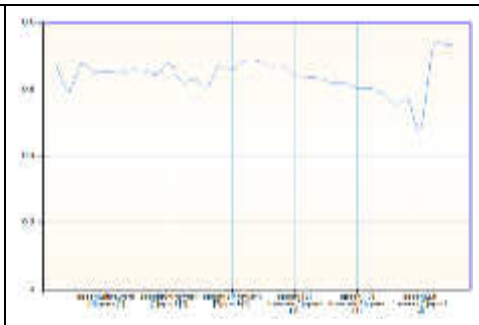
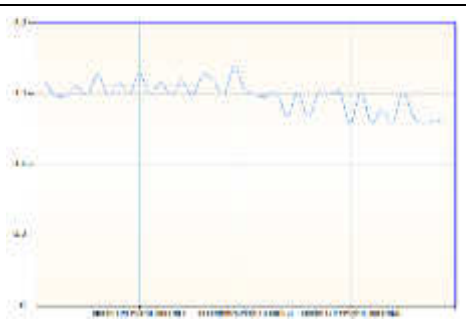
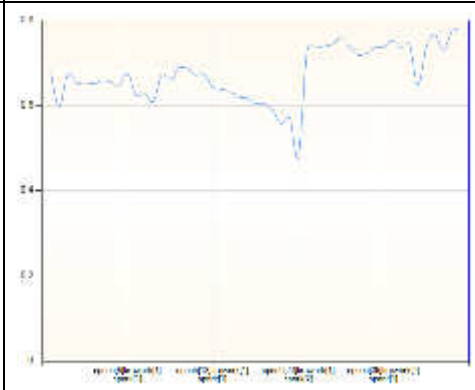
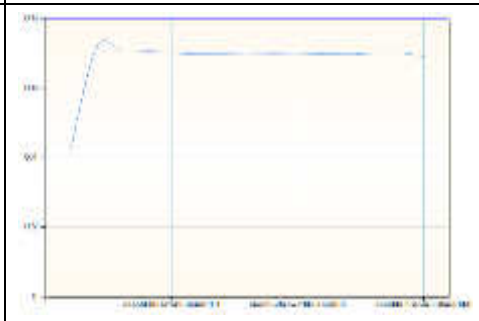
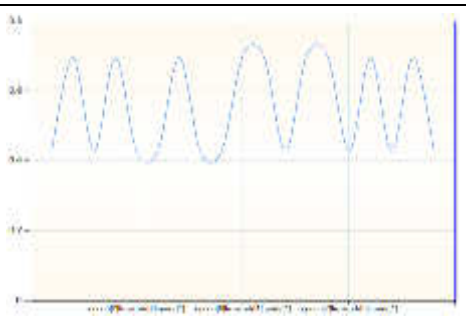
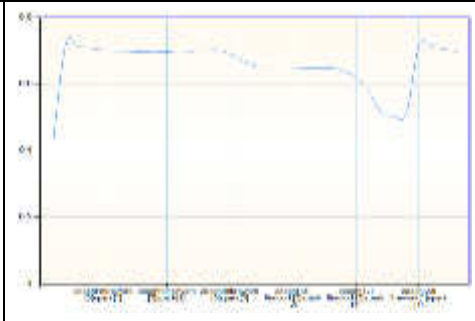
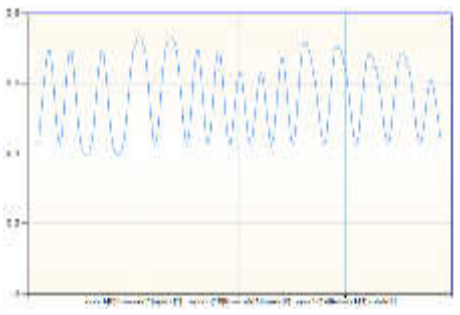
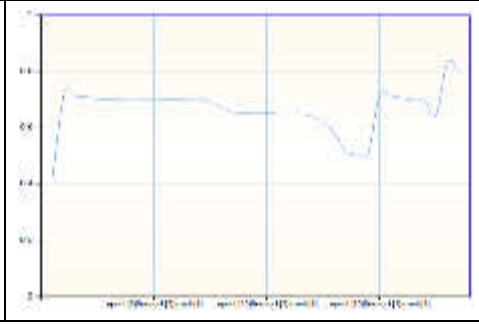
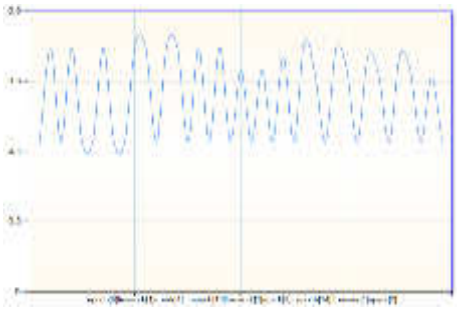
logistic chaotic map are more than solutions without Hybrid due because the hybrid technique with the 3D logistic chaotic map is based on the number of iterations all the greater the number the number of iteration increases arrival to the optimization. Where (Fn) in the table represents the number of the image is used, the point black represents all point coordinates, and Point Yellow represents Implying Mid-point.

Table (4.9): Best Spark Global

Best Spark Global				
#	**Image**	**Iteration**	**Fireworks with the 3D logistic map**	**Hybrid with the 3D logistic map**
1	**F1**	**10**		
		30		
		60		

2	F2	10		
		30		
		60		
3	F3	10		
		30		

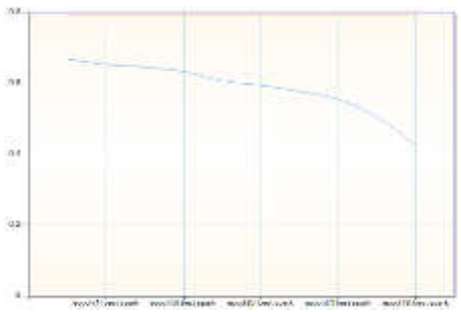
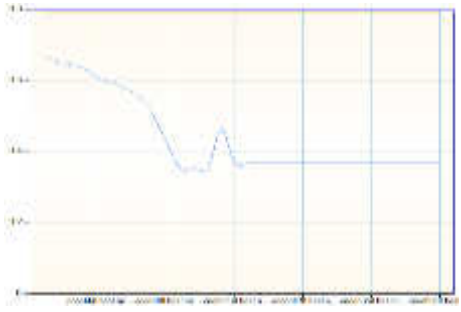
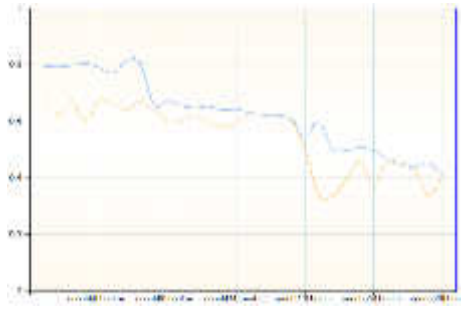
		60		
4	F4	10		
		30		
		60		
5	F5	10		

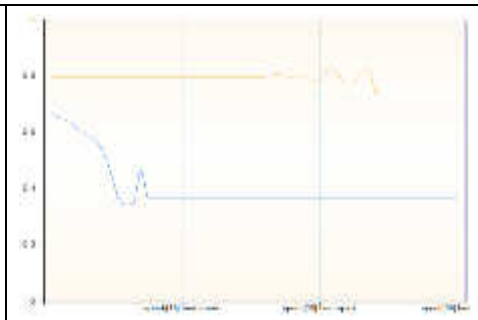
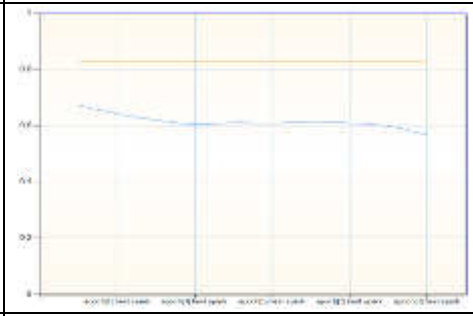
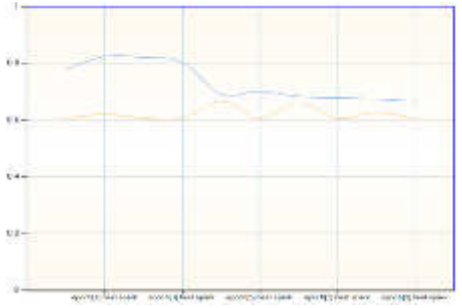
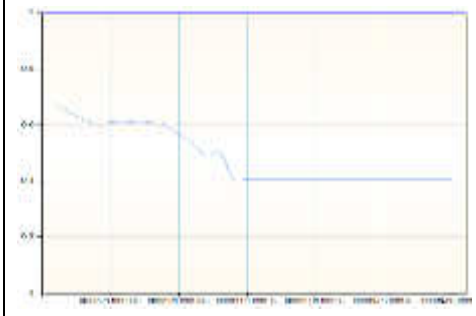
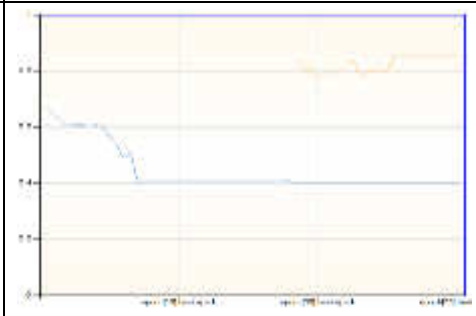
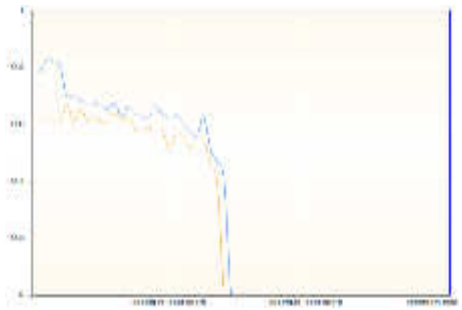
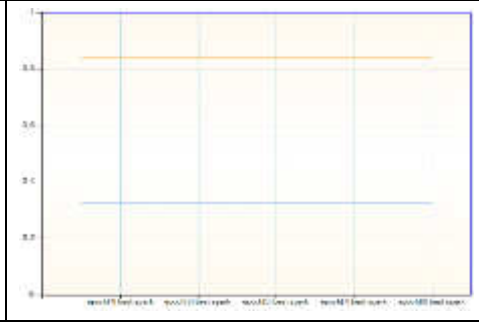
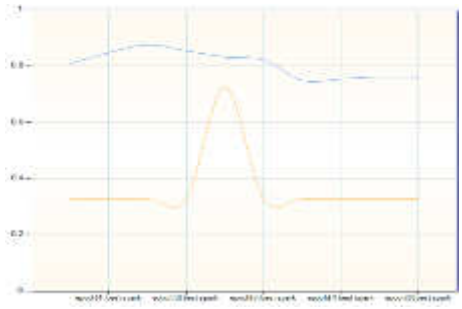
		30		
		60		
6	F6	10		
		30		
		60		
				Best Spark Global

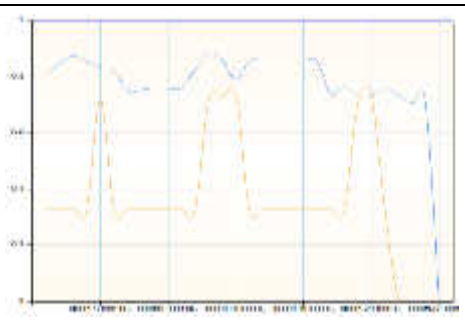
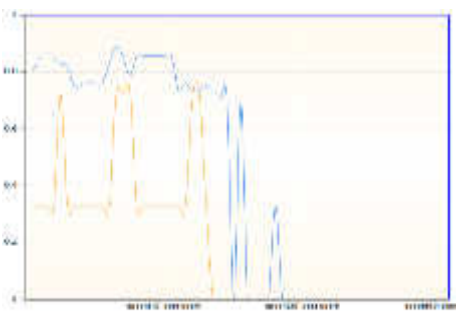
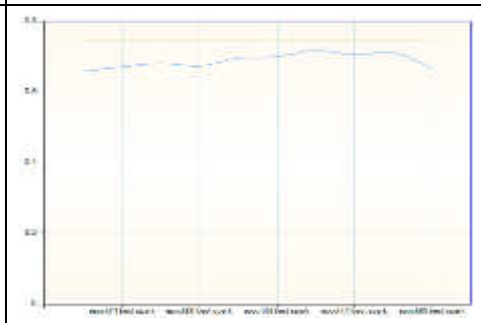
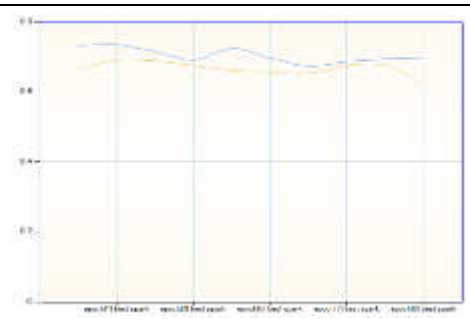
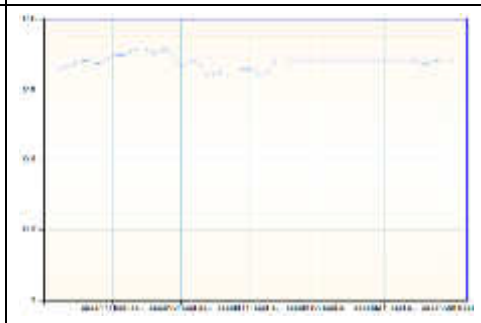
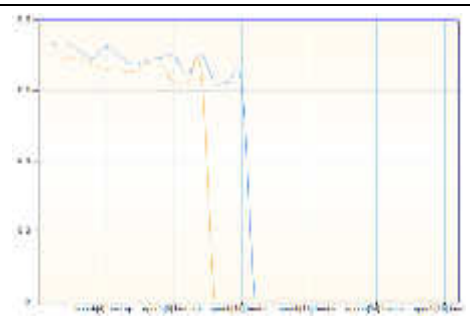
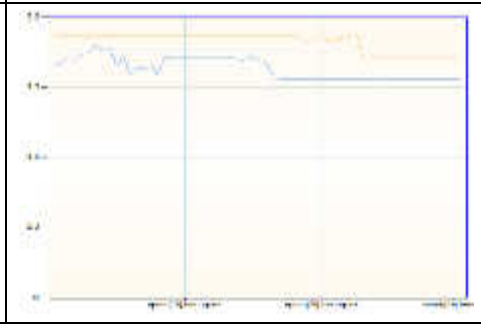
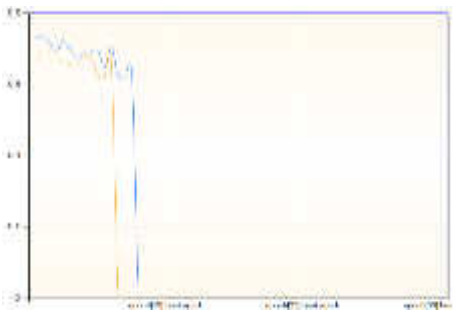
4.5.5 Optimization Based on 3D Map (Best / worst Spark)

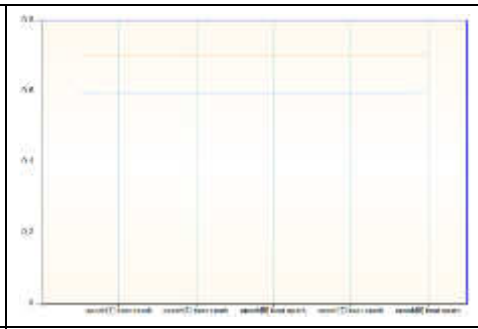
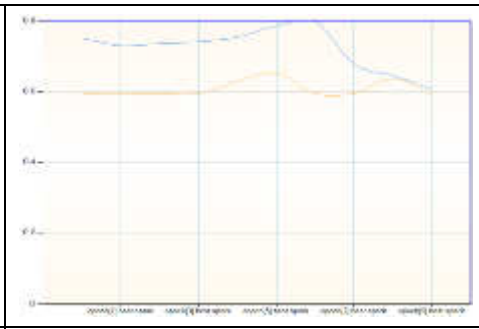
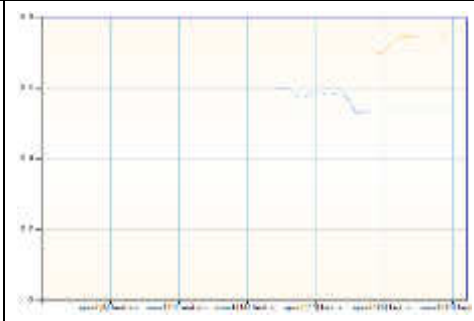
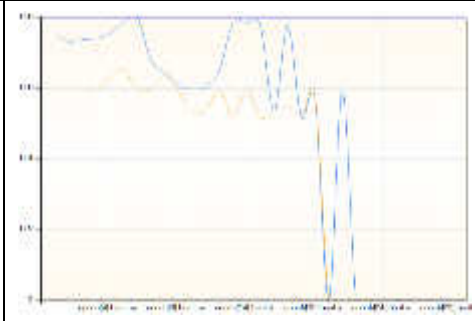
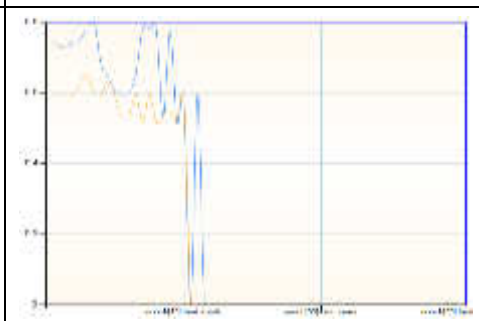
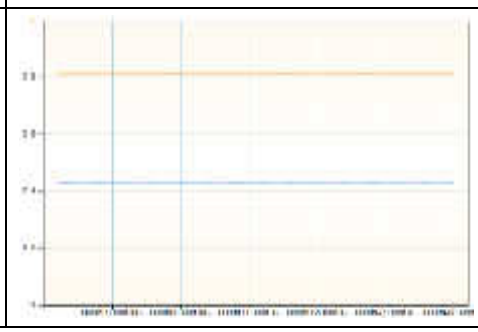
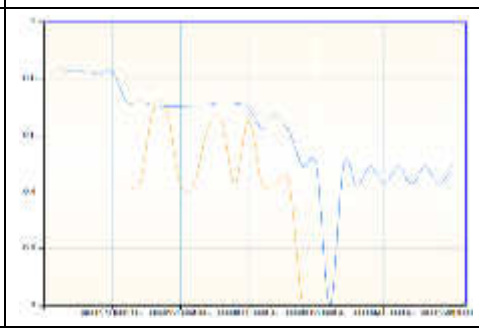
Table (4.10) Case Best / worst Spark Error, this table based on (6) samples of the fingerprint biometric images. Shows the optimal coordinates when using fireworks with the 3D logistic chaotic map and hybrid with the 3D logistic map to find the optimal solution. We find that the solutions with hybrid with the 3D logistic chaotic map are more than solutions without Hybrid due because the hybrid technique with the 3D logistic chaotic map is based on the number of iterations all the greater the number the number of iteration increases arrival to the optimization. Where (Fn) in the table represents the number of the image is used, the point black represents all point coordinates, and Point Yellow represents Implying Mid-point.

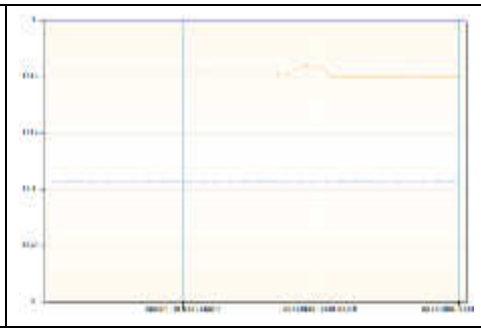
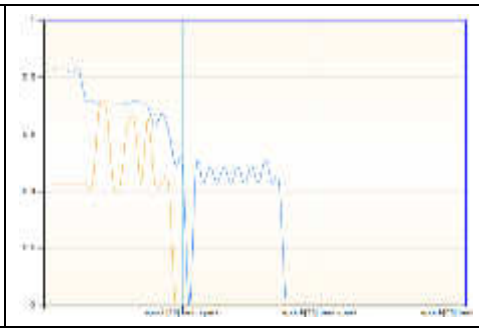
Table (4.10): Best / worst Spark Error

Best / worst Spark				
#	**Image**	**Iteration**	**Fireworks with the 3D logistic map**	**Hybrid with the 3D logistic map**
1	**F1**	**10**		
		30		

		60		
2	F2	10		
		30		
		60		
3	F3	10		

		30		
		60		
		10		
4	F4	30		
		60		

5	F5	10		
		30		
		60		
6	F6	10		
		30		

		60		

4.6 QR Code based on secrete key

Table (4.11) shows QRCode based on the secrete key. One of the fingerprint biometric images is used in this table. The table generates a set of points between the best coordinates of the optimization algorithms and the imposed mid-point based on the Linear Interpolation. It shows the effect of the length of the secrete text used on the coordinate location. Where the yellow dots are shown in the table are the points chosen by the algorithm and they represent the best solution for an optimization.

Table (4.11): Dropping coordinate

#	Text Key	QR Code	Dropping coordinate
1	A		
2	AB		
3	ABC		
4	ABCD		
5	ABCDE		

6	ABCDEF		

4.6.1 QR Code (Dropping Coordinate)

Table (4.12) shows QRCode (Dropping Coordinates). One of the fingerprint biometric images is used in this table. The table generates a set of points between the best coordinates of the optimization algorithms. Where the green dots are shown in the table are the dots that connect the mid-point and the yellow dot.

Table (4.12): Dropping Coordinate of QR Code

#	QR Code	Dropping Coordinates
1		Mid Point | Point | Count | List Point {X=26,Y=62} | {X=4,Y=41} | 44 | {X=4,Y=41},{X=5,Y=41},{X=5,Y=42},{X=6,Y=42},{X=6,Y=43}, {X=26,Y=62} | {X=4,Y=42} | 87 | {X=4,Y=41},{X=5,Y=41},{X=5,Y=42},{X=6,Y=42},{X=6,Y=43}, {X=26,Y=62} | {X=4,Y=43} | 129 | {X=4,Y=41},{X=5,Y=41},{X=5,Y=42},{X=6,Y=42},{X=6,Y=43}, {X=26,Y=62} | {X=10,Y=65} | 129 | {X=4,Y=41},{X=5,Y=41},{X=5,Y=42},{X=6,Y=42},{X=6,Y=43}, {X=26,Y=62} | {X=10,Y=66} | 129 | {X=4,Y=41},{X=5,Y=41},{X=5,Y=42},{X=6,Y=42},{X=6,Y=43}, {X=26,Y=62} | {X=10,Y=67} | 129 | {X=4,Y=41},{X=5,Y=41},{X=5,Y=42},{X=6,Y=42},{X=6,Y=43},
2		Mid Point | Point | Count | List Point {X=13,Y=52} | {X=13,Y=56} | 5 | {X=13,Y=52},{X=13,Y=53},{X=13,Y=54},{X=13,Y=55},{X=13,Y=56} {X=13,Y=52} | {X=13,Y=57} | 11 | {X=13,Y=52},{X=13,Y=53},{X=13,Y=54},{X=13,Y=55},{X=13,Y=56} {X=13,Y=52} | {X=13,Y=58} | 18 | {X=13,Y=52},{X=13,Y=53},{X=13,Y=54},{X=13,Y=55},{X=13,Y=56} {X=13,Y=52} | {X=14,Y=71} | 39 | {X=13,Y=52},{X=13,Y=53},{X=13,Y=54},{X=13,Y=55},{X=13,Y=56} {X=13,Y=52} | {X=14,Y=72} | 61 | {X=13,Y=52},{X=13,Y=53},{X=13,Y=54},{X=13,Y=55},{X=13,Y=56} {X=13,Y=52} | {X=14,Y=73} | 84 | {X=13,Y=52},{X=13,Y=53},{X=13,Y=54},{X=13,Y=55},{X=13,Y=56}
3		Mid Point | Point | Count | List Point {X=37,Y=62} | {X=24,Y=51} | 25 | {X=24,Y=51},{X=25,Y=51},{X=25,Y=52},{X=26,Y=52},{X=26,Y=53} {X=37,Y=62} | {X=24,Y=52} | 49 | {X=24,Y=51},{X=25,Y=51},{X=25,Y=52},{X=26,Y=52},{X=26,Y=53} {X=37,Y=62} | {X=24,Y=53} | 72 | {X=24,Y=51},{X=25,Y=51},{X=25,Y=52},{X=26,Y=52},{X=26,Y=53} {X=37,Y=62} | {X=28,Y=24} | 120 | {X=24,Y=51},{X=25,Y=51},{X=25,Y=52},{X=26,Y=52},{X=26,Y=53} {X=37,Y=62} | {X=28,Y=25} | 167 | {X=24,Y=51},{X=25,Y=51},{X=25,Y=52},{X=26,Y=52},{X=26,Y=53} {X=37,Y=62} | {X=28,Y=26} | 213 | {X=24,Y=51},{X=25,Y=51},{X=25,Y=52},{X=26,Y=52},{X=26,Y=53}
4		Mid Point | Point | Count | List Point {X=26,Y=48} | {X=28,Y=67} | 22 | {X=26,Y=48},{X=26,Y=49},{X=26,Y=50},{X=26,Y=51},{X=26,Y=52}, {X=26,Y=48} | {X=28,Y=68} | 45 | {X=26,Y=48},{X=26,Y=49},{X=26,Y=50},{X=26,Y=51},{X=26,Y=52}, {X=26,Y=48} | {X=32,Y=64} | 68 | {X=26,Y=48},{X=26,Y=49},{X=26,Y=50},{X=26,Y=51},{X=26,Y=52}, {X=26,Y=48} | {X=32,Y=65} | 92 | {X=26,Y=48},{X=26,Y=49},{X=26,Y=50},{X=26,Y=51},{X=26,Y=52}, {X=26,Y=48} | {X=33,Y=34} | 92 | {X=26,Y=48},{X=26,Y=49},{X=26,Y=50},{X=26,Y=51},{X=26,Y=52}, {X=26,Y=48} | {X=33,Y=35} | 92 | {X=26,Y=48},{X=26,Y=49},{X=26,Y=50},{X=26,Y=51},{X=26,Y=52},
5		Mid Point | Point | Count | List Point {X=4,Y=72} | {X=3,Y=65} | 9 | {X=3,Y=65},{X=3,Y=66},{X=3,Y=67},{X=3,Y=68},{X=3,Y=69}, {X=4,Y=72} | {X=3,Y=66} | 17 | {X=3,Y=65},{X=3,Y=66},{X=3,Y=67},{X=3,Y=68},{X=3,Y=69}, {X=4,Y=72} | {X=3,Y=67} | 24 | {X=3,Y=65},{X=3,Y=66},{X=3,Y=67},{X=3,Y=68},{X=3,Y=69}, {X=4,Y=72} | {X=5,Y=53} | 24 | {X=3,Y=65},{X=3,Y=66},{X=3,Y=67},{X=3,Y=68},{X=3,Y=69}, {X=4,Y=72} | {X=5,Y=54} | 24 | {X=3,Y=65},{X=3,Y=66},{X=3,Y=67},{X=3,Y=68},{X=3,Y=69}, {X=4,Y=72} | {X=5,Y=55} | 24 | {X=3,Y=65},{X=3,Y=66},{X=3,Y=67},{X=3,Y=68},{X=3,Y=69},
6		Mid Point | Point | Count | List Point {X=32,Y=91} | {X=12,Y=86} | 26 | {X=12,Y=86},{X=13,Y=86},{X=14,Y=86},{X=15,Y=86},{X=15,Y=87}, {X=32,Y=91} | {X=12,Y=87} | 51 | {X=12,Y=86},{X=13,Y=86},{X=14,Y=86},{X=15,Y=86},{X=15,Y=87}, {X=32,Y=91} | {X=12,Y=88} | 75 | {X=12,Y=86},{X=13,Y=86},{X=14,Y=86},{X=15,Y=86},{X=15,Y=87}, {X=32,Y=91} | {X=13,Y=95} | 75 | {X=12,Y=86},{X=13,Y=86},{X=14,Y=86},{X=15,Y=86},{X=15,Y=87}, {X=32,Y=91} | {X=13,Y=96} | 75 | {X=12,Y=86},{X=13,Y=86},{X=14,Y=86},{X=15,Y=86},{X=15,Y=87}, {X=32,Y=91} | {X=53,Y=94} | 100 | {X=12,Y=86},{X=13,Y=86},{X=14,Y=86},{X=15,Y=86},{X=15,Y=87},

4.6.2 Generating stream cipher key

Table (4.13) shows coordinate QRCode. The stream cipher key is generated depending on the points that are extracted during dropping the point of QR code points, which is selected as the pattern of the used mask. The process of generating ironing depends on several conditions:

Table (4.13): Coordinate of QRcode

#	Mask	QRcode
1	1=3*3	# | Point | No. W | No. B | Key 1 | {X=4,Y=41} | 5 | 4 | 001101010 2 | {X=5,Y=41} | 4 | 5 | 101010101 3 | {X=5,Y=42} | 5 | 4 | 010101010 4 | {X=6,Y=42} | 4 | 5 | 101010101 5 | {X=6,Y=43} | 4 | 5 | 011101010 6 | {X=7,Y=43} | 3 | 6 | 101011101 7 | {X=7,Y=44} | 4 | 5 | 010111010 8 | {X=8,Y=44} | 4 | 5 | 101101100 9 | {X=8,Y=45} | 4 | 5 | 011011001 10 | {X=9,Y=45} | 4 | 5 | 100110011
2	2=5*5	# | Point | No. W | No. B | Key 1 | {X=24,Y=51} | 49 | 32 | 100110100 2 | {X=25,Y=51} | 47 | 34 | 001101000 3 | {X=25,Y=52} | 52 | 29 | 011010000 4 | {X=26,Y=52} | 49 | 32 | 110000011 5 | {X=26,Y=53} | 48 | 33 | 100000110 6 | {X=27,Y=53} | 46 | 35 | 001001001 7 | {X=27,Y=54} | 45 | 36 | 010010010 8 | {X=28,Y=54} | 43 | 38 | 001100000 9 | {X=28,Y=55} | 43 | 38 | 011000001 10 | {X=29,Y=55} | 42 | 39 | 010010010
3	3=7*7	# | Point | No W | No B | key 1 | {X=4,Y=41} | 26 | 23 | 110001101 2 | {X=5,Y=41} | 23 | 26 | 110010111 3 | {X=5,Y=42} | 24 | 25 | 100101010 4 | {X=6,Y=42} | 28 | 21 | 001000100 5 | {X=6,Y=43} | 26 | 23 | 010001101 6 | {X=7,Y=43} | 24 | 25 | 100110111 7 | {X=7,Y=44} | 25 | 24 | 001101010 8 | {X=8,Y=44} | 25 | 24 | 011010100 9 | {X=8,Y=45} | 24 | 25 | 110101001 10 | {X=9,Y=45} | 23 | 26 | 101010011

4.7 Random number generation

There are two types of random number generation:

4.7.1 Random Number Generation Tests (without hybrid)

Table (4.14) shows the random number generation test of fireworks without hybrid. These tests are important and updated to measure the randomness of complete binary sequences.

Table (4.14): the NIST test of fireworks without hybrid

The key test type	Test Name	Total Number	Percentage of tests
512	Approximate Entropy	512	97%
	Block Frequency	512	100%
	Cumulative Sum (Forward)	320	93%
	Fast Fourier Transform	512	100%
	Frequency	500	0%
	Longest Run of Ones	600	100%
	Non-Periodic Template	812	41%
	Overlapping Template of all one	1066	5%
	Rank	512	100%
	Run	51	100%
	Serial	0	0%
1024	Approximate Entropy	1024	100%
	Block Frequency	1024	100%
	Cumulative Sum (Forward)	2048	0%
	Fast Fourier Transform	1024	100%
	Frequency	1024	0%
	Longest Run of Ones	1024	100%
	Non-Periodic Template	19549	30%
	Overlapping Template of all Ones	1024	100%
	Rank	1024	100%
	Run	51	100%
	Serial	2048	0%

4.7.2 Random Number Generation Tests (with hybrid)

Table (4.15) shows the random number generation test of fireworks with the hybrid. These tests are important and updated to measure the randomness of complete binary sequences.

Table (4.15): The NIST test of fireworks with hybrid

The key test type	Test Name	Total of Number	Percentage of Tests
512	Approximate Entropy	511	99%
	Block Frequency	512	100%
	Cumulative Sum (Forward)	410	96%
	Fast Fourier Transform	512	100%
	Frequency	520	30%
	Lempel Ziv Compression	600	43%
	Longest Run of Ones	600	100%
	Non-Periodic Template	812	72%
	Overlapping Template of all Ones	10136	30%
	Rank	512	100%
	Run	51	100%
	Serial	110	20%
1024	Approximate Entropy	1024	100%
	Block Frequency	1024	100%
	Cumulative Sum (Forward)	2048	0%
	Fast Fourier Transform	1024	100%
	Frequency	1024	0%
	Longest Run of Ones	1024	100%
	Non-Periodic Template	18683	99%
	Overlapping Template of all Ones	1024	100%
	Rank	1024	100%
	Run	51	100%
	Serial	2048	33%

4.7.3 Average Random Number Generation Tests (512)

Figure (4.1) the figure presents information about the average random number generation tests are performed in two cases of firework: fireworks without hybrid and fireworks with hybrid based on the key bit 512. The process is shown in figure (4.1). The blue color is shown in the figure implies the fireworks without hybrid and the orange color in the figure implies the fireworks with the hybrid.

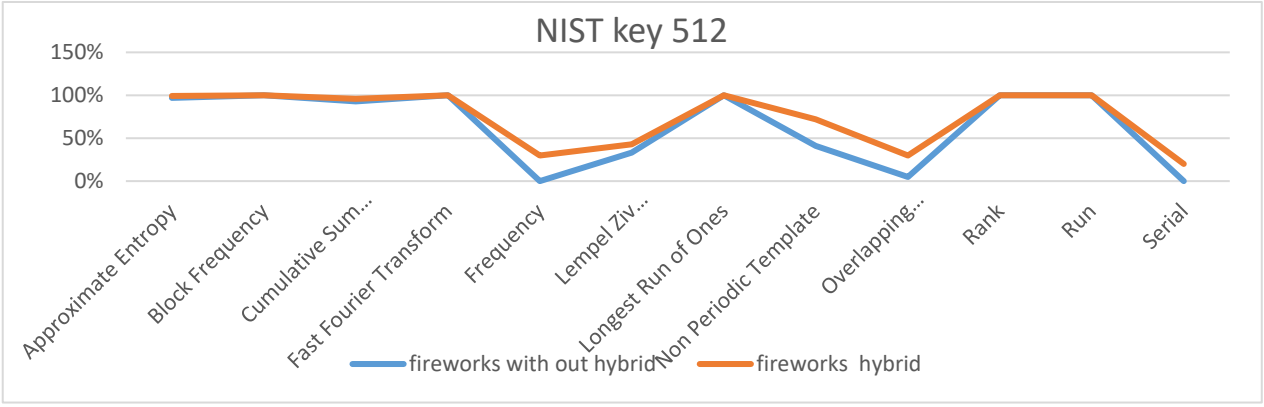


Figure (4.2): Average random number generation test (512)

4.7.4 Average random number generation tests (1024)

Figure (4.2) presents information about the average random number generation tests is performed in two cases of fireworks: firework without hybrid and fireworks with hybrid based on the key bit 1024. The process in figure (4.2). The blue color is shown is implies the fireworks without hybrid and the orange color in the figure implies the fireworks with the hybrid.

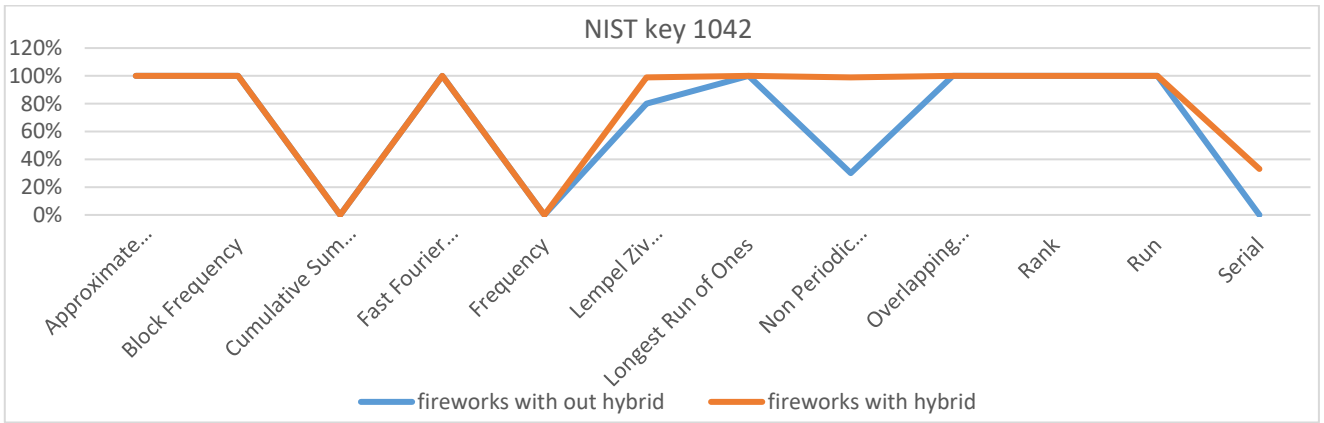


Figure (4.3): Average random number generation test (1024)

4.8 Uses Key

The key is extracted after measuring the strength of randomness by using several tests from the random number test. The extracted key is used in two important cases:

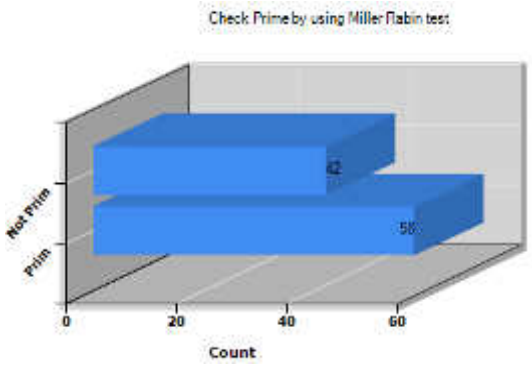
1. Generating prime Key for multiple users

2. Generating key used to hide text inside the image

4.8.1 Prime key

Table (4.16) shows generating a stream key with variable length using the best coordinate position feature. Which are founded through applying the hybrid optimization. It is checked by using the Miller Rabin test to get the highest percentage of the prime key.

Table (4.16): Generating Prime Key

Key	Check Key	Check Key by using the Miller Rabin Test
000111000011 **111100011101** **001111000001** **101000011100** **100011101001** **01110000111**	# | Block Bit | Number | Check Prime 0 | 1000011110... | 1351311... | True 1 | 0000111100... | 1562856... | True 2 | 0001111000... | 3012561... | Flase 3 | 0011110000... | 6024112... | Flase 4 | 0111100000... | 1204822... | Flase 5 | 1111000001... | 2409719... | True 6 | 1110000011... | 2241951... | Flase 7 | 1100000110... | 1931351... | True 8 | 1000001100... | 1311428... | True 9 | 0000011000... | 6285612... | Flase 10 | 0000110000... | 1256112... | True	

4.8.2 Hidden text

The system uses steganography to hide text inside the image. This technique will make it difficult to detect that there is a hidden message inside the image. Depending on some metrics are calculated results is the Mean Square Error

(MSE), Peak Signal to Noise Ratio (PSNR), fidelity Image (FI), and Universal Image Quality Index (UIQI) morals of the stego image as shown in table (4.17).

Table (4.17): Error Sensitivity

Image	Key length	Error Sensitivity			
		Mean Square Error (MSE)	**Peak Signal to Noise Ratio (PSNR)**	**Image Fidelity (IF)**	**Universal Image Quality Index (UIQI)**
	128	0.0000044321	101.6646758012	0.9999999717	0.9999999996
	256	0.0000099723	98.1428506201	0.9999999363	0.9999999992
	512	0.0000138504	96.7161755844	0.9999999115	0.9999999988
	1024	0.0000249307	94.1634505333	0.9999998407	0.9999999979
	128	0.0000055402	100.6955756711	0.9999999557	0.9999999996
	256	0.0000130194	96.9848970484	0.9999998960	0.9999999992
	512	0.0000191136	95.3173847204	0.9999998473	0.9999999988
	1024	0.0000379501	92.3386699562	0.9999996968	0.9999999977
	128	0.0000070363	99.6573555969	0.9999999505	0.9999999995
	256	0.0000129468	97.0091773668	0.9999999088	0.9999999991
	512	0.0000168871	95.8552431797	0.9999998811	0.9999999987
	1024	0.0000329299	92.9548970661	0.9999997681	0.9999999976

CHAPTER FIVE

CONCLUSIONS AND FUTURE WORK

Chapter Five

Conclusions and Future Work

5.1 Conclusions

This thesis proposed a new technique based on multi level biometric to generate stream key using swarm intelligence algorithms. This work presents the design of an authentication system based on a hybrid technique by using two algorithms fireworks algorithm (FWA) and camel herd algorithms (CHA). Fireworks algorithms based on the 3-dimension logistic chaotic map to enhance the performance of the fireworks algorithms to generate stream cipher key. It is used for many purposes and make the system more secure and authentication.

The proposed system consists of four-stage, each stage included several steps. The analysis and discussion of the proposed work, implementation stages and the obtained results are illustrated below:

1. Preprocessing image: Preparing images for further analysis, including uploading a fingerprint biometric image. Proposing a threshold algorithm in order to extract the value of the threshold of an image based on the Otsu method. This case includes one table: Preprocessing image.
2. Extracting Feature: Extracting features of the image by using the convolution technique depending on the pattern mask. This technique is important because it has the ability to detect important and less important regions in the fingerprint biometric image depending on the mask pattern. These cases include two tables: Effect different mask and max and min of histogram convolution.
3. Proposing hybrid technique: The optimization coordinate of the fingerprint biometric image that is extracted by using convolution technique from the previous step, proposing a hybrid technique (fireworks and camel herd) algorithm to find the best coordinate position feature is used to generate stream cipher key used to secure the process of authentication. As shown in the three tables: All Points, Best Spark Global, and Best / Worst Spark. This

hybrid technique is based on the number of iteration as the number of iteration increases coverage to the optimal solution (optimization).

4. Generating Final the key: The QRcode is active by using a secrete text, then dropping the best coordinate position feature comes from hybrid optimization to QRcode lead to generating a variable size key is produced called stream cipher key. This stage includes several steps is represented a number of figures and tables to represents coordinates optimization (hybrid technique) to generate stream cipher key.

The advantages of this key are unique, unpredictable, and suited for cryptography because the stream cipher key is checked by several parameters of "Random Number Generation Tests" to measure the strength of the key with a focus on a variety of different types of non-randomness that could exist in a sequence. The random number generation tests are performed in two cases: fireworks without hybrid and fireworks with hybrid based on the length key 512 and 1024. The results of these tests show that the resulting key is strong, active, and not broken and the stream cipher key is used for the following purposes:

1. Generating a prime key is used for multiple users. The prime key also is checked by using the "Miller Rabin test" to get the strength of the prime key. This key can be employed in many places such as banks, security companies, and Iraqi debt (QI) cards.

2. Generating a key that is used to hide text inside the images by steganography method depending on universal images.

5.2 Future Work

This work hoped to be continued in the future in several directions as explained in the following suggestions:

1. Adapting the proposed system for a large-scale fingerprint database in different environments to make the system more reliable.
2. Building fingerprints based on the use of part of the image and studying the feature of the fabric to reduce the size of storage and increase processing speed to suit computers with limited efficiency.
3. Representing the texture of the fingerprint in the local region and reducing the dimensionality coordinate. Thus, it is expected a further work that improves the performance of the current approaches.
4. Analyzing of the differences between the fingerprint codes of the same person on identical twins would serve to determine if they are dangerous and can penetrate. Furthermore, research can also be done on different methods of trying to crack code.
5. In addition, not all government secrets need the best in encrypted protection because the costs for that protection can outweigh the value of the secret under protection.
6. The possibility of integrating the fingerprint with other biometric systems to format a multi-biometric system is more durable and accurate in other work.

REFERENCE

Reference

[1] S. R. Kodituwakku “Biometric Authentication: A Review” International Journal of Trend in Research and Development, Volume: 2, No: 4, ISSN pp.2394-9333, August (2015).

[2] Wencheng Yang and Song Wang, et.al. "Security and Accuracy of Fingerprint-Based Biometrics: A Review" Symmetry, Volume: 11, No. 2, Issue 2, pp.141, April (2019).

[3] Soriful Hoque “Multilevel and Biometric-Graphical Secure Authentication System Using Pattern Matching and Gene-Based Data Extraction” International Journal of Engineering and Computer Science ISSN: 2319-7242, Volume: 5, Issue: 10, pp. 18714-18717, Oct (2016).

[4] Sushma Jaiswal and Dr. Sarita Singh Bhadauria et al. "Biometric: Case Study" Journal of Global Research in Computer Science, Volume: 2, No. 10, ISSN-2229-371, pp.19-48, October (2011).

[5] Julian Fierrez and Aythami Morales, et.al. “Multiple classifiers in biometrics. Part 1: Fundamentals and review” Information Fusion, No.44, pp.57-64, Nov (2018).

[6] Dr. M V Bramhananda Reddy and Dr. V. Goutham “Iris Technology: A Review on the Iris-Based Biometric System for Unique Human Identification” International Journal of Research – Granthaalayah, Volume: 6, ISSN: 2394-3629, pp.80-90, Jan (2018).

[7] D. Shobana1 and A. Logeshwarim et.al. “A Study on Multimodal Biometrics System” International Journal of Computer Science and Mobile Applications, Volume: 5, Issue: 10, Pg. 117-122, October (2017).

Reference

[8] Waleed Dahea and HS Fade war “Multimodal Biometric System: A Review” International Journal of Research in Advanced Engineering and Technology, Volume 4, Issue: 1, pp. 25-31, January (2018).

[9] H. Almahafzah and M. Z. Alrwashdeh, "A Survey of Multi-biometric Systems” International Journal of Computer Applications Volume: 43, No. 15, Pp. 36-43, (2012).

[10] Ramadan Gad and AYMAN EL-SAYED, et.al. “Multi-Biometric Systems: A State Of The Art Survey and Research Directions” International Journal of Advanced Computer Science and Applications Volume: 6, No. 6, (2015).

[11] Meligy and Ali M., et.al. “Chaos encryption algorithm using key generation from biometric images” International Journal of Computer Applications Volume: 149, No.1, pp.0975 – 8887, (2016).

[12] A. Sarkar and B. K. Singh et.al. "RSA Key Generation from Cancelable Fingerprint Biometrics," International Conference on Computing, Communication, Control and Automation (ICCUBEA), pp. 1-6, (2017).

[13] Panchal, G., and Samanta, D. “A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security” Computers & Electrical Engineering, Volume: 69, pp.461–478, (2018).

[14] Murooj Aamer and Naji Mutar Sahib, et.al. “Retina Random Number Generator for Stream Cipher Cryptography” International Journal of Computer Science and Mobile Computing (IJCSMC), Volume: 8, Issue: 9, pp. 172-181, September (2019).

[15] Rahouma and Kamel H., et al. “Design and Implementation of a New DNA Based Stream Cipher Algorithm using Python” Egyptian Computer Science Journal, Volume: 44, No.1, pp.1-12, January (2020).

[16] R. Karthiga and S. Mangai "Feature Selection Using Multi-Objective Modified Genetic Algorithm In Multimodal Biometric System" Journal Of Medical Systems, Springer Nature Switzerland AG. Part of Springer Nature, Volume: 43, No.7, pp.214, May (2019).

[17] Marcos Faundez-Zanuy "Biometric security technology" IEEE Aerospace and Electronic Systems Magazine, Volume: 21, No. 6, pp.15-26, June (2006).

[18] Jammi Ashok and vaka shivashankar, et.al. "An overview of biometrics" International Journal on Computer Science and Engineering (IJCSE), Volume: 02, No. 07 (2010).

[19] Ramadan Gad and AYMAN EL-SAYED, et.al. "Multi-Biometric Systems: A State of the Art Survey and Research Directions" International Journal of Advanced Computer Science and Applications (IJACSA), Volume: 6, No. 6, (2015).

[20] Sushma Jaiswal, Dr. Sarita Singh Bhadauria and Dr. Rakesh Singh Jadon "Biometric: Case Study" Journal of Global Research in Computer Science, Volume: 2, No. 10, October (2011).

[21] Shilpa Shrivastava "Biometric: Types and its Applications" International Journal of Science and Research (IJSR), Volume: 6, No.14, (2013).

[22] Yudong Zhang and Praveen Agarwal et.al. "Swarm Intelligence and Its Applications" Hindawi Publishing Corporation, the Scientific World Journal, ID: 528069, pp.3, (2013).

[23] Hazem Ahmed and Janice Glasgow "Swarm Intelligence: Concepts, Models and Applications" Research is introducing to School of Computing Queen's University Kingston, Ontario, Canada K7L3N6, February (2012).

[24] Singiresu S. Rao "Engineering Optimization Theory and Practice" Book from a Ch13 in pp.693, (2009).

[25] Tan, Ying and Yu, Chao et.al. "Introduction to Fireworks Algorithm" International Journal of Swarm Intelligence Research, No.4, pp.39-70, (2015).

[26] Vijay Kumara and Jitender Kumar Chhabrab et.al. "Optimal Choice of Parameters for Fireworks Algorithm" 4th International Conference on Eco-friendly Computing and Communication Systems, (2015).

[27] Yu Jun and Tan Ying et al. "Accelerating the Fireworks Algorithm with an Estimated Convergence Point" Kyushu University Institutional Repository, Springer, pp. 263-272, (2018).

[28] Y. Tan and Y. Zhu "Fireworks algorithm for optimization, in Advances in Swarm Intelligence" Springer, Berlin, PP. 355–364, (2015).

[29] Evans BAIDOO "fireworks algorithm for unconstrained function optimization problems" Paper, Applied Computer Science, Volume: 13, No. 1, pp. 61-74, (2017).

[30] Graeme Phipps and Jacki Salkeld et al. "Arabian Camel" Western Sydney Institute of TAFE, Richmond, (2008).

[31] A. Iqbal and B. Baidar Khanm et.al. "Feeding behavior of camel" Volume: 38, pp. 3-4, (2001).

[32] Zied Othman Ahmed "Artificial Arabian Camel and Meerkat Algorithms to Solve Flexible Job Shop Scheduling Problems" An Unpublished Thesis

Submitted to the Department of Computer Science / University of Technology (2018).

[33] K. Bhargavi and S. Jyothi "A survey on threshold-based segmentation technique in image processing" international journal of innovative research & development, Volume: 3, Issue: 12, November (2014).

[34] Miss Hetal J. Vala and Prof. Astha Baxi "A Review on Otsu Image Segmentation Algorithm" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume: 2, Issue: 2, February (2013).

[35] Saad M. Ismail and Siti Norul Huda Sheikh Abdullah et.al. "Statistical Binarization Techniques for Document Image Analysis" Faculty of Information Science and Technology, University Kebangsaan Malaysia, Malaysia, Volume: 14, No. 1, pp. 23.36 (2018).

[36] Senthil kumaran and Vaithegi "Image segmentation by using thresholding techniques for medical images" Computer Science & Engineering: An International Journal (CSEIJ), Volume: 6, No.1, February (2016).

[37] Jamileh Yousef "Image Binarization using Otsu Thresholding Algorithm" University of Guelph, Ontario, Canada, April (2015).

[38] Amruta B. Patil and J.A.shaikh "OTSU Thresholding Method for Flower Image Segmentation" International Journal of Computational Engineering Research (IJCER), Volume: 6, Issue: 5, (2016).

[39] Gaurav Kumar and Pradeep Kumar Bhatia "A Detailed Review of Feature Extraction in Image Processing Systems" Fourth International Conference on Advanced Computing & Communication Technologies, IEEE (2014).

[40] Paul G. Brown "Convolution is a Database Problem" Paper Paradigm4's SciDB is a scalable, scientific database management system (2015).

[41] Scott Krig "Computer Vision Metrics: Survey, Taxonomy, and Analysis" The book trade worldwide by Springer Science \ Business Media New York, ISBN: 978, No0. 1, pp.4302-5929-9, by Apress Media, LLC, all rights reserved (2014).

[42] Pawan N. Khade and Prof. Manish Narnaware "3D Chaotic Functions for Image Encryption" IJCSI International Journal of Computer Science Issues, Volume: 9, Issue: 3, No. 1, May (2012).

[43] Ahmad Shokouh Saljoughi and Hamid Mirvaziri "A new method for image encryption by 3D chaotic map" Pattern Analysis and Applications, (2018).

[44] Musammet Tahmina Akter and Mohammad Abul Mansur Chowdhury "Observation of Different Behaviors of Logistic Map for Different Control Parameters" International Journal of Applied Mathematics and Theoretical Physics ISSN: 2575-5927, (2018).

[45] Jamal Mustafa Al-Tuwaijari "Image Encryption Based on Fractal Geometry and Chaotic Map" Diyala Journal for Pure Science, ISSN: 2222-8373, Volume: 14, No: 1, pp. 166-182, January (2018).

[46] Andrew Rushin and Juan Soto et.al. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" Book Called National Institute of Standards and Technology, April (2010).

المُستخلص

توجد بعض التقنيات الجديدة التي يمكن استخدامها للحفاظ على سلامة المعلومات الشخصية. إن مفتاح التشفير هو تقنية مستمدة من القياسات الحيوية بطريقة غير مباشرة ، إذ أن بصمات الأصابع تمثل نمط حيوي لتأكيد الهوية يتميز به كل فرد، حيث تعتمد أنظمة استخراج بصمات الأصابع المعروفة حاليًا على الميزات العالمية وتفاصيل بصمات الأصابع.

مراحل تنفيذ العمل تتضمن عملية تجهيز الصورة باستخدام طريقة أوتسو وذلك بتقسيم الصورة الى تدرجات اللون الرمادي ومنها تتحول الصورة الى صورة نظام ثنائي متمثل بـ (0,1) لجعل الصورة سهله التعامل رقمياً مع نظام الحاسبة. ثم بعدها يتم استخدام تقنيات الالتواء لأستخراج الخصائص من صورة بصمات الأصابع من أجل الوصول السريع إلى المناطق المهمة داخل صورة بصمات الأصابع هذه الخصائص تساعدنا في إيجاد الحل الأمثل بعد استخدامها في خوارزميه نظام المختلط.

أن النظام المقترح يتكون من خوارزميتين هما الألعاب النارية وقطعان الجمال تعتمد خوارزمية الألعاب النارية على خرائط فوضوية ثلاثية الأبعاد، يتم تحسين أداء الألعاب النارية لغرض انتاج مفتاح رئيسي- يستخدم لعده أغراض وذلك بالاعتماد على أحداثيات صور بصمات الأصابع.

يتم تفعيل رمز الاستجابة السريعة بإدخال نص سري، ثم يتم إسقاط أفضل ميزة موضع إحداثي ناتج من التحسين المختلط على رمز الاستجابة السريعة لتوليد مفتاح متغير الطول يسمى(Stream cipher key).

من مزايا هذا المفتاح انه فريد ولا يمكن التنبؤ به ومناسب للتشفير وذلك لأن (Stream cipher key) يتم فحصه بواسطة العديد من مقايس "اختبارات إنشاء الأرقام العشوائية" لقياس قوة المفتاح مع التركيز على مجموعة متنوعة من الأنواع المختلفة من غير العشوائية التي يمكن أن توجد ضمن التسلسل ، يتم إجراء اختبارات توليد الأرقام العشوائية في حالتين: الألعاب النارية بدون تقنية المختلط والألعاب النارية مع تقنية المختلط استنادًا إلى طولين من المفتاح هما 512 و1024. أظهرت نتائج هذه الاختبارات أن المفتاح الناتج قوي، وغير قابل للكسر و فريد وأن مفتاح (Stream cipher key) يستخدم للأغراض التالية:

1.إنشاء مفتاح يستخدم لإخفاء نص داخل الصور بالاستعانة بطريقة (Steganography) وبالاعتماد على نماذج من الصور العالمية.

2.توليد مفتاح أولي (Prime key) يستخدم لعدة مستخدمين يتم التحكم به عن طريق النظام وهذا المفتاح يمكن أن يستثمر في أماكن عدة منها البنوك، الشركات الأمنية، بطاقة كي كارد.

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة ديالى

مُتعدد القياسات الحيوية لتوليد مفتاح التشفير بأستخدام خوارزميات سرب الذكاء

من قبل

حسين علي أسماعيل

بإشراف

أ.م. د. جمال مصطفى عباس

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

٢٠٢٠