LOVELY PROFESSIONAL UNIVERSITY

IMAGE ENCRYPTION ALGORITHM BASED ON MODIFIED AES

A Dissertation submitted

By Sumit Sidhu

To

Department of Computer Science and Engineering

In partial fulfillment of the requirement for the

Award of the degree of

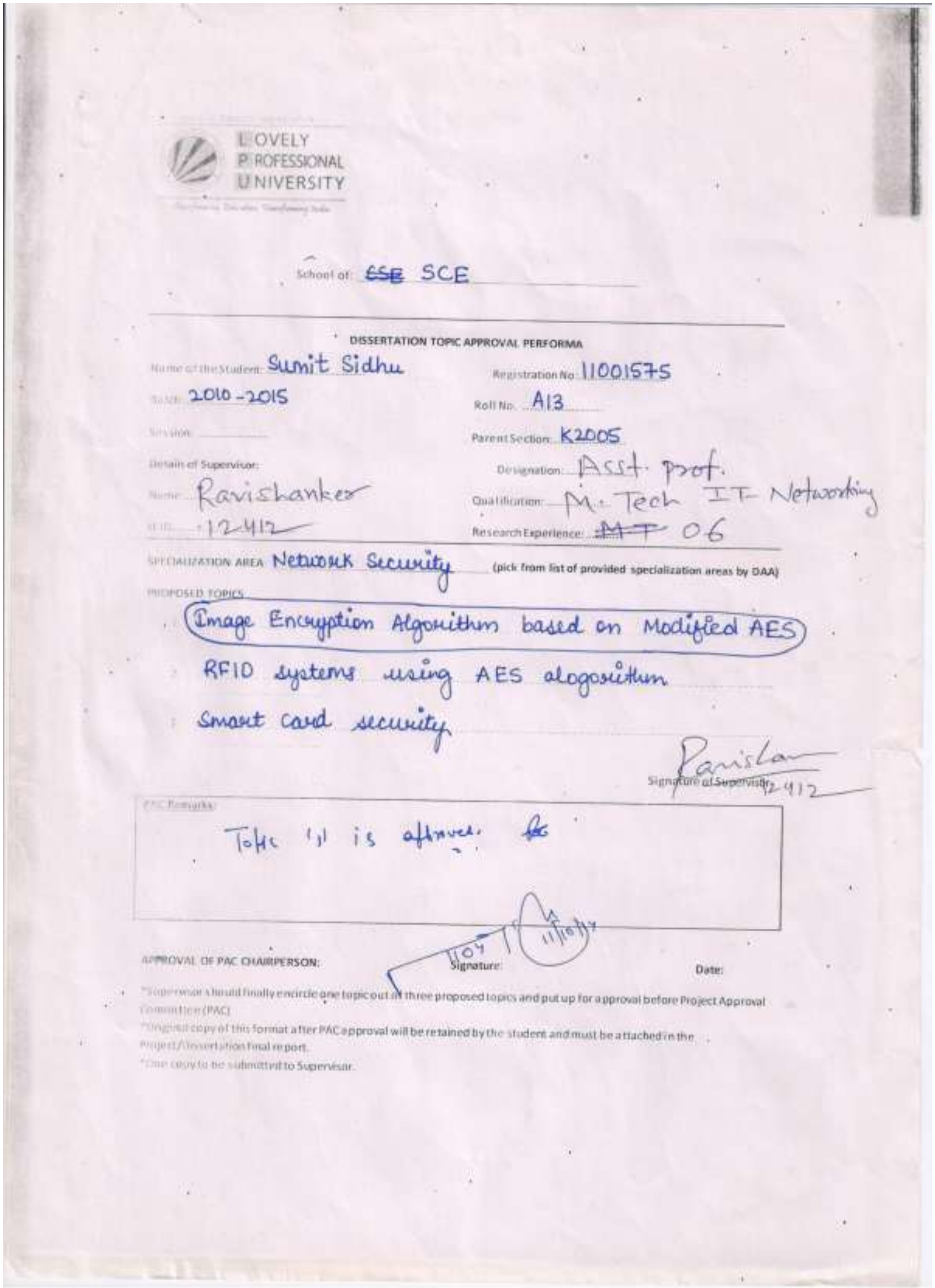
Master of technology in CSE

Under the guidance of

Er. Ravishanker

(Advisor)

May, 2015



LOVELY
PROFESSIONAL
UNIVERSITY

School of: ~~CSE~~ SCE

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Sumit Sidhu

Registration No: 11001575

Batch: 2010-2015

Roll No. A13

Session:

Parent Section: K2005

Details of Supervisor:

Designation: Asst. prof.

Name: Ravishanker

Qualification: M. Tech IT Networking

UID: 12412

Research Experience: ~~M-T~~ 06

SPECIALIZATION AREA Network Security (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Image Encryption Algorithm based on Modified AES
2. RFID systems using AES alogorithm
3. Smart card security

Ravishan 12412
Signature of Supervisor

PAC Remarks:

Topic '1' is approved.

APPROVAL OF PAC CHAIRPERSON: 1104 Signature: 11/10/14 Date:

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

In today’s world images that are being transmitted over internet are not safe. Therefore, it is required to transmit an image using some secure methods. Many algorithms can be applied but AES is more secure than others. Here AES algorithm is used to encrypt images with certain modifications. Modifications are done to the shift row stage and mix column stage. These changes have been done to reduce the computation time of AES. The key is generated using IDEA (International Data Encryption Algorithm) and mix column step is added to the key part to make the key stronger because attackers focus on the key to get the plain text. Hence two phases are involved in this process. One is the encryption phase while other is the decryption phase. First the image will be passed to the modified AES for the encryption process and then the ciphered image will be send to the receiver for decryption process. The modified AES can use both HD and normal images.

CERTIFICATE

This is to certify that **SUMIT SIDHU** has completed M.Tech dissertation titled **IMAGE ENCRYPTION ALGORITHM BASED ON MODIFIED AES** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech Computer Science and engineering.

Date: ______________

Signature of Advisor

Name:

ACKNOWLEDGEMENT

Gratitude cannot be seen or expressed. It can only be felt in the heart and is beyond description. Often words are inadequate to serve as a model of expression of one's feeling, specially the sense of indebtness and gratitude to all those who helped in our duty.

It is of immense pleasure and profound privilege to express my gratitude and indebtness along with sincere thanks to **Mr. Ravishanker** for providing me the opportunity to work for the thesis on **IMAGE ENCRYPTION ALGORITHM BASED ON MODIFIED AES.** During the entire training, I have received endless help from him.

I want to formally acknowledge my sincere gratitude to all those who has assisted and guided me in completing this work. I am beholden to my family and friends for their blessings and encouragement.

SUMIT SIDHU

11001575

DECLARATION

I hereby declare that Dissertation entitled **IMAGE ENCRYPTION ALGORITHM BASED ON MODIFIED AES** submitted for the M.Tech degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Investigator

Registration Number

TABLE OF CONTENTS

S. No	Topic	Page No.
1.	Introduction	1-15
2.	Review of Literature	16-25
3.	Present Work	26-28
4.	Results and Discussions	29-37
5.	Conclusion and Future Scope	38-38
6.	References	39-40
7.	Appendix	41-42

LIST OF FIGURES

S. No Name of Figure	Page No.
1.2.1 Flowchart of AES-128 Algorithm	07
1.2.2 Sub Byte Transformation	08
1.2.3 Shift Row Transformation	08
1.2.4 Mix Column Transformation	09
1.2.5 Add Round Key	09
1.3.1 Encryption by CBC Mode	10
1.3.2 Encryption by ECB Mode	11
1.3.3 Encryption by CFB Mode	12
1.3.4 Encryption by OFB Mode	13
1.4.1 Basic Structure of IDEA	15
3.3.1 Flowchart of proposed methodology	28
4.1 Browse an image	29
4.2 Select particular folder	30
4.3 Select particular image	31
4.4 Click on encrypt to start encrypting an image.	32
4.5 Select encrypted image to decrypt it	33

4.6 Screenshot of encrypted image 34

4.7 Select encrypted image for decryption 35

4.8 Click on decrypt to start decryption 36

4.9 Final decrypted image 37

Chapter 1

INTRODUCTION

In this modern world, there is a vast enhancement of communication techniques like internet, Whatsapp, facebook, tweeter, mobile ad-hoc network, cloud computing, satellite communication, ground communication, etc. have connected the people with each other throughout the world. But with the increase in communication techniques it is important to protect the data which is being shared through internet. Many techniques have been built to protect the data from intruders. Many encryption algorithms are there such as AES, DES, SHA, RSA, etc. which convert the data send from the sender to incomprehensible form so that intruder/hacker/attacker cannot understand it.

1.1 ENCRYPTION

Encryption is the methodology of changing information to make it confused to every unauthorized party with the exception of the recipient and hence maintains data integrity as well as privacy which are important for e-business. This means the entire reason for encryption is to verify that the recipient is the singular case out of many others who gets understandable information which has been scrambled.

Encryption has long been utilized by military and governments to encourage mysterious communication. It is presently ordinarily utilized as a part of ensuring data inside numerous sorts of non military personnel communications. Encryption can be utilized to ensure data "at rest", example, records on PCs as well as capacity/storage gadgets like USB, flash drives. Lately there are various reports of secret data, example, and clients near home records are uncovered through misfortune or we can say burglary or theft tablets (laptops) or backup devices. Encrypting those records at rest aides secure them through physical efforts to develop safety measure.

Encryption is utilized to make sure data in travel, suppose data is exchanged by systems (e.g. the Internet, e-business), cell phones, remote mouthpieces, remote radio frameworks, Bluetooth gadgets and bank programmed teller machines. There have been various reports of data in travel being blocked in late years. Encrypting data like that serves to secure it. Actually it is difficult to frequently physically secure all entries to systems.

Guaranteeing the security of private communications excluding platforms such as – email, VOIP, direct message – ought to be a top need of the internet business. The business needs to at any rate meet up to offer encryption for private communications as protection against government surveillance. There are essential 3 encryption methodologies: hashing, symmetric cryptography as well as asymmetric cryptography. All encryption routines have particular merits, points of interest, as well as demerits. Hashing, example, is extremely against altering, however is not as adaptable as alternate routines. Each of the three encryption types depends upon cryptography, or exploration of encrypted/scrambling data/information.

Individuals utilize encryption to modify clear text, called plaintext, to a mysterious form known as cipher text. Encryption of data gives extra advantages rather than ensuring the confidentiality of a data. Such points of interest incorporate guaranteeing that messages are not modified amid travel as well as confirming identity of sender. Such advantages are acknowledged by utilizing any 1 of these encryption techniques.

Encryption strategy, known hashing, makes an extraordinary (unique), modified signature of length particular message or information set. Hash functions are made with algorithm, or hash function, as well as user/individuals ordinarily utilizes those for analyzing data sets. Since hashes are one of kind to particular message, even small modifications to that message bring about significantly diverse hash, consequently cautioning (alerting) client to potential modification/altering. Key contrast between hashing as well as other 2 encryption techniques is once data is encoded, procedure cannot be turned around or deciphered implying that regardless of possibility that potential attacker has capacity to acquire/get hash, he or she cannot has capacity/power to utilize decryption system/method to get first message. Any regular hashing algorithms are Message Digest 5 (MD5) as well as Secure Hashing Algorithm (SHA).

Symmetric cryptography, can alternatively known as private-key cryptography, is 1 of most established as well as best secure encryption routines. The term "private key" derived from way key utilized to encrypt as well as decrypt data should secure on grounds that anyone who read coded messages. Sender encrypts message to cipher data utilizing key, as well as beneficiary utilizes similar key to decode. Individuals utilize this for encoding/encryption system as "stream" cipher or "block" cipher, contingent upon measure of data is encrypted or decrypted on same time. Stream cipher encrypts information 1 character/alphabet at 1 time when it is sent or got, in contrast block cipher methods settled lumps /data blocks. Regular symmetric encryption algorithms incorporate Data Encryption Standard (DES), Advanced Encryption Standard (AES), as well as International Data Encryption Algorithm (IDEA).

Asymmetric or public key, cryptography is, actually, better as compared to symmetric strategies for encryption. Such kind cryptography utilizes 2 keys, "private" key as well as "public key," for encryption as well as decryption. Utilization of 2 keys beats significant shortcoming in case of symmetric key cryptography. Solitary key does not have to be safely overseen among various individuals. In asymmetric cryptography, public key usually is openly accessible 2 everyone as well as utilized to encode messages ahead sending them. An alternate, private key stays with collector of encrypted/cipher text messages, which is then utilized to decrypt. Algorithms which utilize public key encryption techniques incorporate RSA as well as Diffie-Hellman.

When communication takes place, sender sends some mystery data (either image or text) to the destination. When the message has been sent, nobody in transit ought to unveil message except the receiver (collector). If by chance attacker/intruder gets hold of message in transit it is known as an attack. Different sorts of assaults(attacks) are there, for example, brute force assault, known plain text assault, chosen plain text assault, and so on. Subsequently encryption and decryption of the message is done keeping in mind the end goal to keep the message from any revelation. From the literature survey, encryption and decryption has been done in different courses like executing AES, DES, modified AES, changing S-box and P-box, Spartan- 6, partial image encryption, chaotic technique and so forth.

Ms E. KakaiKavitha introduced technique to secure login using one time password encryption with AES. Salim Muhsin Wadi et al. [14] introduced technique to encrypt the HD images. Modifications done by them are reduced number of mix-column transposition and use of simple s-box. Rashmi Ramesh Rachh et al. [12] have introduced two different architectures for AES where bitwise implementations of add round key and mix column transposition has been done.

Look Ahead technique is also used by some researchers to reduce the computation time of AES. Some used Novel Image encryption to construct the S-Box for the AES, so that less hardware is required and computation time is also reduced. Various key wrapping [] methods are also used to improve the performance of AES. And lot of work is also done on the diffusion (changing the values of the pixel) and confusion (changing the location of the pixels) on the images to protect them from intruders.

Partial image encryption is strategy which encodes just some piece of the image. After encryption that image is completely unrecognizable by the gatecrasher/intruder. Consequently partial image encryption diminishes the time to scramble information and additionally conceal the information from being exposure. Different partial encryption plans utilized for images are: Quad tree image compression algorithm, Wavelet compression in view of zero trees and numerous more.

One of the difficulties in cryptography is to create random numbers for the keys to be utilized as a part of encryption. However, random number created by a PC are not random, but rather are pseudo-random i.e. the numbers originate from recursively understanding a mathematical calculation from a given starting number. Every time the number delivered will be distinctive with every given beginning number, and on the off chance that we have an arrangement or set of numbers and access to the algorithm that made them, it wouldn't take a PC long to determine initial value being utilized. Advanced symmetrical encryption frameworks utilize a beginning "key" which is 256 bits long in length and combine or join this with an initialization vector (up to 256 bits in length). By applying the vector to the key through some scientific equation or mathematical formula, a great many one of a kind changes can be made, and these are consolidated with the information. This methodology can then be run backward to recover the first or original data.

An issue with these numerical encryption frameworks is that the methodology is numerically determined, and the algorithm published. For each encryption calculation that is created, in the long run somebody works out a scientific method for explaining it. Indeed, even the most recent and most noteworthy AES calculations have now been hypothetically split or cracked. The thought that chaos theory could be utilized to produce encryption keys is not innovative one, but rather up 'til now I have not seen any illustration. Chaotic based encryption algorithms have some disadvantages such as:

- Low security levels
- High computation costs

Naïve encryption algorithm is utilized in various real time systems such as smart cards, cellular telephones, ATMs, World Wide Web, etc.

1.2 ADVANCED ENCRYPTION STANDARD (AES)

The AES encryption algorithm block cipher algorithm utilizing encryption key and encryption rounds. A block cipher is an encryption calculation/algorithm which works on 1 piece of block/information at once. On account of standard AES encryption block is of 128 bits long. The AES calculation is not PC program or PC source code. Rather is numerical methodology to get secure information.

AES encryption utilizes a solitary/single key for process of encryption. The key which is utilized may be 128 bits, 192 bits, or 256 bits long. Term 128-bit encryption alludes/means to utilization of 128-bit encryption key. With AES encryption as well as decoding is performed utilizing same key. This is known as symmetric encryption calculation. Encryption calculations utilizes 2 unique keys, open as well as private key, are known asymmetric encryption algorithms.

Encryption key essentially parallel string of information utilized in process of encryption. Since same encryption key was utilized to encode as well as unscramble information, it is vital to keep the encryption key a mystery and to utilize keys that are difficult to guess. There are diverse techniques for utilizing keys with AES encryption system. Those diverse strategies are known as “modes of operation".

Modes of operation of AES are:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Counter (CTR)
- Cipher Feedback (CFB)
- Output Feedback (OFB)

Initial version of AES

AES stands for Advanced Encryption Standard. There are three versions of AES:

- Advanced Encryption Standard-128
- Advanced Encryption Standard-192
- Advanced Encryption Standard-256

Where 128, 192, 256 are key length. In AES-128 the key is represented as an array of 4*4 and has 10 rounds. In AES-192 the key is represented as an array of 4*6 and has 12 rounds. In AES-256 the key is represented as an array of 4*8 and has 14 rounds. Each round has four states except the last round. The last round in all versions has all the above states except mix-column transformation.

- Substitution transformation
- Shift-row transformation
- Mix-column transformation
- Add round key transformation

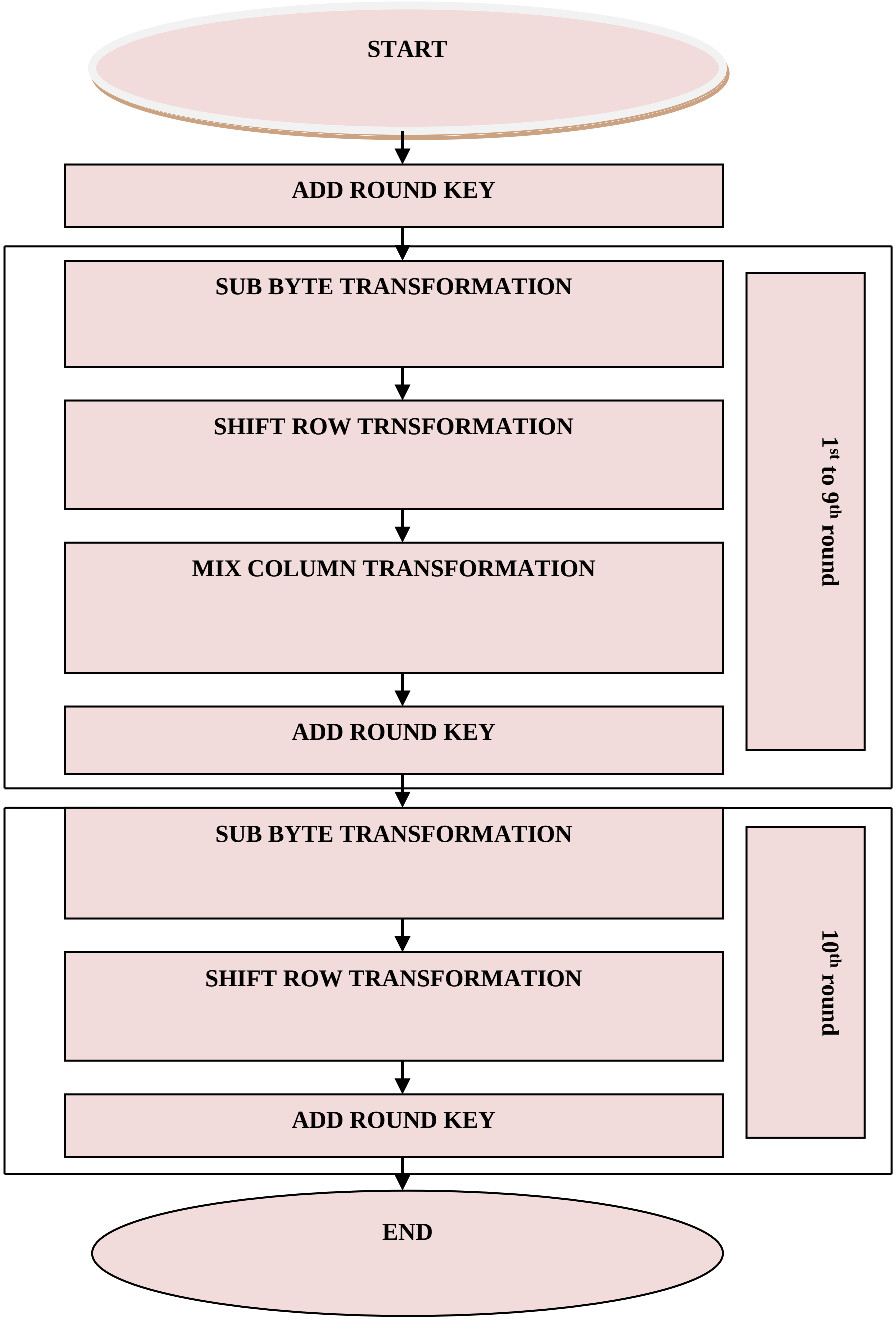


Fig.1.2.1 Flowchart of AES-128 Algorithm

- Substitution transformation involves replacing each element of an array with S-Box values. Suppose if an element of an array is a9 then the value corresponding to a row and 9th column of the S-Box is used to replace the a9 value.

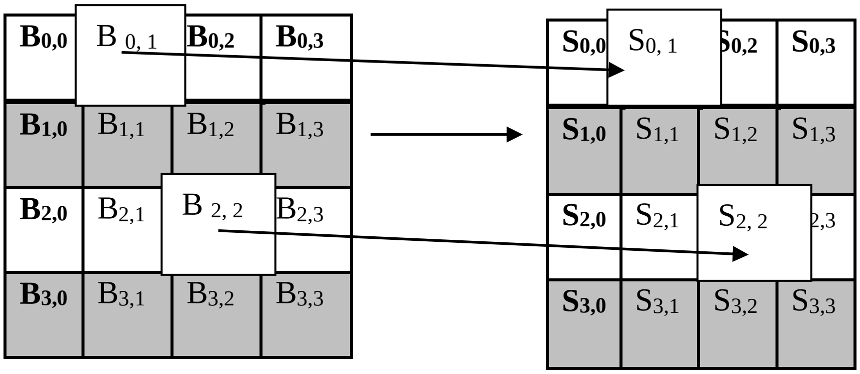


Fig. 1.2.2 Sub Byte Transformation

- Shift-row transformation involves the action on the rows of an array. The first row not shifted at all. 2nd row is moved towards left by 1 step, 3rd row is moved towards left for 2 steps and fourth row is moved towards left to 3 steps.

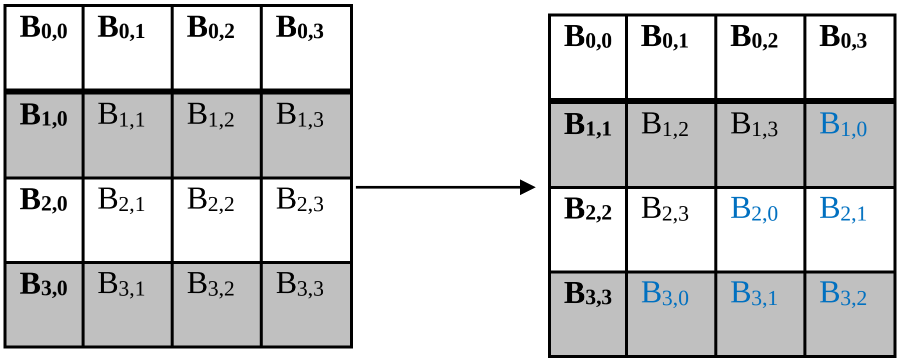

$B_{0,0}$ $B_{0,1}$ $B_{0,2}$ $B_{0,3}$
$B_{1,0}$ $B_{1,1}$ $B_{1,2}$ $B_{1,3}$
$B_{2,0}$ $B_{2,1}$ $B_{2,2}$ $B_{2,3}$
$B_{3,0}$ $B_{3,1}$ $B_{3,2}$ $B_{3,3}$
$B_{0,0}$ $B_{0,1}$ $B_{0,2}$ $B_{0,3}$
$B_{1,1}$ $B_{1,2}$ $B_{1,3}$ $B_{1,0}$
$B_{2,2}$ $B_{2,3}$ $B_{2,0}$ $B_{2,1}$
$B_{3,3}$ $B_{3,0}$ $B_{3,1}$ $B_{3,2}$

Fig. 1.2.3 Shift Row Transformation

- Mix-column transposition involves each column of state array multiplied by fixed 4*4 arrays.

$$\begin{array}{|c|c|c|c|}\hline \mathbf{B_{0,0}} & \mathbf{B_{0,1}} & \mathbf{B_{0,2}} & \mathbf{B_{0,3}} \\ \hline \mathbf{B_{1,0}} & B_{1,1} & B_{1,2} & B_{1,3} \\ \hline \mathbf{B_{2,0}} & B_{2,1} & B_{2,2} & B_{2,3} \\ \hline \mathbf{B_{3,0}} & B_{3,1} & B_{3,2} & B_{3,3} \\ \hline \end{array} \quad * \quad \begin{array}{|c|c|c|c|}\hline \mathbf{M_{0,0}} & \mathbf{M_{0,1}} & \mathbf{M_{0,2}} & \mathbf{M_{0,3}} \\ \hline \mathbf{M_{1,0}} & M_{1,1} & M_{1,2} & M_{1,3} \\ \hline \mathbf{M_{2,0}} & M_{2,1} & M_{2,2} & M_{2,3} \\ \hline \mathbf{M_{3,0}} & M_{3,1} & M_{3,2} & M_{3,3} \\ \hline \end{array}$$

Fig. 1.2.4 Mix Column Transformation

- Add round key involves xoring each element of an array with each element of the key.

$$\begin{array}{|c|c|c|c|}\hline \mathbf{B_{0,0}} & \mathbf{B_{0,1}} & \mathbf{B_{0,2}} & \mathbf{B_{0,3}} \\ \hline \mathbf{B_{1,0}} & B_{1,1} & B_{1,2} & B_{1,3} \\ \hline \mathbf{B_{2,0}} & B_{2,1} & B_{2,2} & B_{2,3} \\ \hline \mathbf{B_{3,0}} & B_{3,1} & B_{3,2} & B_{3,3} \\ \hline \end{array} \quad \oplus \quad \begin{array}{|c|c|c|c|}\hline \mathbf{K_{0,0}} & \mathbf{K_{0,1}} & \mathbf{K_{0,2}} & \mathbf{K_{0,3}} \\ \hline \mathbf{K_{1,0}} & K_{1,1} & K_{1,2} & K_{1,3} \\ \hline \mathbf{K_{2,0}} & K_{2,1} & K_{2,2} & K_{2,3} \\ \hline \mathbf{K_{3,0}} & K_{3,1} & K_{3,2} & K_{3,3} \\ \hline \end{array}$$

Fig. 1.2.5 Add Round Key

The main challenges in the AES algorithm are encryption and decryption time and attacks. So much of the work is need to be done on time and security of AES algorithm. To lessen encryption time and decryption time, the usage of 3rd state (mix-column transformation) is reduced to lesser number of rounds i.e. mix column transformation is used in 1st, 3rd, 5th, and 9th round (in AES-128) and shift row transformation is divided into odd and even rounds. For odd round 1st and 4th row is shifted and for even rounds 2nd and 3rd row is shifted. And security is improved by generating key using IDEA algorithm.

1.3 MODES OF AES

A. CIPHER BLOCK CHAINING (CBC)

Cipher block chaining (CBC) a method of operation for block cipher (one in which an arrangement of bits scrambled as solitary unit and block, cipher key connected to whole block). Cipher block chaining utilizes initialization vector (IV) of certain length. One of its key attributes is that it utilizes chaining instrument that causes decryption of block of cipher text to rely upon all first cipher text blocks. Accordingly, whole legitimacy of every single going before block is contained in quickly past cipher text block. Solitary bit slip in cipher text block influences the decryption of every resulting block. Improvement of request of cipher text blocks causes decryption to wind up adulterated. Fundamentally, in cipher block chaining, every plaintext block Xored with quickly past cipher text block, as well as afterward scrambled.

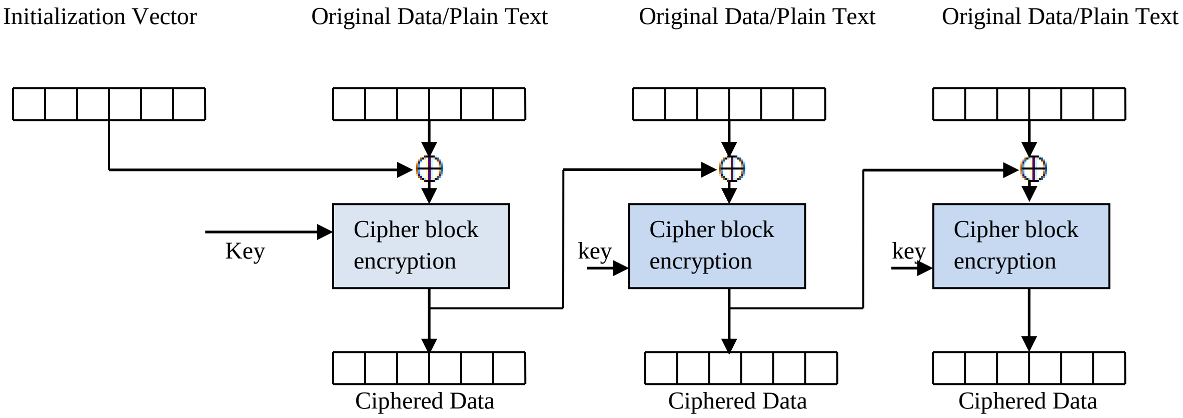


Fig. 1.3.1 Encryption by CBC Mode

Indistinguishable cipher text blocks just result if same plaintext square is encoded utilizing both same key as well as initialization vector, moreover if order of cipher text block is not changed. Its merits are over Electronic Code Book mode in that Xoring procedure conceals plaintext designs.

In a perfect world, the initialization vector ought to appear as something else for any 2 messages scrambled with same key. Despite of fact that the initialization vector require not to be mystery, a few uses may locate it to be attractive.

B. ELECTRONIC CODE BOOK (ECB)

This mode essentially AES function having no feedback applied, put plain data through AES function as well as use resulting cipher data directly. Repeated plain data encrypted using similar key will often produce same cipher data, this mode is generally considered vulnerable as well as rarely utilized in practical systems. However, where simplicity is required is random access within long encrypted stream. Data can processed in blocks only which match block-size of encryption function as well as synchronization at this block level should be provided between encrypting as well as decrypting engines, otherwise data is indecipherable.

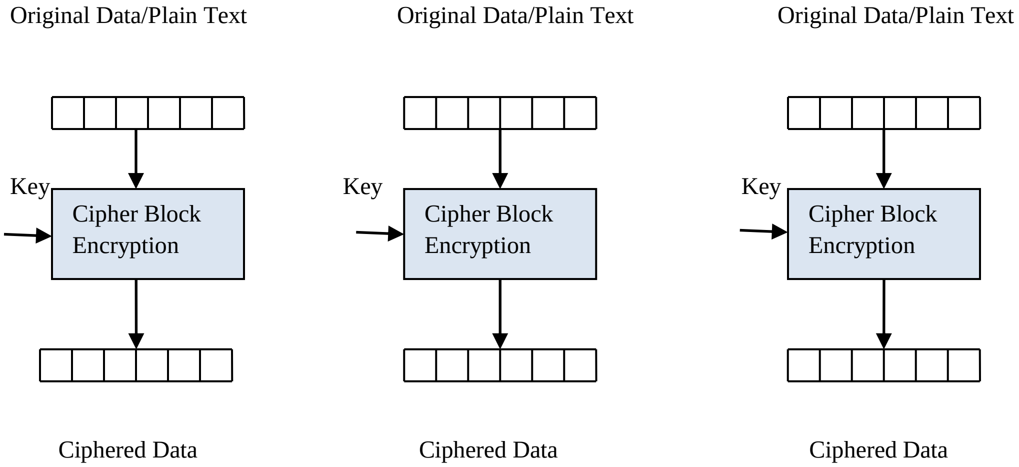


Fig. 1.3.2 Encryption by ECB Mode

C. CIPHER FEEDBACK (CFB)

This mode typical mode, as well as offers likelihood to make hidden block cipher works similar to stream cipher; i.e. so that data gets prepared is stream of shorter data values (instance/example bytes or bits) instead of processing is much bigger blocks. In CFB mode, data does not experience AES, but rather is Xored to quality which AES produces from past history of message. This means that delay through CFB capacity could be reduced, as main processing connected to data is a XOR function. Data widths could be set to any size to basic cipher block size. However throughput diminishes as widths get smaller in proportion of data width to block size. Synchronization at picked data width level should be given between encrypting as well as decrypting modules, generally data is indecipherable.

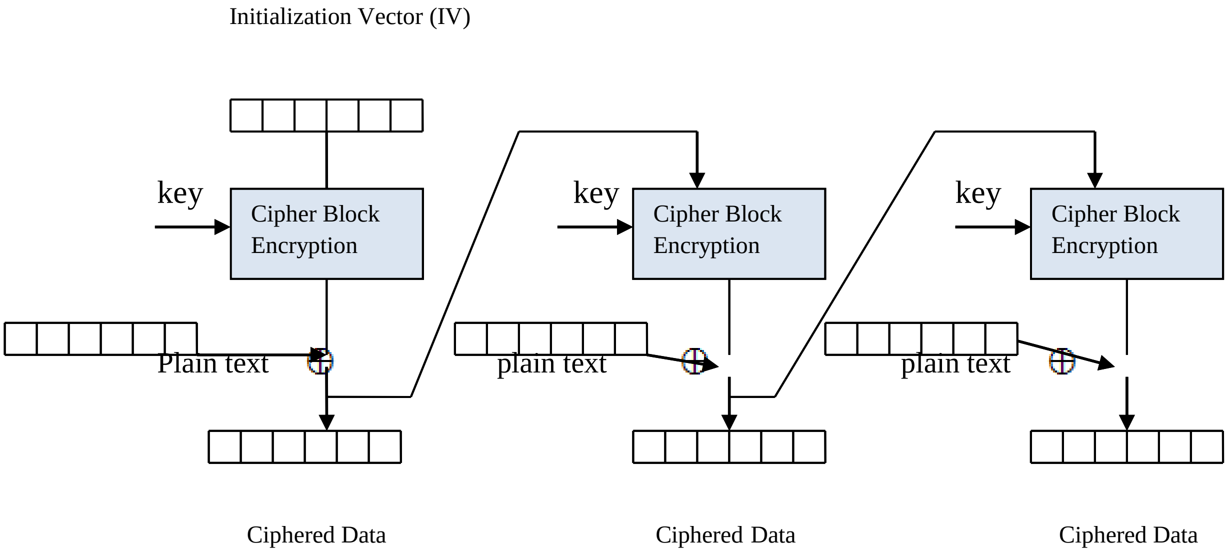


Fig. 1.3.3 Encryption by CFB Mode

D. OUTPUT FEEDBACK (OFB)

The Output Feedback (OFB) mode produces block cipher to synchronous stream cipher. It creates key parts (blocks), which Xored to plain data parts to get cipher text. Pretty like stream ciphers, if bit is flipped in cipher text flipped bit in plain data is generated same location. The property permits numerous error correcting codes to function regularly notwithstanding when connected in front of encryption. Due to symmetry of XOR operation, encryption as well as decryption is same.

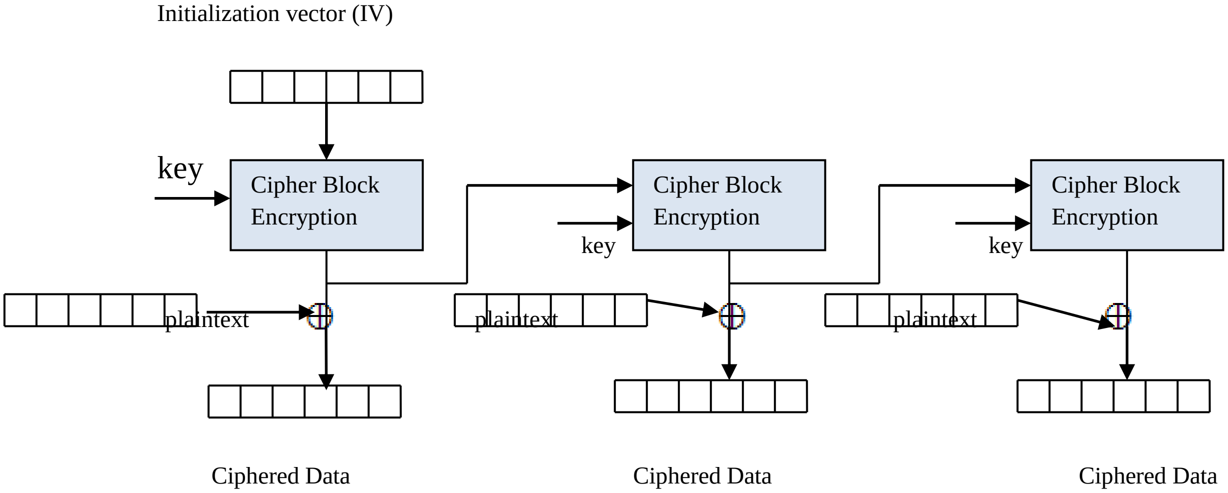


Fig. 1.3.4 Encryption by OFB Mode

Every output feedback cipher block operation relies on every past one, thus performance can't be in parallel. In any case, in light of the fact that the plain data and cipher data is utilized for last XOR, block cipher operations are performed ahead of time, permitting the last step is be performed parallel if plain data or cipher data is accessible. It feasible get OFB mode keystream by utilizing CBC mode to consistent series of 0s as input. This is helpful, in light of the fact that it permits the use of hardware equipment usage of CBC mode for OFB mode encryption. Utilizing OFB mode to fractional block as input as CFB mode lessens normal cycle length to component of 2^ (32) or even more than this.

1.4 IDEA (International Data Encryption Algorithm)

The IDEA encryption algorithm:

- provides security to high level not in light of making algorithm secret
- endless supply of secret key used to completely determined as well as effectively caught on i.e. understandable and is accessible to everyone
- suitable for utilization in an extensive variety of applications and can be financially executed in electronic segments (VLSI Chip)
- can be utilized efficiently and may be sent out around the world

In round 1, initial 4 16-bit key sub-pieces are consolidated with 2 of 16-bit plaintext squares utilizing expansion modulo 216, as well as with other 2 plaintext pieces utilizing augmentation modulo 216 + 1. Outcomes are transformed further as demonstrated in Figure , whereby 2 more 16-bit key sub-squares enter estimation as well as 3 arithmetical gathering administrator, little bit at a time selective OR, is utilized. Towards end of 1st encryption cycle 4 16-bit qualities are delivered which can be utilized as info to 2nd encryption round in an incompletely changed request. Methodology depicted above for cycle 1 is rehashed in each of resulting 7 rounds of encryption utilizing distinctive 16-bit key sub-hinders for every mix. Amid resulting yield change, 4 16-bit qualities created towards end of 8th encryption round are consolidated with last 4 of 52 key sub-pieces utilizing expansion modulo 216 as well as duplication modulo 216 + 1 to frame subsequent 4 16-bit cipher text squares.

DECRYPTION ALGORITHM

The square figure Thought works to 64-bit plaintext as well as figure content squares and controlled with 128-bit key. Basic advancement in outline of calculation is utilization of operations of 3 diverse mathematical gatherings. Substitution boxes as well as related table lookups utilized as a part of the square figures accessible to-date have been totally maintained a strategic distance from. The calculation structure has been picked such that, with the special case that distinctive key sub-pieces are utilized, the encryption procedure is indistinguishable to the unscrambling methodology.

The computational procedure utilized for decoding of cipher text is basically same as utilized for encryption of plaintext. Main distinction contrasted and encryption is that amid decoding, distinctive 16-bit key sub-squares created. All decisively, all 52 16-bit key sub-squares utilized for decoding is reverse of key sub-square utilized amid encryption as a part of appreciation of connected arithmetical gathering operation. Also, key sub-pieces should be utilized as a part of the opposite request amid decoding to invert the encryption process.

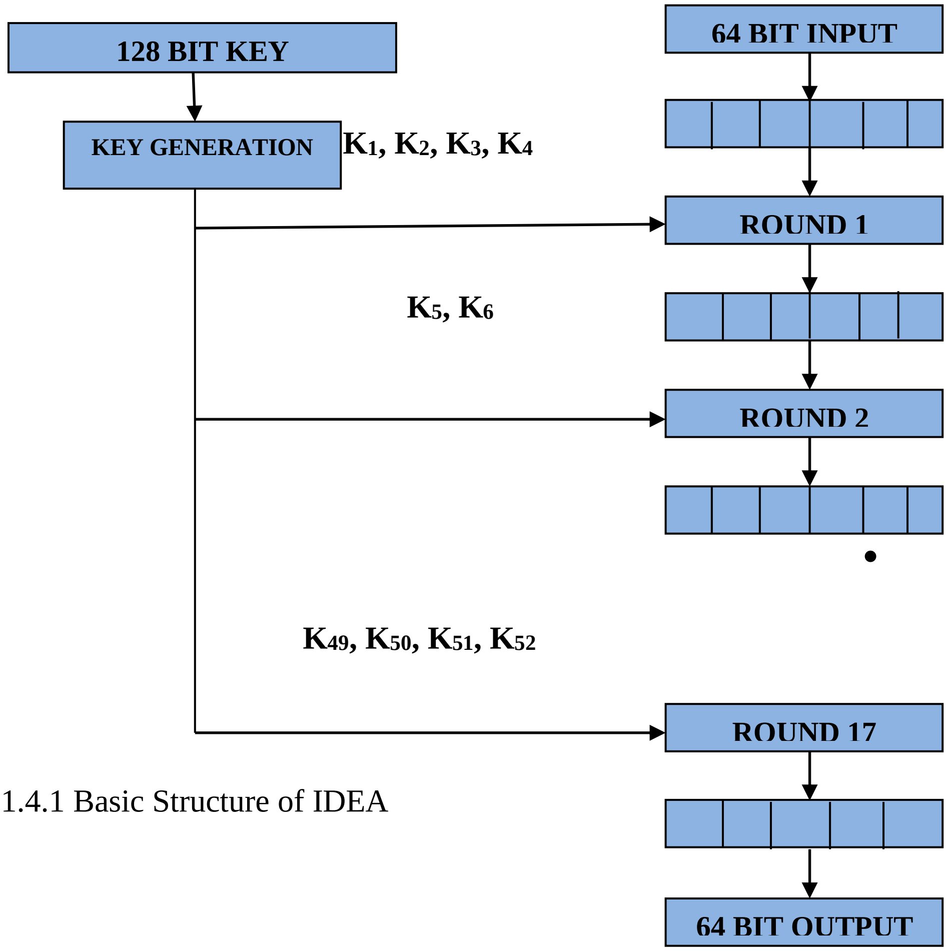


Fig. 1.4.1 Basic Structure of IDEA

Chapter 2

REVIEW OF LITERATURE

Daemen, Joan, and Craig Clapp (1998) [4] presented PANAMA which is a module that can be utilized as cryptography hash function and in addition stream cipher. They have demonstrated that quick executions of programming could be possible utilizing inherent/innate parallelism on VLIW processor. Panama is basically based upon a machine which utilizes 8192 buffer and 544 bit state. These two are updated by utilizing loops/cycles/iterations. Panama utilizes hermetic hash function which must include: The normal workload of creating a collision is of the request of 2^(n/2),if n bit worth/value is given then expected workload of discovering the message is 2^n executions of hash function, when message and its hash value is given then expected workload of discovering the second message is of the request of 2^n executions of the hash function, Panama is likewise K-secure if a key stream output alongside a given key and picked estimation of q is given then the compelling approach to get the learning of the key could be possible by doing exhaustive search. The future scope of panama is that it will be utilized as a part of set top boxes and digital televisions which will be utilized as a part without bounds in future that they utilize media processors for decompressing videos for performing different tasks. The panama gives high information/data rates.

Canright, David (2005) [3] defined more complex/intricate S-Box. In S-Box every subfield was filled by polynomial basis as well as ordinary basis which gave 432 cases altogether. The best case with the implementation of this algorithm gave 20 % change/improvement. They have shown optimizations in GF (2^8) inverter for best case. Implementations include two distinct representations of GF (2^8). The standard structure used the vector of 8 bits. The best approach to use these two methods is to encode/encrypt every block of plain text using AES algorithm and decrypting it in the reverse request.

The above algorithm consumed smaller region in ASIC hardware versions of AES. So, this saved region which can adjust one more chip of S-Box which works parallel in future. They have contrasted their work and 431 versions accessible yet have demonstrated that their algorithm is superior to all. This reduced S-Box can be used for some future hardware implementations of AES for many security applications.

Harrison, et al.(2007) [9] proposed novel encryption methodology for implementing AES Algorithm. An AES utilized block cipher method for encryption. By actualizing or implementing AES on GPU, various processes could be possible in parallel. First both electronic code book and chaining block cipher mode was connected to check the execution of the proposed implementation. In any case, chaining block cipher revealed the best results. At long last they have reasoned that the operating system reports 100 % burden amid GPU's task execution.

Key stream generators (A5/1, W7) (Zeghid, Medien, 2007) [17] are used to enhance the performance of AES for images which have reduced entropy. The researchers have implemented image encryption by vector quantization i.e. image is decomposed into vectors and then encryption and decryption is done vector by vector. After encryption the image is transformed into shadows which are not understandable to intruders. Image text encryption has also been achieved by chaotic algorithms by them. The chaotic algorithm used by them is based on Lorenz equations.

They tried implementing DES (Data Encryption Standard) but it was so complex and involved very large computations. It was also not fast to process huge data formed by multimedia applications and hardware which was used to implement DES was so costly. So, the solution to all problems was solved with the introduction of AES .AES is used in those applications which requires fast processing. They have also done analysis of various security issues. Like statistical approach, key space analysis to prevent data from cipher text attack, statistical attack, plain text attack, brute force attack, etc. In histogram analysis, histogram of original image was showing so many peaks whereas that of the encryption image the histogram was fairly uniform without many ups and downs. Applying all above techniques the problem of textured zones was not solved. But when they applied W7 key stream generator the problem of textured zones was easily solved. W7 key generator was proved better than A5/1 key stream generator.

Block cipher mode (Morris Dworkin 2010) [5] is one of the mode upon which AES is implemented. The researchers have provided recommendation for the block cipher mode of AES. Mode is known as key wrap (KW). When the key wrap is done with the padding to provide interoperability then this is known as key wrap with padding (KWP). The triple idea key wrap (TKW) is used to support legacy applications. The above all techniques provide confidentiality as well as integrity to keys as well as data.

Forward transformation is permutation of data is caused by the block cipher in conjunction with the key. The key used in forward transformation is called key encryption key (KEK). The inverse of forward transformation is known as inverse transformation. For key, the wrapping and the unwrapping functions are applied on the 3 or more blocks. But the resulted length of output is same as input for both functions. Prerequisites are KEK and K and 128 bit cipher block. Two types of algorithms are explained for the key wrapping.

The plain text is expanded in the authentication encryption function which provides the authenticity to the data. If the output is a plaintext then the cipher text is authenticated else it is not authenticated.

Hermassi, Houcemeddine et al. (2013) [10] proposed better versions of picture cryptosystem by adjusting/modifying S-box as well as P-box of classical cryptography. By applying such modification the brute force attacks reduced and execution of encryption and decoding/decryption has increased. Problems confronted by previous chaotic cryptosystems were that they were not secure to attacks like chosen and known plain text. Two modifications done here are basically to S-Box and P-Box. They made plain text which is in connection with key stream. Therefore, at whatever point plain text changes key stream changes naturally. They used PWLCM map for shuffling which reduces the quantity of iterations to transform the rows as well as columns. Instead of using ECB they utilized CBC in which every plain text block gets Xored with previously used ciphered data block.

Security was broke down using co-connection of adjoining pixels and histograms. In any case, the issue still exists in generation of key and in the permutation process. At last they concluded that attacker will be more confused when user will take the above described method. Subsequently it has shown better execution as contrast with DES, AES, and triple DES. Thus future take a shot at key stream and change could be possible.

Manoj B et al. (2012) proposed AES encryption and decryption on Xilinx ISE 12.4 tool coded in VHDL (Very High Speed Integrated Circuit Hardware Description Language). They have done symmetric key encryption because they are relatively easy to implement and are faster and consumes less power. Here implementation is done with AES 128.7-bit of data was shifted to 128 bit register to AES encryption algorithm and 128 bit encrypted image was produced and then this encrypted image was send to decryption algorithm to get back the original image. Performance of algorithm was calculated n stands for number of clock cycles. Problems were encountered to them while implementing asymmetric key encryption because it was consuming so much power due to which its implementation was becoming harder. They have concluded that maximum frequency achieved using above technique is 164.562 MHz and the throughput value they observes was 252.132 Mbit/sec for encryption and decryption of the image. Hence they thought the symmetric key encryption a better approach. This same procedure or implementation can be very useful in forensics, Artificial intelligence system, Military communication etc.

Rashmi Ramesh Rachh (2014) [13] has introduced two different systems for hardware computation of AES. The first system for encryption used better S-Box, then implementing add round key and mix column transposition bit wise. And for decryption inverse S-Box, then implementing inverse mix column and inverse add round key bit wise. This architecture takes input if three blocks.

Second system involves encryption by combining block 3 of S-Box with mix-column and add round key. Block 3 of S-Box with inverse mix column and inverse add round key for decryption. These two methods were implemented in VLSI with lesser delay.

Wang, Jing et al. (2012) [15] proposed kerchofs standard for scrambling a picture by utilizing pseudo random permutations. Certain problems were faced when user utilized this encryption scheme. Those problems were if every line and section of the matrix is similar then collector can't decode the message accurately. Besides this each plain text word is connected with one cipher text word yet is not dependent of other cipher text. Consequently can't meet the diffusion and confusion property and if the quantity of iterations is small then statistical attacks can uncover visual data easily. At that point they made new algorithm which solved above problems. After various hypothetical analysis as well as simulations they demonstrated that proposed algorithm acquire better confusion and diffusion properties and is more secure to many attacks.

XTS-AES (Morris Dworkin 2012) [6] is utilized to maintain confidentiality of information stored in storage device. XTS-AES algorithm is an XES i.e. XOR then Encryption and then XOR again with the help of cipher text stealing to increase the data input size. It only provides confidentiality but not authentication. Because when there is no authentication then it gives more protection to the encrypted data. Three elements used in this procedure are a secret key, data unit of fixed length and the apparatus which implements XTS-AES encryption.

Benrhouma et al. (2013) [2] proposed modified technique to actualize partial image encryption. They perceived that today users need a swift response henceforth RSA, AES, DES, IDEA, and so forth algorithms are no more relevant to encryption because they consume huge time. Thus they implemented partial picture encryption based on spatiopartial systems which encrypts just a small portion of the information/image to confuse intruder/attacker. Anyhow, when the matter comes to scramble the picture then cryptosystems develops each and every shading/color of picture. Yet at the same time issue was there i.e. there was weakness in security during key generation stream. Subsequently they have infer that when they utilized the same key for many communications like brute force attacks, chosen plain text attacks and so on. However, when they made key to be subject to plain text and infer halfway picture encryption (i.e. to scramble just some portion of the plain text) decreased various attacks.

Gnanaraj et al. (2013) [8] proposed a smart card application to get authentication or access in a specific system. They proposed validation scheme which asks user's identification and password before going into a system. The algorithm is executed in such a way that the processing delay is less when contrasted with the previous algorithms. In this improved version of remote based confirmation scheme has been connected. The secret information entered by the user acts as key and whole information of the user is kept inside server. At whatever point user enters key that information is contrasted with the information present inside server. The smart card first does the acceptance of user and then forwards the information to server for validation purpose. If valid user then is permitted to go into the system else it is rejected or said to login once more. Various attacks are possible such as man-in-the-middle assault/attack, mutual authentication, ID theft assault, and modification assault and so forth. In future other light weight algorithms can be used other than overwhelming AES or RSA. Additionally deal with blending the algorithms can also be finished.

Majid Babaei (2013) [1]described that in today's reality the security of picture is exceptionally essential and it has gotten to be extremely hard to secure the images using just a single method so keeping in mind the end goal to secure the picture another strategy for DNA encryption is produced. Various scientific problems were solved using DNA figuring. They used One Time Pad algorithm to solve the issue of picture encryption furthermore the chaotic map as input to one time pad. There are various complex numerical which are used as a device to build up the key and scramble the message so that another strategy is produced to encode the message used as DNA processing in which various DNA framework/matrix were made. As DNA can store substantial (large) measure of information furthermore can perform parallel response so it fastens and made the encryption stronger. In this chaos hypothesis is joined with the DNA computation and after that one time pad algorithm is connected over it to scramble the information or picture.

One Time Password (Ms. E. Kalaikavitha 2013) is key which is valid for 1 session only. The researchers have proposed secure login using encrypted one time password (OTP) and mobile of the user to provide authentication to the system. Their main idea was to increase security. They introduced technique because online based applications mainly use STATIC passwords which are more prone to attacks. Static password are easy to remember and easy to hack because generally users keep their passwords as their birthdays, anniversaries, etc.

When user enters username and password, the pseudo random generator generates one time password (OTP) at the web server and encrypts it using AES algorithm. This encrypted OTP is send to the user’s mobile but the user is not able to read it because it is in encrypted form.

Then user forwards that OTP with his password back to the server. At the server OTP is decrypted to know whether the user is authorized or not.

Two types of methods are used to generate OTP:

- **Time synchronized-** user is given a token (piece of hardware) containing a clock synchronized with the server.
- **Mathematical algorithms-** mathematical methods are used to generate new password from the earlier passwords or the new password is generated randomly.

Problems faced were increased load on the system and increased encryption and decryption time.

Chaos technique (Xingyuan Wang 2014) [16] is used to shuffle the pixels of the image so that intruder cannot understand it. The researchers have introduced a scheme to construct the S-Boxes for the AES algorithm using chaos theory. The key and the end pixels of the image are used to create the first S-Box. In this the image is divided into four parts and to damage the interaction between the nearby pixels, the image has been divided into four directions. Then encryption of first S-Box is done followed by the preparations of the next group construction begins. Security is highly achieved using this method. Less than 50 S-Boxes are generated in this technique.

Initial conditions for the chaotic system are:

- Pseudo randomness
- Periodicity
- Reproduction

For the different group of images different times encryption is done on various S-Boxes. Due to which plain text attacks are protected.

High definition (Salim Muhsin Wadi 2014) [14] image has huge amount of data attached to it. Therefore the researchers have introduced technique to encrypt the HD images. Many problems were faced when AES was used to encrypt HD images because it consumed lots of time (large amount of data is attached to the HD images). Problems were:

- High computation cost
- Pattern appearance problem
- High hardware requirement

Modifications done in this paper are:

- To reduce encryption time, mix columns were used only 5 times instead of 9 times in 128 bit key. 5 times used was in 1st, 3rd, 5th, 7th, and 9th rounds.
- Key schedule was made more secure by adding mix column transposition to this part.
- To decrease hardware requirements, one simple s-box was used to encrypt and decrypt images instead of using 2 complex s-boxes one for encryption and other for decryption.
- The pattern appearance problem was solved by using one of the ciphering modes:
    - ECB- Electronic Code Book
    - CBC- Ciphering Block Chain
    - CFB- Cipher Feedback
    - OFB- Output Feedback

Experimental results were seen in MATLAB 2010b where two types of images were used:

- RGB
- Grayscale

Security is implemented through:

- **Entropy-** Entropy is a measure of randomness. The results shows that the entropy values for the modified AES algorithm executed using CBC and CFB mode are near the ideal value 8.
- **Co-relation of adjacent pixels**- actually adjusted pixels is highly related to each other. The best encryption scheme is a system that introduces encrypted images with a little co-relation between the adjacent pixels to prevent from various attacks. The values of the co-relation co-efficient are low especially when CBC and CFB modes were applied.

- **Histogram-** histogram of ciphered image should be uniformly distributed. Histogram of encrypted image has low or no same statistics to the original image. In the different experiments, the modified AES executed using the CBC and CFB modes have uniform distribution therefore satisfying the good diffusion and confusion conditions.
- **Visible scene-** ciphered image hides the basic detail. This proposed algorithm of AES satisfied visual scene requirement while executing cipher block chaining as well as cipher feedback modes.

Comparisons of computation and execution time:

- Reduction in computation time compared to original AES is 29 %
- Reduction in execution time is 35 %
- Best execution time was achieved using CBC mode.

K.Ganesan et al. (March 2014) [7]realized security of information is one of the critical issue which ought to be remembered .Therefore so as to do keep up security there are different chaotic techniques which utilizes look up tables to build the rate of encryption and unscrambling procedure. So here they utilized eight dimensional chaotic techniques in light of the fact that from the late/recent years a substantial number of other chaotic techniques were given which were confronting different issues like security issues and robustness. So with a specific end goal to evacuate such mistake/issues they utilized eight dimensional chaotic technique which uses look table which works as per the cipher block chaining. this technique does not utilizes XOR or XNOR as these are extremely delicate before known plain text assault. This encryption gives mass data capacity has more noteworthy repetition.

Norouzi, Benyamin, et al. (2014) [11] proposed the utilization of 512 bit long key a secret value acting as input value for salsa20 hash function. In this as a matter of first importance the hash function is changed and after that produces a key which results in secure encryption. The encrypted content is made by associating the key stream and the first content to make the encrypted text. As we realize that diffusion can split the relationship of the values which are given furthermore change the pixel values. At that point the picture is encrypted again by utilizing two rounds of diffusion. In the first round most importantly the picture is divided in horizontal direction and in second round of diffusion again same is performed yet in the vertical direction to transpose picture which is received.

Rashmi Ramesh Rachh (2014) [13] introduced faster methods for decryption of Advanced Encryption Standard algorithm. The researchers have proposed a technique to get a key of last round of AES algorithm faster and key of other rounds of AES parallel. Accordingly the keys can be easily and faster generated before encryption process and decryption process starts. But the condition is that the decryption process starts only after the last round key is found. The implementations are done on the FPGA using XC5VLX85 device. To produce the design Xilinx ISE 9.1 was used. Hence keys can be generated faster by pipelining.

S.Dharanidharan et al. (2013) Scrambled pictures from multiple points of view; few procedures have utilized diverse encryption techniques. In this exploration, they apply another adjusted International Data Encryption Algorithm to scramble full picture in effective secure way, after encryption first document will be divided as well as changed over to another picture records. By utilizing Huffman Algorithm divided picture records are blended. What's more, we union whole sectioned picture to pack into a solitary picture? At long last recover completely unscrambled picture. Next locate a proficient approach to exchange scrambled pictures to multipath steering methods, above packed picture has been sent to single way as well as now upgraded with multipath directing calculation, at last get effective transmission and dependable, productive picture.

They present three vital systems in particular cryptography, multipath steering calculation as well as steganography. Cryptography presents novel plan for distinguishable reversible information concealing, Steganography approach for Least Significant Bit (LSB). Multipath steering calculation includes in dynamic nature of remote connections. These three procedures are consolidated together alongside Huffman calculation, to encode picture in proficient way. Picture that can be partitioned into six sections as well as which finished results in an alternate new picture

Chapter 3

PRESENT WORK

3.1 PROBLEM FORMULATION

Although AES is secure algorithm and can be implemented but still it has some drawbacks like:

- High hardware requirement
- Encryption and decryption time

Therefore some modifications need to be done on AES to improve its performance. The main challenges in the AES algorithm are encryption and decryption time and attacks. So much of the work is need to be done on time and security of AES algorithm. To lessen encryption time and decryption time, the usage of 3rd state (mix-column transformation) is reduced to lesser number of rounds i.e. mix column transformation is used in 1st, 3rd, 5th, and 9th round (in AES-128) and shift row transformations are reduced to odd and even rounds. And security is improved by using some modifications to the key schedule part.

3.2 OBJECTIVE OF THE STUDY

The main objectives of doing this study are:

- Protect the image which is being shared on internet using AES
- Reduce the encryption and decryption time of AES
- Enhance security

People feel very safe by exchanging data and images over internet. But actually this is not safe because intruders may get access to that data and may misuse it. Therefore it is important to convert the data and image into a form which hacker cannot understand. This is called encryption.

In this work image is encrypted using AES algorithm with certain modification to reduce the encryption and decryption time and to enhance security of AES.

3.3 RESEARCH METHODOLOGY

The main challenges in the AES algorithm are encryption and decryption time and attacks. So much of the work is need to be done on time and security of AES algorithm. To lessen encryption time and decryption time, the usage of 3rd state (mix-column transformation) is reduced to lesser number of rounds i.e. mix column transformation is used in 1st, 3rd, 5th, and 9th round (in AES-128) and shift row transformation is divided into odd and even rounds. For odd round 1st and 4th row is shifted and for even rounds 2nd and 3rd row is shifted. And security is improved by generating key using IDEA algorithm.

With the increase in communication techniques it is important to protect the data which is being shared through internet. Many techniques have been built to protect the data from intruders. Various phases are as follows:

- Encryption phase
- Decryption phase

Encryption phase:

AES consumes time to do encryption and decryption. To reduce that time little modification is done in the original AES algorithm i.e. the usage of 3rd state (mix-column transformation) is reduced to lesser number of rounds i.e. mix column transformation is used in 1st, 3rd, 5th, and 9th round (in AES-128) only and shift row transformations is shifted to lesser rounds depending upon whether the round is even or odd. And to enhance security certain modifications such as mix column transformation is added to the key schedule part. And finally the image is sent to the receiver via internet.

Decryption phase:

When the receiver gets the data, the stream of data will be decrypted by inverse AES to get the original stream of data.

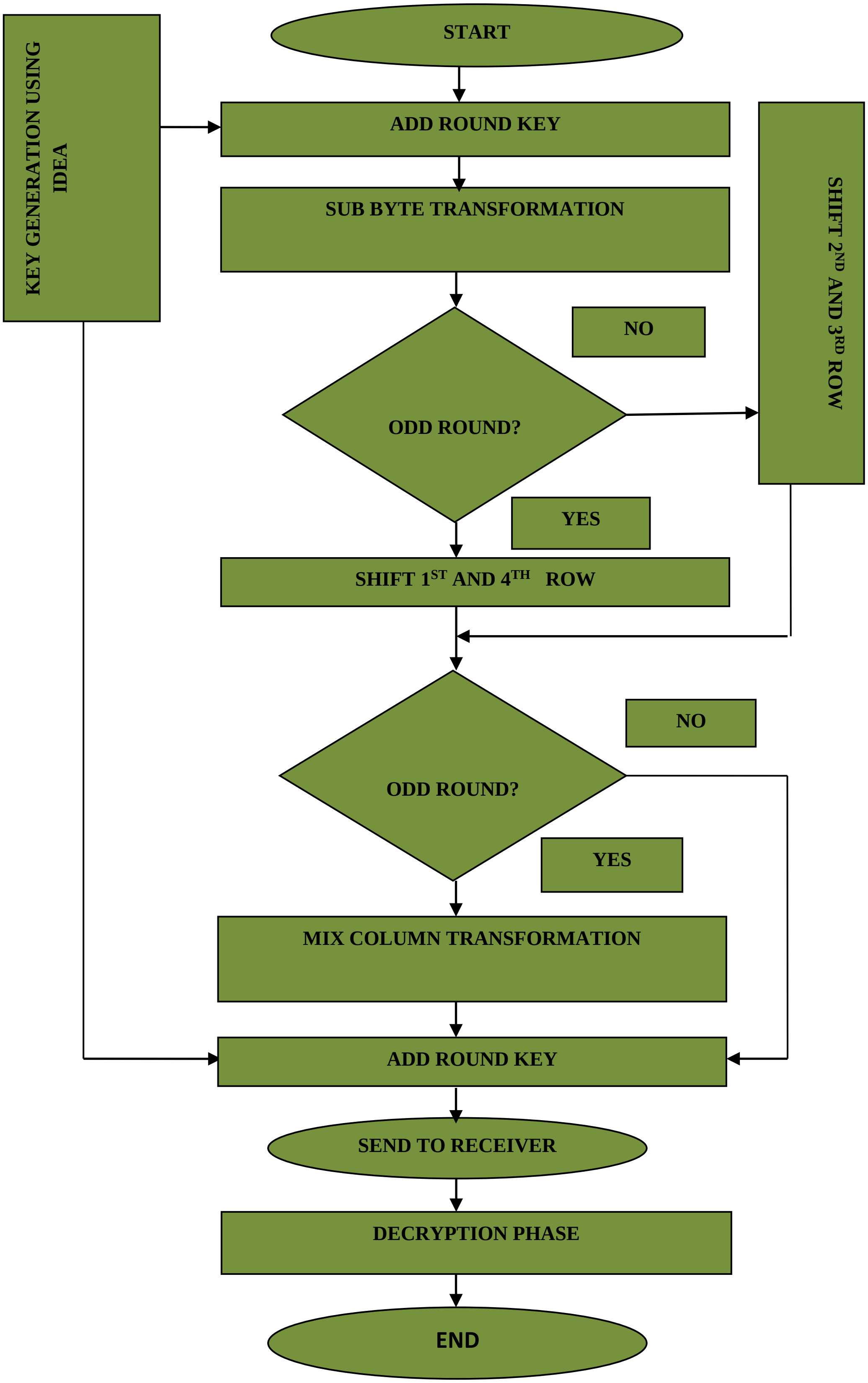


Fig. 3.3.1 Flowchart of proposed methodology

Chapter 4

RESULTS AND DISCUSSIONS

The image obtained after using these techniques is more secure by doing some modifications in AES and expectations are that the outcomes of the encryption will be faster because encryption and decryption time has been reduced. The image reaches to the destination more securely and the intruder is not able to see or change the image.

Step 1: Browse the image which needs to be encrypted.

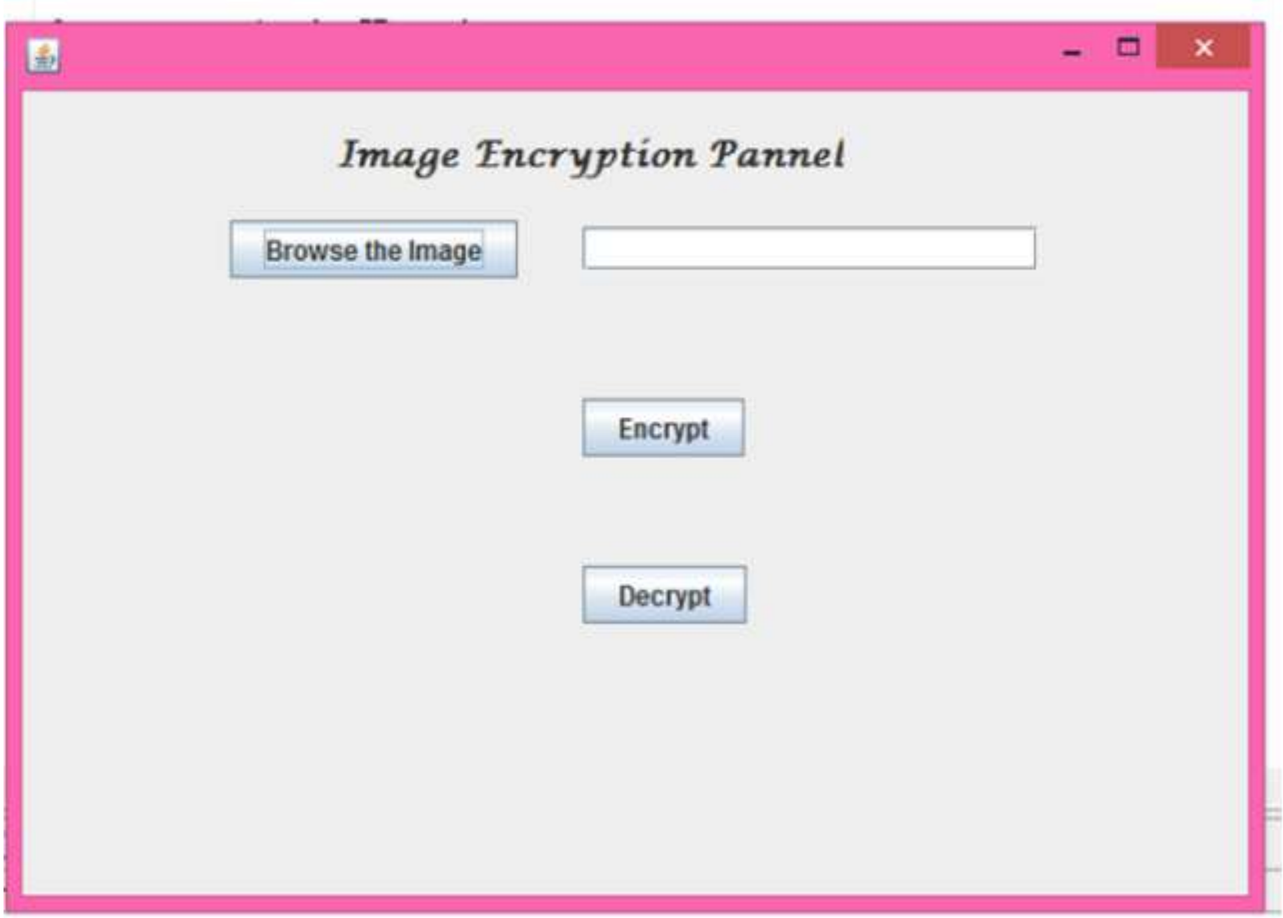
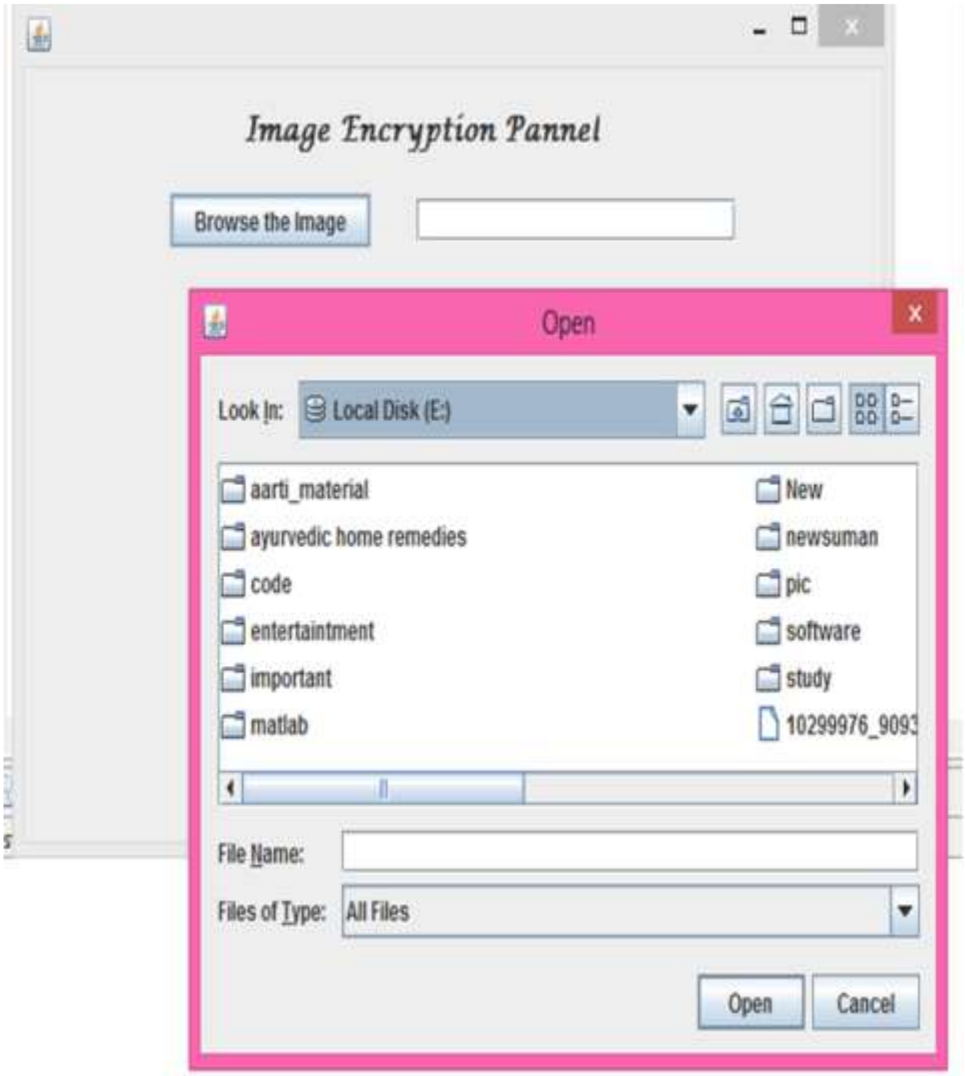


Fig. 4.1 Browse an image

Step 2: Select an image to be encrypted from the drive or folders.



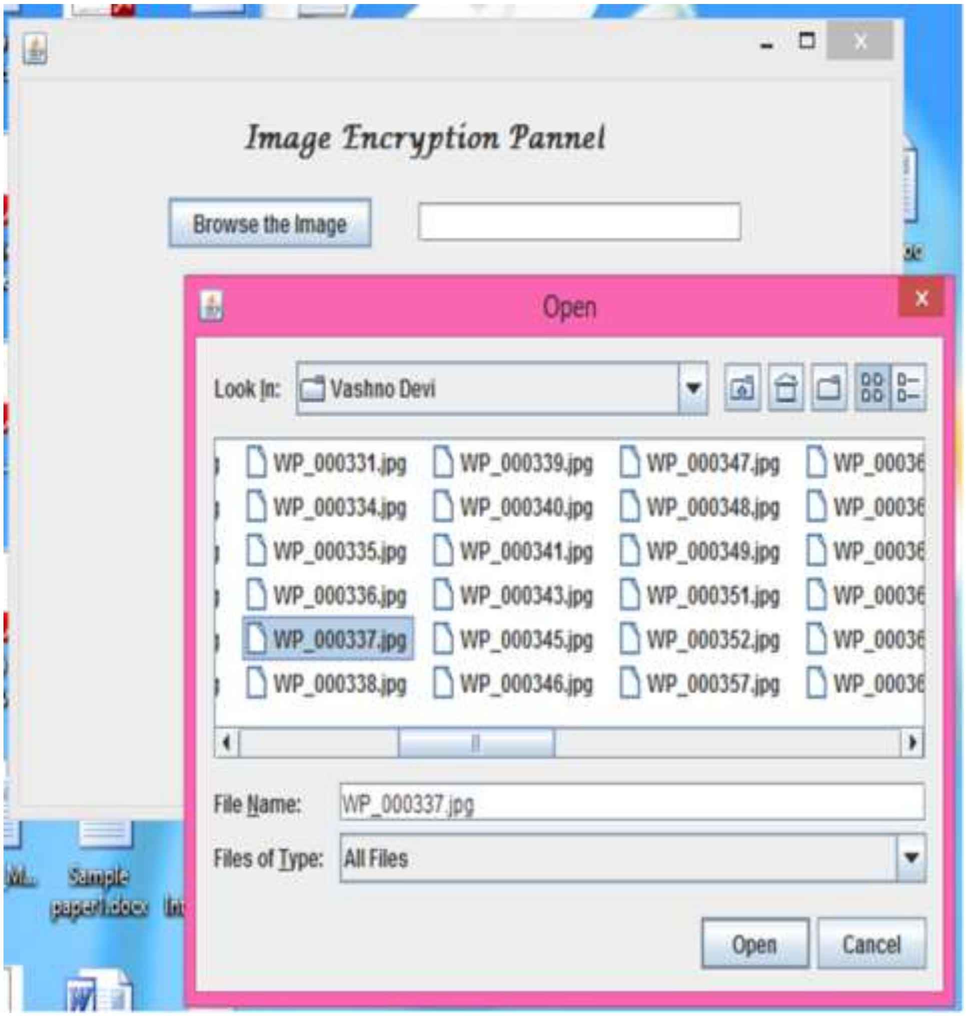
Look In: Local Disk (E:)

File Name:

Files of Type: All Files

Fig. 4.2 Select particular folder

Step 3: Click on the image



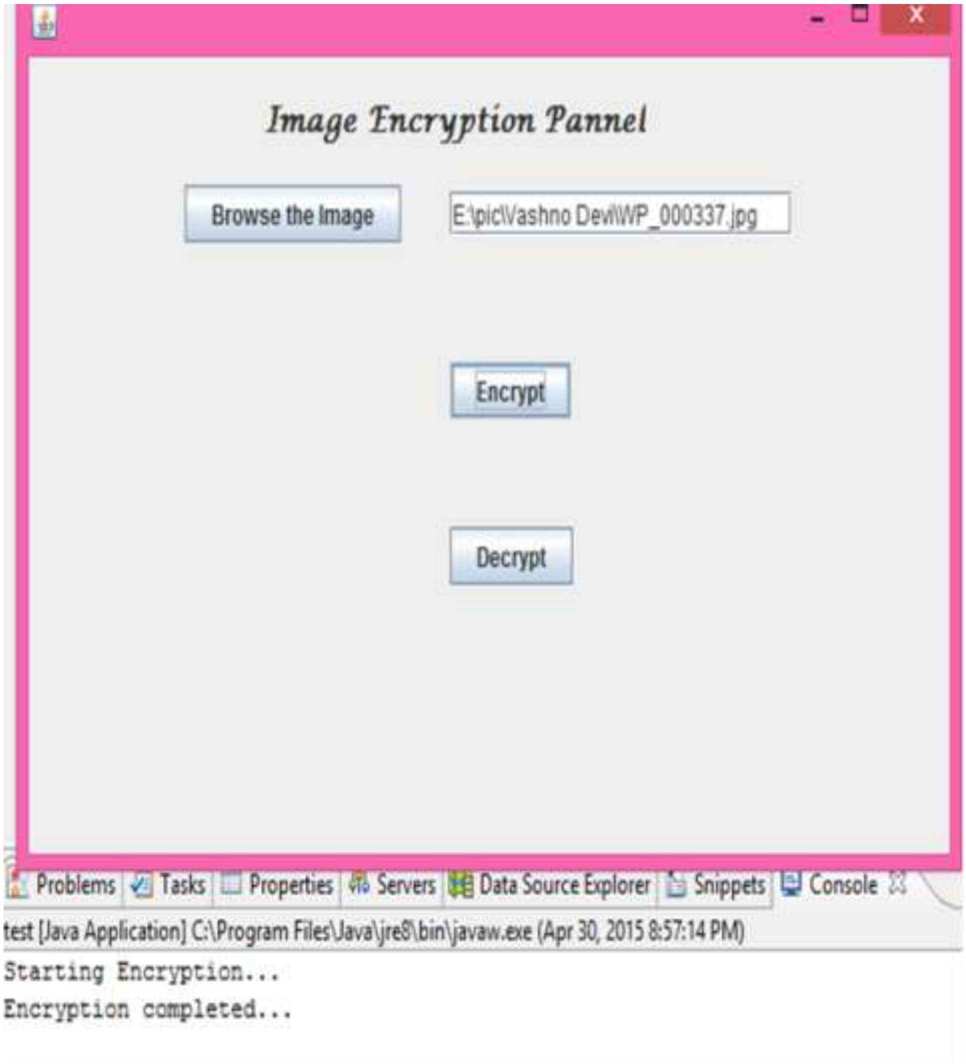
Look In: Vashno Devi

File Name: WP_000337.jpg

Files of Type: All Files

Fig. 4.3 Select particular image

Step 4: After selecting an image click on encrypt to start encrypting an image.

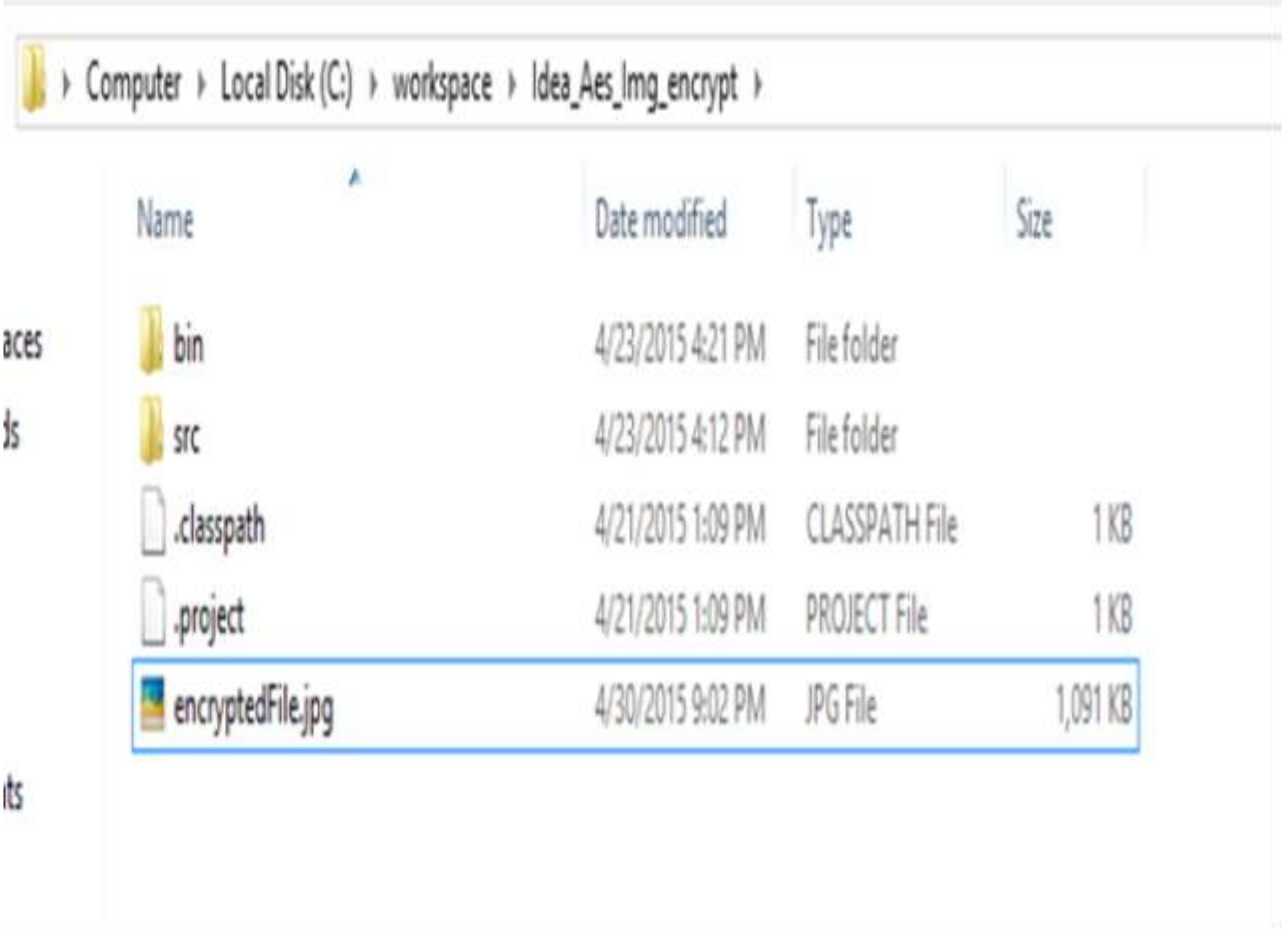


E:\pic\Vashno Devi\WP_000337.jpg

```
test [Java Application] C:\Program Files\Java\jre8\bin\javaw.exe (Apr 30, 2015 8:57:14 PM)
Starting Encryption...
Encryption completed...
```

Fig. 4.4 Click on encrypt to start encrypting an image.

Step 5: To see the encrypted file, select the encrypted file from the folder.

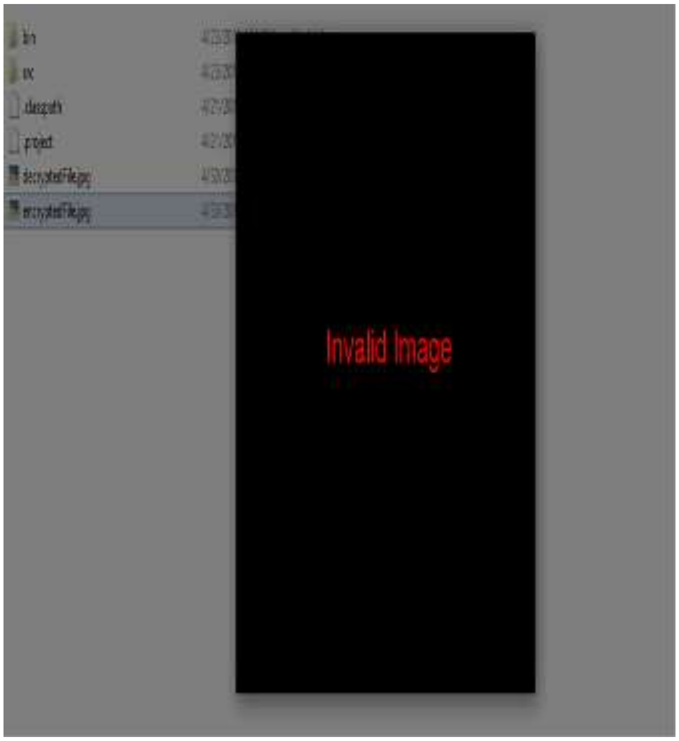


Computer › Local Disk (C:) › workspace › Idea_Aes_Img_encrypt ›

Name	Date modified	Type	Size
bin	4/23/2015 4:21 PM	File folder	
src	4/23/2015 4:12 PM	File folder	
.classpath	4/21/2015 1:09 PM	CLASSPATH File	1 KB
.project	4/21/2015 1:09 PM	PROJECT File	1 KB
encryptedFile.jpg	4/30/2015 9:02 PM	JPG File	1,091 KB

Fig.4.5 Select encrypted image to decrypt it

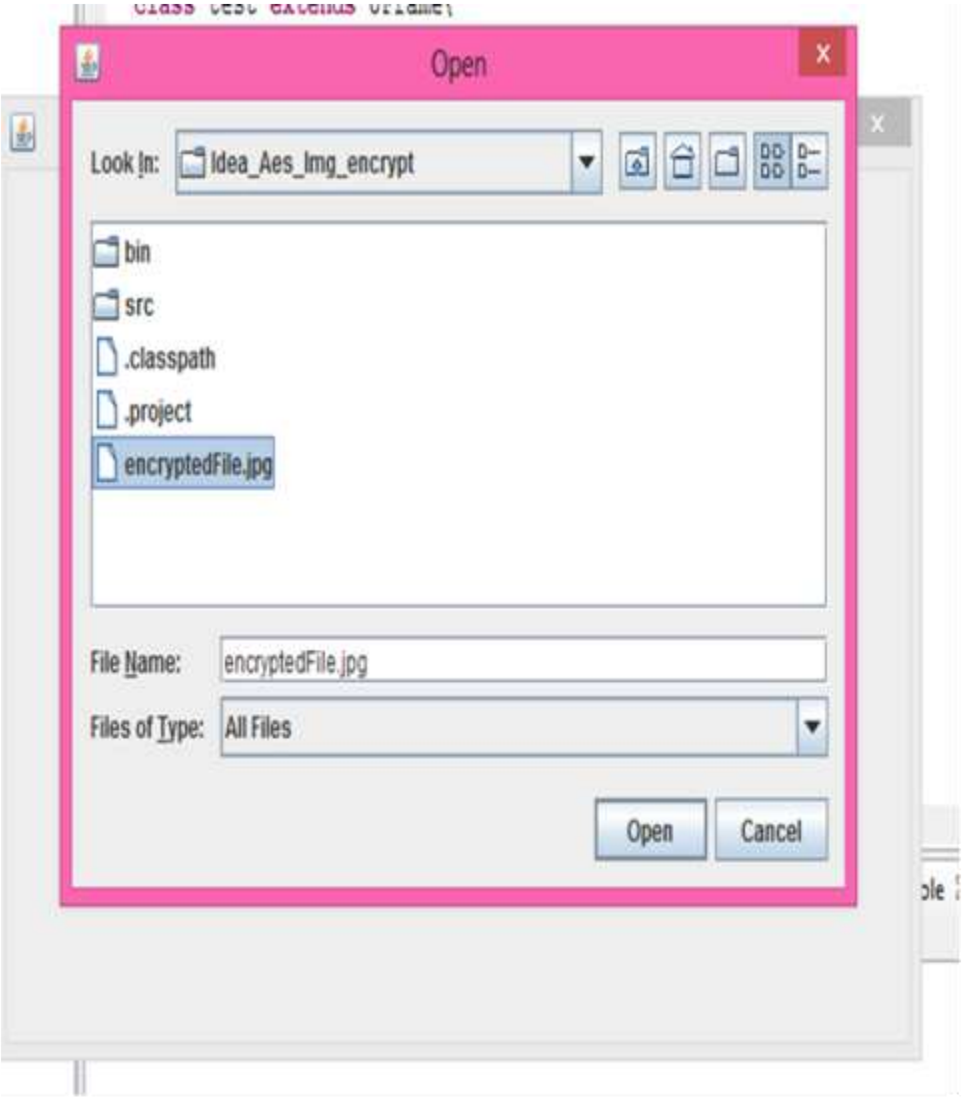
Step 6: This is the encrypted image.



Invalid Image

Fig 4.6 Screenshot of encrypted image

Step 7: To decrypt the encrypted image, select the encrypted image from the folder.



Look In: Idea_Aes_Img_encrypt

File Name: encryptedFile.jpg

Files of Type: All Files

Fig 4.7 Select encrypted image for decryption

Step 8: After browsing an image, click on decrypt to get the decrypted image.

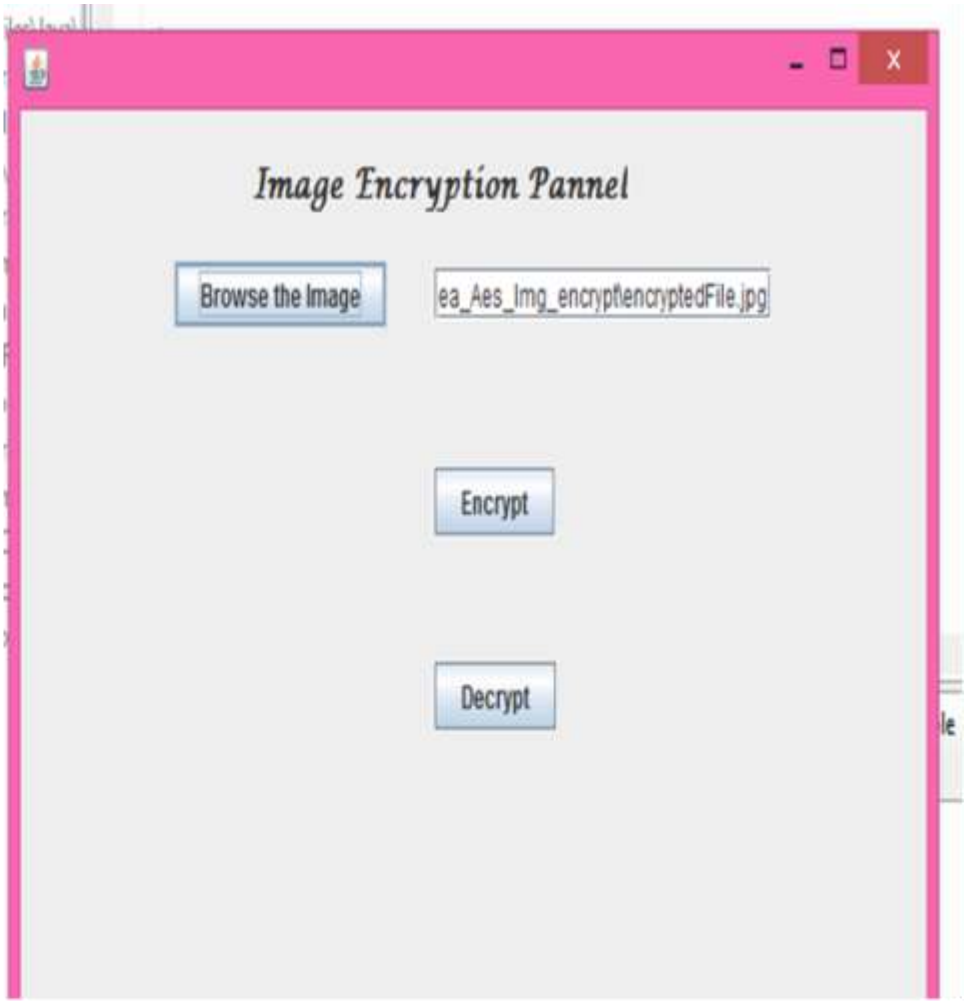


Fig. 4.8 Click on decrypt to start decryption

Step 9: Here is the decrypted image which was encrypted earlier.

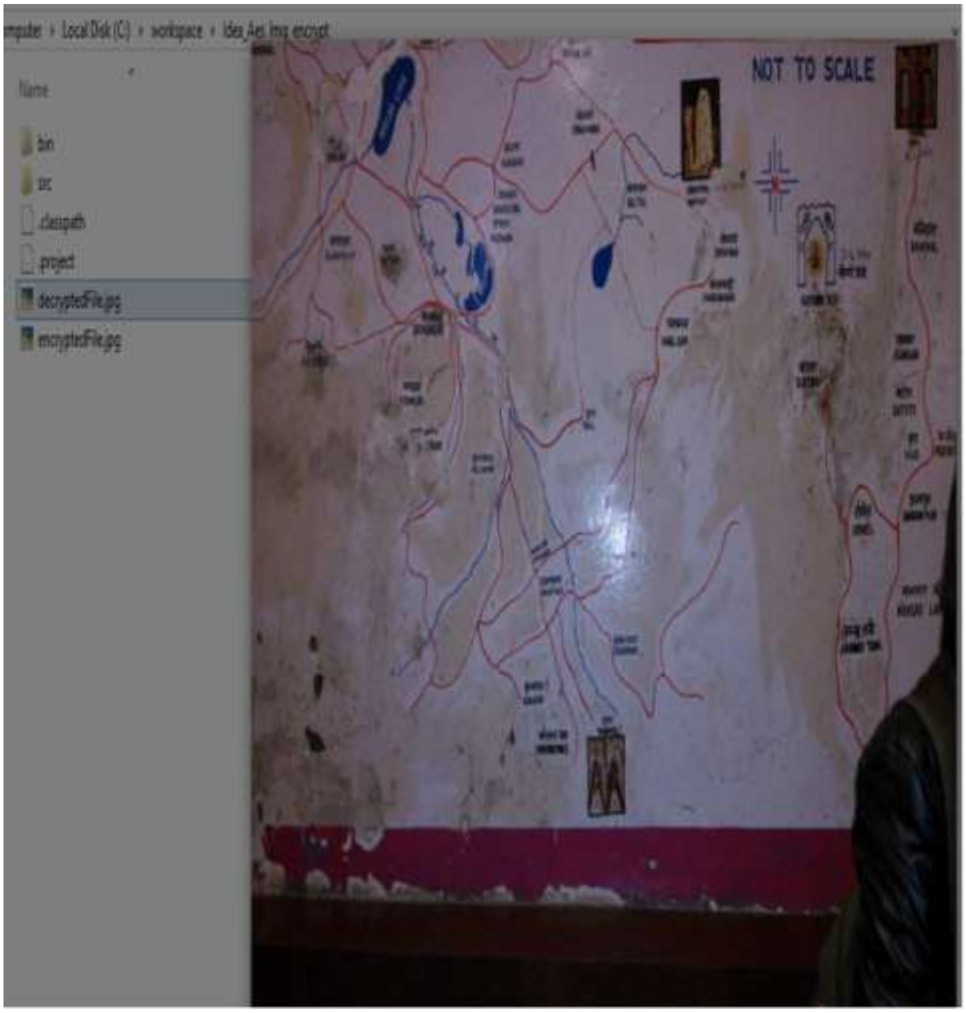


Fig. 4.9 Final decrypted image

Chapter 5

CONCLUSIONS AND FUTURE SCOPE

In this exploration image security and processing time is the primary concern. Altered AES is utilized to scramble the picture. Changes are done to the AES to build its performance and proficiency. To lessen the time utilization, the operations of shift row stage and mix column stage are lessened to odd and even parts. Last but not the least; the key will be produced utilizing IDEA to make the picture more secure for transmission over the web. Along these lines by applying every one of these progressions AES is required to diminish its encryption and decryption time and secure and faster transmission of picture will happen. Future scope is try to xored pixels of image to convert the image into single stream of data so that intruder cannot understand whether it is a data or the compressed image.

Chapter 6

LIST OF REFERENCES

[1] Babaei, Majid. "A novel text and image encryption method based on chaos theory and DNA computing." *Natural Computing* 12, no. 1 (2013): 101-107.

[2] Benrhouma, Oussama, Houcemeddine Hermassi, and Safya Belghith. "Security analysis and improvement of a partial encryption scheme." *Multimedia Tools and Applications* (2013): 1-18.

[3] Canright, David. "A very compact S-box for AES." In *Cryptographic Hardware and Embedded Systems–CHES 2005*, pp. 441-455. Springer Berlin Heidelberg, 2005.

[4] Daemen, Joan, and Craig Clapp. "Fast hashing and stream Encryption with PANAMA." In *Fast Software Encryption*, pp. 60-74. Springer Berlin Heidelberg, 1998.

[5] Dworkin, Morris. "Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices." *NIST Special Publication* (2010).

[6] Dworkin, Morris. "Recommendation for block cipher modes of operation: methods for key wrapping." *NIST Special Publication* 800 (2012): 38F.

[7] Ganesan, K., and K. Murali. "Image encryption using eight dimensional chaotic cat map." *The European Physical Journal Special Topics* (2014): 1-12.

[8] Gnanaraj, Jaspher Willsie Kathrine, Kirubakaran Ezra, and Elijah Blessing Rajsingh. "Smart card based time efficient authentication scheme for global grid computing." *Human-centric Computing and Information Sciences* 3, no. 1 (2013): 1-14.

[9] Harrison, Owen, and John Waldron. "AES encryption implementation and analysis on commodity graphics processing units." In *Cryptographic Hardware and Embedded Systems-CHES 2007*, pp. 209-226. Springer Berlin Heidelberg, 2007.

[10] Hermassi, Houcemeddine, Rhouma Rhouma, and Safya Belghith. "Improvement of an image encryption algorithm based on hyper-chaos." *Telecommunication Systems* 52, no. 2 (2013): 539-549.

[11] Norouzi, Benyamin, Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki, and Mohammad Reza Mosavi. "A novel image encryption based on hash function with only two-round diffusion process." *Multimedia Systems* 20, no. 1 (2014): 45-64.

[12] Rachh, Rashmi Ramesh, PV Ananda Mohan, and B. S. Anami. "Efficient implementations for AES encryption and decryption." *Circuits, Systems, and Signal Processing* 31, no. 5 (2012): 1765-1785.

[13] Rachh, Rashmi R., PV Ananda Mohan, and B. S. Anami. "Implementation of AES Key Schedule Using Look-Ahead Technique." *Circuits, Systems, and Signal Processing* (2014): 1-8.

[14] Wadi, Salim Muhsin, and Nasharuddin Zainal. "High Definition Image Encryption Algorithm Based on AES Modification." *Wireless Personal Communications* 79, no. 2 (2014): 811-829.

[15] Wang, Jing, Guoping Jiang, and Bing Lin. "Cryptanalysis of an image encryption scheme with a pseudorandom permutation and its improved version." *Journal of Electronics (China)* 29, no. 1-2 (2012): 82-93.

[16] Wang, Xingyuan, and Qian Wang. "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos." *Nonlinear Dynamics* 75, no. 3 (2014): 567-576.

[17] Zeghid, Medien, Mohsen Machhout, Lazhar Khriji, Adel Baganne, and Rached Tourki. "A Modified AES Based Algorithm for Image Encryption." *International Journal of Computer Science & Engineering* 1, no. 1 (2007).

APPENDIX

AES	Advanced Encryption Standard
RSA	Ron Shamir Adelman
DES	Data Encryption Standard
FFT	Fast Fourier Transformation
XOR	Exclusive OR
FPGA	Field-Programmable Gate Array
KW	Key Wrap
TKW	Triple Idea Key Wrap
K	Key
CBC	Ciphering Block Chain
CFB	Cipher Feed Back
ECB	Electronic Code Book
OFB	Output Feed Back
OTP	One Time Password
KEK	Key Encryption Key
DFT	Discrete Fourier Transform
ATM	Automated Teller Machine

SHA	Secure Hash Algorithm
RGB	Red Green Blue
IDEA	International Data Encryption Algorithm