IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-5, Issue-5 E-ISSN: 2347-2693

Image Encryption and Decryption System Using AES for Secure Transmission

P. Thakkar[1*], H.K. Mishra[2], Z. Shaikh[3], D. Sharma[4]

[1]Department of Computer Engineering, K J Somaiya College of Engineering, Mumbai, India
[2]Department of Computer Engineering, K J Somaiya College of Engineering, Mumbai, India
[3]Department of Computer Engineering, K J Somaiya College of Engineering, Mumbai, India
[4]Department of Computer Engineering, K J Somaiya College of Engineering, Mumbai, India

Corresponding Author: pranay.thakkar@somaiya.edu

Online Available at www.ijcseonline.org

Received: 19/Apr/2017, Revised: 25/Apr/2017, Accepted: 24/May/2017, Published: 30/May/2017

***Abstract*—** Internet is the greatest blessing for all the people over the world. Large amount of data is constantly transmitted over the internet. Data means any image, videos, audio etc. Also, confidential information from Banking, Military, Government etc are transmitted over the internet, but the security of these information is not always looked upon. Privacy & Security of information is very important in data storage and transmission. So as to secure the information, various data hiding techniques & encryption of images is done. Image Encryption can be done using various symmetric and asymmetric key algorithms. But, it is found that symmetric key algorithm is much faster and easier to implement and required less processing power as compare to asymmetric key algorithm. Therefore, we use AES Algorithm for the encryption of images. Here, the proposed system mainly deals with the encryption of image using AES algorithm to secure our data during transmission. Different image file formats are given as the input to the AES Algorithm in our system.

***Keywords*—** Encryption, Decryption, Image Processing, AES

I. INTRODUCTION

Nowadays, use of various devices such as mobile phones & computers have increased rapidly. People use internet on a daily basis for transmitting images from one person to another person. While transmission of images, security is one of the issues that is often overlooked. There is always a risk of confidential information being leaked & accessed by unauthorized user during transmission. Thus, to enable sending images secretly in any application a method needs to be developed. There should be reliable security in transmission of digital images.

Data need to be stored & transmitted in encrypted format to solve the problem of unauthorized access. Cryptography is the science of writing messages in secret codes. The components of cryptography are plain image, cipher image, encryption, decryption. Let us understand these components. Plain image is the original image ,that is to be sent. Encryption is the process of converting plain image into cipher image. Cipher image is the encrypted image, image obtained after encryption. Decryption is the process of converting cipher image into plain image.

Existing Systems for encryption of images are encryption using DES, 3DES algorithms etc. DES was the first algorithm developed for the encryption of images & text. DES is the Symmetric Key Algorithm developed in early 1970s at IBM. DES is the Symmetric block cipher, with the key length of 56 bits & block size of 64 bits[1]. And it was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977. But DES had a small key size & hence it was officially withdrawn later. In 1999, Electronic Frontier Foundation and distributed.net put a series of challenges on DES algorithm to see how long it takes to decrypt a message & were able to break the DES key in 22hours & 15minutes. Therefore, DES proved to be insecure. 3DES was used later on, & avoids the problem of small key size. 3DES, a way of using DES encryption 3 times, it offers key size options of 168,112 or 56 bits & block size of 64 bits. But, 3DES also proved ineffective against Brute Force Attacks, in addition to that it slowed down the process substantially.

AES known by its original name as Rijndael, was developed to replace 3 DES. AES was designed by Vincent Rijmen & Joan Daemen, & was first published in 1998. AES was announced as a Federal Information Processing Standard (FIPS) by the National Institute of Standards and Technology (NIST) for the United States in 2001. AES is the Symmetric Key Algorithm with the block size of 128 bits & key size options of 128, 192 or 256 bits [1,2,3,4,5,6].

Drawbacks of existing system :

- DES has small key size of 56 bits.
- DES is better in hardware implementation and relatively slow when implemented in software.
- 3DES, has different key size options, but it is very slow in hardware implementation.
- DES & 3DES, both are not much secure, and proved inadequate against Brute Force Attacks.

Advantages of AES :

- AES was developed to replace DES & 3DES, hence has more block size of 128bits.
- AES offers key size options of 128,192 or 256bits.
- AES is faster in both software & hardware implementation.
- AES is better over 3DES such as high computational efficiency and cryptanalysis resistance is strong against differential truncated , linear, interpolation and square attacks[1,2,3,4,5,6,7,8,9,10].

AES proved to be better in all cases than DES & 3DES. Hence, we use AES algorithm for the encryption & decryption of images in the proposed system. Thus, the main purpose of the proposed system is to provide an Image Encryption & Decryption system which provides high security level, and is more efficient. And it is achieved by using AES algorithm.

The paper contains different sections as follows: Section I contains the introduction, Section II describes the proposed system along with the system architecture. Section III contains the methodology used to develop the system, Section IV contains the prototype of the proposed system. Section V describes the Conclusion & the Future Scope.

II. PROPOSED SYSTEM

Figure 1 represents the system architecture. The user first has to register into the system. Enter the required details & details of the user are stored in the database. User can now login into the application. Application verifies the details of the user , and only authorized users are allowed to access into the system. If the user wish to send an image, he/she has to go into the encrypt window & then select that required image.

Application allows the user to browse the drive & select that particular image. After the image is selected, user enters a password, then the user can select the encrypt option. Application reads the image selected by the user, performs pre-processing operation on the image. Later on, AES, encryption algorithm is applied on the image to get the encrypted image as the output. User can find the encrypted image in the F drive of the computer. User can sent these encrypted image to any intended receipent via email.

On the receiver side too, the user needs to register & login into the system. After login into the system, he/she has to go into the decrypt window & then select the received encrypted image. Receiver has to enter the same password, as entered by the sender, or else we can’t decrypt the image. After entering the password & selecting the encrypted image, select the decrypt option. AES, decryption algorithm is applied on the encrypted image to get the original image back as the output. User can find the decrypted image in the F drive of the computer.

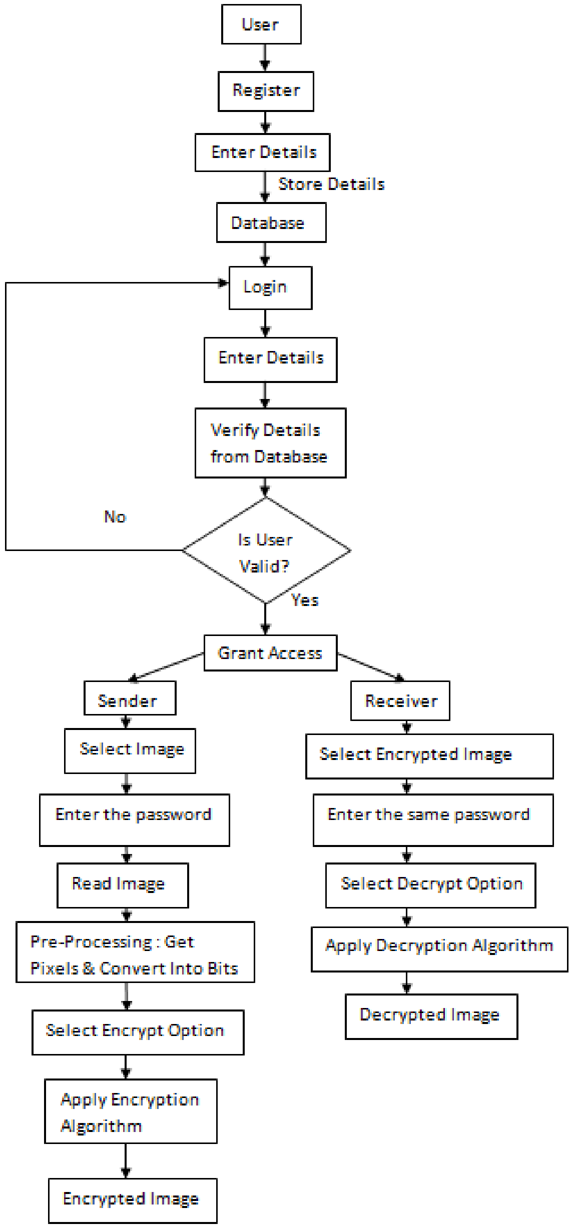


Figure 1: System Architecture

III. Methodology

Image Encryption & Decryption System is a Desktop Application. It is implemented using Visual Studio & SQL Server Management Studio. AES Algorithm is used for the Encryption & Decryption of images[2,6,7,9].

Conversion of original image i.e plain image into encrypted image i.e cipher image is known as image encryption. And conversion of encrypted image i.e cipher image into the decrypted image i.e original image is known as image decryption. For AES algorithm based on the key size length, the number of execution rounds changes. The proposed system consists of block size of 128 bits & key size of 256 bits[2] . As the size of the key increases , the level of the security also increases. It will take 14 rounds, as the key size is of 256 bits. Image Encryption & Decryption, both is carried out using the AES Algorithm.

In image encryption, the round consists of the following stages as below :

- SubstituteBytes
- ShiftRow
- MixColumns
- AddRoundKey

SubstituteBytes:

In these, each of the state bytes are operated independently, it includes non-linear byte substitution. S-box, the substitution table is used to perform these, it contains of 256 numbers (0 to 255) and their corresponding values.

ShiftRow:

ShiftRows transformation involves transforming the rows of the state cyclically left. Here, the Row 0 remain unchanged, Row 1 is shifted 1byte to the left, Row 2 is shifted 2bytes to the left & so on.

MixColumns:

In MixColumns, the columns of the state are referred to as polynomials over GF (28) and multiplied by modulo x4+1 with a fixed polynomial c(x), given by:

c(x)={03}x3+{01}x2+{01}x+{02}.

AddRoundKey:

Here, in the AddRoundKey transformation, a Round Key is added to the state resulted from the MixColumns Transformation, using bitwise XOR operation.

For each round we obtain the RoundKey from the MainKey. Fourteen 256-bit RoundKey are required for encryption & decryption algorithm.

In image decryption, the round consists of the following stages as below:

- AddRoundKey
- InverseShiftRow
- InverseSubstituteByte
- InverseMixColumns

AddRoundKey:

In this step, the round keys are needed to be selected in reverse order. As XOR function is its own inverse, therefore AddRoundKey is its own inverse function.

InverseShiftRow:

This step is same as ShiftRow transformation,but in opposite direction. Here, the Row 0 is not shifted, Row 1 is shifted 1byte to the right, Row 2 is shifted 2bytes to the left & so on.

InverseSubstituteByte:

InvS-box, the substitution table is used to perform these transformation, it contains of 256 numbers (0 to 255) and their corresponding values.

InverseMixColumns:

In the InvMixColumns transformation, the polynomials of degree less than 4 over GF(28), which coefficients are the elements in the columns of the state, are multiplied modulo (x4+1) by a fixed polynomial d(x)={0B}x3 + {0D}x2 + {09}x + {0E}, where {0B}, {0D}, {09}, {0E} denote hexadecimal values.

AES is a more mathematically efficient, elegant cryptographic algorithm and its main strength lies in the key options offered.

IV. Prototype

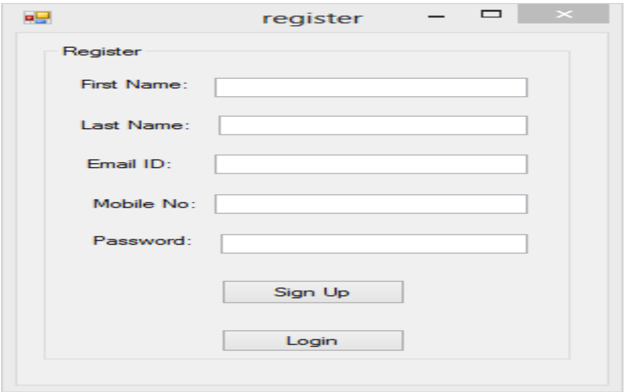


Figure 2: Registration Page

Figure 2 represents the registration page for a new user. They have to enter their details such as first name, last name, email_id, mobile_no and password. These details will be stored in the database.

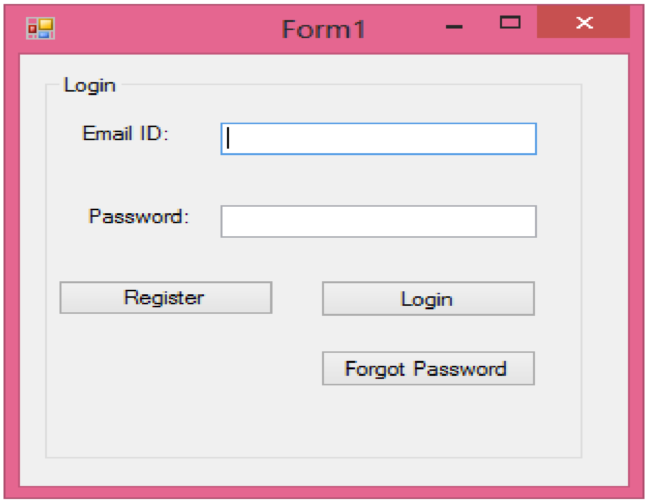


Figure 3: Login Page

Figure 3 represents the login page. The user has to enter the email_id & password as entered in the registration form. The system validates and verifies whether the user has entered the correct details or not & grants the access, else the error message will get displayed.

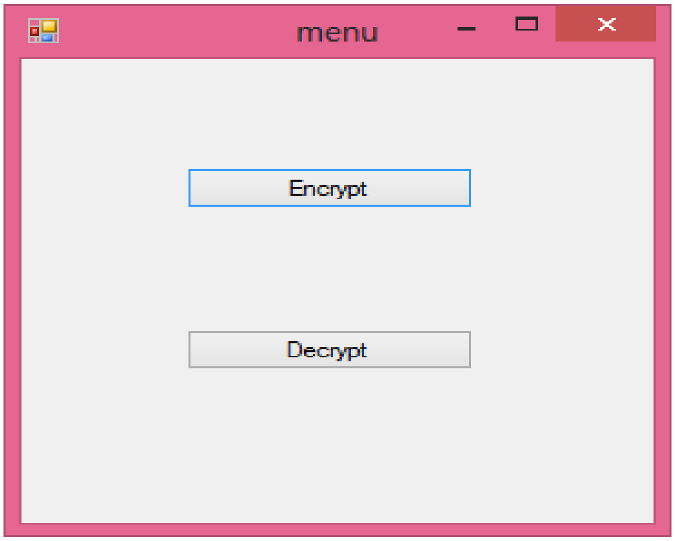


Figure 4: Application UI main window

Figure 4 represents the next page after the register & login. If the user is sender, he/she selects the encrypt option. And if the user is a receiver, he/she selects the decrypt option.

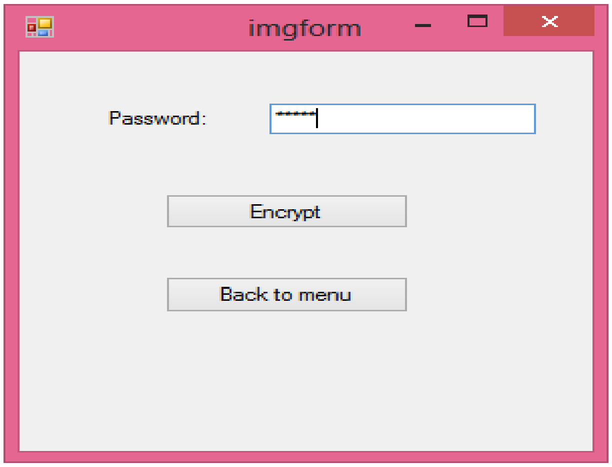


Figure 5: Encryption UI Window

Figure 5 represents the window after selecting the encrypt option. User browses for the required image he/she wishes to encrypt, enters the password & click on the encrypt button to get the encrypted image.

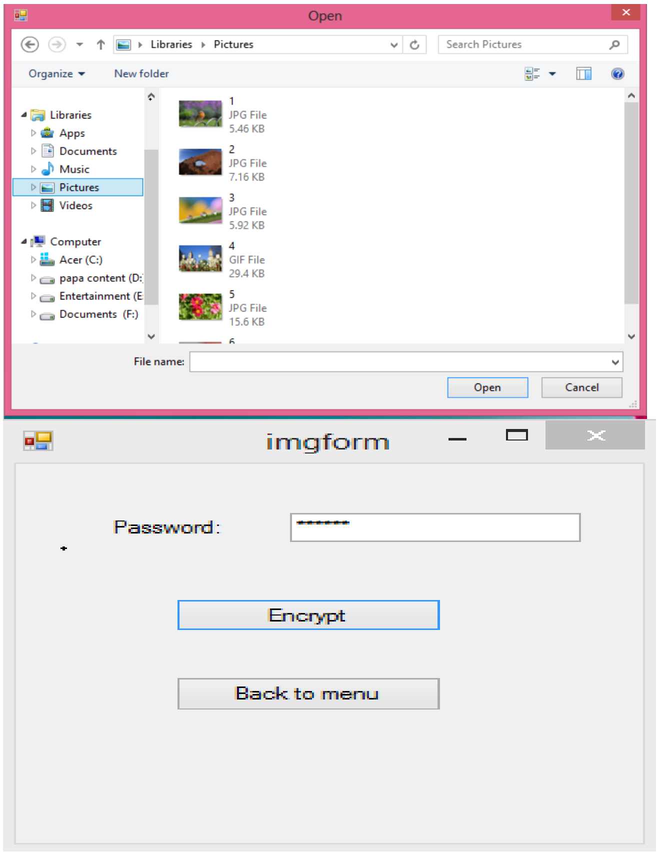


Figure 6: Window after browsing images and entering the password

Figure 6 represents the window that appears on browsing images & selecting the required image. Select the image & enter the password.

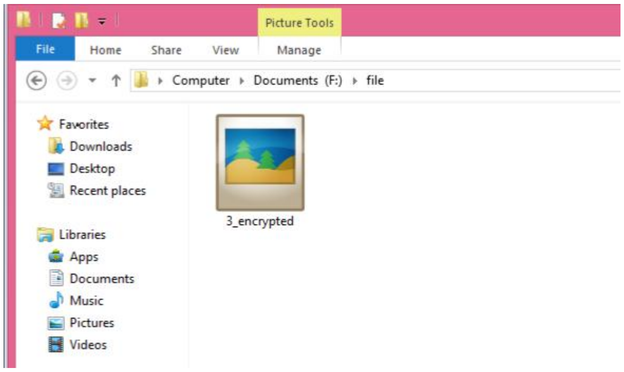
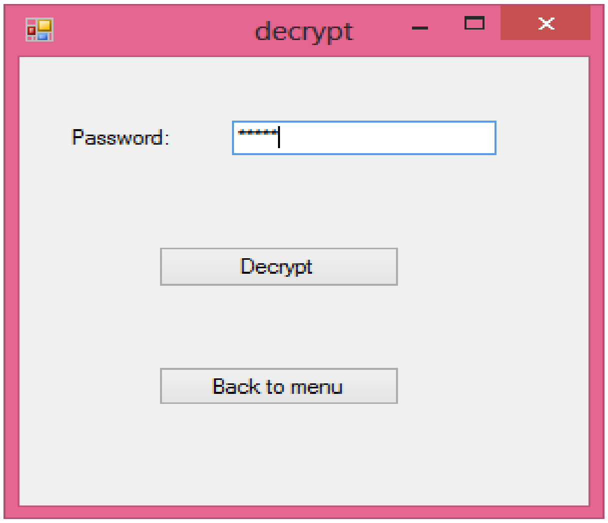


Figure 7: Window showing the Encrypted Image

Figure 7 represents the window that shows the image after encryption is performed. Encrypted Image is obtained in the drive of the computer.



Password: *****

Figure 8: Decryption UI Window

Figure 8 represents the window after selecting the decrypt option. User, that is, receiver browses for the encrypted image to perform decryption, enters the same password as sender & click on the decrypt button to get the decrypted image.

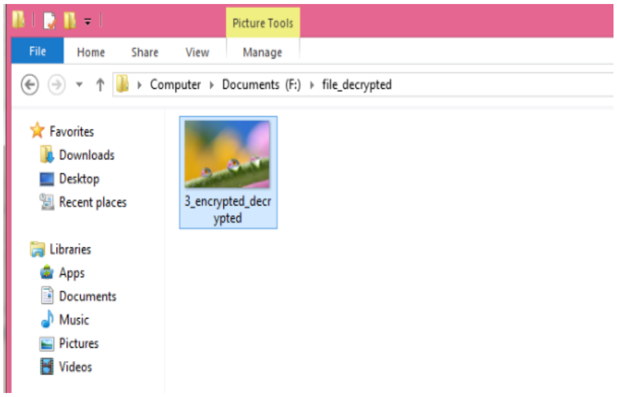


Figure 9: Window showing the Decrypted Image

Figure 9 represents the window that shows the image after decryption is performed. After decryption, we get the original image back.

V. CONCLUSION and Future Scope

Thus, our proposed system is implemented using AES Algorithm, block size of 128 bits & key size of 256 bits is used for the image encryption & decryption. More the key size, the system is more secured & can't be easily broken. 256 bit key size helps us to achieve high security. As a result, secure transmission of images is possible. In Future, the system can be integrated with the web application & can be developed using AES Algorithm & Visual cryptography.

REFERENCES

[1] S. Mewada, P. Sharma, S. S. Gautam, "*Exploration of efficient symmetric algorithms*", 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, pp.663-666, 2016.

[2] V. Kapoor, "*Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and 'n'prime Number*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.35-38, 2013.

[3] A. Sharma, RS Thakur, S. Jaloree, "*Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.5, pp.5-11, 2016.

[4] V. Kapoor, "*A New Cryptography Algorithm with an Integrated Scheme to Improve Data Security*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.39-46, 2013.

[5] A. Sharma, RS Thakur, S. Jaloree, "*Investigation of Efficient Cryptic Algorithm for Storing Video Files in Cloud*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.6, pp.8-14, 2016.

[6] L.R. Mathew , "*A Survey on Different Cryptographic Techniques*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.2, pp.27-29, 2017.

[7] R. Arya, "*Data Encryption Approach For Security*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.5, pp.176-179, 2014.

[8] Ajay Hirne, Shital Namdev, H.S. Tomar, "*Secure Data Distribution in Cloud Environment Using Key Aggregation Cryptic*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.2, pp.15-19, 2016.

[9] SO. OKOLIE, BT. ADETOBA, "*Comparative Analysis of Performance Characteristics of well-known Symmetric Key Encryption Algorithms*", International Journal of Scientific Research in Network Security and Communication, Vol.4, Issue.3, pp.1-6, 2016.

[10] Sachin sharma, Jeevan Singh Bisht, "*Performance Analysis of Data Encryption Algorithms*", International Journal of Scientific Research in Network Security and Communication, Vol.3, Issue.1, pp.1-5, 2015.

Authors Profile

Mr. Pranay Thakkar pursuing Bachelor of Technology in Computer Engineering, from KJ Somaiya College of Engineering. He has attended various workshops & is aware of the latest technologies. He has completed Oracle Certified Programmer in Java Programming (OCPJP) course.

Mr. HemantKumar Mishra pursuing Bachelor of Technology in Computer Engineering, from KJ Somaiya College of Engineering. He has done various internships in different fields such as Web Development & Marketing.

Mr. Zaheed Shaikh has received his M.E Degree in Computer Engineering from University of Mumbai in 2009. He has received B.E Degree in Computer Engineering from Vidyalankar Institute of Technology in 2007. He is an Assistant Professor, and has a teaching experience of 8 years in KJ Somaiya College of Engineering, Mumbai.

Dr. Deepak Sharma received his B.E Degree in Computer Engineering from VJTI, in 1999. He is Professor, and has a teaching experience of 15 years in KJ Somaiya College of Engineering, Mumbai.