T.R.
USKUDAR UNIVERSITY
INSTITUTE OF SCIENCE

DEPARTMENT OF CYBER SECURITY

MASTER'S DEGREE PROGRAM OF CYBER SECURITY

MASTER'S DEGREE THESIS

GENERATİON OF HYBRİD BİO-SECRET KEY BASED ON FİNGERPRİNT

ABDIRAHMAN ABDULLAHI MIRE

Thesis Advisor

Dr. IHAB ELAFF

ISTANBUL-2022

T.R.
USKUDAR UNIVERSITY
INSTITUTE OF SCIENCE

DEPARTMENT OF CYBER SECURITY

MASTER'S DEGREE PROGRAM OF CYBER SECURITY

MASTER'S DEGREE THESIS

GENERATİON OF HYBRİD BİO-SECRET KEY BASED ON FİNGERPRİNT

ABDIRAHMAN ABDULLAHI MIRE

Thesis Advisor

Dr. IHAB ELAFF

ISTANBUL-2022

ABSTRACT

Generation of Hybrid Bio-Secret Key Based On Fingerprint

Privacy policies that were previously limited to paper documents are becoming more prevalent in online commercial transactions. Internet commerce, medical privacy, and a variety of other fields benefit from highly secure connections. Individuals who communicate with one another through the Internet increasingly require secure connections. Various techniques, such as encryption, steganography, watermarking, and scrambling, can be used to keep data private, safe, and copyright-protected. Secure online transactions and other private networks necessitate the use of encryption, while sensitive data also necessitates the use of this technology in business. The most important thing that can be done to ensure data security is to keep it out of the hands of those who don't need it or are actively trying to gain it. Let me remind you at this point that there is an issue in that the server knows the PIN code, or, to put it another way, the PIN code is saved in the database. And, as we all know, utilizing a symmetric cryptography key requires the use of a single safe secret key. Therefore, we address this problem by producing a secret bio-key derived from a fingerprint image and using that key for encryption and decryption to protect the sensitive information. This study may also be validated by developing a PIN code that is independent of the system and can be thought of as a table based on the fingerprint image.

MATLAB, Advanced Encryption Standard, Fingerprint image, fingerprint recognition, all those things we used as a tool to develop this work.

Encrypted and decrypted with large text file by using generated Bio-Key and Advanced Encryption Standard (AES). Is the effectiveness of this research and also be characterized by the development of a training for new approach that helps the user to isolate the PIN code from the system.

Keywords: PIN code, Bio-Key, Fingerprint, AES.

ABSTRACT

Parmak İzine Dayalı Hibrit Biyo-Gizli Anahtar Üretimi

Daha önce kağıt belgelerle sınırlı olan gizlilik politikaları, çevrimiçi ticari işlemlerde daha yaygın hale geliyor. İnternet ticareti, tıbbi mahremiyet ve diğer çeşitli alanlar, son derece güvenli bağlantılardan yararlanır. İnternet üzerinden birbirleriyle iletişim kuran bireyler giderek daha fazla güvenli bağlantıya ihtiyaç duyuyor. Verileri gizli, güvenli ve telif hakkı korumalı tutmak için şifreleme, steganografi, filigranlama ve karıştırma gibi çeşitli teknikler kullanılabilir. Güvenli çevrimiçi işlemler ve diğer özel ağlar, şifreleme kullanımını zorunlu kılarken, hassas veriler de bu teknolojinin iş hayatında kullanılmasını zorunlu kılmaktadır. Veri güvenliğini sağlamak için yapılabilecek en önemli şey, onu ihtiyacı olmayan veya aktif olarak elde etmeye çalışanların elinden uzak tutmaktır. Bu noktada sunucunun PIN kodunu bilmesi veya başka bir deyişle PIN kodunun veritabanına kaydedilmesi gibi bir sorun olduğunu hatırlatalım. Ve hepimizin bildiği gibi, simetrik bir şifreleme anahtarı kullanmak, tek bir güvenli gizli anahtarın kullanılmasını gerektirir. Bu nedenle, bir parmak izi görüntüsünden türetilen gizli bir biyo-anahtar üreterek ve hassas bilgileri korumak için bu anahtarı şifreleme ve şifre çözme için kullanarak bu sorunu ele alıyoruz. Bu çalışma, sistemden bağımsız bir PIN kodu geliştirilerek de doğrulanabilir ve parmak izi görüntüsüne dayalı bir tablo gibi düşünülebilir.
MATLAB, Gelişmiş Şifreleme Standardı, Parmak İzi görüntüsü, parmak izi tanıma. Bu çalışmayı geliştirmek için bir araç olarak kullandığımız tüm bu şeyler.

Oluşturulan Bio-Key ve Advanced Encryption Standard (AES) kullanılarak büyük metin dosyasıyla şifrelenir ve şifresi çözülür. Bu araştırmanın etkinliği ve ayrıca, kullanıcının PIN kodunu sistemden izole etmesine yardımcı olan yeni bir yaklaşım için bir eğitimin geliştirilmesi ile karakterize edilir.

Anahtar Kelimeler: PIN kodu, Bio-Key, Parmak İzi, AES.

THANKS TO

To begin, I would want to give thanks to God for making it possible for me to take on such a significant challenge. Second, I would like to express my gratitude to my adviser, Dr. IHAB ABDALA. I believe that he would have assisted me even if he had not collaborated with me and supported me in the manner in which he assisted me; in fact, I would not have written this thesis and would not have finished it without his assistance. Once more, sir, I cannot explain how grateful I am for your constant support. In addition, I want to express my gratitude to each and every professor for helping me expand my knowledge while I was learning. In addition, I would like to express my gratitude to the whole management of both the department and the university. In addition, I am thankful to my father, who has supported me throughout my life and encouraged and provided me with all I've need.

In conclusion, I would want to express my gratitude to everyone who assisted me in the writing of this book, including those individuals whose work I utilized as a resource.

FORM OF DECLARATION

Herewith I declare, that I obtained all the information and documents in this study within the framework of academic rules, presented all visual, auditory, and written information and results in accordance with scientific ethics, did not falsify the data I used, referred to the sources I used in accordance with scientific norms, that my thesis was original except in the cases cited, produced by me and written in accordance with the Thesis Writing Guide of Uskudar University Institute of Health Sciences.

Date_____

Abdirahman Abdullahi Mire

Signature_____

CONTENTS

INDEX OF TABLES

page

INDEX OF FIGURES

INDEX OF IMAGERY AND ABBREVIATIONS

AES : Advance Encryption Standard

DES : Data Encryption Standard

RSA : Rıvest Shamır Adlı

İBE : İdentity Based Encryption

1. CRYPTOGRAPHY OVERVIEW AND INTRODUCTION

1.1 introduction

Privacy guidelines, the likes of which were to paper documents alone, are increasingly turning up in online business dealings nowadays. E-commerce conducted over the internet, medical privacy, and other areas all benefit from communications that are extremely well protected. Secure connections between individuals who interact with one another through the Internet are now an absolute necessity. People are able to keep their data secure, confidential, and protected by copyright by utilizing a variety of methods, including cryptography, steganography, watermarking, and scrambling. Encryption, on the other hand, has made its way into the business sector as a result of the requirement for safe financial dealings in online commerce and other private networks, in addition to the security of sensitive data. When it comes to security, preventing information from being viewed by individuals who have no use for it or who are actively working to obtain it is the single most critical thing that can be done.

Within the scope of this thesis, we will generate a Bio-Key and using it into encrypt information utilizing one of the most well-known encryption protocols known as AES, which stands for Advanced Encryption Standard. In addition, rather than using an email address or any other form of identification, we will encrypt the data using a Bio-Key derived from a fingerprint image. We will concentrate on a few aspects, such as how generated key will be secure enough and effectively, we can do tasks such as using that key to encrypt and decrypt data, we will also create PIN code and brief explanation about how it is useful.

1.2 Threats

In order for anything to be regarded as potentially hazardous, it must be feasible for anyone to enter the system or institution that is under scrutiny. It is possible for harm to be caused even in the absence of a violation. Any behavior that could violate the rules has to be put to a halt or foreseen in advance so that appropriate action can be taken. The individuals who commit these offenses are referred to as assailants. When discussing information or resources that are not open to the general public, we refer to these things

as "confidential" or "private." In settings like the government and business, where computers are utilized often, the protection of sensitive data is of the utmost importance. Both the military and civilian branches of the government, as two examples each, are guilty of keeping some facts from the general public. Efforts were made by the military to develop rules and regulations in order to

confident that the idea was successfully implemented. As a direct consequence of this, the very first exhaustive study on computer security was carried out. It is good business practice to take measures to stop other people from using one's own designs without permission. A further point to keep in mind is that it is standard practice for companies to protect the confidentiality of the personal information of their staff members.

Maintaining confidentiality is made easier by taking precautions against unauthorized entry. Encrypting your communications is the best way to stop anyone from listening in on them. A cryptographic key is necessary in order to get access to the data once it has been decoded. In addition to this, the key to the cryptographic algorithm needs to be kept secure. This refers to the capability of preventing information or resources from being changed in a manner that does not adhere to the standards of "integrity." Integrity is a word that may be used to define both the content of the data as well as the source of the data. Authentication and data source integrity are both included in the concept of integrity. The trustworthiness and dependability of the information itself can be used as a gauge to determine the trustworthiness and dependability of the source of the information. It is clear from this that the reliability of a system is an essential component to the success of the system's There are two approaches to maintaining security: preventative measures and detection protocols. On the other hand, anti-measures are meant to keep information from getting into the hands of people who aren't supposed to see or change it.

Data or resources that can be depended upon to be available are considered to be in the "available" category. When it comes to dependability and the design of systems, system failure is the worst conceivable consequence that may occur. This facet of accessibility has a significant influence on security since there is a risk that data or services might be rendered purposefully inaccessible. Therefore, the designs of systems almost always begin with the assumption that there is a statistical model for analyzing the consumption patterns that are anticipated, and mechanisms assure availability only when such statistical models are accurate. If someone is able to affect the usage of the model or the

parameters that govern it, such as network traffic, then the statistical model's assumptions could no longer be valid. As a direct consequence of this, the processes that are supposed to guarantee that information can be accessed quickly and readily aren't performing as well as they should be. Consequently, as a direct consequence of this, they have a greater risk of failing than their contemporaries.

Let's pretend that everything that we discussed up until this point is a generic threat that exists in some places and at certain times. However, the threat that we are referring to in this particular endeavor is that the majority of people are unaware of it. However, I will provide you with a few examples of this threat. Perhaps a member of your family or one of your friends knows your PIN code When I say "your," I'm not talking about a specific device like a mobile phone, credit card, or any other one that you are using with a PIN code, but you don't know if that person knows your PIN code. I am absolutely sure that when you find out that someone knows your PIN code, you will definitely regret it. But what about the system? If the system knows your PIN number, how many other individuals can see it?

The majority of the systems to which we are connected nowadays are connected to the internet, and we are not all aware of the potential dangers that exist on the internet.

1.3 Symmetric

Alice and Bob are unable to communicate with one another since their messages are encrypted using symmetric keys. If an adversary is successful in obtaining a communication, they should be unable to derive any actionable intelligence from the content of the message.

Alice and Bob need to reach a consensus on a key k before they can move forward with the process of creating a secure channel of communication. These individuals are tasked with guarding the common key. Before transmitting the message to Bob, Alice encrypts

it with the encrypted data computation E and the key k. Bob then receives the message. She use the following formula in order to generate the ciphertext: (k, m). The same way that she sent it to me, she sends it to Bob. Bob applies the same technique and uses the same key in order to decode the letter c. (k, c).

Strictly speaking, symmetric encryption occurs when both users of the network use the same key, k, to encrypt and decode data. This type of encryption is considered to be the most secure form of encryption. The public is well aware of the computations needed for encryption and decryption, denoted by the letters E and D. If you know K, you will be able to decrypt the ciphertext. As a consequence of this, the key needs to be safeguarded. Alice and Bob are in need of a secret key, denoted by k, that is reliable and efficient. Prior to the development of public-key cryptography, nobody had ever come up with a method for exchanging keys, making it impossible to carry out this essential transaction.(Hall 2005)

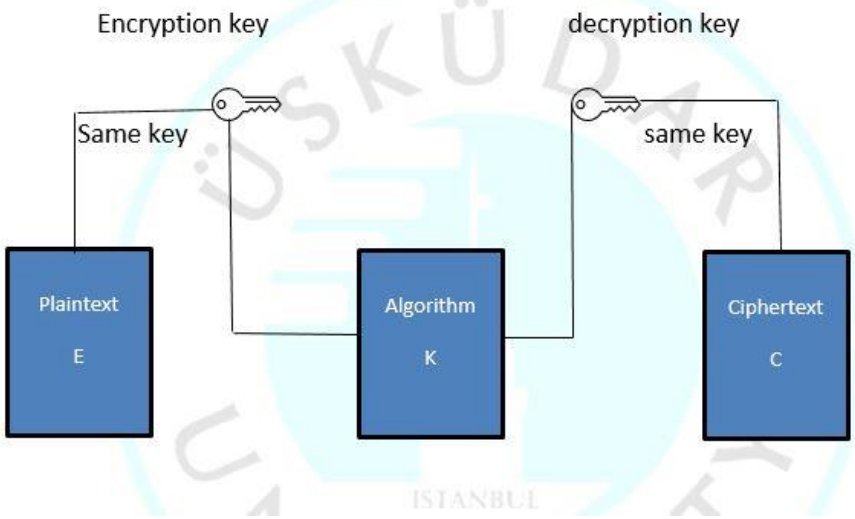


Figure 1 This figure is showing how symmetric process uses encryption and decryption alone one single key

Symmetric Despite the fact that it is a type of cryptography, there are algorithms that are based on the idea of a single key. Although we are unable to describe each of these algorithms in depth individually, we will highlight those that we believe to be the most significant to include in this thesis.

As of today, the vast majority of symmetric block encryption algorithms are built on the so-called Feistel block cipher. The Feistel Cipher is a kind of block cipher that does not

have a very exact design. It is the foundation upon which a large variety of block ciphers are built.

1.3.1 Caesar cipher

Caesar cipher is a popular and extensively used method of encrypting data. Using this sort of substitution cipher, each character in the plaintext is substituted by a different character located at a predetermined distance down the alphabet.

For instance, shifting can be done with three words in the alphabet, either the first three or the last three letters in the alphabet. (Gowda, 2016).

Alphabet before shifted → ABCDEFGHIJKLMNOPQRSTUVWXYZ → NORMAL

Alphabet after shifted → DEFGHIJKLMNOPQRSTUVWXYZABC → +3 or -3

If I try to write my name using any of these two alphabets, I can guarantee that the result will not be the same. On the other hand, the number of shifted characters is not predetermined; it might be three or more than three there also many hypothesis such as this one. The english alphabet is 26 characters so if we devide into into two it will be

13 * 2 so if we overlap those two groups it looks like this

First thirteen → [ABCDEFGHIJKLM]

Second thirteen → [NOPQRSTUVWXYZ]

İf i write the word “CIPHER“ considering this type of alphabet the word will changed into like this "PVCURE", "This means the downside words will represent the upside words while the upside words will represent the downside words." This is called ROT13

There are also many other parts that I can say are the origin or foundation of symmetric encryptions including Vigenere Cipher,One Time Pad (OTP), Data Encryption Standard, and Advanced Standard Encryption. Et, al (Biswas 2019).

1.3.2 Data Standard Encryption (DES)

In the early 1970s, it was not long before it was obvious that enterprises, like governments, required cryptography to be more secure.

DES divides the plaintext into blocks of 64 bits each. A number of blocks are used to convert the plaintext to the ciphertext. The 16 round blocks' inputs come from these blocks. This means there are 16 iterations and every iteration there are some work that are acurring in the process for example; substitution, XOR operations and so on. Those 16 iterations or rounds each of them would be 64 bits or A block that contain 8 * 8 box from the input value. İmportant thing is that each iteration has it’s own key the total key that was used to encrypt and decrypt is 16 but all those keys was generated from the input key. For one thing, the encryption and decryption processes are remarkably similar As long as they reverse the key schedule, they will possess the plaintext. The key size will aso be reduced and also re-encreased inside the process fore example the original key size is 64 bits there are some tables called permuted chioce one, permuted choice two intial permutation, inverse permutation, and so on. So, when applying the input into these tables the data would be reduced and also re-increased.(hall 2005)

Block size = 64 bits

Key size = 64 bits (inside the itaretion process key size = 56bits)

Number of Rounds = 16 Rounds

Number of Subkeys = 16 (while all the subkeys have same size = bits)

Ciphertext size = 64 bits

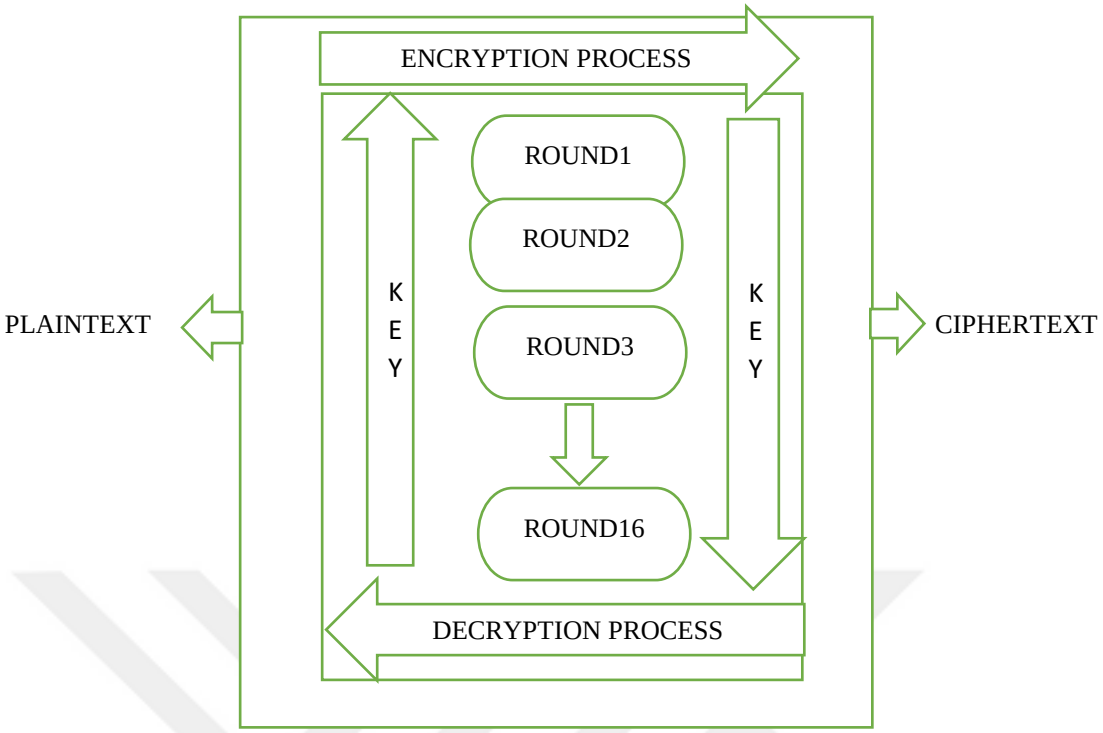


Figure 2 This is figure is showing how DES process works

1.3.3 History of Advance Encryption Standard (AES)

The National Institute of Standards and Technology (NIST) was the organization that first created it as a block cipher encryption technology in the year 2000. It is a data-protection algorithm that works in a similar way to other algorithms that employ block ciphers. The major goal of this method was to replace the DES algorithm, which featured areas that were considered to be dangerous, with a version that was safer. The National Institute of Standards and Technology (NIST) wanted to demonstrate a novel block cipher algorithm that is both powerful and difficult as part of its effort to bring together experts in the fields of encryption and data security. As part of this effort, the agency sought out experts from all over the world.

The algorithms came in from all around the world, and each and every one of them was successful. NIST decided to test these five different algorithms. After giving a number of factors considerable consideration, one of the five techniques of encryption that were proposed by two Belgian cryptographers named Joan Daeman and Vincent Rijmen was selected as the best option. AES was first called "Rijndel" in the period when it was being

developed. This is not a very popular choice for a newborn boy's name. This method is known as the Advanced Encryption Standard (AES) so that there is no room for misunderstanding (AES).

The utilization of substitution and permutation networks is done so that a secure environment may be created for your data. Because it can manage plaintext blocks of 128 bits and 16 bytes that are always the same size, AES is ideally suited for use as an encryption algorithm. These 16 bytes are shown using a 4x4 matrix. When data is encrypted with AES, a matrix of bytes is used. The number of rounds that are utilized throughout the encryption process is yet another essential component of the AES algorithm. It is vital to take into account the length of the key when figuring out the number of rounds that need to be completed. The Advanced Encryption Standard (AES) provides support for three distinct key sizes: 128 bits, 192 bits, and 256 bits. When encrypting 128-bit keys, AES uses 10 rounds; when encrypting 192-bit keys, it uses 12 rounds; and when encrypting 256-bit keys, it uses 14 rounds.

Encryption is currently one of the most common and widely used strategies for preventing the theft of one's data. Utilizing the AES method is necessary in order to guarantee the confidentiality of your data. There are several sub-processes included in each round, and each round has its own unique set of sub-processes. The following are the four stages that comprise one round: (Abdullah 2017)

1.3.4 From an input Data into Hex Decimal

For instance, our plaintext will be “This is testing,” and our key will be “My original key.” Therefore, when we convert from characters to hexadecimal, That would be the first step convert from characters to hexadecimal using an ascii table. “This is testing” and the key that we are using is “My original key,” so when we convert it to hexadecimal, the result will look like this.

Plaintext = “54 68 69 73 20 69 73 20 74 65 73 74 69 6E 67 20”

Key = “4D 79 20 6F 72 69 67 69 6E 61 6C 20 6B 65 79 20”

As we mentioned before we are converting hex decimal, we will locate our state into 4 * 4-or 16-byte table.

54	**68**	**69**	**73**
20	69	73	20
74	65	73	74
69	6E	67	20

Table 1 s-box table

		Y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	a	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	b	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	c	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	d	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	e	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	f	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

The second step will sub-Byte or what they call SPN substitution permutation network, and we are using below table to convert our original state.

20	**45**	**F9**	**8F**
B7	F9	8F	B7
92	4D	8F	92
F9	9F	85	B7

1.3.5 Shifting rows

Instead of row zero, the bytes should be moved left for each row of the state. This is a core tenet of the system. During this process, the bytes in row zero are in no way altered in any way. Only one byte in the first row is rotated counterclockwise and moved one circle to the left. The second row moves to the left by two bytes as part of the shift. The final row is moved to the left by three bytes when it shifts. The size of the new state has not been altered; therefore, it still consists of 16 bytes. However, the order in which the bytes are stored within the state has been reorganized, as shown in the figure. (Hall, 2005)

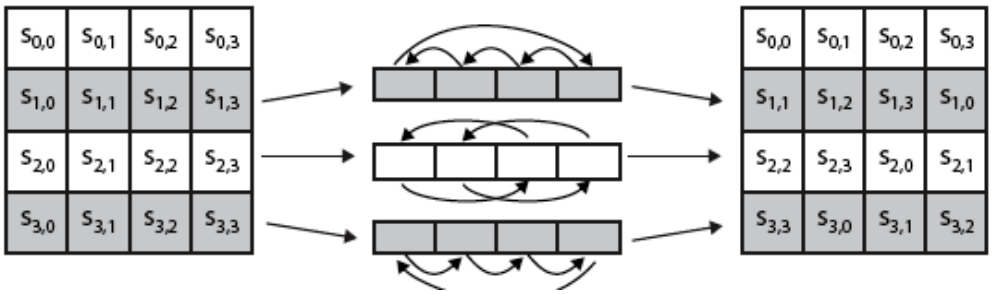


Figure 3 This figure is showing the process of shifting rows

(Hall, 2005)

Before shifted rows			
20	45	F9	8F
B7	F9	8F	B7
92	4D	8F	92
F9	9F	85	B7

After shifted rows			
20	45	F9	8F
F9	8F	B7	B7
8F	92	92	4D
B7	F9	9F	85

1.3.6 Mix columns

Mix-Column is a further significant component of the state. Outside of the state of California, a large portion of the activity referred to as multiplication takes place. A matrix can be changed into something else in one of two ways: The result of multiplying each value byte in the state column by each byte in a row is displayed. Multiplying each row of the matrix transformation by each column of the state will result in the creation of the new matrix. After these multiplications have been finished to produce the new set of four values, the XOR operation is carried out in order to generate a fresh set of four bytes for the subsequent state. However, the dimensions of the state will not change as a result of this step; they will continue to be 4 by 4.

Before mixex columns			
20	45	F9	8F
F9	8F	B7	B7
8F	92	92	4D
B7	F9	9F	85

X

After mixed columns			
02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

20 * 02 + F9 * 03 + 8F * 01 + B7 * 01

1.3.7 Add round Key

The AddRoundKey is essential to the operation of the AES algorithm. Each row of the key and the input data, collectively referred to as the state, is composed of four bytes. The byte matrices show how the 128-bit key and the input data are introduced into the system. Utilizing the AddRoundKey function while encrypting your data will make the data safer. At this stage, the objective is to establish a connection between the key and the cipher text. During the step before this one, the encrypted text was employed in order to construct the text. The result of using AddRoundKey is very dependent on the key that is entered by the user. As a direct consequence of this, the state and the subkey will be shown simultaneously at the stage that comes after this one. The subkey for each round can be gained in a variety of different ways. Utilization of Rijndael's key schedule is what leads to the discovery of the main key. Both the subkey and the state have the same amount of space available. Instructions on how to add the extra key: A bitwise XOR operation is performed on the extra key together with each component of the state.

First step our key we have to assign 4 * 4 mitrix table to process it

"4D 79 20 6F 72 69 67 69 6E 61 6C 20 6B 65 79 20"

4D	**79**	**20**	**6F**
72	69	67	69
6E	61	6C	20
6B	65	79	20

Original key			
4D	79	20	6F
72	69	67	69
6E	61	6C	20
6B	65	79	20
w_0	w_1	w_2	w_3

ROTATE	SBOX	XOR
72	40	41
6E	9F	9E
6B	7F	7E
4D	E3	E2

The above table contains 4 * 4, the same as our plaintext, and in this state key we have w_0 w_1 w_2 and w3; considering these, we have to process them to get another four words, w_4 w_5 w_6 and w7, to fill the quorum.

After that, we reorder the columns by rotating the first column, and then we XOR the result using SBOX.

Table 2 Round constant Table

ROUND	ROUND CONSTANT (hex)
1	01 00 00 00
2	02 00 00 00
3	04 00 00 00
4	08 00 00 00
5	10 00 00 00
6	20 00 00 00
7	40 00 00 00
8	80 00 00 00
9	1b 00 00 00
FINAL	36 00 00 00

Each of our processing columns has to have the XOR operation performed on it with the first row of the Round Constant (HEX) table.

Our new key, which is w4 or the first column of our new key, is something that we can XOR into the columns of our old table, and this will allow us to get the remaining words.

W5 = w4 XOR w1, W6 = w5 XOR w2, and lastly W7 = w6 XOR w3.

The table that follows contains a key zero, and from here on out we are going to keep going until all of the round keys have been found. There will never be more than one use of any one key throughout any given round. The number zero will be used to start each round, followed by one, then two, and so on.

Original key			
4D	79	20	6F
72	69	67	69
6E	61	6C	20
6B	65	79	20
w_0	w_1	w_2	w_3

keys zero			
41	38	18	77
9E	F7	90	F9
7E	1F	73	53
E2	87	FE	DE
W_4	W_5	W_6	W_7

It is now feasible to add a round key to plaintext, and this technique was repeated until the last round, which did not contain a mix column when the process was finished. During this time, the process was also finished.

You should be aware that the processes of expanding the plaintext and the key operate simultaneously, and that the process of expanding the key is the XORed version of the process from the previous round.

Round zero state			
20	45	F9	8F
F9	8F	B7	B7
8F	92	92	4D
B7	F9	9F	85

XOR

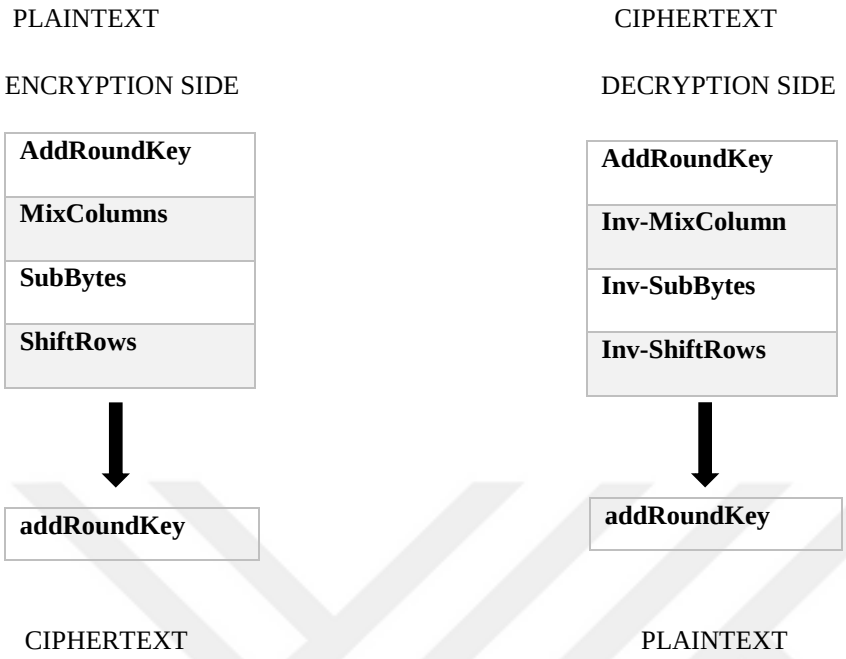
Round zero key			
41	38	18	77
9E	F7	90	F9
7E	1F	73	53
E2	87	FE	DE

1.3.8 Decryption side

During the process of decryption, it is possible to recover and restore the encrypted data as it was originally saved. At this point, the key belonging to the data sender becomes relevant. Through the use of, messages may be delivered and received.

The Advanced Encryption Standard (AES) uses the same key to both encrypt and decode the same data, functioning similarly to how encryption works in reverse. The process of

decryption consists of three stages: the InvSubBytes stage, the InvShiftRows stage, and the AddRoundKey stage.



1.4 Asymmetric

Text can be encrypted with public keys so that it cannot be read by anybody who does not have permission to read it. In the same manner, the recipient of the message will utilize the private key in order to decrypt the encrypted content. The entire process is referred to by its technical name, decryption. This explains how asymmetric key cryptography works in practice.

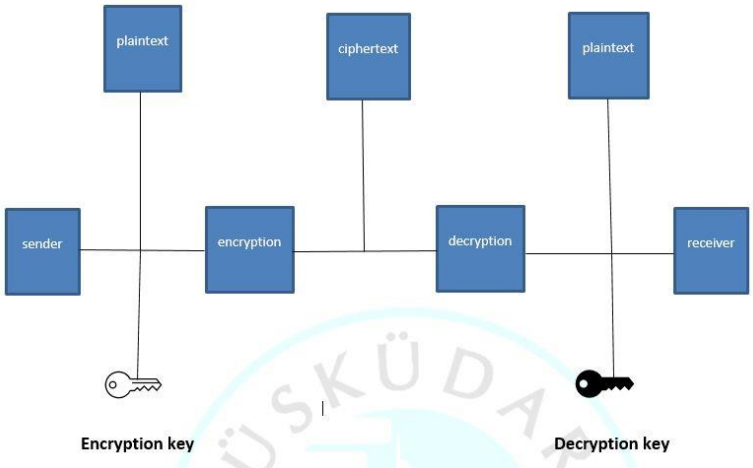


Figure 4 This figure is showing how asymmetric key cryptography works with using two different keys

The use of cryptographic protocols is by far the superior choice when looking for an approach that will protect data both at the level of the network and throughout the entirety of the internet. There are two distinct categories of algorithms used in the field of cryptography: symmetric key-based cryptographic algorithms and asymmetric key-based cryptographic algorithms. Both of these approaches are utilized in order to guarantee the confidentiality of the data. As was said earlier, symmetric key algorithms encrypt and decrypt data with the use of a single key in both processes. Is it a secret key or a shared key? This is the kind of key that may be found in this location.

An asymmetric key technique is applied when it is necessary to make use of two separate keys, which are referred to as public and private respectively. One of the most important algorithms in the area is called the RSA algorithm, and it employs asymmetric cryptography to protect data. Two enormous prime numbers were used by Ron Rivest, Adi Shamir, and Leonard Adleman in their method to generate "public" and "private" keys. In order to decrypt the first transmission, the private key must be utilized, and then the public key must be used to decode the message. You may put it to work to accomplish a wide range of helpful activities, including the following: (hall 2005)

1.4.1 RSA

It is generally agreed upon that RSA is the most superior algorithm available for public key encryption. It has a wide variety of applications, some of which include digital signatures and encryption as well as decoding. When the level of confidentiality is increased, the length of the RSA key also rises.

There are two varieties of RSA keys: a public key and a private key. Both encrypting and decrypting using RSA need the use of these two separately.

Et, al (Ambedkar, 2011)

Step one: create two large random numbers and call them p and q. p does not equal q. Then, figure out N, which is equal multiplication of p and q.

step two, choose an odd number e that is less than ϕ (n) and ϕ (n) = (p-1) *(q-1). the numbers ‘n’ and ‘e’ should both be relatively prime numbers.

Step three generating private key or decryption key d.e≡1 (mod ϕ (n))

$$d = \frac{k * \phi(n) + 1}{e}$$

while d is the private key or the receiver’s key it should use to decrypt the ciphertext.

And finally after generating all those keys now by using those keys we can encrypt and also decrypt processing as below.

Sender side → ($c = m^e \bmod n$) while receiver side will looks this ($m = c^d \bmod n$).

1.4.2 Deffie Hellman

When Whitfield Diffie and Martin Hellman released their work in 1976, it marked a significant turning point in the history of cryptography. This was the issue that was being discussed at the time. To put it another way, Diffie and Hellman are widely recognized as the two individuals who laid the groundwork for modern cryptography. It was not until after another two years had passed that Rivest, Shamir, and Adleman conceived of the RSA cryptosystem. Diffie and Hellman are credited with the development of both digital signatures and the public-key system.

DH allows a connection to be shared between two entities that are located on different networks, even if one of the networks is not trusted. It is essential to be able to confide in someone else in order to communicate with someone you have never met before since doing so enables you to encrypt the communications you send. It is utilized in a variety of protocols, including Secure Sockets Layer, Secure Shell, and IP Security, to name a few. I'll make an attempt to explain using the DH algorithm as an illustration.

You can see that there are two ways to do this task; one of them is straightforward, while the other is challenging.

$S = g^n \bmod p$ → this way is easy to calculate “s“ when you have g, n, & p

$g^{a*b} \bmod p = g^{b*a} \bmod p$ →but it is hard to calculate "n" when you have s, g, & p. Suppose we have two person Alice and Bob after selecting the primes each of them will select secret key to compute their public and shared secret keys.

Public keys generating

$A = g^a \bmod p$

$B = g^b \bmod p$

Private key generating

Alice → $s = (B \bmod p)^a \bmod p$ →($s= g^{b*a} \bmod p$).

Bob → $s = (A \bmod p)^b \bmod p$ → ($s = g^{a*b} \bmod p$).

(Ueli, Stefan, 2000)

1.4.3 Identity based encryption IBE

In 1984, Shamir was the one who came up with the idea of identity-based encryption. However, in order to successfully develop and execute an identity-based encryption (IBE) system, a significant amount of time was necessary. In the years 2000 and 2001, Boneh and Franklin were the first people to propose IBE systems that were based on elliptic curve pairings. In the year 2001, Cocks developed a strategy that could solve the quadratic problem that picked areas presented. Encryption of email is one of the key focuses of IBE.

(hall, 2005)

To determine a user's public key in Identity-based encryption (IBE), an arbitrary string, such as the user's name or email address, can be used instead of the user's private key. To ensure the confidentiality of communications, a framework that does not require encryption keys or certificates might be utilized. This procedure may be broken down into four individual phases.

setup

- Security prams
- Master secret
- Massage space
- Cipher space
- Params (E,q,p,n,P,e,H1,H2,H3,H4)

Extract

- Master secret
- ID
- Private key of ID (d_{ID})
- Params

Encryption

- ID
- $m \in M$
- $c \in \mathbf{C}$
- params

decryption

- d_{ID}
- $c \in \mathbf{C}$
- $m \in M$
- params

2. TYPES OF BIOMETRIC IDENTIFICATIONS

2.1 Early History Of Biometric Identification

Biometrics have been around for quite some time. In general, it's impossible to state that biometrics first existed in this location at this period. Using human body parts for various purposes has become popular all around the world. Biometrics have been used as far back as 29,000 BC, when cavemen used their fingerprints to sign their art.

The Babylonians used the same method to sign clay tablets for business transactions.

Biometric authentication was common among merchants in China in the 14th century. Biometrics in its early stages relied on the use of paper and ink, which allowed for the collection of children's palm and footprint prints. However, despite its simplicity, this type of biometric authentication is still in use and has become the most used method.

Psychologist Alphonse Bertillon set out in 1870 to discover a method for locating and identifying people who had committed crimes. It was not just prints on the ground that he employed, but bodily motions and a variety of other indentations. Bertillonage, a term he coined, was adopted by American and British police departments and helped to reduce the number of potential suspects. The most remarkable detail about Bertillon's system is that fingerprints, the most commonly used biometric method today, were included, although Bertillon himself didn't think it was significant.(Babich, 2012).

2.2 The Types of Biometrics Recognition

Behavioral recognition, also known as characteristic recognition, and physical recognition are the two distinct categories that fall under the category of biometric recognition.

The individual can be recognized by their physical characteristics such as fingerprints, face recognition, and other identifying factors.

The second component is the ability to recognize people based on their behaviors, such as their gait, voice, and so on.

2.2.1 Gait Recognition

Images of human and animal movement may now be caught by photography and videography, allowing viewers to discover details that would otherwise go unseen. This is a significant advancement over previous methods.

In a typical gait analysis laboratory, video or infrared cameras are positioned all around a treadmill or walkway and are linked up to a computer. This allows for the collection of gait data. Markers may be located in various places on the patient's body, or they may be put in groups to a portion of the patient's body. In each scenario, the patient is required to walk on either a catwalk or a treadmill while the computer draws the three-dimensional trajectories taken by the markers. A mathematical model may be used to make predictions about the mobility of bones. (Johnston, Weiss, 2015)

2.2.2 Voice Recognition

The voice, like many other biometric features, is one-of-a-kind.

Analyzing a voice and recognizing a person takes only a brief amount of time, similar to how a human walks.

With the emergence of AI and intelligent assistants, such as robotic voice recognition assistants that we can see on the internet has increased importance and use.

Computers have been utilized in the field of medicine as well as in commercial settings for many years now in order to recognize human speech. In the late 1980s, radiologists and other medical subspecialists began employing pricy dedicated hardware systems that made use of specific language in order to identify reports that were stated in a particular manner. The voice recognition technology that had been in use for a number of years was not capable of meeting the majority of the transcription requirements posed by radiology clinics. (mehta 2002)

2.2.3 Facial Recognition

Face recognition is a biometric technology that can be used to identify a person or verify their identity based on their appearance alone. The security personnel make use of a device that can recognize faces. It is expected that utilising robotic face recognition

would be able to correctly identify persons in photographs. It is a difficult procedure to isolate its characteristics and then recognize it, independent of the lighting, expression, or illumination, as well as the effects of aging, changes, or attitude.

In facial recognition systems, the face of a person is what is utilized to identify that individual. Face recognition systems may establish the existence of an authorized individual, as opposed to merely validating if a legitimate identity (ID) or key is being used. This is in contrast to only checking if the user knows the secret personal identification numbers (Pins), or passwords. See the example given below for further clarification.

In light of the fact that there have been cases in which the same individual has been assigned several identities, it is imperative that the national voter registration system be made free of duplication. The facial recognition technology does not rely on ID numbers in any way; instead, it directly compares the faces of the voters in order to distinguish one from another. When the top two matched faces are so similar to the query face image that it is hard to tell them apart, a manual inspection is required to determine which face is which. Et, al (Goudail, 1996).

2.2.4 Fingerprint Recognition

The process of comparing known and unfamiliar fingerprints to determine if they belong to the same individual is known as fingerprint recognition. There are a variety of methods, strategies, and systems in use today to match fingerprints and address associated issues.

The quantity of matched minutiae on the query and reference fingerprints is often returned by a minutiae-based fingerprint matching system, and it is used to create similarity ratings. In general, higher similarity ratings result from more closely matched details. We can tell the difference between a real fingerprint and an impostor by counting the amount of minutiae that match between the two. It is generally accepted in the field of forensics that two fingerprints with a minimum of 12 matching microstructures are those of the same finger. Partial fingerprints can't only be identified by a total number of matching minutiae. To arrive at a similarity score, we must additionally take into account the overlapping regions on both prints as well as the overall distance between all of the matched minutiae.(Tsai-Yang, Venu 2005).

2.3 Security

Because the safety of our whole society is dependent on security, each and every one of us requires it. We also know that it's not natural for people to live together in communities without fighting.

When I go back into the digital world later today, I will find that everything from government services and private businesses to schools and hospitals can be found on the internet.

Therefore, the issue that has to be answered is whether or not the large volume of data that pertains to society can be accessible online in a secure manner.

A loud "no" is the answer to that question because it is a location that is home to a diverse population of people. It is a site where anybody may come and go as they like, which has led to a significant amount of exploitation that can be both excessive and detrimental. The adverse effects significantly outweigh the beneficial ones. I have to concede that point. There are many ways to protect the information stored on a network that is important to both everyday life and business.

However, because of the circumstances, I won't be able to go into as much depth as I'd like to.

- Salting
- Encrypting and decrypting
- Hashing
- Authenticating, And so on.

A key is required in order to encrypt and decode data, and it is my opinion that if the key is sufficiently robust, then the data will be safe. For instance, a business that has huge locks rather than little ones is a safer option than the other.

Cryptographic techniques are frequently employed with the aim of securing data storage or transmission. Using a secret key, encryption is used in cryptography to alter data before it is either stored or sent. In cryptography, this is the most fundamental principle. You

must have this secret key in order to decode the data that was changed while it was being encrypted.

To maintain security, cryptographic keys must be extremely long. Each of these keys must be at least 128 bits in length to meet the requirements of the Advanced Encryption Standard (AES). Due to the difficulty of memorizing these key lengths, they are maintained in a secure area. However, such hybrid systems, also known as cryptographic systems, utilize fingerprint verification to increase security levels. This is done to prevent unauthorized individuals from gaining access to the keys.

Therefore, we have decided to generate a key from a fingerprint of a person and use the Advanced Encryption System to use it to encrypt data because we believe it is one of the easiest ways to create or implement cryptographic systems. However, when we look at the other side, even if they try to breach this key, it is more difficult because there are a lot of circumstances. Nevertheless, there is not a single system or organization in existence that is willing to admit that their system is susceptible to attack and simple to access. There are a lot of elements to take into consideration, but the three most critical ones are: confidentiality, integrity, and availability. From my perspective, the process of encrypting data always seems to have a bias toward integrity, with the primary focus being on preventing tampering with the data. The reliability of the key is everything when it comes to the security of the information, particularly when we are discussing symmetric cryptography. On the other hand, if the key is reliable, it is highly likely that the data is reliable as well. But if the key is unreliable, this indicates that the system is susceptible to attack, and it is vulnerable.

2.4 Literature Review

The storage of the private key is required by all currently available asymmetric encryption algorithms. In many cases, the protection of stored keys is provided by poorly selected user keys that may easily be guessed or obtained through the use of brute force attacks. There is a risk that the confidentiality of sensitive data might be compromised if there are any loopholes in the overall encryption method. In order to generate consistent keys, any cryptosystem that relies on biometrics needs to be able to handle even minute variations in the biometric data it collects from different acquisitions.

An evaluation of the method utilizing 3D facial data shows that it can consistently generate keys with a length appropriate for the 128-bit Advanced Encryption Standard (AES). (Chen, Chandran, 2007)

Biometrics is a powerful and distinctive tool, even though it relies on the physical and behavioral characteristics of individuals to operate. In this context, the term "biometrics" refers to several characteristics of the human body, including the fingerprint, the Finger Knuckle Print (FKP), the eye, the retina, the voice pattern, the iris, and hand measurement. An individual's fingerprints, iris, face, and palm print are the anatomical characteristics that are most frequently utilized in the context of security applications. The user may be identified based not only on their physical characteristics, such as their voice, signature, and gait patterns, but also on their behavioral characteristics, such as these. For this reason, authentication is so important to the process of securely transmitting information. The use of passwords and smartcards is currently the sole way to verify that a user has the necessary authorization.

On the other hand, dictionary attacks have the potential to crack passwords in a short amount of time, and smart cards can be misplaced or stolen. Because of this, computer hackers are allowed to enter systems because they won't be discovered. Biometrics is the only technology that can give a solution to these problems. (Arunachalam, Subramanian 2015)

When biometric cryptosystems are used, a cryptographic key is created from a user's biometric template, which is then safely kept in the database. This key is used to decrypt information. (Aru, Shanmugam 2009)

A photograph of the customer can be taken using a technology that captures fingerprints. The acquired picture is sent to the device that processes images in the automated teller machine. After converting the picture into 1024-bit binary data, which is the input data for the AES processor, data is encrypted using a four-digit decimal key that the user gives as a password. This occurs after the processing of the image. A communication channel is utilized to transmit information that has been encrypted to the bank server. The bank makes use of the same key to decrypt the encrypted communication that it has received. At this very time, duplicated photos are being produced. The encoded fingerprint picture

is compared to a previously saved image of a legitimate customer, and there is a perfect match found between the two. (Hossian, Nawaz, Grihan 2013)

Identification and verification are the two most important functions that may be performed by a biometric system. In today's world, fingerprint processing is a widely recognized form of biometric technology that is simple to use for the purpose of enhancing the amount of security and safety afforded to the user's fingertips. The procedure of having a person's fingerprints collected on an identifying device is straightforward, and it does not need a lot of time or effort on the person's part. As a consequence of this, the process of recognizing fingerprints is included on the list of those that require the least amount of effort and hence create the least amount of annoyance. Since the 1800s, fingerprints taken from people's thumbs have been utilized by both private law companies and public authorities as a method of identification. The United States of America provides a solution on electronic platforms that is technologically equivalent to the international standard. There is a first phase in which images of the user's fingerprints are obtained, but these photographs are not stored in the system in any form. On the other hand, the images of the original fingerprints are used as a basis for developing fingerprint templates, which are then applied to the fingerprints themselves. No, you will not be able to regrow it. As a result, there is no way to mess up the system in any way. (Phys, 2021)

During the first interview, the director of an e-commerce company at a prominent bank addressed concerns in a simple manner about replacing PIN codes with a form of fingerprint verification. It was agreed upon by him that the use of biometric technology would enhance safety, authentication, and the overall quality of the customer experience; however, he issued a word of caution that widespread adoption and user acceptance would take some time to achieve due to concerns regarding the ease of use, the level of privacy maintained, and other factors. All the leaders in information technology came to the conclusion that the newly developed technology would initially be more cost-effective, that biometric technology would remove the need for people to be involved in the process, and that security would be increased to protect both customers and banks. The purpose of the conversation with the legal adviser was to obtain a legal opinion on legal problems connected to the misuse of privacy and to fraudulent activity. (Janahi 2018)

The fingerprint picture is split, equalized, improved, binarized, and thinned, as well as other processes, as illustrated in Figure 4, to produce a fingerprint refinement map that has crisper fingerprint feature spots, textures, and other distinctive information. A multichannel integration approach is used to enhance the fingerprint characteristic data even further. A new feature map is stitched together using the fingerprint picture as a guide, as seen in Figure 5. The produced fingerprint key is more random since it contains more detailed information about the fingerprint. Et, al (Wu 2021)

As the Internet expands, so does the need for better information security. Traditional cryptography approaches need the user to keep track of keys, which is inconvenient. There are approaches for generating cryptographic keys based on biometrics directly. Face biometrics are the basis for a biometric cryptosystem we propose in this work. First, a 128-dimensional principal component analysis (PCA) feature vector is collected from the facial picture during the encryption step. Thresholding is used to produce a 128-bit binary vector. Once we have the bits that make up the bio-key, we preserve the optimal bit order number in a lookup table for future use. In addition, a Reed-Solomon error-correct-code (ECC) is created. symmetric DES and bio-key are used to secure the communication. A picture of the query face is decrypted using a 128-dimensional PCA features vector. The look-up table formed during the encryption step is then used to construct a bio-key. In order to get the final key, both the bio-key and the Error Correct Code are used (ECC). To decode the message using the final key, the symmetric DES algorithm was used. Et, al (Wu, 2010).

2.5 Problem Definition

My primary objective in this research was to devise a method for producing a secret key that is both dependable and enough for the purpose of protecting an individual's data, in particular the connection that exists between an individual and his data. There are a great number of papers that have been wrote on the topic of data security in the internet but the only thing of my objective is to generate a secure Bio-Key to use encryptions and decryption of data for example someone stored his data in his computer let’s say he encrypted that data and also tried to decrypt so the thing that this research is appointing is the key that this person is used to secure into his own data.

How many people are able to know your personal identification number?

How was generated the key that you are using to secure into your data?

Does the system recognize your personal identification number?

What happens if someone hacks your system?

Is there even a small possibility that your PIN code will be protected even if the system is hacked?

The solutions to the issues raised above may be found in this thesis, and I believe that they will be sufficient for anyone who is seeking these answers.

This research is made up of two parts. The first part is processing the fingerprint and getting the key from it. The second part is using that key and the AES method to encrypt and decrypt the data.

Also inthe beginning the system is training all the steps and after trainning it is recognising the steps of the process to make secure the data.

3.SYSTEM DESIGN

3.1 System Training Diagram

The sequence of how the system is training the process of learning all of the stages is depicted in the diagram that can be found below. First, it learns the person's fingerprint, then it learns the two distinct types of ridges and bifurcations on the person's fingerprint, and finally, it learns the two distinct types of minutiae points on the person's fingerprint. This is all depicted in the diagram. It will first create a filter for each of them on their own, followed by the sorting of the arrays that were derived from the user's fingerprint, then it will learn how to concatenate the sorted arrays with the PIN code digits, then it will put together the sorted array and uses it as a Bio-Key, and finally AES will be used to encrypt it. Those are the steps that will be taken. However, there is something that I need to make clear about this situation, and that is that all of those actions are merely training the system, and the system was learning all of those operations.

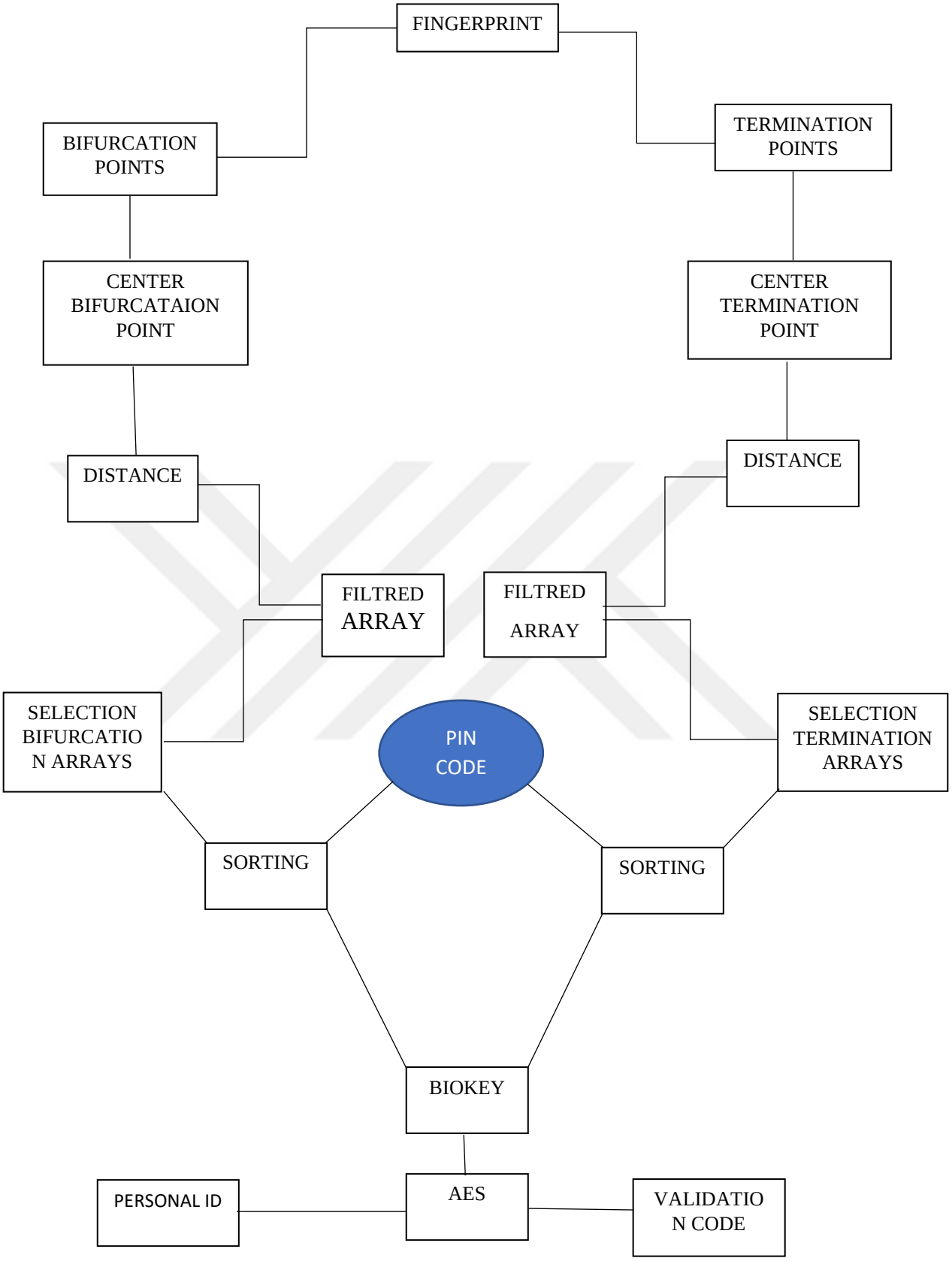


Figure 5 This figure is showing system training block

3.2 System Recognition Diagram

The process of system training starts with the person's fingerprint, and the process of system recognition starts with the same situation. The training side only studies or saves the input data, not all the data or all the stages that were discussed above, but most of them. There are many similarities between these two systematic processes. The main distinction is that the training side only trains or saves the input data. And it happens only once, while the other one happens multiple times, which means the client is accessed multiple times.

What steps should be taken after the data has been saved?

That is the topic that will be covered in this part. If a customer or user wanted to access his account or any other kind of restricted or authorized entity, then when he entered the pin code or key or password or any other kind of protocol that protected the data, there must be a backup, because after entering those digits, there could be a place that the key has been stored, and so the system then compares the key that was stored in the database and the new one that was entered, and if they are the same, then you did it. If they were different, unfortunately, the authorization would be denied.

The overall idea that these two stages are working together to demonstrate is really something along the lines of this illustration, and this side is the side that the system looks at to determine whether the customer has the authorization to view the information

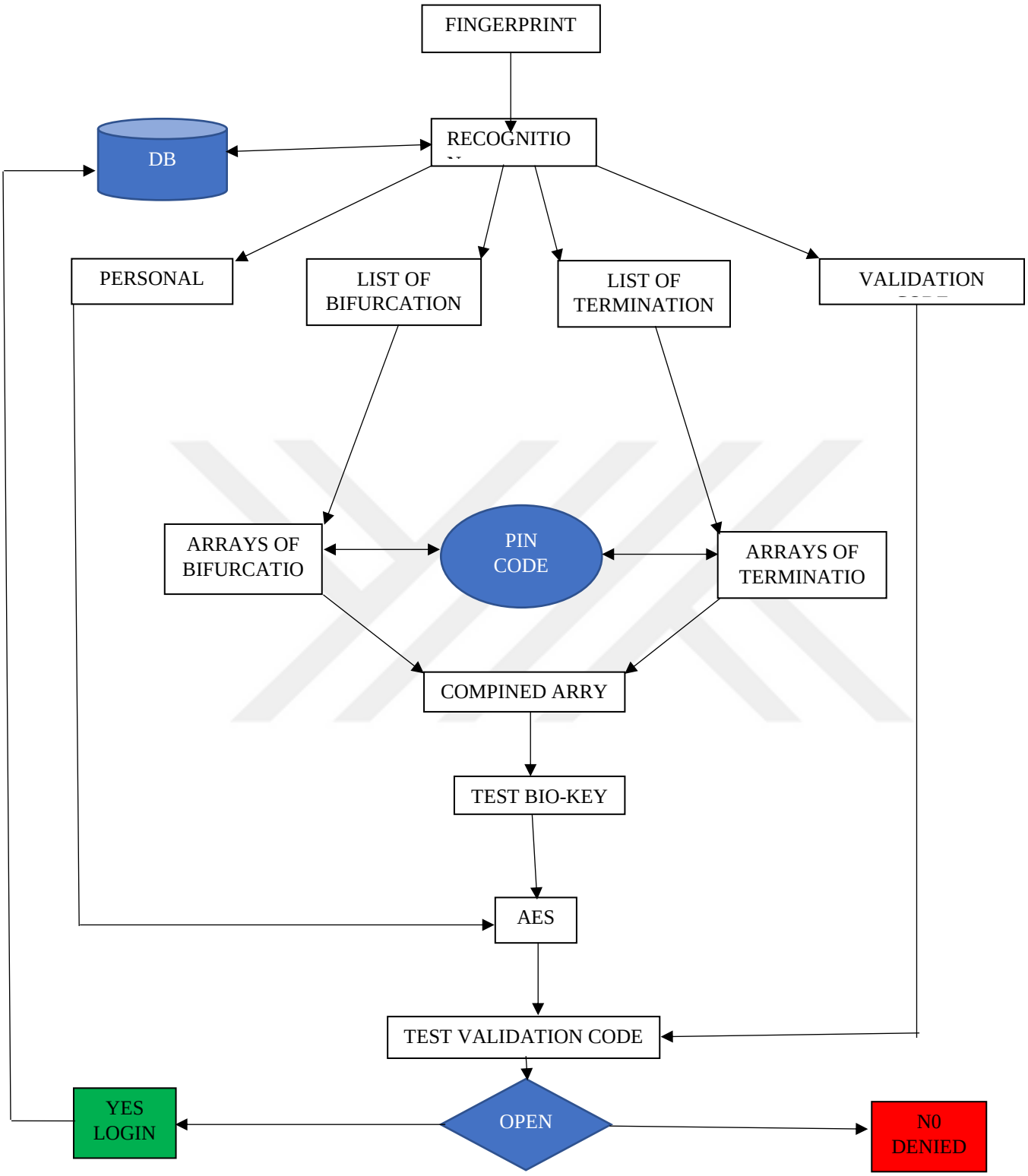


Figure 6 This figure is showing system recognition block

3.3 Fingerprint Overview

There is no more unique creation than a fingerprint, with each one carrying a unique combination of characteristics. In certain ways, even the fingerprints of identical twins differ from one another. Scaling and identifying fingerprints is done using the delicate details of a person's fingerprints. The most readily recognizable microscopic features are ridges and bifurcations. These little features on the fingers make it easy to hatch the hands to grasp any object.

At some point, the maximum number of fingerprints that can be made will be reached. Generic and common segments are found on their borders, like the rest of our organs. Skin characteristics of the embryo are pre-programmed, but its form is the result of random circumstances. Pre-programmed. The precise location and thickness of each edge is determined by the womb and the amniotic fluid that surrounds it. Finger traits can be influenced by an infinite number of biological factors because there are so many

variations in our genetic make-up. Advancement is so chaotic that it is virtually impossible to escape the same cautious paradigm that has constrained human history for double the amount of time.

This means that fingerprints can be used to identify a person even if they are genetically related to someone else. A well-prepared operator or a relocated piece of code may also be able to discover clear, documented errors even if two prints are identical. One-of-a-kind imprint assessment is the most significant concept when it comes to crime and surveillance.

If you want a unique imprint scanner to replace a human analyst, you must conduct a print test and identify it from other models on record. we cannot copy it.

The fingerprint acquisition, fingerprint image pre-processing, feature extraction, fingerprint categorization, and fingerprint matching are all essential phases in an automated fingerprint recognition application. Each step of fingerprint recognition has a variety of methods and technologies to choose from. To perform a fingerprint matching operation, a new fingerprint is compared to previously processed fingerprints stored in a database.

3.3.1 Normalization

Not every fingerprint image is good and clean Most images are very unquality so the machine it is hard to find the correct minutiae and it would be difficult to extract ridges and bifurcation or any other necessery minutiae points.

In order to find a solution, for this issue it is necessary to enhance the quality of image.

So the process of enhancing the quality image is called normalization.

It is also necessary to reduce the pixels of the image to get a smaller number, more visible and less noise. (Shi, Govindaraju)

Figure 7 In these two pictures the difference between them is the black one is the original fingerprint while the other one is normalized.

3.3.2 Orientation

The orientation field of a fingerprint picture shows the characteristic of the ridges in a fingerprint image. Fingerprint image analysis would be incomplete without it. Numerous approaches exist for estimating the fingerprint image's orientation field.

Orientation is an essential part of a fingerprint's story. The ridge pattern of fingerprints may be seen in the image. In the event of low-quality images, fingerprint separation and augmentation can be aided by a thorough understanding of fingerprint orientation process. (Gu, Zhou, Zhang 2003)

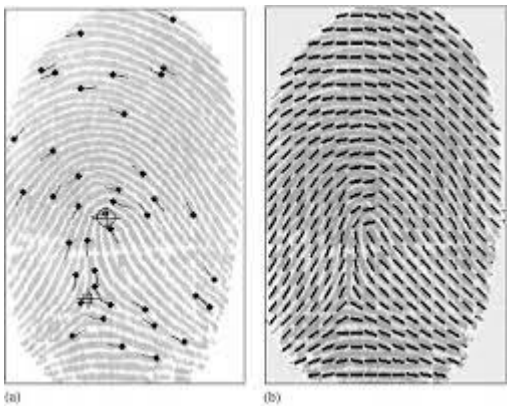


Figure 8 This image is showing the difference between a fingerprint image of oriented with and without

3.3.3 Region of interest (RIO)

The next step is to find the region of interest using the enhanced fingerprint picture that has been obtained. If you want to get the most information out of your fingerprint image, you need focus on a specific area known as the "region of interest" (ROI). It is necessary to divide the fingerprint data into a 16x16 square block before proceeding further. After that, the gradient for each block is determined. The standard deviation of the data must be calculated by averaging the X and Y direction gradients. If the procedure fails to satisfy the threshold level of success, each segment is replaced with zeros.

This theory makes the assumption that each collection may serve as the basis for an area. This is due to the fact that photographs typically feature groupings of items. It is necessary for an advanced image processing system to have the capability to apply specific processing techniques to particular regions of the image. Different processing styles can be used on different parts (regions) of a picture. (Kristensen, 2010)

3.3.4 Ridges and Bifurcations

There are more than ten distinct sorts of minutiae; Pores, short ridges spots or islands, cores, deltas, and other sorts of minutiae can also be found. Even so, these other kinds of minutiae can be seen as important. however, for the sake of this thesis, we only made use of the two that are the most widely utilized and well-known, which are termination and bifurcation.

After the minutiae have been extracted, the location and angles of the minutiae can be calculated. A Crossing Number is used to locate the minutiae points in a fingerprint picture to exclude the terminations that are located outside of the borders. When calculating the "crossing number," consider half of the difference in intensity levels between two adjacent pixels as your starting point. Miniature points are classed as termination, normal ridge, or bifurcation if the number of crossings is 1, 2, or 3.

(Sarraju, Franklin Bein 2021).

3.3.5 Minutiae Extracting.

Terminations and bifurcations are the two most distinctive aspects of the minutiae. Individual bent components are called terminations, while the diversion between two edges is called valleys.

There are a lot of Minutiae types such as island or short ridges, bridges, eye, or enclosure, delta, dots, spurs, double bifurcations, trifurcations.

When thinning is done, the background and foreground of the image are also classified, a tiny, shaped line would appear clearly. Each of the two tiny lines that divide the point where they separate is called a bifurcation, while each of two straight tiny lines wherever they end is called ridge endings or terminations, as I mentioned earlier.

After that, we marked all those points by considering two different colors. However, it turned out that there were some false minutiae, so the first task would be to differentiate between the true and the false minutiae; after that, they should be placed in a graph to locate the actual place where each point is located.

After we had determined where each point was located within the graph, we were then able to easily determine the distance between each of those points by making use of the Manhattan Euclidean distance, as I had mentioned in the previous section. Finally, we were able to identify the point that was represented as the center of gravity or the center point for both sides. (Al qadi, 2020)

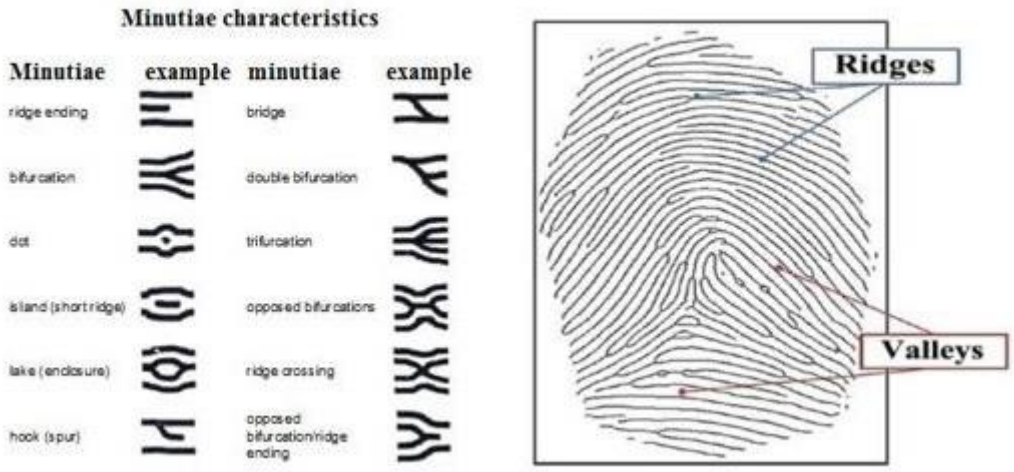


Figure 9 Ridges are located along the dark or black lines, whereas valleys are found in the white space that separates them.

3.3.6 The Center Point

Therefore, we need to determine the point that is central to each group, and once we have that, we can calculate the averages by adding up all of the points in each group. We need to divide the total number of points in order to acquire an accurate average of X and Y for the bifurcation and termination sites.

After calculating the the center point in order to locate the point at which each component of the points has its center point, the next step is to calculate the distance between each pair of points in the graph. For instance, all of the termination points have their own center point, and the bifurcation points also have their own center point.

For example, if the array of Termination points is

X	**Y**
12	12
7	8
3	4
5	6

Then we are going to add up all the X value

Also, we are adding all the Y value

And then we have to divide the total value.

To calculate the average.

X	Y
12	12
7	8
3	4
5	6

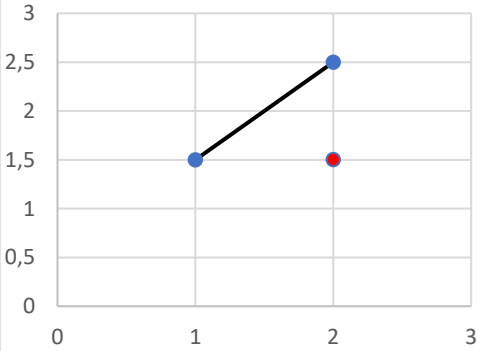
there for 27/4 is equal to 6.75 and also 30/4 is equal to 7.5 **27** **30**

So, the center point of the above array point is X = 6.75 and Y = 7.5

3.3.7 The Distance Between Minutiae Points

Primarily, we need to understand the Euclidean technique based on distance since we need to assign or know the true place of every point in the graph. Once we have the actual place of every point, we will be able to consider the center point of each side termination and bifurcation.

In general, if we have two points like A_1 and A_2 or consider any other dimension by applying Euclidean and Manhattan distance parameters.



now we can see where the actual place of every point is for example.

point 1 = (1, 1.5)

point 2 = (2, 2.5)

point 3 = (2, 1.5)

GRAPH 1

This graph is showing the distance between two points

this means we can assume it as a triangular shape that contains A, B and C.

$AC^2 = AB^2 + BC^2$ which can be also assigned as this $AC = \sqrt{AB^2 + BC^2}$

Why not put it in this way, given that the calculation was written up above, as I mentioned in the previous sentence?

$$\text{Distance} = \sqrt{(X_2 - X_1)^2 + (Y_2 - Y_1)^2}$$

$$D = \sqrt{(2 - 1)^2 + (2.5\text{-}1.5)^2} = 2.6457$$

So, the distance between point one and point two is approximately **2.6457**

This procedure is part of the system's training, and while it is learning all of the procedures that were described before, it will identify them after it has finished its training.

3.4 Sorting Arrays

Since there are two portions to the arrays, which respectively represent termination arrays and bifurcation arrays, we need to sort the data in order to create some kind of order. In general, when we are sorting items, there are a number of different approaches, such as ordering by date, ordering by size, and so on. However, we have placed them in a different order which is sorting from bottom to top, and the other one also sorting from top to the bottom for example the bifurcation arrays was sorted from bottom to top while the termination arrays sorted from top to pottom.

This procedure of sorting the data does have the most significant relevance in relation to this project; because the BioKey contains form of sorted arrays of both side and also it accomplishes is to prevent the data from becoming confused and to provide it with a uniform structure that is simple enough for everyone to understand.

3.5 Pin Code

A PIN code always consists of four to six digits; to put it another way, it is a numerical number that we use for most electronic devices, such as phones, computers, ATMs, and every other electronic aspect that we want to protect or make private, or perhaps there is some privacy data that we want to integrate. PIN codes are always in the range of four to six digits. Therefore, it is essential to select numbers that are unrelated to one another. However, the risk is not only associated with the fact that you selected numbers that are related to one another, such as your birthday, four numbers that are contained in one number or only two numbers, such as 4444; the risk is also associated with the fact that you selected unrelated numbers, such as a number that is difficult to predict. The problem is not only both of these things, but there are some other risks.

The fact that the system knows your PIN code is, in my opinion, maybe it is not the most significant security risk, but it is part of the risk. For example, If a server were to be compromised, the hackers who gained access would then know your PIN code and would be able to get into everything else that was protected by your PIN code.

The question now is, what is the solution?

We already have an array that contains termination and bifurcation, and we need to sort it based on the numbers 0 to 9. After that, we will link the user's PIN code and the array in the order that they appear in the sorted list.

This procedure is part of the system's training, and while it is learning all of the procedures that were described before, it will identify them after it has finished its training.

Table 3 PIN code of person one

NO	BIF_ARRY	TERM_ARRY
0	68	109
1	73	179
2	76	171
3	81	93
4	82	232
5	85	269
6	86	94
7	85	308
8	90	99
9	90	112

person one

Table 4 PIN code of person two

NO	BIF_ARRY	TERM_ARRY
0	55	143
1	56	163
2	56	186
3	57	121
4	57	200
5	59	210
6	61	215
7	62	224
8	63	233
9	64	101

person two

If someone’s PIN code is 5215, the system will immediately recognize the array because it has this person’s array as a backup. If the digits that were entered belong into his/her array, then he/she can get permission, but if it does not, then it will deny absolutely. If the PIN code isn’t in the array, then it will deny permission.

Even if they have the same PIN code their fingerprint arrays are different as you see on the above tables.

In general, the steps that we mentioned above are only for system training. Once the system learns, it will be divided into two parts, some of which will be saved in the database while the other parts will belong to the person. This means that the security parameters will be partitioned, which I believe is better than the alternative, which is to accumulate all of the source data in one location. The validation code, the person’s ID,

sorted arrays from his fingerprint, and personal fingerprint will all be saved in the database.

You might be thinking that nothing is left and that all of them have been saved in the database. However, the PIN code has not been saved in the database, and the only person who knows the PIN code is the customer or user. This shows, in my opinion, that splitting the security parameters to make a secure and reliable key is not something that everyone can do, even though it is one of the most important things.

3.6 System Recognition process

When the user places his or her fingerprint on the reader, the system recognizes four separate processes in parallel: a list of bifurcation arrays that belong to the minutiae point of the user's fingerprint; a list of termination points of arrays that also belong to the user's fingerprint; the validation code; and the user's personnel ID. The fact that these four things are stored in the database is the most important aspect of this, as it ensures that the system is aware of all three factors.

Because it is easier to determine the distance between it and all the other location points, the center point is the one that is sometimes referred to here as the center of gravity.

Suppose the customer has entered his/her PIN code, and I would like to emphasize once more that the system does not know your PIN code; consequently, it goes straight to your fingerprint directory listings, where it will take a measurement using the digits you entered and look up the database that is stored. Therefore, I would like to emphasize that.

In this part of the system, which deals with recognition, the system will always compare two or more distinct measures in order to determine who knew him/her previously or had information about him/her and who are the strangers.

3.7 Personal ID

I can only describe personal ID as the personal data that an individual has the right to preserve, in addition to personal information such as date of birth, name, and the common personal details.

When the system learns the fingerprint of a person, it requires the person's specific information in order to match it with the fingerprint. Therefore, this person's information is saved in a database in order to identify him or her. This is why some detailed information of the person is required to store the database.

For instance, when a person walks to an ATM, the reason why he inserts his card before beginning to input his PIN number is that he is attempting to authenticate himself by providing his identification.

Okay, so let's look at this from the other perspective: when someone uses an ATM and enters their PIN code, the machine will ask them to enter their PIN code. This is done for security reasons, of course, but we also know that the machine knows who the card's owner is, which is why it is asking for the PIN code.

So, this is the same issue when someone his fingerprint was stored then there could be matched information about this fingerprint.

3.8 Testing Bio-Key

The Bio-Key that we established is simple to comprehend; in my opinion, even someone with a fundamental comprehension of cryptography can do so. Furthermore, the Bio-Key is dependable and adaptable; it contains an array of fingerprints, which are then used to encrypt an AES containing the person's identification information; finally, the Bio-Key was balanced with a validation code to verify the righteous.

At the training stage, it was previously stored in a database, and at the same time, when it goes to the recognition stage or testing status, it will be available in the database, which is remarkable through all the conditions that are mentioned above.

At the same time, it is a sustainable solution to take away the power of safeguarding the individual's data and split it between the individual and the system. The diagram below demonstrates in detail the stages it goes through when someone wants to access his data, including Bio-Key. This indicates that the system does not know the user's PIN code, but it also does not need to know it because it already knows the user's fingerprints and other personal identity information.

4.RESULT

4.1 fingerprint processed resulties

4.1.1 Binarization

In the context of image segmentation, the phrase image binarization refers to a basic technique. An image may be reduced to binary form, or an object can be separated from the pixels that make up its background using this technique, which is all it is in the majority of circumstances. Or, to put it another way, only those pixels in a grayscale image whose values above a pre-determined threshold are transformed to white, while the rest of the pixels stay black.

Figure 10 This is the result of binarized fingerprint images of three persons

This picture was converted to black and white and then divided into a foreground and a background in order to emphasize certain features, such as the lines and the main purpose is to clarify terminations, bifurcations, and vallies.

4.1.2 Thinning

This step is quite similar to the one that we discussed previously; the only difference is that the width of the picture is reduced. When I refer to the width of the image, I am not referring to the entire image; rather, I am referring to the width of the

object or the foreground. This is due to the fact that the foreground is composed of all of the lines of fingerprints that it includes. Don't forget that the background has been erased from the image, so all that is visible is the foreground, and the background is absolutely empty of any content. It is just like an empty white page. So skeletonization or thinning is the process in which they use to reduce the width of the ridges of an image. The main purpose of this process is to get clean ridges to mark terminations and bifurcations or any needed intersections.

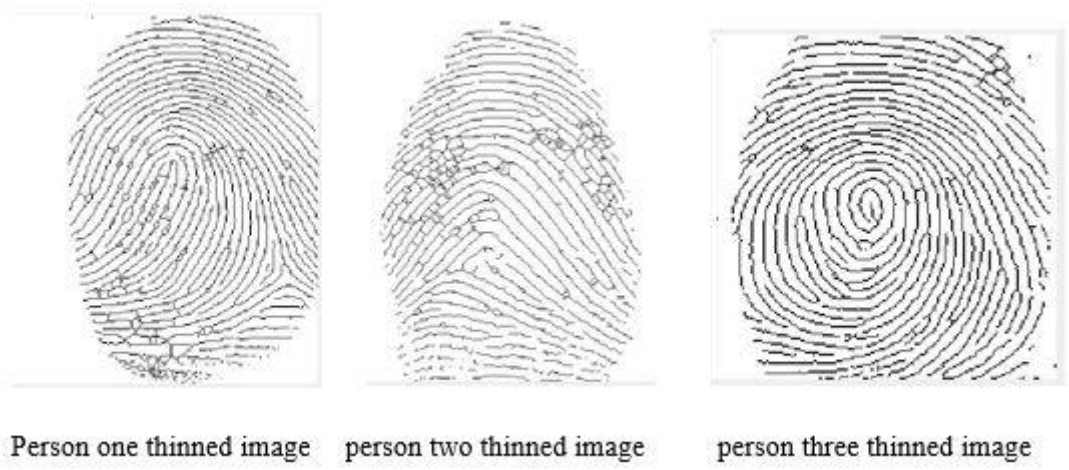


Figure 11 This is the result of skeletonized fingerprint images of three persons

4.1.3 Extraceted Termination Points

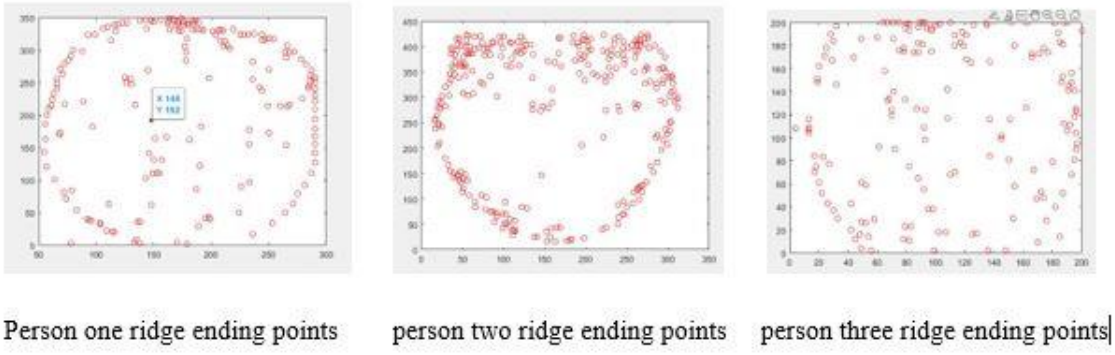


Figure 12 This is an extracted minutiae termination points result of three persons

All of the termination points have been extracted, as shown in the figure 12.1, and also inserted into the graph, such as the point that we have indicated as an example, which is

X is equal to 148 while Y is equal to 192. You can see in the picture that every single point has a definite position between X and Y. You are aware that these points are not being unloaded into a picture such as a fingerprint; rather, they are merely being retrieved. Also it contains many false termination points.

4.1.4 Extracted Bifurcation Points

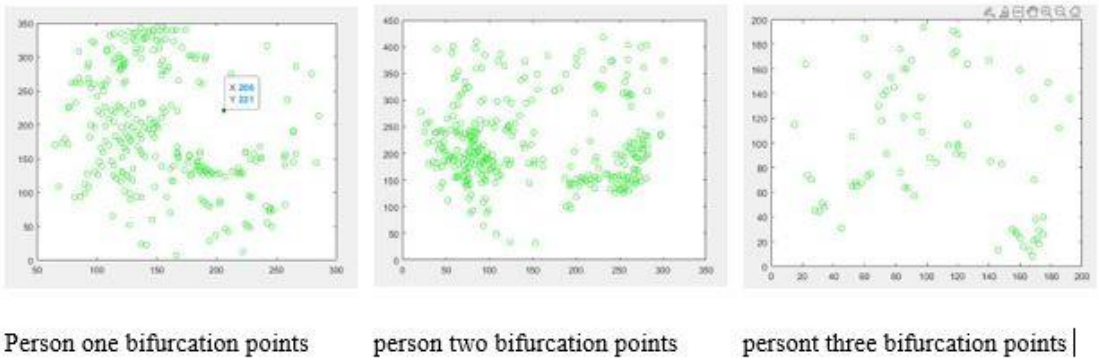


Figure 13 This is an extracted minutiae bifurcation points result of three persons

All the bifurcation points have been retrieved and added to the graph, such as the example point where X equals 206 and Y equals 221 (see figure 12.2). X and Y are clearly visible in the photo, and each point has its own location in the graph, yet these points are not being put into an image, they are just being recovered. There are also several incorrect bifurcation points in this model.

4.1.5 Putting Together And Over Laying The Fingerprint Image

After combining or bringing together in one graph all of the termination points and bifurcation points, the fingerprint picture is then placed on it, at which time many false minutiae will emerge on both sides. In this situation, a red dot indicates the point at which a line in the image comes to an end, whereas a green dot indicates any place at which two lines intersect or branch off from one another, as illustrated in figure 13. It would appear that there are a great number of points that are not marked by either of them; we refer to these points as “false minutiae points.”

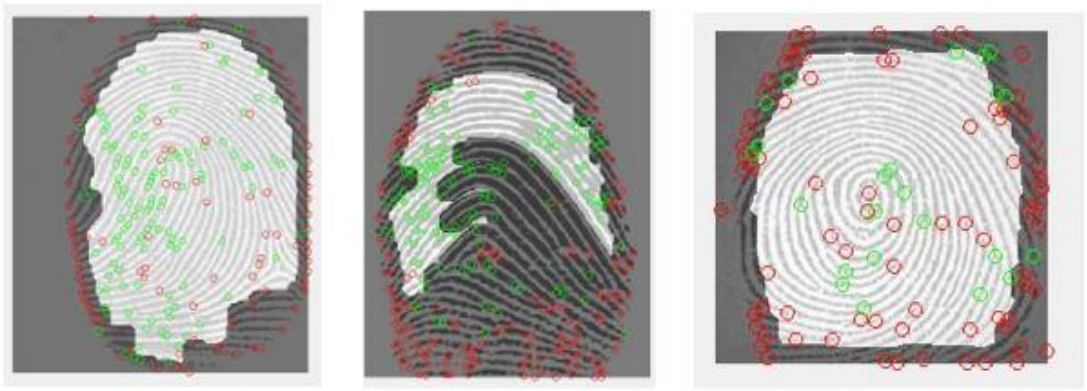


Figure 14 This is an extracted of termination and bifurcation points result three persons

4.1.6 After Filtering

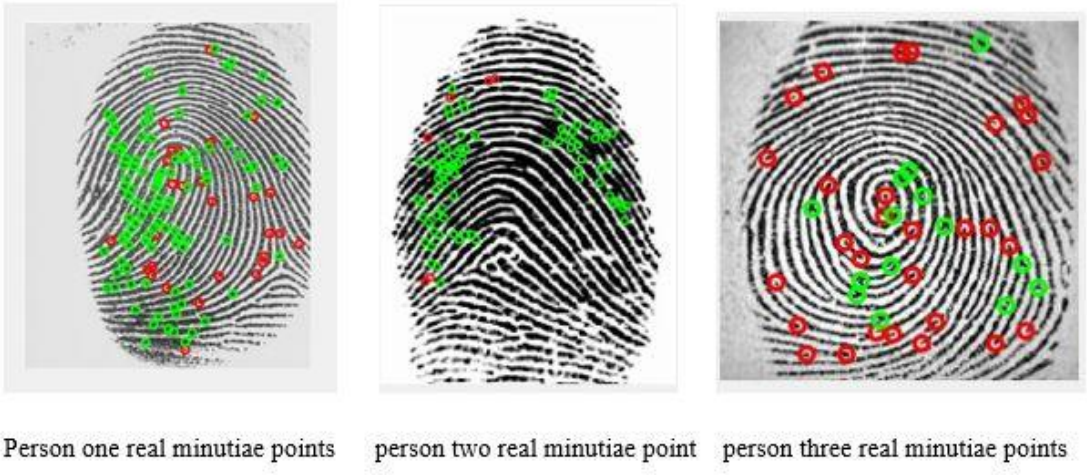


Figure 15 This is after filtering minutiae points results of three person

We need to filter in order to get rid of all of the irrelevant points of minutiae. This procedure will assist us in obtaining a few specifics about which we can be certain and in distinguishing the image from the regions that require marking. Also, this technique enables us to obtain a defined array that is a representation of all the points in the graph. If you compare these two images, you'll see that there is a significant difference between them. This picture and the one before it show a significant departure from one another. This is the difference between the image before the filter and the image after the filter: the amount of minutiae is less than it was before, all of the false minutiae has been deleted, and the picture is cleaner than it was before the filter.

4.1.7 Center point

After performing all of those things, we were able to find the minute details that we needed, and we have placed them all in the locations that we wanted them to be marked in.

Therefore, what we need to do is figure out the center of gravity or the center point for each group. For instance, we need to figure out the center point for all of the termination points, and we also need to know where the center point is for all of the bifurcation points.

As can be seen in Figure 15, the blue point belongs as the center point for all of the minutiae points that are classified as bifurcation points, and the pink point belongs as the center point for all of the minutiae points that are classified as termination points.

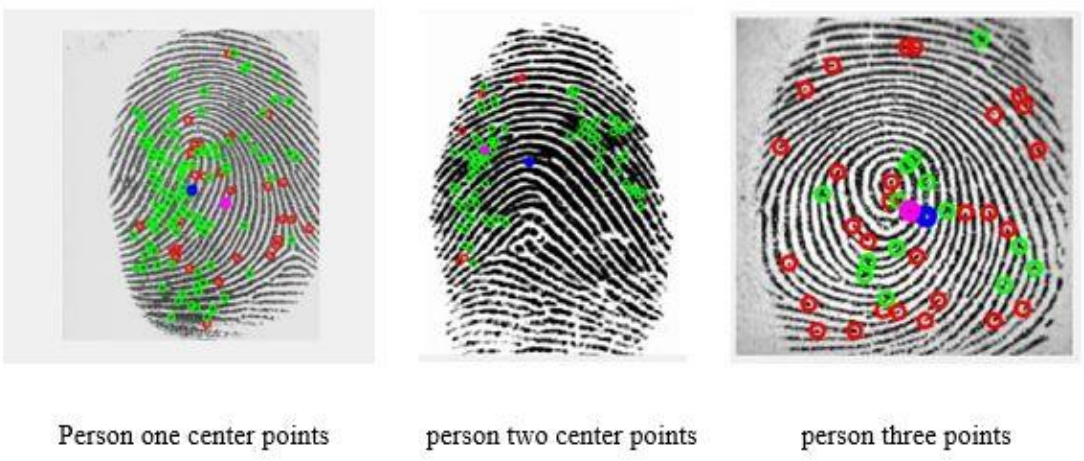


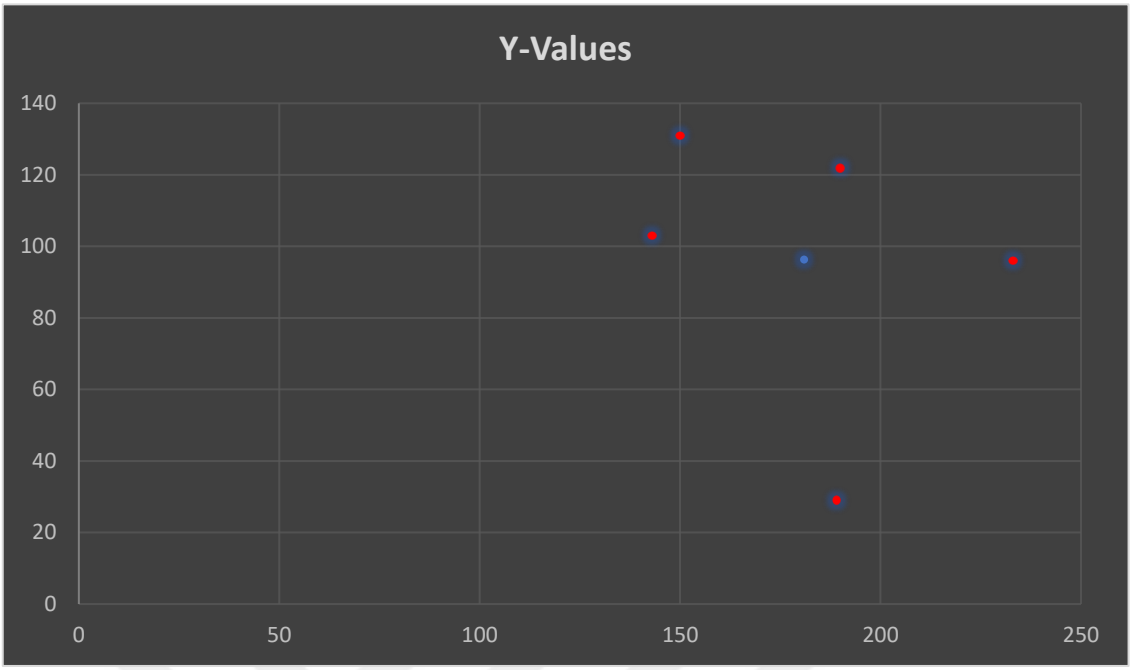
Figure 16 This picture is after extracting the center point of both sides

How can we compute or locate the points that are in the middle of each group?

We collected all of the points in each group, and then we divided the total by the number of points in that group. For example, if the termination points X = [189, 233, 143, 190, 150], and the termination points Y = [29, 96, 103, 122, 131], then X = [189 + 233 + 143 + 190 + 150] = [905/5] = [181]. This is because we added all the points.

Y = [29 + 96 + 103 + 122 + 131] = [481/5] = [96.2]

As a result, the center termination points are going to be X = [181] and Y = [96.2].



GRAPH 2

This graph is showing the center point

4.1.8 Sorted array result

We have to sort the array because we need to sort it, and we can either begin at the top and work our way down, or we can begin at the bottom and work our way up. The primary motivations for our sorting efforts are twofold. Because we indicated in Chapter [3] that the PINcode is considered to be the array of the fingerprint image, the system considers it based on the array, so I can only say that they are kind of indirect proportional. The Bio-Key will have a specified number that has a starting point and an ending point. This indicates that we need to construct the array in the form of a suitable list. I sincerely hope that both of these points are understood.

Table 5 Array of ridge endings and bifurcations of person one

TERM X	TERM Y		BIF X	BIF Y
189	29		194	28
233	96		210	42
143	103		207	46
190	122		127	52
150	131		242	55
157	131		161	70
146	141		241	80
181	162		257	82
151	164		128	89
161	166		158	93
250	173		86	94
233	177		227	95
191	182		127	98
249	214		90	99
260	214		123	102
134	216		93	108
89	221		90	112
279	225		120	116
244	237		130	118
242	243		207	123
131	247		101	126
126	250		92	127
236	255		188	127
130	256		98	130
198	257		173	133
145	269		130	135
178	284		161	135
164	331		218	136
			104	139
			154	139
			164	139
			114	140
			257	140
			176	144
			102	145
			264	145
			112	146
			233	146
			228	148
			121	152
			140	153
			149	153
			186	155
			137	157
			105	159
			186	160

Table 6 array of terminations and bifurcations of person two

BIF X	BIF Y		TERM X	TERM Y
27	255		17	239
29	219		19	265
31	258		20	204
35	223		22	210
39	172		25	303
41	206		29	283
43	217		29	321
45	175		33	167
46	210		34	304
47	221		34	328
48	187		35	155
49	237		35	347
52	184		36	336
51	265		37	362
53	189		36	386
55	243		39	143
58	289		40	152
58	270		40	345
59	341		40	358
59	187		41	371
60	175		41	384
61	253		44	393
62	345		44	405
63	206		45	339
64	235		47	368
64	292		48	133
65	180		48	154
66	193		49	403
67	257		51	121
68	311		51	140
71	190		51	309
70	178		51	379
70	227		54	148
71	157		54	343
73	199		54	366
72	238		55	413
72	321		56	136
77	173		57	304
74	184		58	107
75	162		62	386
77	115		65	95
78	88		65	395
79	122		65	420

Table 7 array of ridge endings and ridge bifurcations of person three

TERM X	TERM Y		BIF X	BIF Y
4	108		23	74
17	70		26	70
17	84		31	44
18	75		45	31
20	61		52	105
22	52		77	153
23	83		79	145
24	171		90	167
25	178		96	137
27	77		97	109
28	190		102	88
29	167		106	84
30	37		114	98
30	184		126	115
32	146		146	13
32	197		160	159
33	30		162	16
42	20		166	13
42	43		170	38
44	170		169	136
45	12		175	40
48	16		178	149
49	4		192	136
49	186			
54	14			
56	2			
58	29			
61	92			
70	124			
71	186			
79	133			
88	174			
92	109			
93	98			
97	175			
99	2			
102	18			
103	199			
107	18			
108	117			
108	142			
110	200			

The data presented in the aforementioned Excel sheet displays the array on both sides before sorting, and the array on the bottom table shows the array on both sides after it has been sorted.

Additionally, we added the numbers zero through nine on top in order to display the PIN code selection options.

Table 8 This table is showing the way was concateneted the array and PIN code digits

Pin code	0	1	2	3	4	5	6	7	8	9
Selected Terms	167	136	111	102	99	98	88	83	81	80
Selected Bif	1	6	11	12	17	20	23	24	24	24

As you can see in the sheet that is displayed above, the bifurcations are arranged in the opposite direction of the terminations, or from the bottom up, while the terminations are arranged in the order of increasing number size.

Every personal identification number, or PIN code, consists of a standard number that falls between 0 and 9. We need to create a selection by choosing the array of 10 digits, and then we need to place it on 0 to 9 so that the pin code and the array match. In order to do this, we need to make a selection.

Example:

Table 9 PIN code of person one

Pin code digit	0	1	2	3	4	5	6	7	8	9
Selected Terms	167	136	111	102	99	98	88	83	81	80
Selected Bif	1	6	11	12	17	20	23	24	24	24

Table 10 PIN code of person two

Pin code digit	0	1	2	3	4	5	6	7	8	9
Selected Terms	104	96	93	89	89	85	84	83	81	81
Selected Bif	10	10	13	14	23	24	24	25	25	25

Table 11 PIN code of person three

Pin code digit	0	1	2	3	4	5	6	7	8	9
Selected Terms	97	97	97	95	94	92	90	89	86	84
Selected Bif	13	19	20	26	33	35	44	50	54	58

This array from the fingerprint will be used by the system if your personal identification number (PIN) is 6937; nevertheless, the system will never know this PIN code and will not store it in the database.

As you see on the above three different tables are belongs into a three person that have the same PIN code but according to their fingerprint the system will consider selected termination and bifurcation points which is the value on the table and PIN code digits are user defined.

4.2 The Final Bio-Key

The final Bio-Key is nothing more than the combination of the two arrays that we used for earlier terminations and bifurcations. The essential thing to note about it is that it likewise includes between 32 and 127, and the reason why we picked it is because the keyboard of the ASCII table contains between those two values. The second significant fact that needs to be brought up is that the Bio-Key consists of only 16 digits. We chose to design it in this manner because we are using an AES algorithm, which operates on an algorithm of 4*4 blocks. As a result, the final Bio-Key consists of only 16 digits.

The generation of the final Bio-Key is one of the two sections of my program, and it is the most significant aspect of my software. The final Bio-Key, which is created from the fingerprint picture, is displayed in the excel sheet that can be found below.

Table 12 This table belongs to the final Bio-Keys

The Bio-key person one	39	39	40	40	41	41	43	43	43	44	44	46	46	46	47	32
The Bio-key person two	48	49	50	51	53	53	55	55	58	59	60	62	62	63	65	66
The Bio-key person three	33	35	44	50	54	58	62	63	71	110	97	97	97	95	94	92

As you on the above table these are the result of three different fingerprint that we were generated and took it from the key to secure the data every single fingerprint was generated from a specific Bio-Key thus we need only one Bio-Key to secure the data but the reason that we did those three different thumbs is to clarify the uniqueness of the key.

4.3 Using Advanced Standard Encryption With Final Bio-Key

It was vital to employ one key in this process since we are all aware that AES works best with just one key. Just like standard encryption procedures, we utilized an AES algorithm. used three different notepad files to encrypt and also decrypt; of those three files, two of them are empty while the third one is the PlainText; therefore, in the beginning, the system is reading the PlainText file as a binary file while it is taking the first 16 digits of the file and it is encrypting and decrypting, and then it goes back and takes the next 16 digits and doing that process until it carries all the digits inside file; this process is repeated If the balance or the most recent trip is less than 16 digits, the system will pick up the remaining digits and automatically add zeros until the length of the quorum will reach 16 digits. This process will continue until the quorum length reaches 16 digits.

4.3.1 PlainText

Within the confines of that procedure, the CipherText will be written to the first empty notepad file, and the PlainText or decrypted text will be written to the second empty file.

The picture that can be seen below displays the plaintext, as well as an inside view of the process of reading the file as a binary file.

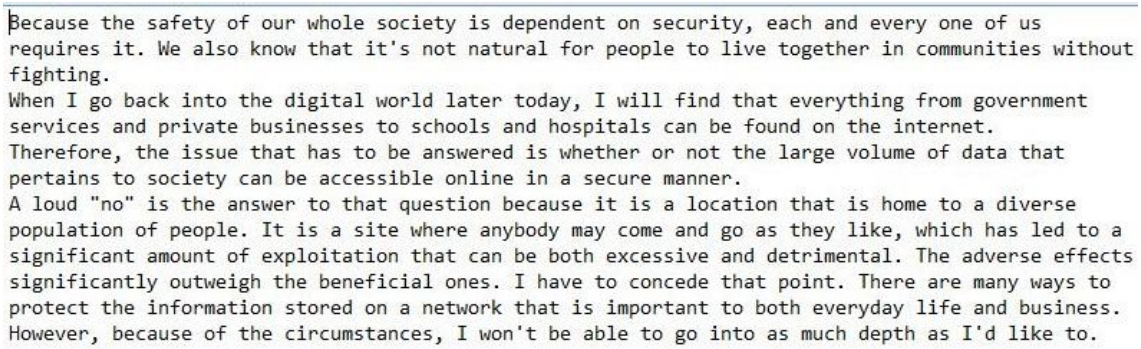

Because the safety of our whole society is dependent on security, each and every one of us requires it. We also know that it's not natural for people to live together in communities without fighting.
When I go back into the digital world later today, I will find that everything from government services and private businesses to schools and hospitals can be found on the internet.
Therefore, the issue that has to be answered is whether or not the large volume of data that pertains to society can be accessible online in a secure manner.
A loud "no" is the answer to that question because it is a location that is home to a diverse population of people. It is a site where anybody may come and go as they like, which has led to a significant amount of exploitation that can be both excessive and detrimental. The adverse effects significantly outweigh the beneficial ones. I have to concede that point. There are many ways to protect the information stored on a network that is important to both everyday life and business. However, because of the circumstances, I won't be able to go into as much depth as I'd like to.

Figure 17 This is the plaintext file that we are trying to encrypt

As I mentioned in the previous statement, This file is readed as 16 digits in every iteration, as indicated in figures 19 and 20, and since the iteration that has just been completed is the first one, the first 16 digits have been processed.

```
****AES Encryption****

Plaintext is:
    66   101    99    97   117   115   101    32   116   104   101    32   115    97   102   101

Key is:
3239394040414143

Ciphertext is:
'‡ Mªêóõ8CÉaå‡

****END OF ENCRYPTION****
```

Figure 18 This is first iteration of encryption process

```
****AES Decryption****

Ciphertext is:
'‡ Mªêóõ8CÉaå‡

Key is:
3239394040414143

Plaintext is
Because the safe

****END OF DECRYPTION****
```

Figure 19 This is first iteration of decryption process

Figure 21 represents encrypted data, also known as ciphertext, and Figure 22 represents text that has been decrypted; the system encrypts the whole file iteration after iteration. When the system has finished its job, it writes to the empty files. When you compare, there is absolutely no difference between the decrypted file and plaintext file. For example, look at Figure 18; it is the original plain text.

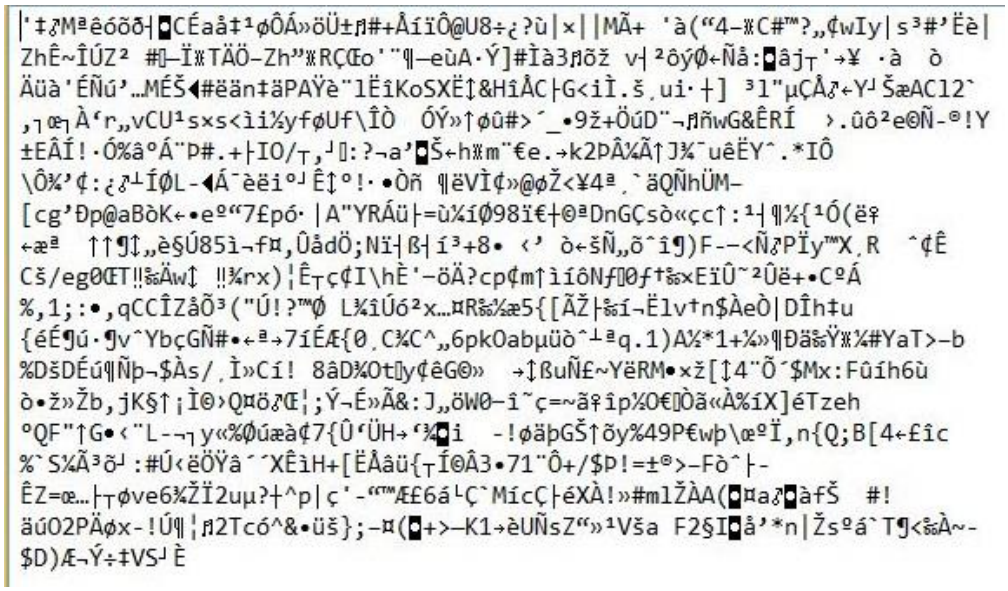


Figure 20 This the encrypted cipher text file result

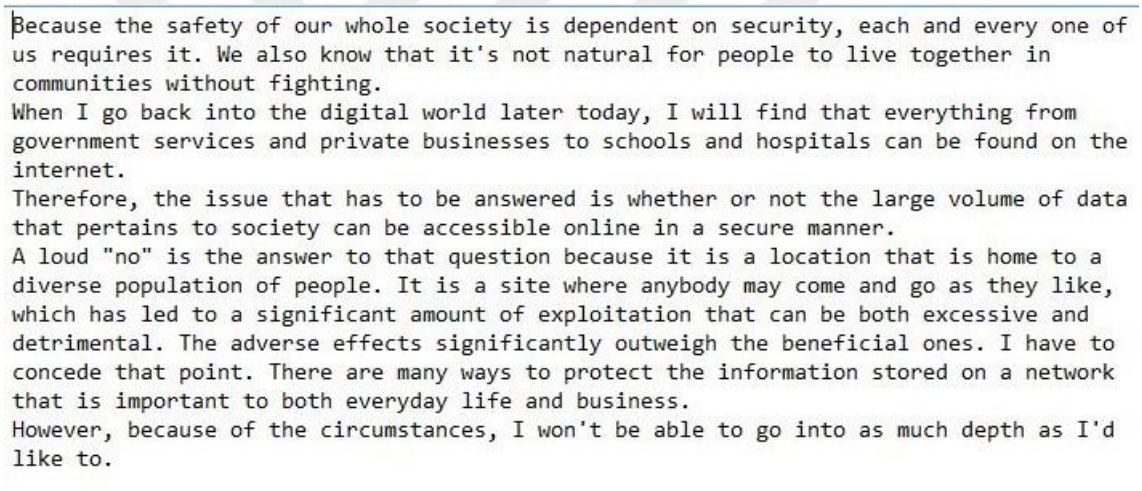


Figure 21 This is a decrypt text file result

According to what is stated in this thesis, my goal was to demonstrate the difficulty of removing a user's PIN code from the system and then demonstrate the solution to this problem, which is to divide the responsibility and ensure that the user is the only one who knows his PIN code. As a result of my research, I discovered that the solution to this problem is to use fingerprints because it is safe, and it is guaranteed also permanent.

5. Conclusion and Future Work

We started the process of processing a fingerprint image that I downloaded from the internet because I was thinking about making a secure key, and I realized that the most appropriate thing to do is the fingerprint of the person. Since I was thinking about making a secure key, I realized that the most suitable thing to do is the fingerprint of a person.

With a fingerprint, there is no greater expression of individuality than a unique collection of features. A person's fingerprints are used to identify and scale their fingerprints. When comparing fingerprints in a database, a new one is compared to previously processed ones.

After that we extracted minutiae points as you know Crossing numbers can be used to determine a fingerprint's minute points' locations and angles. The terminations that are located outside of the boundaries are separated using a Crossing Number. There are three types of termination points: regular ridges, bifurcations, and trifurcations.

In this case we used two of them regular ridges or terminations and bifurcations, after that, we determined the location of the center of gravity as well as the distance from the center of gravity to each point. After marked all of those points, we got an array with both sides in it. After that, the array has sorted because we need to sort it, and we may either start at the top to bottom or start at the bottom to top. Either way, we have sorted the array. The main purpose of sorting was because of the PIN code that consisting of zero to nine is considering with this array and also the Bio-Key contains the collection of these arrays as well the Bio-Key will have a specified number that has a starting point and an ending point. It consists of 16 digits in between anything from 32 to 127 numbers, we thought it would be best to build it in this fashion. The completed Bio-Key, which derived from the image of the fingerprints. Due to the fact that we are utilizing an AES technique, which is based on an algorithm consisting of 4 by 4 blocks, it only has 16 digits. In conclusion, the foundation of this program is made up of two separate works.

To begin, the system is put through its paces and instructed on all of the procedures included in the system, as detailed in chapter [3].

The second thing is execution, which may be thought of as simply recognizing all of the procedures that were learned it during its training period.

In the future, there is a lot of work that can be done on this project, but in my opinion, the first thing that should be noted is that this project is local, or to put it another way, private, and it focuses on how the user may protect his information from being viewed by unauthorised people. You have the option of making this project public, creating a project that protects the data of two persons or more than two people during the connection or streaming time or even inside the storing process, or creating a project that protects the user as well as the user's data that is stored on the server.

6. RESOURCES

Babich Aleksandra (2012) “Biometric Authentication. Types of biometric identifiers” Bachelor’s Thesis Degree Programme in Business Information Technology, HAAGA-HELIA University of Aplied Science

Sarraju Sridevi (2019), “fingerprint enhancement using fuzzy logic and deep neural networks,” department of computer science and engineering, Graduate School of Ulsan National Institute of Science and Technology.

E. Nurfadhilah *et al*., (2021), "Evaluating the BPPT Medical Speech Corpus for An ASR Medical Record Transcription System," *2021 9th International Conference on Information and Communication Technology (ICoICT)*, pp. 657-661

Hall Parantice (2005) Cryptography and Network Security Principles and Practices, Fourth Edition by William Stallings

Yijun Yang, Jianping Yu, Peng Zhang, and ShulanWang (2015), Hindawi Publishing Corporation Computational and Mathematical Methods in Medicine Volume, Article ID 673867, 10 pages

Sergei, Dotcenko, Andrei, Vladyko, Ivan, Letenko, (2014), “A fuzzy logic-based information security management for software-defined networks” PP 167 – 171, SN - 978-89-968650-3-2
Ambedkar B R, Gupta Ashwani, Gautam Pratiksha, Bedi S S, (2011), Department of CSIT, Department of CS SRMS CET, MJP Rohilkhand University Bareilly, India.

Joan Daemen, Vincent Rijmen, (1999), “The Rijndael Block Cipher” Katholieke Universiteit Leuven, ESAT-COSIC, K. Mercierlaan 94, B-3001 Heverlee, Belgium.

S. J. Aboud, M. A. AL-Fayoumi, M. Al-Fayoumi and H. S. Jabbar, (2008), "An Efficient RSA Public Key Encryption Scheme," *Fifth International Conference on Information Technology:* pp. 127-130.

Abdullah, Ako, (2017), “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data”, Department of Applied Mathematics & Computer Science
Eastern Mediterranean University - Cyprus

Hong, Lin, Wan, Yifei, Jain, Arjun, (1998), “ Fingerprint Image Enhancement: Algorithm and Performance Evaluation”, 777 - 789, VL - 20, DO - 10.1109/34.709565, JO - Pattern Analysis and Machine Intelligence, IEEE Transactions on.

Miron, Radu, Letia, Tiberiu, (2010), “Improved personal identification method based on partial fingerprints”, 24 – 29, VL - 12, JO - Control Engineering and Applied Informatics.

Shengbao Wang, (2017), “Practical Identity-Based Encryption (IBE) in Multiple PKG Environments and Its Applications”, Department of Computer Science and Engineering, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, China

Bauer F. L. (2000), "*Decrypted Secrets*, 2nd edition, Springer". ISBN 3-540-66871-3

Shi, Zhixin, Govindaraju, (Venu, 2006), "Fingerprint Image Enhancement Based on Skin Profile" PP 714 – 717 Approximation, VL - 3

Jinwei Gu, Jie Zhou, David Zhang, (2003). "a combination model for orientation field of fingerprint." Department of automation Tsinghua university Beijing, Biometric technology center Department of computing Hong Kong Polytechnic university Kowloon Hong Kong.

Kristensen, Terje, (2010), "Fingerprint Identification - A Support Vector Machine Approach", PP - 451 – 458, VL - 1

Alqadi, Ziad (2020), "Analysis of fingerprint minutiae to form fingerprint identifier" VL - 4, DO - 10.30630/joiv.4.1.332, JO - JOIV: International Journal on Informatics Visualization

Jea, Tsai-Yang, Govindaraju, Venu, (2005), "A minutia-based partial fingerprint recognition system" PP 1672 – 1684, VL – 38.

Divyarajsinh N. Parmar , Brijesh B. Mehta (2013), "Face Recognition Methods & Applications" 1 P.G. Student of Computer Engineering 2Asst.Prof. Dept.of Computer Engineering C.U. Shah College of Engg. & Tech Wadhwan city, India

Elvira Nurfadhilah, Asril Jarin, Lyla Ruslana Aini, Siska Pebiana, Agung Santosa, Muhammad Teduh Uliniansyah, Eduward Butarbutar, Desiani and Gunarso Conference: (2021) 9th International Conference on Information and Communication Technology (ICoICT), Year: 2021, Page 657

Roli Bansal , Priti Sehgal and Punam Bedi, (2011) "Minutiae Extraction from Fingerprint Images - a Review" Department of Computer Science, University of Delhi, New Delhi - 110001, India. Reader, Department of Computer Science, Keshav Mahavidyalaya, University of delhi, Pitampura , New Delhi - 110034, India. Associate Professor, Department of Computer Science, University of Delhi, New Delhi - 110001, India.

Al-Najjar, Yusra, Sheta, Alaa, (2008), "Minutiae extraction for fingerprint recognition" PP 1 – 5, SN - 978-1-4244-2205-0

Mann, V.A Diamond, R, Carey, S, (1979), "Development of voice recognition: Parallels with face recognition", PP 153 – 165, VOL – 27

McGehee, Frances, (1944), "An Experimental Study of Voice Recognition" PP 53 – 65, VOL -35

F. Goudail, E. Lange, T. Iwamoto, K. Kyuma and N. Otsu, (1996) "Face recognition system using local autocorrelations and multiscale integration," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 18, no. 10, pp. 1024-1028

W. E. Burr, (2003), "Selecting the Advanced Encryption Standard," in *IEEE Security & Privacy*, vol. 1, no. 2, pp. 43-52

A. H. Johnston and G. M. Weiss, (*2015),* "Smartwatch-based biometric gait recognition," *IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS),* 2015, pp. 1-6

Khan, Tariq M, Bailey, Donald G, Khan, Mohammad A. U, Kong, Yinan (2019), "Efficient hardware implementation strategy for local normalization of fingerprint images" Journal of Real-Time Image Processing, PP 1263 – 1275, VL – 16

B. Stojanović, O. Marques, A. Nešković and S. Puzović, (2019), "Fingerprint ROI segmentation based on deep learning," *2016 24th Telecommunications Forum (TELFOR),* pp. 1- 4

Dr. Neeraj Bhargava, Dr. Ritu Bhargava, Manish Mathuria, Pooja Dixit, (2013), "Fingerprint Minutiae Matching using Region of Interest" Department of Computer Science, School of Engineering & System Sciences, MDS University, Ajmer, Rajasthan, India, Department of MCA, Govt. Women Engineering College, Ajmer, Rajasthan, India, Department of CE & IT, Govt. Engineering College Ajmer Ajmer, Rajasthan, India, PP 1 – 3

Haralick, Robert M, (1983), "Ridges and valleys on digital images" PP 28 – 38, VOL – 22 Computer Vision, Graphics, and Image Processing, VL - 22, SN - 0734-189X

X. Bultel *et al.*, 2018,"Security analysis and psychological study of authentication methods with PIN codes," *2018 12th International Conference on Research Challenges in Information Science (RCIS),* pp. 1-11,

Tang, Jian, Terziyan, Vagan, Veijalainen, Jari, (2003), "Distributed PIN Verification Scheme for Improving Security of Mobile Devices" PP 159 – 175, VL – 8, JO - Mobile Networks and Applications

Lin Yen-Chun, (1993), "On balancing sorting on a linear array," in *IEEE Transactions on Parallel and Distributed Systems,* vol. 4, no. 5, pp. 566-571

Seung-Jo Han, Heang-Soo Oh and Jongan Park, (1996) "The improved data encryption standard (DES) algorithm," *Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications*, pp. 1310-1314 vol.3

R. Davis, (1978), "The data encryption standard in perspective," in *IEEE Communications Society Magazine,* vol. 16, no. 6, pp. 5-9

Md. Shamim Hossain Biswas , Dr. Md. Asraf Ali, Dr. Mostafijur Rahman, Mr. Md. Khaled Sohel, Mr. Md. Maruf Hasan, Kausik Sarkar, Abu Shamim Aminur razzaque, (2019). "A systematic study on classical cryptographic cypher in order to design a smallest cipher" Department of Software Engineering, Daffodil International University Bangladesh, PP 1 – 6

S. N. Gowda, (2016), "Innovative enhancement of the Caesar cipher algorithm for cryptography," *2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall)*, pp. 1-4

Maurer, Ueli M, Wolf, Stefan, (2000) "The Diffie–Hellman Protocol" PP 147 – 171, VL – 19, JO - Designs, Codes and Cryptography.

P.Arul , Dr.A.Shanmugam (2009), "GENERATE A KEY FOR AES USING BIOMETRIC FOR VOIP NETWORK SECURITY", PP 1 – 6, VL – 6.

Fakir Sharif Hossian , Ali Nawaz, Khan Md. Grihan, (2013) "Biometric Authentication Scheme for ATM Banking System Using Energy Efficient AES Processor", Department of Electrical and Electronic Engineering, International Islamic University Chittagong, Dhaka, Bangladesh, PP 1 – 7 VL – 7.

Disha Agarwal Amodini Vardhan and Pooja S (2017) "AES BASED SYMMETRIC-BIOMETRIC CRYPTO SYSTEM USING USER PASSWORD" Department of Information and Communication, Technology Manipal Institute of Technology, Manipal, Karnataka, India.

R. Matsumura, T. Sugawara and K. Sakiyama, (2018), "A Secure LiDAR with AES-Based Side-Channel Fingerprinting," *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)*, pp. 479-482

N. E. Costea and E. V. Moisi, (2019), "Fingerprint Authentication for Budget Application," *2019 15th International Conference on Engineering of Modern Electric Systems (EMES)*, 2019, pp. 105-108

R. Guest and O. Miguel-Hurtado, (2011) "Enhancing off-line biometric signature verification using a fingerprint assessment approach," *2011 Carnahan Conference on Security Technology*, pp. 1-4

F. Alonso-Fernandez, R. N. J. Veldhuis, A. M. Bazen, J. Fierrez-Aguilar and J. Ortega-Garcia, (2006), "Sensor Interoperability and Fusion in Fingerprint Verification: A Case Study using Minutiae-and Ridge-Based Matchers," *2006 9th International Conference on Control, Automation, Robotics and Vision*, pp. 1-6

H. Xu and R. N. J. Veldhuis, (2010), "Complex spectral minutiae representation for fingerprint recognition," *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition - Workshops*, pp. 1-8

S. S. S. Priya, P. Karthigaikumar and N. M. S. Mangai, (2014) "Mixed random 128 bit key using finger print features and binding key for AES algorithm," *2014 International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 1226-1230.

S. Cheepchol, W. San-Um, S. Kiattisin and A. Leelasantitham, (2014), "Digital biometric facial image encryption using chaotic cellular automata for secure image storages," *The*

4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE), pp. 1-5.

Jea, Tsai-Yang, Govindaraju, Venu (2005) "A minutia-based partial fingerprint recognition system" VL - 38, PP 1672 - 1684

Muthukumar Arunachalam, Kannan Subramanian,(2015) "AES Based Multimodal Biometric Authentication using Cryptographic Level Fusion with Fingerprint and Finger Knuckle Print" Vol. 12 PP 1-10

Journal of Physics: Conference Series, Volume 1916, 2021 International Conference on Computing, Communication, Electrical and Biomedical Systems (ICCCEBS) 2021 25-26 March 2021, Coimbatore, India.

Yousuf Janahi (2018) "Biometric Fingerprint Replaces PIN code on Point of Sale Machines in the Kingdom of Bahrain" International Business and Management Vol. 16, No. 2, pp. 48-51

Zhendong Wu, Zhengyin Lv, Jie Kang, Wenqian Ding, Jianwu Zhang, (2021) "Fingerprint bio-key generation based on a deep neural network" Volume37, PP 4329-4358

B. Chen and V. Chandran, (2007) "Biometric Based Cryptographic Key Generation from Faces," *9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications (DICTA 2007)*, pp. 394-401

L. Wu, X. Liu, S. Yuan and P. Xiao, (2010) "A novel key generation cryptosystem based on face features," *IEEE 10th INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING PROCEEDINGS*, pp. 1675-1678
Hua Yang, Zhendong Wu (2019)," A Biometric Key Generation Method for Fingerprint and Finger Vein Fusion" Cyberspace Safety and Security, 2019, Volume 11983, ISBN: 978-3-030-37351-1

M.Marimuthu, A.Kannammal (2015), "Dual Fingerprints Fusion for Cryptographic Key Generation" Assistant Professor Coimbatore Institute of Technology, Professor Coimbatore Institute of Technology, Volume 122

Panchal, Gaurang, Samanta, Debasis, (2018), "A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security" VL - 69, PP 461 – 478.