PROPOSED AES USING STEGANOGRAPHY TECHNIQUE FOR IMAGE, TEXT AND AUDIO ENCRYPTION

A Dissertation submitted

By

Yojna Goyal
to
Department of Computer Science and Engineering

In fulfilment of the Requirement for the
Award of the Degree of

Master of Technology in
Computer Science and Engineering

Under the guidance of

Mr. Manmohan Sharma

(16073)

November 2014

CERTIFICATE

This is to certify that Yojna Goyal has completed M.Tech dissertation titled **“Proposed AES using Steganography Technique for Image, Text and Audio Encryption"** 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 fulfilment of the conditions for the award of M.Tech Computer Science & Engg.

Date:

Signature of Advisor

Name: Manmohan Sharma

UID:16073

DECLARATION

I hereby declare that the dissertation entitled "**Proposed AES using Steganography Technique for Image, Text and Audio Encryption** “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 for the work of any other degree or diploma.

Date: **Yojna Goyal**

Reg No. 11208077

ABSTRACT

Digital image processing is a broadly used in the area of research. Images are mostly used and Steganography of image means hiding the covert information into the cover information and transmit to the channel so eavesdropper cannot tell the existence. Encryption is used for programming the pixels of an image into something that cannot be understandable by unauthorized persons. Currently all the people needs only information so; it's a necessity to secure the (confidential) information. We introduce the concept of key expansion helps us against brute force attacks or arithmetical attacks with modified shifting of rows and mixing of columns. This method helps us to provide a good security and quality of encryption and decryption. Result shows that our proposed method takes less time for encryption.

ACKNOWLEDGEMENT

I would like to express my gratitude towards my thesis supervisor Mr. Manmohan Sharma, Department of Computer Science and Engineering, for his kind co-operation and encouragement which help me in completion of my work.

I would like to express my special gratitude and thanks to Mr. Dalwinder Singh, Head of Department, Computer Science and engineering, for giving me such attention and time providing me the opportunities for the completion of my work.

Yojna Goyal

RegnNo.11208077

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLE

Chapter 1

INTRODUCTION

1.1 Digital Image Processing

Digital image processing is the utilization of computer algorithm to carry out processing of the image on digital images. Basic Steps in the image processing are – Segmentation is dividing the images into parts and we do the improvement. Image enhancement is way to get the detail and features of the image. Contrast color of television increase gives great impact on the screen is the best example of image enhancement. Image restoration also compacts with the progress of image. It deals with mathematical and probabilistic value of the image.

There are two different ways of Image processing: Analog image processing and Digital image processing. By which Digital image processing has many overcomes on the analog image processing. Since it permits a broad range of algorithms that can be used in the inputting data and also avoid problems such as the increase of noise and signal distortion during processing.

1.1.1 Applications of digital image processing:

- Digital image camera changes the rough information to the colour correct image.
- It is used in intelligent transportation systems mainly in page number identification.
- Image processing is also used in Films.

1.2 Steganography

Steganography is the capacity of covering information/data in such way that avoid the exposure of covered data. By the combination of two Greek words we get the word steganography, who's precisely means "enclosed script." It takes a huge collection of undisclosed communications procedures that wraps the message's survival. The procedures are invisible inks, microdots, arrangement of characters and covert channels, digital signatures, and spread spectrum. Steganography and cryptography are different ways for hiding. Cryptography changes a message so it cannot be understood easily but we cannot hide its existence. Steganography covers the message so it cannot be seen without help of decoders. Information in cipher text may misguide brain of the recipient for some time, while “undetectable” information produced with steganographic procedures will not. After embedding the cover information in original image we get the stego image with the help of steganography.

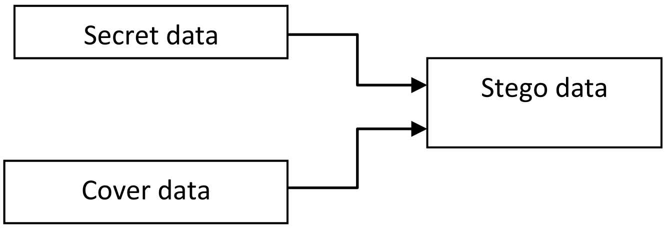


Figure1.1 Steganography Data

1.3 Why Steganography:

The main motive of steganography is to encode the data so we can represent the information in ordered format. We can exchange the bit randomly and information materializes shows that it is unique and true that cannot be detectable by most of the persons with naked human eyes. By this sender doesn’t feel that there can be any type fear from third party can use their secret information. And receiver can get the data secretly.

1.4 Uses of Steganography:

Steganography is only used for security purpose of information that we want to send to another side safely. There are basic elementary classes of steganography

a) Subliminal communication
b) Integrity and authentication
c) Illicit exfiltration

a) Subliminal communication: This type of communication hides that some information is transferred in a particular file. For passing the information from sender to receiver secretly hidden in one another type of information is wrapping as a single unit. The secret canal is a medium of transformation of information. There are number of ways to conceal a information: by adjusting least significant bit of pixel in a cover information.

b) **Integrity and authentication:** By using steganography technique we can say that our information is much more secure. Since nobody can alter any information till they can know the proper method of extracting the information. Integrity defines that our information is not altered by any other sources. Once you lock the data by sender key, it only provides the authentication to valid receiver to open and extract the original information from the file.

c) **Illicit exfiltration:** This can supply a large value of bandwidth communiqué channel which requires a complicated user to put into operation. It is special type of malware in an surroundings where unformatted files are downgraded to lower level class from high level security. The wrappers created are firstly downgraded and then information is carried out when file is transferred to a low protection area.

1.5 Applications of Steganography:

- **Private Communication-** Used in defence organisations for information exchange without knowing of third party.
- **Protection against information alteration-** Smart identity cards is used in which details of the persons are embedded inside the card.
- **Access Control-** Used for voting system to reduce toughness and increase safety.
- **Media Database Systems**- Used in Media Database systems so audio, video can transform.

1.6 Steganography techniques

Techniques are categorized as:

a) Spatial domain technique
b) Transform domain
c) Masking and Filtering

a) Spatial domain technique inserts message in the pixel's intensity honestly, simplest method used in steganography is least significant bit (LSB) which covers the most secret message in the LSBs without launching the appreciable alteration. This type of technique works on gray diagram. This type works for less data hiding ability. Mostly used Spatial Domain techniques are categorized as:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Random pixel embedding method (RPE)
4. Histogram shifting methods

b) Transform domain technique insert message in occurrence domain of last changed image. It is process of inserting data in the field of signal. Transform imaging strategy gather the information required for image renovation. In this, image information are recovered as well as image reconstruction for display are basically separated. More benefits of using it are image processing, cropping. Transform domain technique are categorized as:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).

c) Masking and filtering techniques works as paper marking technique. This covers the information into important area than the noise levels. Watermarking is most used technique in masking and filtering. This technique is having more robustness than LSB technique. This can be applied only to Grey Scale images.

Steganography is made to obtain improved quality of programmed image and to get better hiding capacity. This job is a kind of spatial domain technique. Every digital file layouts are used in steganography, but the designs with high redundancy are extra appropriate. Redundancy can be defined as object bit's which gives accuracy far better than required for the use of object and displays. Redundant object bits are those bits which can be changed with no modification being noticed simply. Specially Audio and Image records are satisfied with these conditions, even research also have naked files designs which can be used to keep data secretly. The four main types of file layouts in steganography are

a) Text: While the text files have a extremely less quantity of unnecessary information digital files are not often used.

b) Images: We are using images mostly to sent a information securely to send on internet.

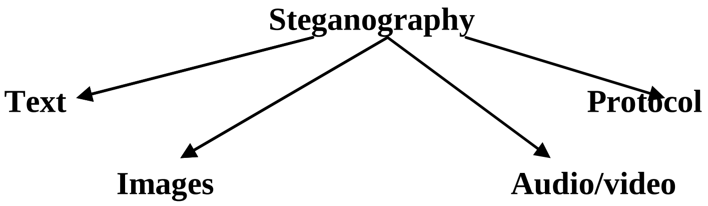


Figure 1.2 Types of Layouts of Steganography

c) Audio/Video: Are much difficult to embed and use.

d) Protocol: we embed data into the message and network control protocol is used to transfer.

To hide message in audio files it uses same methods as they are used in images. Another way used in audio steganography is masking with advantage of the human ear to hide message invisibly. A soft and clear noise becomes unfeasible to listen in the existence of another louder clear sound. By using these belongings channel is created, which was used to hide data. In steganography if the equal data is possible, the greater volume of significant audio files formulate them less popular to apply than images. The word protocol steganography submits the method of implanting information within messages and system control protocols used in system transmission. In OSI network model covert channels are existing in which steganography can be applied. Example is when we hide the data in the heading of the TCP/IP package in various areas that are optional or not anywhere used. Initially it was consideration that steganography will not be feasible to apply with JPEG image, because they applied lossy compression whose outcomes in portion of the image data being changed. The chief characteristics of steganography are the actual message is unseen in the redundant object bits because unnecessary bits are absent while using JPEG. It was panic that the secret information would be smashed. Although one can carry the message and break it into different parts it would be very complicated to implant the message in which changes are not detectable since we have used harsh compression. The compression algorithm properties have been broken in order to produce a steganography algorithm for JPEG. JPEG is broken into parts so we can modify to images which cannot be seen by human eyes. Steganography uses different techniques for encryption. Those techniques are:

1.7 AES (Advanced Encryption Standard)

AES is Symmetric block cipher which is generated to substitute the DES which use the 128 bit block and key size is of 128,192,256 which function with the fixed number of bytes. In AES same steps are repeated multiple times.AES is a process espoused by the U.S. government National Institute of Standard and technology.AES is a reversible process which will perform encryption and decryption in reverse order. This is symmetric key algorithm. The AES algorithm works on bytes with simpler implementation. This key is stretched into single sub keys, a sub keys for all function round. This process is called Key Expansion. Four steps are performed for functioning again and again are

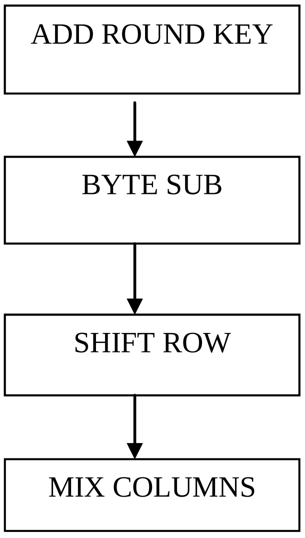


Figure1.3 Flow Diagram of AES

1.7.1 Add Round Key

In these sixteen bytes of the current state is XOR with the sixteen bit of key for extended key for the state. Expended key is not reused again. By the subsequent time byte 17 to 32 are used as add round key and XOR to the current state.

1.7.2 Byte Sub

We obtain the values of s-box from multiplicative inverse. For avoiding attacks on mathematical based while doing encryption we will replace all the value by using S box values corresponding to it. When we are decrypting us can use inverse s-box table for it to get revert back all the values.

1.7.3 Shift Row

By performing this step we can control on rows. Firstly we will order the value into the matrix for AES where first row will be constant and shifting of next rows is done episodically. As second row will do one byte shift and third will perform two byte shift and fourth will do three byte shift to left. For block of 128 bits as well as 192 bits pattern of shifting is similar. Rows are always shifted to cyclically to same pattern.

1.7.4 Mix Columns

Multiply the values of first column mean four byte and first column of other matrices. And by finding all the corresponding values will create circulation.

1.8 Modified Advanced Encryption Standard (AES)

They uses the 128 bit plaintext as sixteen 8 bit byte. MAES is a byte oriented and improves the security of the AES. In Modified AES Shifting of rows is performed which defines that security level is achieved by using the steps of Transformation in Modified AES are:

a. Add Round Key: Round Key is added to execute the XOR among given state with the round key.

b. Sub Bytes: Sub Bytes is a replacement of all byte from S box in the current state.

c. New Shift Row: The Shift Rows is executed; firstly write into the form of matrix. It regularly rotates the bytes based upon the initial element of state. The value of first row and column of the current matrix is even then first row values remain unchanged; and all bytes in all the rows are regularly shifted over different numbers.

d. Mix Column: In this, every one column of the current state is develop with a fixed polynomial

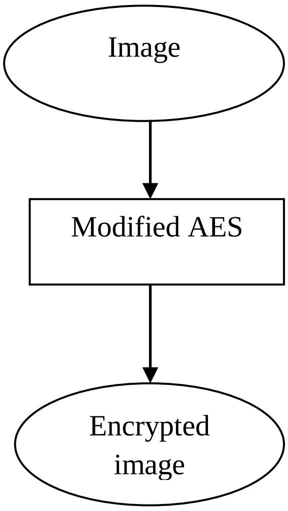


Figure 1.4 Image Encrypted

1.9 Least Significant Bit Substitution (LSB)

LSB is simple widespread technique used in steganography to embed information The least significant bit i.e. 8 bit of some bytes contained by an picture are altered to a bit of the covert message. In every pixel, 3 bits are saved. Example a system has 3 pixels of a 24-bit image can be like this:

(00011101 10011100 01011100)
(00100110 10000100 00011100)
(11000010 10001101 01101011)

Let us take the figure 201 as message, which binary representation is 11001001, is settled down inside the least significant bits of the image, the results after converting are :

(0001110**1** 1001110**1** 0101110**0**)
(0010011**0** 1000010**1** 0001110**0**)
(1100001**0** 1000110**1** 01101011)

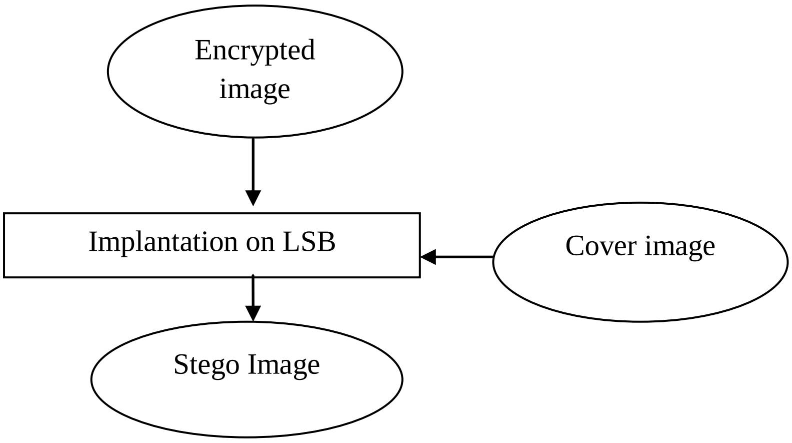


Figure 1.5 Steganographic image with LSB

Chapter 2

REVIEW OF LITERATURE

Smitha Suresh, Dr.KChitra, Deepak.P[1] (2013) describes a video observation system is popular to ensure security in major areas. Current video observation system analyzes the tracking of multiple human in the video. The difficulty of detecting moving targets in crowded scenes is one of the most challenges in this system. Occlusion is defined as an object which hides another object by multiple human tracking in a one/series of frames. Occlusion detection and handling is an important and main objective of the planned work is to detect occlusion. In this, patches in each object are used to identify the parts which are going to be occluded. The system can find the occlusion between humans in a scene and can recognize the occluded parts of every object. Goal is to develop a observation system that is free from occlusion. Occlusion is verified by calculating the distance between the centres of mass of both objects and if the difference in a frame is zero, and then object is occlusion.

Mr. Arjun R. Nichal, Mr. Vinod B. Kumbhar[2] (2013) describes that data like image, text, audio are encrypted then embedded into another data with the key.. Data is entered secretly to maintain its confidentiality. Firstly, images are converted into binary images then key is XOR with it encrypted image is formed. And secret image are XOR with key we get encrypted secret image. Encrypted Secret image is embedded on the eighth bit of the encrypted cover image. By same inverse process decryption is performed and result are defined on the basis of high PSNR value, number of bits embedded (NBE), Embedding Capacity(EC). This work provides a strong result of steganography.

G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan(2013) describes that digital media has various advantages like editing, compassing in high quality data. So that, Steganography helps sender to send the data to receivers by using some techniques so that nobody can know that document contains confidential data. By this paper, we read Steganography technique and steganalysis technique from which we conclude that LSB to easiest method used as embedded message. The author says that there are two main stages one is data embed and other is data extract for transferring the information. In this, plain text is encrypted and then edge detection is performed on the image using Least

Significant bit, now merge the plain text with image and result obtained will be stego image. For saving arithmetical and diagrammed features we use this method.

Jaspal Kaur Saini[3] (2013) describes that there exist different algorithm in today's world to secure our communication on the internet in multimedia. In this we will combine the encryption steganography. Firstly, data is encrypted using modified AES by making change in shift rows and then steganography the data by using LSB technique which makes 8 bit encryption. This method helps to increase the security and improve the quality. MAES is byte matrices. We convert bits of plaintext into bytes of eight bit combined. Cyclically shifting of bytes of all rows is performed by watching in first element. Results are shown by the help of calculating PSNR and MSE.

RigDas, Themrichon Tuithung[7] (2012) describes encoding technique is used, where two different eight bit grey color images are taken one is wrap image and other is confidential image of different sizes M*N and P *Q. Encoding is executed on confidential information earlier than embedding and every bit of code is inserted in the wrapped image by changing the LSB of every pixel strength of wrapped image. Size is obtained of confidential image and multiplied by eight for image of eight bit, also calculate the Huffman table of confidential image. Huffman encoding bit stream is found and size obtained .Now modify the LSB of wrapped image of all bit of Huffman encoded bit stream and obtained stego image turn into more secure information for recipient. This algorithm achieves a large value of capacity and high-quality of invisibility. This technique has large capacity with fine invisibility and PSNR (Peak Signal to Noise Ratio) of Stego image had shown better results with wrapper class. Quality is also improved and suitable safety is maintained as the hidden image could not taken out lack knowing of knowledge of the decrypting policy also Huffman tables. Size of secret image lies only inside the stego image and decoder should be known to the Extract method to pull out the hidden image.

Amit Asthana, Sherish Johri[8] (2012) describes the two main areas of research are Steganography as well as Steganalysis. Steganography introduce a message into a cover media and hide its presence. Hackers utilize Steganalysis method which hits Steganography by recognizing the hidden message and extracting. At first novel picture and Text document of confidential information is selected**.** Stego Key is used for safety and dispatcher and recipient knows that .If the receiver knows the Stego key then only decrypts the hidden message. By using Alteration Method with Palette Based Images we insert the data and key into the image. Now obtain all pixel and characters from file and key .Decide the 1st pixel and select character and put in the first part of pixel. Like this place all in next. Put a few identification signs and insert the all characters, at the end place some signs. Palette Based Images are used for hiding original information into information. The transferred information of bits is there into the expanded palette of image without knowledge of others.

M.Grace Vennice, Prof.Tv.Rao, M.Swapna, Prof.J.Sasi kiran[9] (2012) describes steganography launches by screening a top secret message and cover message so third party cannot get the correct information. It is added with cryptography for lager security point of view in communication means. This paper includes text based steganographic methods and overview of manuscript steganography was introduced and problem defined in this paper is in the part of steganography of text and problem is resolved by using by inter word spacing along with inter paragraph spacing when a hybrid procedure is used. Four different steps are performed: first is registration to defend the law that person using is right present in the records and then Encryption if text message in the structure of the bit design identification method. The designed method gives forceful stego text with another six alternatives of supreme capacity based on length of hidden message.

Vijay Kumar Sharma,Vishal Shrivastava[10] (2012) describes that steganography permits people to communicate confidentially by information hiding. Mostly information is released to hacker's by using steganographic tools hidden in files. In last few years, steganalysis algorithm is introduced which is used to find stego communication by static examination of pixel value to guarantee security, a new Steganography algorithm for 8 bit – 24 bit is represented by logical operations. In this we perform extraction of pixels, character and keys known as pixel array, character array, and key array. By selecting the first pixel and character array and store it in the pixel starting component and rest all are stored like this. Store zero at the end so that can define our terminating point. In this on secret image is taken MSB of underground image is merged into LSB of original image by decreasing the computational complexity so that stego image cannot be detected.

Yongzhen Zheng, Fenlin Liu, Xiangyang Luo, Chunfang Yang[11] (2012) describes steganography trustworthy detection is important and how we can verify the steganography software based on the individuality of the steganography algorithm. From this paper we conclude that the morality of LSB Steganography algorithm which involves LSB Replacement and LSB Matching and suggest an advance method to classify steganography software by attribute similarity matching. The procedure of pixels changing considered as a feature in the LSB steganography algorithm is a important commands, and then they find out whether LSB steganography software according to the presence of the codes coordinates with the attribute.

Anil Kumar, Rohini Sharma[12] (2013) describes security of information is most important in past few years. We always want to send the data without showing it to anyone. In this paper we combine the RSA Algorithm with Hash-LSB for the purpose of the security. We first encrypt the secret information using RSA method then on the other hand we will find RGB pixels of cover image. And estimate the value of LSB of the cover image. By applying the hash function to get the position that where we can embed the data. We will embed 3, 3, 2 to the in Red, Green, and Blue, since blue colour gives more chromatic influence so only two values are changed. After obtaining the position we will embed the secret message into the values the after that we obtain the Stego image. This method helps to increase the PSNR value and Low the MSE value which improves the quality of the image.

H.B. Karaman, s.saguroglu[14] (2012) describes the different types of methods are used and compared to each other in steganography with which simplicity and robustness are used. The techniques used in steganalysis to find different types of steganography like images, audios/videos and file system steganography are scanned. The unique information of the visitors are encoded and introduced in the images using LSB technique on BMP images. Stego images and original images are evaluated with each other after the implantation process and the strength is measured against steganalysis violence using VSL tool.

Neda Raftari and Amir Masoud Eftekhari Moghadam[15] (2012) describe novel image steganography technique joins the Integer Wavelet Transform (IWT) and Discrete Cosine

Transform (DCT). In this confidential image is launched in frequency domain of wrapper image coordinated with feature by using Munkres' assignment algorithm, with addition of the confidential image in various coefficients of wrapper image groups for instance horizontal detail, vertical detail and diagonal detail and monitor the result of implantation on the presentation of stego image in Peak Signal to Noise Ratio (PSNR), which demonstrates large robustness adjacent to six various attacks. This process is scanned with wavelet based steganalysis algorithm also.

Prabakaran. G, Bhavani.R[16] (2012) describes that undercover image is inserted into the wrapper image by using such method that its presence is invisible while transmitting. In this a suggestion is to modify scheme of secreting a large-size undercover image into a small-size cover image to secure and high capacity based steganography scheme. Arnold transformation is executed to jumbles the undercover image. Discrete Wavelet Transform (DWT) is executed on both images which were tracked by Alpha blending operation. And behind this Inverse Discrete Wavelet Transformation (IDWT) is executed to obtain the stego image. The results of our design are checked by evaluating different qualities of the stego image with wrapper image. The result explains algorithm for transforming steganography is extremely secured with its strength.

R Praveen Kumar, V Hemanth, MShareef[19] (2013) describes a Communication medium used in these days is internet and hackers are present there to cut the information transferred through various channels, Information is encoded so that third party cannot understand it and by using cryptanalysis data is again retrieved to original form. Main problem is that by cryptography visual is present of data transferred but by using Steganography transformation technique generates noise in image transferred to remove that noise we uses a LSB insertion method and then confidential message is compressed and sent by wavlet transform technique. When compression is done then bits are encrypted In this paper, text is firstly compressed then encoded, after that LSB insertion takes place and finally stego image is obtained.

Mahmud Hasan, Kamruddin Md. Nur, Tranzee Bin Noor[21] (2012) describes that Steganography can used in images, audio signals due to higher redundant data easy use in different transmission medium. From this paper we conclude that cover image is retrieved to its original image after pulling the secret data. So we use Lossless and reversible

Steganography techniques overcome this type of problem. Mainly use of the reversible Steganography technique, trustworthy lossless technique is a great challenge. This technique has high capacity to store data in location based compression domain. This techniques is based on monochromatic images straight forward cryptographic approach is used and bit stream of the location based compression algorithm to hide characters

B.Subramanyan[22] (2011) describes that use of internet and communication methods via sharing the images can’t be avoided. We design a real time application which takes less power and security of level increases. This paper defines a process which bitwise operates of image pixels along with time. Keys are generated at both side and initial keys is any shared between them. Configuration of round constant values takes place then shifting of rows takes place by using s-box and inverse of s box table. This method helps against brute force attack. And at the end they concluded that this method takes less time than other methods.

Chapter 3
PRESENT WORK

This part represents the way for safe communication of the different data or media like images, audio or video can be thing of hiding information method. The main solutions to justification on Medias are cryptography and steganography. The major variation among these procedures is that Steganography aims to hide the presence of information in any valid information transformation without awareness of any third party then the sender and receiver. Encrypted images contain the secret information which can be extracted after performing decryption step. Cryptography only hides the information but third party can detect that sender must be sending the important information.

Steganography: The function of steganography is to insert media into an image in such a manner that nobody can detect that there can be any hidden information transferred via sending the information the following necessities are:

1) Changes should not be noticeable to the naked eye.

2) Recoverable easily by computer program.

These requirements and the performance of image data come up with some properties that Steganographic algorithms must suit:

- Security - The capacity to defend against any type of assault whether passive, active, or malicious.
- Embedding Capability - The utmost amount of bits which can be concealed in a given media file.
- Information Extraction - Whether another party has a duplicate copy of your original file.
- Statistical Undetectability - The chances of identifying a steganographic method based off suppositions.
- False Alarm Rating- The chances that an algorithm will find and inform the existence of hidden information when there is no one.
- Stego Key - Opportunity of inserting the covert information into the cover information by taking advantage of any predefined algorithm.

Proposed AES (P AES)

Combination of Key expansion + M AES + Mixing of columns

We will proceed step by step-

1. **Key Expansion:** In this we take simple grey intensity picture of size pxq, where pxq are pixels of the image. Let's say we will encrypt the image as set of sixteen pixels. By this number of keys used to encrypt the image are n=2*{(p*q)/16}.Formation of Rcon values takes place by its earlier key itself and transpose of Rcon will give better values. Using Inverse of s-box will develops the non linearity in expansion of the key.

2. Sub Bytes modification: In formation of key expansion for input we will perform the formation of R-con values. Using inverse S box for key expansion

3. New Shift Row: The Shift Rows step is executed on the rows of the condition. It regularly Shifts the bytes of each row depending upon the first element of state. If the value is even rotate first row first column to left. Second column second row to left no change in the method, but rotate third row third column to left will not be performed.

If odd rotate first row first column to left. Second row second column to will not be performed. Third row third column are shifted to the left. This means that when state table element has even and odd values one step will not be performed hence it saves the time.

4. Mix Column: In the Mix Columns step, we will define the reducible polynomial.

- Find the inner vector product with the sum of correct row vector.

-Multiply (G F (2^8)) as polynomial multiplication such as the polymultiple(inner vector, state of in matrices , column state)

-Finally, BitXOR (temp state, polystate)

3.1 Problem Formulation

For steganography lot of methods has been given but none of method have capability to encrypt and perform steganography as a generalized method such as hiding audio, image and text in a single file. Thus, this particular problem needs to address with a particular method that not only perform this task but also reduces the complexity in the process.

So, we modify AES with the help of key expansion, mixing columns modification, shift transform to increase the encryption level of the input. But to make the input more secure and to reduce the number of rounds that depends on the key size used for an AES cipher which indicates the number of replications of transformation rounds that convert the input into the final output, an algorithm is to be proposed which will simultaneously modify the key expansion rounds, shift transformation and mixing columns so as to obtain a more encrypted and to reduces the encryption time.

3.2 Objectives

- To propose a generalized technique for text, audio and image in image media.
- To encrypt the digital image to securely transmit over the network.
- To reduce the consumption time for encryption and steganography.

3.3 Research Methodology

This part explains the research methodology phase. A block diagram of proposed algorithm is presented below: This is explained in 4 phases. The first phase is Modified and Bit Rotational Technique. As discussed in the problem definition, a secure algorithm is required for increasing security of images so, an algorithm is proposed for secure image encryption and that is:

3.3.1 Encryption

1. In this first we will enter the image which will be used as cover image known as input image.

2. Checks that message to be inserted as secret information is image, audio or text.

3. Check if first component is Zero then secret information is image. Now find the RGB values of pixels of secret message.

- Place vertical fusion in RGB in cover image.
- Enter the secret key which passes through Proposed AES.
- We will obtain the encrypted stego image.

4. Check if first component is one then secret information is audio, convert 8 bits of pixels into values and place it in RGB channel of carrier image.

- Enter secret key which passes through Proposed AES.

- By this we will get encrypted stego image.

5. Check if first component is Two then secret information is Text , now convert the text data into ASCII values.

- Place in the RGB channels of the cover image.

- With the help of secret key we will pass it into Proposed AES.

- Stego Image is obtained which will have cover image as well as text data.

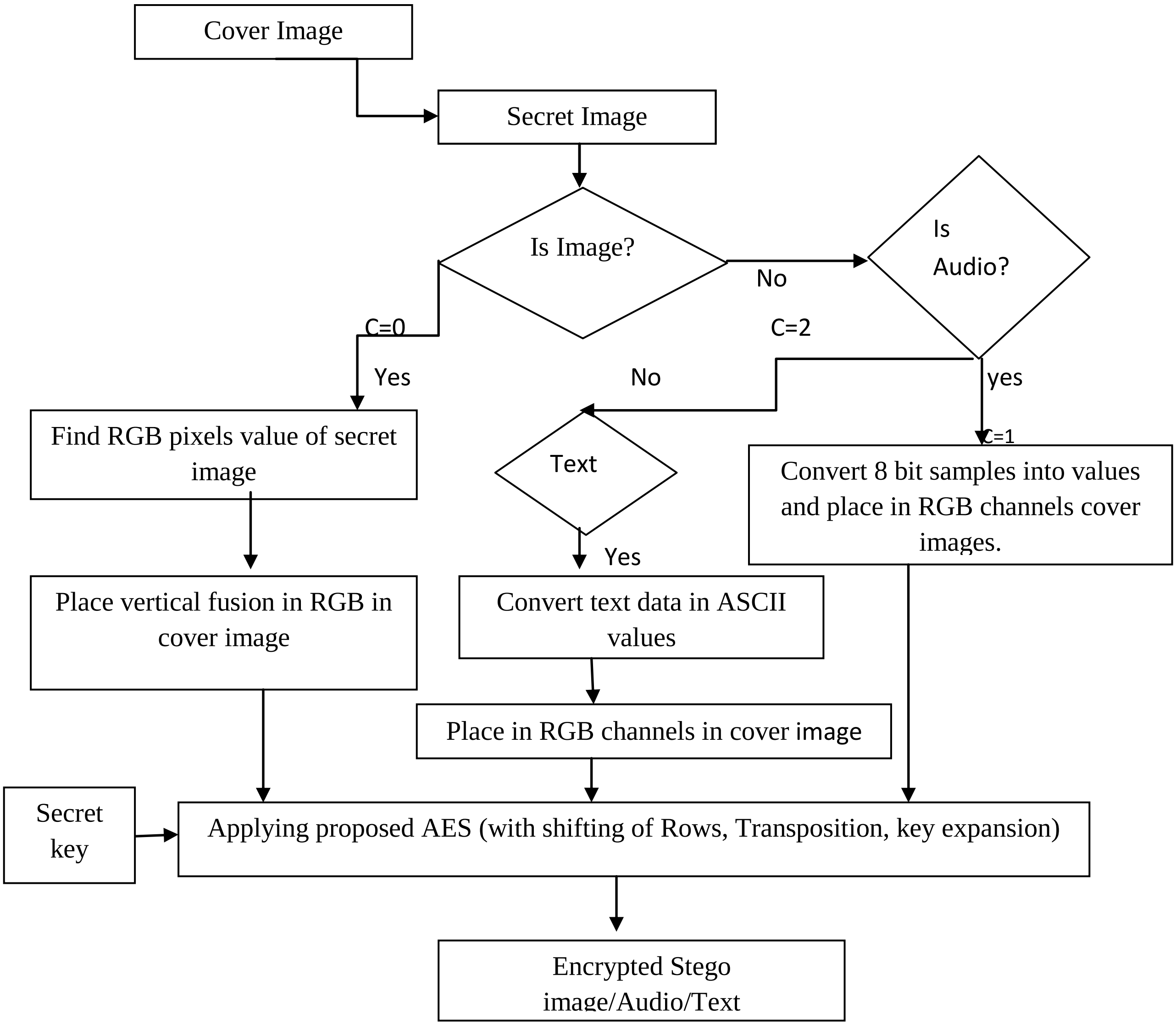

Cover Image
Secret Image
Is Image?
No
Is Audio?
C=0
C=2
Yes
No
yes
C=1
Find RGB pixels value of secret image
Text
Convert 8 bit samples into values and place in RGB channels cover images.
Yes
Place vertical fusion in RGB in cover image
Convert text data in ASCII values
Place in RGB channels in cover image
Secret key
Applying proposed AES (with shifting of Rows, Transposition, key expansion)
Encrypted Stego image/Audio/Text

Figure3.1Block Diagram of Proposed Work For Encryption

3.3.2 Decryption

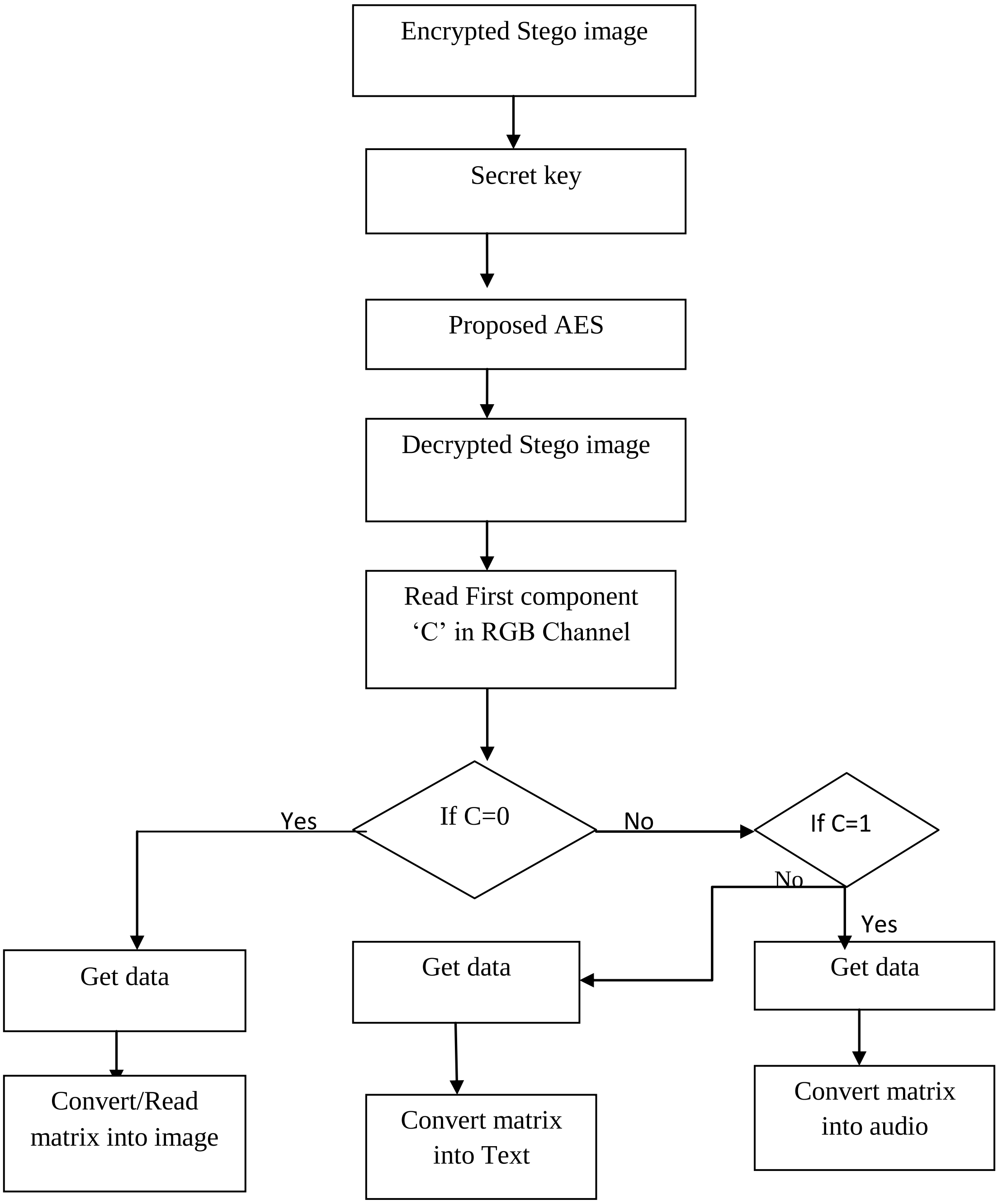


Figure3.2 Block Diagram of Proposed Work for Decryption

Chapter 4
RESULT AND DISCUSSION

In this section, the results of the planned work are shown by using MATLAB tool. MATLAB is considered as MATrix LABoratory with use of vectors and matrices with interactive mathematical working out environment. It is considered as easiest programming apparatus which speeded up the progress of assignment with older languages , c + + or java. MATLAB is used with different numbers of applications image processing and video processing, test and measurements and functions linear algebra, Fourier integration.

We use the two different metrics for evaluating the propose work is Peak Signal-to-Noise ratio (PSNR) and Time Computation. The proposed work shows the comparison of time computation with Modified AES in shifting of rows, Key expansion and Proposed algorithm.

We will show that PSNR value increases by which we can say that quality of our image will be better. The results consist of original image, encrypted information, encrypted image and decrypted image

There are a few results shown by using the defined method with the help of MATLAB.

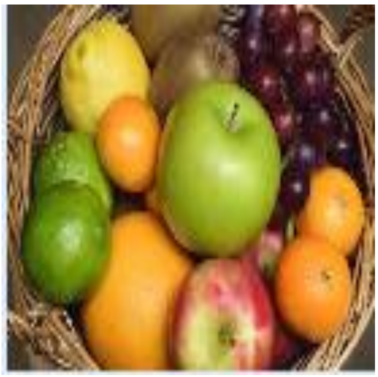


Figure4.1 Cover Image

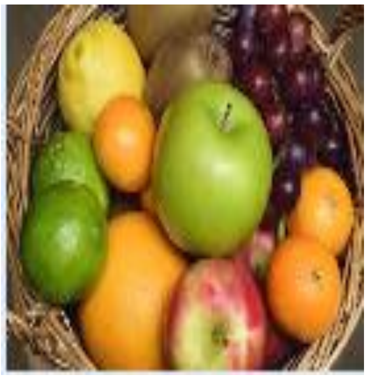


Figure4.2 Cover image with secret data

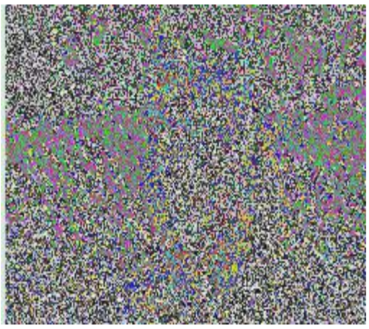


Figure4.3 Encrypted with PAES

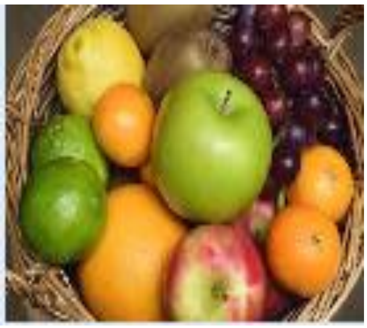


Figure4.4 Decrypted Image

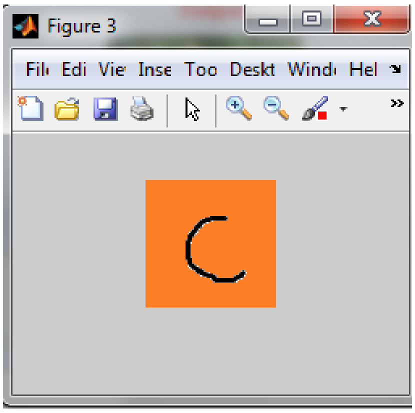


Figure4.5 Extracted hidden data

Figure 4.1: Input image named “images.jpg” from imaging.nikon.com.

Figure4.2: Input image contain secret information named (“hide.png”)

Figure4.3: Image Encrypted using proposed AES.

Figure4.4: Decrypted Image we obtain after decryption process.

Figure 4.5: Extracted Secret Image receiver obtained after performing decryption.

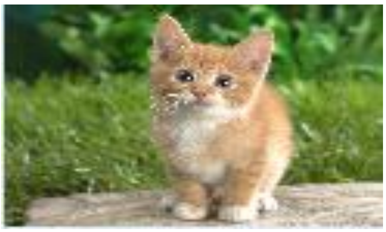


Figure4.6 Cover Image

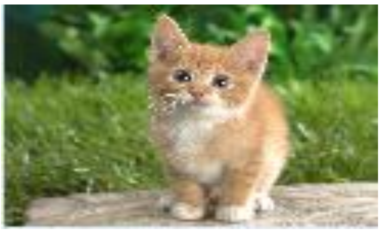


Figure4.7 Cover image with secret data

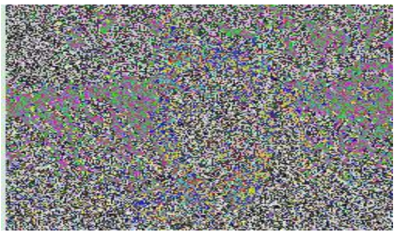


Figure4.8 Encrypted with PAES

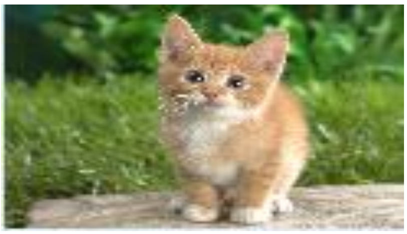


Figure4.9 Decrypted Image

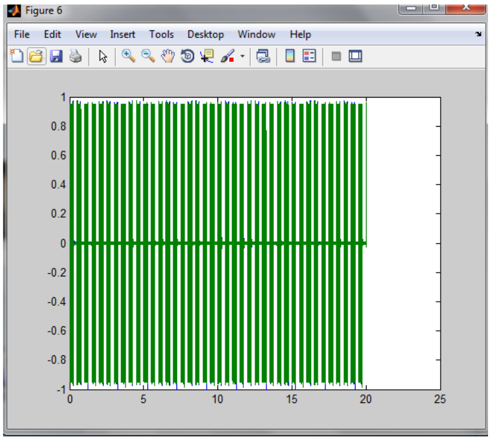


Figure4.10 Extracted hidden data

Figure 4.6: Input image “33.bmp”.

Figure4.7: Input image contain secret information (audio named”Signaltone4.wav).

Figure4.8: Obtained Encrypted Image with proposed AES.

Figure4.9: Decrypted Image obtained.

Figure 4.10: Extracted Secret Audio received by receiver.

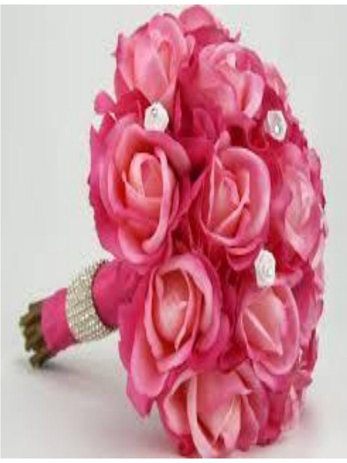


Figure4.11 Cover Image

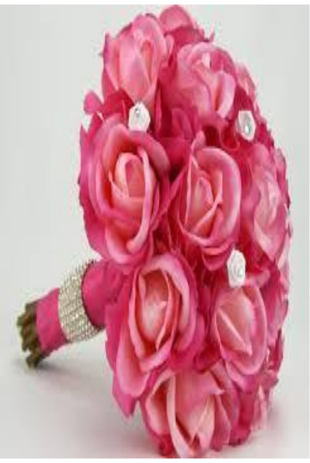


Figure4.12 Cover image with secret data

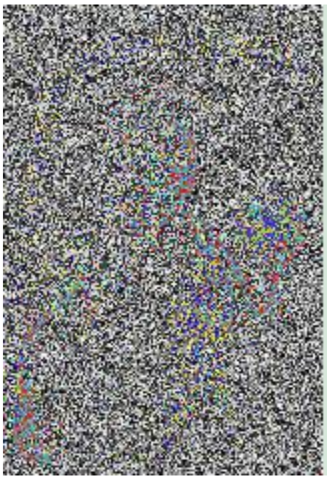


Figure4.13 Encrypted with PAES

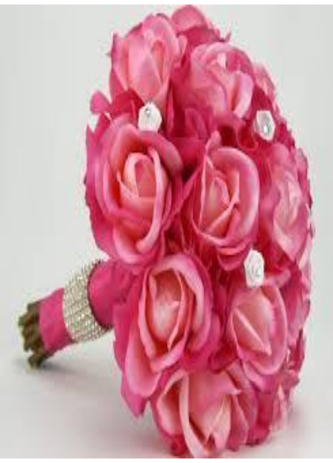
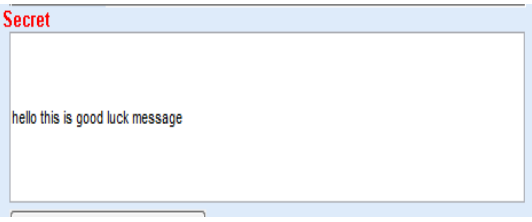


Figure4.14 Decrypted Image



hello this is good luck message

Figure 4.15 Extracted Hidden data

Figure 4.11 represents the input image is “index.jpg” from www.fanpop.com

Fig4.12 Shows cover image embedded with secret information Text written as (“hello this is good luck message”).

Figure 4.13 presents encrypted image that passes from PAES.

Figure 4.14 shows obtained Decryption results on “index.jpg”.

Figure 4.15 presents image represent text message transmitted as secret information.

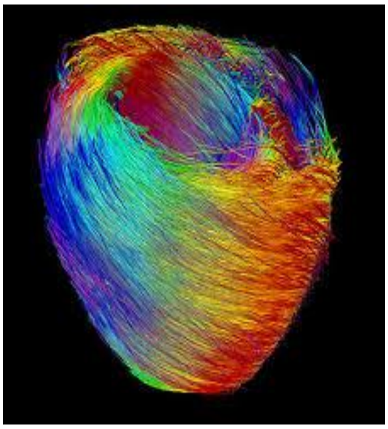


Figure4.16 Cover Image

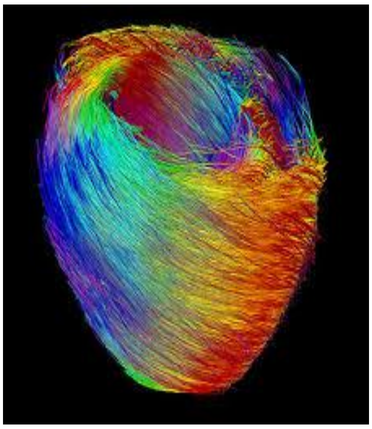


Figure4.17 Cover image with secret data

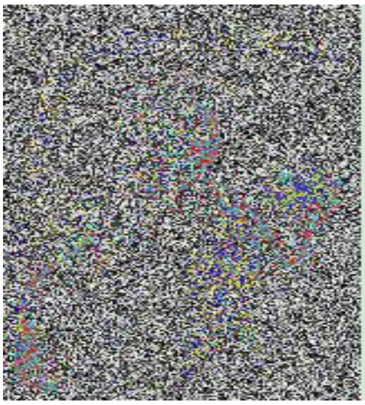


Figure4.18 Encrypted with PAES

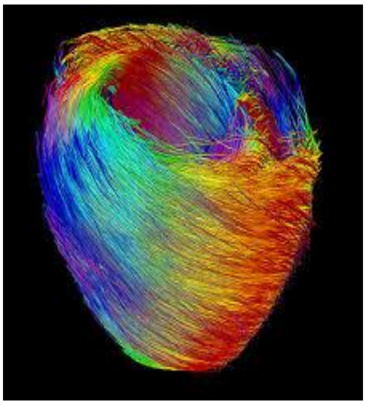


Figure4.19 Decrypted Image

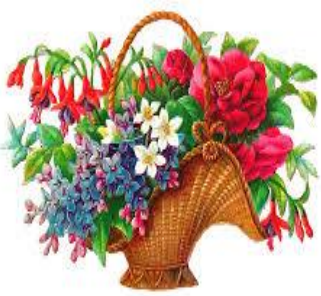


Figure 4.20 Extracted Hidden data

Figure 4.16 represents the input image is “art.jpg” from www.ucl.ac.uk.

Figure4.17 Shows cover image embedded with secret image (“flower.jpg”)

Figure 4.18 presents obtained encrypted image that passes from PAES.

Figure 4.19 shows obtained Decryption image at the receiver side.

Figure 4.20 Shows image as secret information obtained at receiver side.

To present that our enhanced system will take less time than our previous system. Here time consumption values for different media:

Cover image	Secret data	Previous time	New time consumption
Cat.jpg	Text	21.614	17.342
images.jpg	Hide.png	2.1407	1.3774
Cat.jpg	Filewatermark.wav	14.3217	14.2397
Dog.jpg	Hello this is dog	5.1906	2.71312
Dog.jpg	Msg.jpg	4.4442	2.5234
33.bmp	Signaltone4.wav	9.7839	8.4431
index.jpg	Hello this is good luck message	2.1322	1.3185
art.jpg	flower.jpg	2.0806	1.3013
Tom.jpg	Sample.wav	4.1465	3.6326

Table 4.1: Compute time

Chapter 5

CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

Steganography is different from cryptography since steganography is able to conceal the existence of information in cover media whereas cryptography is not able to hide the existence. We use the steganography to hide the different media like Text, Audio, Image in a single media i.e. image media. In this first we are performing steganography and next encryption.

For our second aim of dissertation we use the Modified AES algorithm which will be combined with the Modified Key expansion. This method helps us to create the strong system for the security purpose of the different Medias in single media. By which we are able to encrypt the digital image to securely transmit over the network.

We have concluded that when we take image “Cat.jpg” and text message as “Hello” it takes 17.342 second time but with the previous technique it takes 21.614. When we take two different images that one is “Cat.jpg” and “Hide.jpg” it takes 8.7424 seconds to steganography and encrypt the information rather than 20.1602 seconds. And when we take one image with audio “Cat.jpg” and “Filewatermark.wav” it takes 14.2397 seconds rather than 14.3217 seconds.

5.2 Future Scope

In future, we will perform embedding in any cover media such as image can be hidden in any media like audio or text or we can say simple text file may contains any type of media like text, audio, image can be possible by using the AES encryption which leads to more encrypted or complex form of information.

REFERENCES

Reference to books:

[1]Rafael C. Gonzalez, Richard E. Woods (2002), *Digital Image Processing, Prentice-Hall, Inc.Upper Saddle River*, New Jersey.

[2]William Stallings (2006), *Cryptography and Network Security principles and Practice, Pearson Education,* Inc., New York.

Reference for articles:

[1] Smitha Suresh, Dr.KChitra, Deepak.P "Pateh Based Frame Work for Occlusion Deteetion in Multi Human Tracking ", *2013 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013]*

[2] Mr. Arjun R. Nichal, Mr. Vinod B. Kumbhar, "Novel Steganographic method for Encrypted Image as a cover media for Binary image, Text and Audio", *International Journal Of Innovative Research In Elecrical, Electronics, Instrumentation And Control Engineering Vol. 1, Issue 8, November 2013*

[3] Jaspal Kaur Saini, Harsh K Verma, "A Hybrid Approach for Image Security by Combining Encryption and Steganography", *Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)*

[4]Ritu Pahal, Vikas kumar*, "* Efficient Implementation of AES *", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013*

[5] Harshitha K M, Dr. P. A. Vijaya, " Secure Data Hiding Algorithm Using Encrypted Secret message", *International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012 1 ISSN 2250-3153*

[6] G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan," Steganography Using Edge Adaptive Image"*July 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]*

[7] RigDas, Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding ", *2012 IEEE*

[8] Amit Asthana, Sherish Johri, "An Adaptive Steganography Technique for Gray and Colored Images ", *May 2012 International Journal of Advanced Research in Computer Science and Software Engineering*

[9] M.Grace Vennice, Prof.Tv.Rao, M.Swapna, Prof.J.Sasi kiran, "Hiding the Text Information using Stegnography", *International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 1, Jan-Feb 2012, pp.126-131.*

[10] Vijay Kumar Sharma, Vishal Shrivastava "A Steganography Algorithm For Hiding Image In Image By Improved LSB Substitution by Minimize Detection", *Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1*

[11] Yongzhen Zheng, Fenlin Liu, Xiangyang Luo, Chunfang Yang "A Method Based on Feature Matching to Identify steganography software ", *2012 Fourth International Conference on Multimedia Information Networking and Security*

[12] Anil Kumar , Rohini Sharma," A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique*", International Journal of Advanced Research in Computer Science and Software Engineering(Volume 3, Issue 7, July 2013)*

[13] Rajinder Kaur, Er. Kanwalpreet Singh (2013),"Comparative Analysis and Implementation of Image Encryption Algorithms", *IJCSMC*, April, Vol. 2, Issue. 4, p. 170-176.

[14] H.B. Karaman, s.saguroglu, *"An* Application Based on Steganography*", 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.*

[15] Neda Raftari and Amir Masoud Eftekhari Moghadam, "DCT-IWT", *Aug 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks*

[16] Prabakaran. G, Bhavani.R , " Modified Secure Digital Image Steganography
Based on Discrete Wavelet Transform ", *2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]*

[17] Mr . Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar, "Image Steganography Using Least Significant Bit With Cryptography"*Journal of Global Research in Computer Science* Volume 3, No. 3, March 2012

[18] Jawad Ahmad and Fawad Ahmed (2012)," Efficiency Analysis and Security Evaluation of Image Encryption Schemes", *International Journal of Video & Image Processing and Network Security,* Vol. 12, No. 04

[19] R Praveen Kumar, V Hemanth, MShareef," Securing Information Using Steganography", *2013 International Conference on Circuits, Power and Computing Technologies*

[20] Varsha Bhatt, Gajendra Singh Chandel (2012), "Implementation of new advance Image Encryption Algorithm to Enhance Security of Multimedia" *International Journal of Advanced Technology & Engineering Research,* Vol. 2

[21] Mahmud Hasan ,Kamruddin Md. Nur, Tranzee Bin Noor," A Novel Compressed Domain Technique of Reversible Steganography", *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, March 2012*

[22] B.Subramanyan, Vivek.M.Chhabria, T.G.Sankar babu, “Image Encryption Based On AES Key Expansion”*, 2011 Second International Conference on Emerging Applications of Information Technology*

[23] Subramania Sudharsanan (2005), “Shared Key Encryption of JPEG Color Images”, *IEEE Transactions on Consumer Electronics,* November, Vol.

APPENDIX A

ABBREVIATIONS

AES	Advanced Encryption Algorithm
ASCII	American Standard Code for Information Interchange
BMP	Bitmap image
DES	Data Encryption Algorithm
DFT	Discrete Fourier transformation technique
DCT	Discrete cosine transformation technique
DWT	Discrete Wavelet transformation technique
EC	Embedding Capacity
IWT	Integer Wavelet Transform
IDWT	Inverse Discrete Wavelet Transformation
JPEG	Joint Photographic Experts Group
LSB	Least significant bit
MSE	Mean Square Error
MAES	Modified Advanced Encryption Standard
MATLAB	MATrix LABoratory
NBE	Number of bits embedded
OSI	Open Systems Interconnection
PAES	Proposed AES
PSNR	Peak Signal to Noise Ratio
PVD	Pixel value differencing
RPE	Random pixel embedding method
RSA	Ron Rivest, Adi Shamir and Leonard Adleman
Rcon	Round Constant
RGB	Red, green Blue
TCP/IP	Transmission Control Protocol/ Internet Protocol
XOR	Exclusive or
XML	Extensible Markup Language

APPENDIX B

TEST IMAGES