



M.KUMARASAMY
COLLEGE OF ENGINEERING
NAAC Accredited Autonomous Institution
Approved by AICTE & Affiliated to Anna University
ISO 9001:2015 & ISO 14001:2015 Certified Institution
Thalavapalayam, Karur – 639 113.



A Minor Project Report

on

FINGERPRINT BASED BANK TRANSACTION

Submitted in partial fulfilment of requirements for the award of

the degree of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

Under the guidance of

Mr. V.MANI, M.E., (Ph.D).,

Assistant Professor/CSE

Submitted By

M.MEGHA (19BCS4073)

A.MOUNIKA (19BCS4079)

M.ROSHNI (19BCS4103)

R.SUGANTHIKA (19BCS4116)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

M.KUMARASAMY COLLEGE OF ENGINEERING

(Autonomous)

KARUR – 639 113

May 2021



M. KUMARASAMY COLLEGE OF ENGINEERING
(Autonomous Institution affiliated to Anna University, Chennai)
KARUR – 639113

BONAFIDE CERTIFICATE

Certified that this minor project report “**FINGERPRINT BASED BANK TRANSACTION**” is the bonafide work of “**MEGHA M (19BCS4073), MOUNIKA A (19BCS4079), ROSHNI M (19BCS4103), SUGANTHIKA R (19BCS4116)**” who carried out the project work during the academic year 2020-2021 under my supervision.

Signature

Mr. V.MANI M.E., (Ph.D).,

SUPERVISOR,

Department of Computer Science
and Engineering,
M. Kumarasamy College of
Engineering,
Thalavapalayam, Karur -639113

Signature

Dr. S.THILAGAMANI M.E., Ph.D.,

HEAD OF THE DEPARTMENT,

Department of Computer Science
and Engineering,
M. Kumarasamy College of
Engineering,
Thalavapalayam, Karur -639113.






DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

VISION OF THE INSTITUTION

To emerge as a leader among the top institutions in the field of technical education




MISSION OF THE INSTITUTION

-  Produce smart technocrats with empirical knowledge who can surmount the global challenges
-  Create a diverse, fully-engaged, learner-centric campus environment to provide quality education to the students
-  Maintain mutually beneficial partnerships with our alumni, industry, and Professional associations

VISION OF THE DEPARTMENT

To achieve education and research excellence in Computer Science and Engineering

MISSION OF THE DEPARTMENT

-  To excel in academic through effective teaching learning techniques
-  To promote research in the area of computer science and engineering with the focus on innovation
-  To transform students into technically competent professionals with societal and ethical responsibilities

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

PEO 1: Graduates will have successful career in software industries and R&D divisions through continuous learning.

PEO 2: Graduates will provide effective solutions for real world problems in the key domain of computer science and engineering and engage in lifelong learning.

PEO 3: Graduates will excel in their profession by being ethically and socially responsible.



PROGRAM OUTCOMES (Pos)



Engineering students will be able to:

- 1. Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
- 2. Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
- 3. Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
- 4. Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
- 5. Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
- 6. The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.



- 7. Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
- 8. Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
- 9. Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
- 10. Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
- 11. Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
- 12. Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES (PSOs)

-  **PSO1: Professional Skills:** Ability to apply the knowledge of computing techniques to design and develop computerized solutions for the problems.
-  **PSO2: Successful career:** Ability to utilize the computing skills and ethical values in creating a successful career.



M.KUMARASAMY
COLLEGE OF ENGINEERING
NAAC Accredited Autonomous Institution
Approved by AICTE & Affiliated to Anna University
ISO 9001:2015 & ISO 14001:2015 Certified Institution
Thalavapalayam, Karur – 639 113.



ABSTRACT

In today's world data security is the major problem which is to be face. In order to secure data during communication, data storage and transmission we use Advance encryption standard(AES). AES is a symmetric block cipher intended to replace DES for commercial applications. The AES algorithms use to secure data from unauthorized user. The available AES algorithm is used for text data as well as for image data. In this project an image is given as input to AES encryption algorithm which gives encrypted output. This encrypted output is given as input to AES decryption algorithm and original image is regained as output. The AES algorithm for image encryption and decryption which synthesizes and simulated with the help of MATLAB. Hence the idea of cardless payment has arrived. This project focuses mainly on the security and ensures that no cyber attacks take place during the transactions. The security with the technique of cryptography. Cryptography is used to encrypt and decrypt the images of the user's fingerprint and ensures the secure storage of the image in the database.



ABSTRACT WITH PO AND PSO MAPPING

ABSTRACT	POs MAPPED	PSOs MAPPED
In today's world data security is the major problem which is to be face. In order to secure data during communication, data storage and transmission we use Advance encryption standard(AES). AES is a symmetric block cipher intended to replace DES for commercial applications. The AES algorithms use to secure data from unauthorized user. The available AES algorithm is used for text data as well as for image data. In this project an image is given as input to AES encryption algorithm which gives encrypted output. This encrypted output is given as input to AES decryption algorithm and original image is regained as output. The AES algorithm for image encryption and decryption which synthesizes and simulated with the help of MATLAB. Hence the idea of cardless payment has arrived. This project focuses mainly on the security and ensures that no cyber attacks take place during the transactions. The security with the technique of cryptography. Cryptography is used to encrypt and decrypt the images of the user's fingerprint and ensures the secure storage of the image in the database.	PO 1(3) PO 2(3) PO 3(3) PO 4(2) PO 5(3) PO 6(3) PO 7(2) PO 8(3) PO 9(3) PO 10(3) PO 11(2) PO 12(1)	PSO 1(3) PSO 2(3)

Note: 1- Low, 2-Medium, 3- High

SUPERVISOR

HEAD OF THE DEPARTMENT

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGENO.
	ABSTRACT	i
	ABSTRACT WITH PO PSO MAPPING	ii
	LIST OF ABBREVIATIONS	ix
1	INTRODUCTION	1
	1.1.Biometrics	2
2	LITERATURE SURVEY	3
3	EXISTING SYSTEM	6
	3.1.Description of the existing system	7
4	PROBLEM DESCRIPTION	8
5	PROPOSED SYSTEM	9
	5.1.Module description	10
	5.2.AES Algorithm	11
	5.3.AES Transformation	12
	5.3.1.Substitute bytes	13
	5.3.2.Shift Rows	13
	5.3.3.Mix Columns	13
	5.3.4.Add Round Key	14
6	RESULTS AND DISCUSSIONS	15
	6.1.Cryptography	16
7	CONCLUSION	17
	APPENDIX SOURCE CODE	18
	REFERENCES	23

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
DES	Data Encryption Standard
AES 128	Advanced Encryption Standard 128 bit key length
AES 192	Advanced Encryption Standard 192 bit key length
AES 256	Advanced Encryption Standard 256 bit key length

CHAPTER 1

INTRODUCTION

Security of image data has become increasingly important for many applications like video conferencing secure facsimile, medical, military applications etc. It is hard to prevent unauthorized people from eavesdropping in any communication system including internet. Cryptography provides a method for securing and authenticating the transmission of information over insecure channels. It enables us to store sensitive information or transmit it across insecure networks so that unauthorized persons cannot read it. Thus, image information transmission has increased rapidly and image encryption technology has drawn more attention. Images are generally the collection of pixels. Encryption (sometimes called as Encipherment) is the process of transforming a piece of information (known as the plaintext) using an algorithm (known as the cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The output is known as the cipher text. The reverse process of transforming cipher text to plaintext is known as decryption (sometimes called as decipherment). With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Transmission of sensitive data over the communication channel have emphasized the need for fast and secure digital communication networks to achieve the requirements for secrecy, integrity and nonreproduction of exchanged information.

1.1 BIOMETRICS

Fingerprints are the tiny ridges, whorls and valley patterns on the tip of each finger. They form from pressure on a baby's tiny, developing fingers in the womb. No two people have been found to have the same fingerprints -- they are totally unique. Fingerprints are even more unique than DNA, the genetic material in each of our cells. Although identical twins can share the same DNA -- or at least most of it -- they can't have the same fingerprints. Fingerprinting is one form of biometrics, a science that uses people's physical characteristics to identify them. Fingerprints are ideal for this purpose because they're inexpensive to collect and analyze, and they never change, even as people age. Although hands and feet have many ridged areas that could be used for identification, fingerprints became a popular form of biometrics because they are easy to classify and sort. They're also accessible. Fingerprints are made of an arrangement of ridges, called friction ridges. Each ridge contains pores, which are attached to sweat glands under the skin. You leave fingerprints on glasses, tables and just about anything else you touch because of this sweat. All of the ridges of fingerprints form patterns called Loops, whorls or arches:

Loops begin on one side of the finger, curve around or upward, and exit the other side.

There are two types of loops:

- Radial loops
- Ulnar loops

Whorls form a circular or spiral pattern. Arches slope upward and then down, like very narrow mountains.

CHAPTER 2

LITERATURE SURVEY

The word “biometrics” derived from the Greek words “bios” and “metric” which means life and measurement respectively.

1. To implement this concept, we have studied different investigated works and found following data. Most finger-scan technologies based on minutiae. The downside of pattern matching is that it is more sensitive to the placement of the finger during verification and the created template is several times larger. For fingerprint recognition, a system needs to capture fingerprint and then follow certain algorithm for fingerprint matching. This research paper discusses a minutiae detection algorithm to showed key parameters of fingerprint image for identification. The maturity of Biometric techniques and generally the dramatic improvement of the captured devices have led to the proposal of fingerprinting in multiple applications but in the last years, minutiae have been the main type of algorithm used. The minutiae are relatively stable and robust to contrast, image resolution and global distortion as compared to other fingerprint representation
2. Biometric data separated and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information. They cannot be stolen and used to access personal information to solving the bugs of traditional identification methods the author of designs a new ATM terminal customer recognition system is used for the core of microprocessor and an upgraded enhancement algorithm of fingerprint image intensify the security of bank account as well as ATM machine. For image enhancement, the Gabor filter algorithms and direction filter algorithms are used
3. Miao et al proposed the Gabor filters (GFs) play an important role in the extraction of Gabor features and the enhancement of various types of images. Fingerprint and voice systems have the smallest comparative sizes with eye systems currently the largest.

4. If images of fingerprint are shoddy images, they result in missing features, leading to the degrading performance of the fingerprint system. Hence, it is very important for a fingerprint recognition system to evaluate the quality and validity of the captured fingerprint images. If Authentication Failure then it send the alert message to the Account holder and Bank.
5. To have good process of operation for fingerprint matching, in depending on the spectral details features two feature reduction algorithms given the Column Principal Component Analysis and the Line Discrete Fourier Transform feature reductions. It can perfectly compress the template size with a reduction rate of 94%. Spectral minutiae fingerprint recognition system shows a matching speed with 125000 comparisons per second on a PC with Intel Pentium D processor 2.80GHz, 1GB of RAM. Biometric data are separate and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they not be stolen and used to access personal information.
6. Fingerprint records usually extend to impressions on the last joint of the fingers and thumb, to the extent that fingerprint cards typically record parts of the lower finger areas of the fingers .
7. Among those new technologies for dealing with payment processing, biometric payment technology has recently attracted more and more attention as a viable solution to decrease identity theft .
8. It may be historical, current or theoretical. The underlying principle of electronic money involves the use of computer networks such as the Internet and digital stored value systems. Examples of electronic money are bank deposits, electronic funds transfer, direct deposit, payment processors, and digital currencies. Electronic money can be understood as a way of storing and transmitting conventional money through electronic systems or as digital currency, which

varies in value and is tradable as a currency in its own right .

9. Electronic money transfer at an ATM is a cash equivalent device that is stored on an electronic or remote device in the security of the server and can be described on the one hand as policies, guidelines, processes and procedures necessary to enable electronic transactions to be performed with minimum risk of penetration or intrusion or theft. On the other hand, electronic security is any tool, method or process used to protect system information assets. Information is a valuable strategic asset that is managed and protected accordingly. This insurance is a risk management or risk mitigation tool, and appropriate safety measures mitigate the risk of underlying transaction.
10. It provides more security than normal security in the banking system. Biometrics holds the promise of fast, easy to-use, accurate, reliable, and less expensive authentication for a variety of application. Therefore, that bank introduce Automatic Teller Machine (ATM) instead of teller. This machine provides all facility like teller in transaction.

CHAPTER 3

EXISTING SYSTEM

In our modern world, all the people used to do truncation in banking like deposit money and withdrawing money. For that, the customers will be standing in queue to withdraw money from bank. All the customers felt like waiting for withdraw cash. Therefore, that bank introduces ATM (Automated teller machine) to help the customer to withdraw money quick. In that ATM system, they introduce CARDS (Credit, Debit, master, Visa) to the customer to withdraw cash by using them. Main advantage is quick cash providing by the ATM system. The customer feels happy and they will not waste time to withdraw cash by standing. but it has the disadvantage like, smart cards and physical keys, can be stolen, lost, replicated, or left behind; passwords can be shared, forgotten, hacked or accidentally observed by a third party. The banks required a better system to maintain security for the customer to do the transaction in their banks. To overcome these problems, the developed this fingerprint based ATM system. The existing system does not ensure that the fingerprint is secured or not. Intruder can scam the details. The AEPS(Aadhar enabled payment system) can also be easy to hack.

3.1 DESCRIPTION OF THE EXISTING SYSTEM

The existing system are the credit and debit cards where they are magnetic strips through which one pays amount for the goods purchased. These cards in spite of their benefits have a major drawback in which the data are being theft with the help of skimmers which are physical devices that captures data. Hence there was a wireless revolution which resulted in wireless cards formally known as wi - fi cards. These cards overcame the drawbacks of those cards by just tapping and not by swiping those cards. This ensures the safety and security of cards from intruders and from card skimmers. But these cards are accessible within a distance of 3m. In case of ATM machine, cameras are placed along with the pin which registers the pin and account number of every customer. In order to over-come the above threats this project is developed.

CHAPTER 4

PROBLEM DESCRIPTION

- 1) Card details may be stolen or card may be lost
- 2) Remembrance of passwords, or pins
- 3) Cyberattack during transmission
- 4) Spamming of cards

The above threats may occur at different situations mentioned below:

- 1) By breaching a company where one used his credit card or a company that handles some aspect of credit card processing.
- 2) Credit card skimmer is a small device that captures credit card information in another otherwise legitimate transaction. They are secretly placed over the swipe the gas stations and ATMs retrieve the information captured.
- 3) Hackers can design software that's downloaded in email attachments or other software and sits on computer, tablet, or smartphone undetected.
- 4) In one instance, hackers take advantage of public wireless - fidelity to trick people into installing malware disguised as a software update.
- 5) This software monitors keystrokes or takes screenshots of your page and sends the activity to the hacker.
- 6) Throwing away documents or receipts that have full credit card number printed puts at risk of theft.
- 7) Always shred these documents before tossing them in the trash.

Debit cards are linked to your checking account. When you use one, money immediately gets taken out of the linked account.

CHAPTER 5

PROPOSED SYSTEM

The proposed system is to increase the safe and security by introducing fingerprint system. The advantage of this technology is accuracy. By using this system many disadvantages are rapidly reduced. The system reduces the need to carry ATM card in wallet and chance of card loss or theft, password sharing is absent or, hacking many customers is avoidable because of quick and better service. Moreover, initially we store the fingerprint of customers with the bank which after verification given the time of authentication. If the fingerprints are matched then cashbox will open, otherwise buzzer will give alarm, in case of ATM machine. On the other hand, during purchases if it matches then further payment is proceeded, otherwise the user may not be able to bio – pay the goods they bought.

5.1 MODULE DESCRIPTION

Once the card is swiped, the details are sent to a indian merchantile account which encrypts the data. Once the data is verified it is sent to the processor and networks which in turn enables the transfer of money from the customer's account to the seller's account.

The proposed system has a user interface which has 2 modules

- 1) It allows user to register their fingerprint with their bank account.
- 2) It allows the encryption of the image of the fingerprint being stored in the bank database
- 3) In such case the bank database also has its own decryption algorithm which allows safe and secure storage of data in the database.

The details include user's name, date of birth and other personal details for reference along with bank account details

Once the user registers the details he/she is free to pay the amount without using any cash or credit or debit cards. They need not be worried about the pin or passwords.

5.2 AES ALGORITHM

AES Encryption and Decryption

For each round of AES, 128 bit input data and 128 bit key is required i.e., it needs 4 words of key in one round thus the input key must be expanded to the required number of words depending upon the number of rounds. The output of each round serves as input to the next stage. In AES system, same secret key is used for both encryption and decryption, thus simplifies the design. For both its cipher and inverse cipher, the AES algorithm uses a round function i.e. composed from four different byte-oriented transformations:

- Substitute Bytes
- Shift rows
- Mix columns
- Add round key

The above four transformations are looped N_r-1 times. In the last round Mix column is not performed.

The nine rounds of the decryption algorithm are governed by the following four stages:

- Inverse Shift rows
- Inverse Substitute Bytes
- Add round key
- Inverse Mix columns

5.3 AES Transformation

5.3.1 Substitute Bytes

It is a nonlinear byte substitution, using a substitution table (S-box) each byte from the input state is replaced by another byte. The substitution is invertible and is constructed by the composition of two transformations as described below.

Inverse Substitute Bytes:

It is the reverse operation of the Substitute Bytes transformation, in which the inverse S-box is applied to each byte of the state. This is obtained by applying the inverse of the affine transformation followed by taking the multiplicative inverse in GF (28).

5.3.2 Shift rows

Shift rows operate on individual rows of the state. It provides diffusion throughout the AES algorithm. In the Shift Rows transformation, the first row of the state array remains unchanged. The bytes in the second, third and fourth rows are cyclically shifted by one, two and three bytes to the left, respectively.

Inverse Shift rows:

It is the inverse of the shift rows; the first row of the state array remains unchanged. The bytes in the second, third and fourth rows are cyclically shifted by one, two and three bytes to the right, respectively.

5.3.3 Mix columns

In the Mix Columns transformation, every column of the state array is considered as polynomial over GF (28). Inverse Mix columns: In the Inverse Mix Columns transformation, every column of the state array is considered a polynomial over GF (28). After multiplying modulo x^4+1 with a fixed polynomial $b(x)$, $b(x) = 0B \cdot x^3 + 0D \cdot x^2 + 09 \cdot x + 0E$ The result is the corresponding column of the output

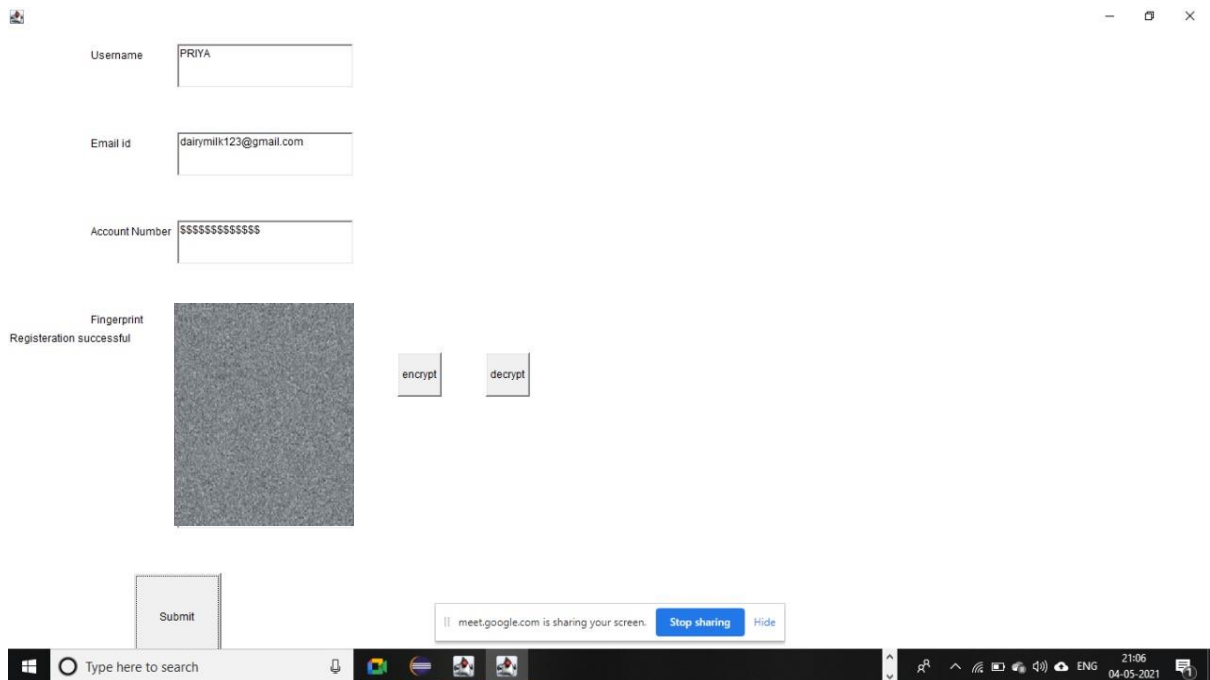
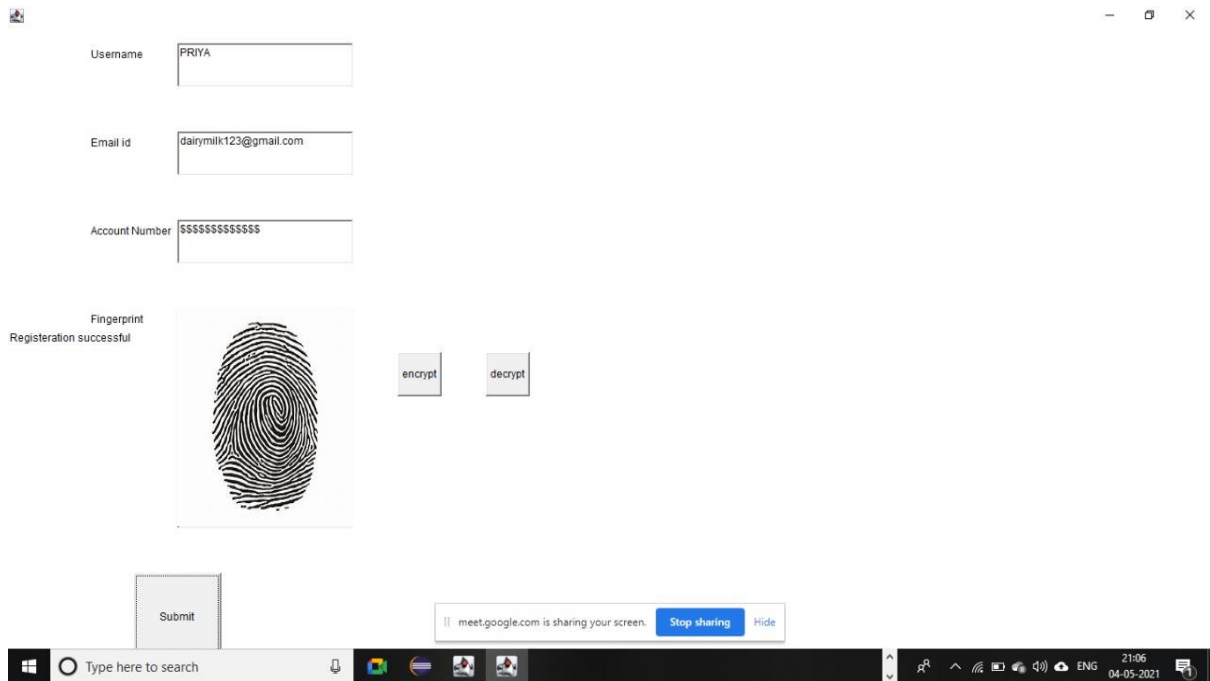
state. As it is not so straightforward hardware implementation as Mix column, so if we compare both, Inv Mix Col requires more logic resources for implementation.

5.3.4 Add round key

The Add Round Key operation is as shown in Figure, which is a simple XOR operation between the State and the Round Key. The Round Key is derived from the Cipher key by means of key schedule process. The State and Round Key are of the same size and to obtain the next State an XOR operation is done per element: $b(i, j) = a(i, j) \oplus k(i, j)$ Where a is the current State, b the next State and k is the round key.

CHAPTER 6

RESULTS AND DISCUSSIONS



6.1 CRYPTOGRAPHY

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables us to store sensitive information or transmit across insecure networks, so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis invokes an interesting combination of analytical reasoning, application of mathematical tools, determination and luck. Cryptanalysis also called as attackers. Cryptology embraces both cryptography and cryptanalysis. Cryptography can be strong or weak, its strength is measured in the time and resources, and it would require recovering the plaintext.

The result of strong cryptography is cipher text that is very difficult to decipher without possession of the appropriate decoding tool. A cryptographic algorithm is a mathematical function used in the encryption and decryption process. It works in the combination with a key-a word, number, or face- to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is thus entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. Cryptography includes the following process such as Encryption and Decryption. Encryption: It is the process of converting plaintext into unreadable form called cipher text. Decryption: It is the process of converting cipher text into readable form called plain text.

CHAPTER 7

CONCLUSION AND FUTURE

Hence the security has been enhanced by the use of cryptographic techniques. The proposed work makes use of AES algorithm to encrypt and decrypt the image and text. The use of steganography has ensured security. The implementation of ATM security by using fingerprint also contains the Original verifying methods, which were inputting customer fingerprint, which is send by the controller and verified properly. The security Features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the fingerprint technology, which makes the system safer, reliable and easy to use. This will be most promising technology at electronic money transaction.

APPENDIX

Source code:

Registration page:

```
import java.awt.*;
import java.awt.event.*;
import java.awt.event.ActionListener;
public class Registrationpage implements ActionListener
{
    Frame f=new Frame();
    Label l1,l2,l3,l4,l5;
    TextField t1,t2,t3,t4;
    Button b1,b2,b3;
    public Registrationpage()
    {
        l1=new Label("Username");
        l2=new Label("Email id");
        l3=new Label("Account Number");
        l4=new Label("Fingerprint");
        l5=new Label();
        t1=new TextField();
        t2=new TextField();
        t3=new TextField();
        t4=new TextField();
        t3.setEchoChar('$');
        b1=new Button("Submit");
        f.add(b1);
        f.add(b2);
        f.add(b3);
```

```
f.add(t1);
f.add(t2);
f.add(t3);
f.add(t4);
f.add(l1);
f.add(l2);
f.add(l3);
f.add(l4);
f.add(l5);
f.setSize(700,700);
f.setVisible(true);
l1.setBounds(100,50,200,25);
l2.setBounds(100,150,200,25);
l3.setBounds(100,250,200,25);
l4.setBounds(100,350,200,25);
l5.setBounds(350,500,100,50);
t1.setBounds(200,50,200,50);
t2.setBounds(200,150,200,50);
t3.setBounds(200,250,200,50);
t4.setBounds(200,350,200,50);
b1.setBounds(150,650,100,100);
b2.setBounds(450,400,50,50);
b3.setBounds(550,400,50,50);
b1.addActionListener((ActionListener) this);
b2.addActionListener((ActionListener) this);
b3.addActionListener((ActionListener) this);
}
public void actionPerformed(ActionEvent a)
{
```

```

if(a.getSource()==b1)
{
l5.setText("Registration successful");
}
else if(a.getSource()==b2)
{
new Encryption();
}
else if(a.getSource()==b3)
{
new Decryption();
}
}
public static void main(String[] args)
{
new Registrationpage();
}
}

```

Encryption:

```

import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;
import java.util.Scanner;
public class Encryption
{
public static void main(String[] args) throws FileNotFoundException,

```

IOException

```
{
Scanner sc = new Scanner(System.in);
System.out.println("Note : Encryption Key act as Password to
Decrypt the same Image,otherwise it will corrupt the Image.");
// Here key is act as password to Encrypt and
// Decrypt the Image
System.out.print("Enter key for Encryption : ");
int key = sc.nextInt();
// Selecting an Image for operation
FileInputStream fis = new FileInputStream(
"C:\\Users\\lenovo\\Pictures\\logo4.png");
// Converting Image into byte array, create a
// array of same size as Image size
byte data[] = new byte[fis.available()];
// Read the array
fis.read(data);
int i = 0;
// Performing an XOR operation on each value of
// byte array due to which every value of Image
// will change.
for (byte b : data)
{
data[i] = (byte)(b ^ key);
i++;
}
// Opening a file for writing purpose
FileOutputStream fos = new FileOutputStream(
"C:\\Users\\lenovo\\Pictures\\logo4.png");
```

```

// Writing new byte array value to image which
// will Encrypt it.
fos.write(data);
// Closing file
fos.close();
fis.close();
System.out.println("Encryption Done...");
}
}

```

Decryption:

```

import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;
import java.util.Scanner;
public class Decryption
{
    public static void main(String[] args) throws FileNotFoundException,
    IOException
    {
        Scanner sc = new Scanner(System.in);
        System.out.println(
        "Note : Encryption Key act as Password to Decrypt the same Image,
        otherwise it will corrupt the Image.");
        System.out.print("Enter a key for Decryption : ");
        int key = sc.nextInt();
        // Selecting an Image for Decryption.
        FileInputStream fis = new FileInputStream(

```

```

"C:\\Users\\lenovo\\Pictures\\logo4.png");
// Converting image into byte array,it will
// Create an array of same size as image.
byte data[] = new byte[fis.available()];
// Read the array
fis.read(data);
int i = 0;
// Performing an XOR operation
// on each value of
// byte array to Decrypt it.
for (byte b : data) {
    data[i] = (byte)(b ^ key);
    i++;
}
// Opening file for writting purpose
FileOutputStream fos = new FileOutputStream(
"C:\\Users\\lenovo\\Pictures\\logo4.png");
// Writting Decrypted data on Image
fos.write(data);
fos.close();
fis.close();
System.out.println("Decryption Done...");
}
}

```

REFERENCES

- 1) William Stallings, —Cryptography and network Security: principles and practice.
- 2) Roshni Padate, Aamna Patel, —Image Encryption and Decryption Using AES Algorithm.
- 3) Priya Deshmukh, —An Image Encryption and Decryption Using AES algorithm.
- 4) Lin Hong, Wan Yifei, Anil Jain. Fingerprint image enhancement: algorithm and performance evaluation.