A
Dissertation
On

A Novel Approach Image Security for Public Network Transmission

Submitted in Partial Fulfillment of the Requirement
For the Award of the Degree of

Master of Technology

in

Computer Science and Engineering

by

Rishi Kant Singh
University Roll No. 2K13/CSE/21

Under the Esteemed Guidance of

Mr. Manoj Kumar
Associate Professor

Computer Science & Engineering Department, DTU

2013-2015

COMPUTER SCIENCE & ENGINEERING DEPARTMENT

DELHI TECHNOLOGICAL UNIVERSITY

DELHI - 110042, INDIA

ACKNOWLEDGEMENT

First of all, I would like to express my deep sense of respect and gratitude to my project supervisor Manoj Kumar for providing an opportunity of carrying out this project and being the guiding force behind this work. I am deeply indebted to him for the support, advice and encouragement he provided without which the project could not have been a success.

Secondly, I am grateful to Dr. O P Verma, HOD, Computer Science & Engineering Department, DTU for his immense support. I would also like to acknowledge Delhi Technological University library and staff for providing the right academic resources and environment for this work to be carried out.

Last but not the least I would like to express sincere gratitude to my parents and friends for constantly encouraging me during the completion of work.

Rishi Kant Singh
University Roll no: 2K13/CSE/21
M.Tech (Computer Science & Engineering)
Department of Computer & Engineering
Delhi Technological University
Delhi – 110042

Computer Science & Engineering Department
Delhi Technological University
Delhi-110042
www.dtu.ac.in

CERTIFICATE

This is to certify that **Rishi Kant Singh (2K13/CSE/21)** has carried out the major project-II titled **"A Novel Approach Image Security for Public Network Transmission"** as a partial requirement for the award of Master of Technology degree in Computer Science and Engineering by **Delhi Technological University.**

The major project is a bonafide piece of work carried out and completed under my supervision and guidance during the academic session **2013-2015**. The matter contained in this report has not been submitted elsewhere for the award of any other degree.

(Project Guide)
Mr. Manoj Kumar
Associate Professor
Department of Computer & Engineering
Delhi Technological University

Date……………….

ABSTRACT

With the progress in Data Transmission by an electronic system, the need of security has Become necessity. Due to Exponential growth of multimedia application, security must be a high priority. Image application have been rapidly used in our digital media world. Some exiting algorithm provides security of image applications. There are different algorithm for image encryption with having different parameter like image encryption ratio, encryption- decryption speed, compression ratio and security level.

With the rapid increase of very high speed wireless networking, the main objective to be controlled like efficient ,robust and secure encryption algorithm required. With the exponential growth of image exchange, security of information is the main concern when information store and transmission over the internet. The objective of encryption algorithm protect the information from unauthorized person. The application of image in field of milarity confidentail image transmission, medical image application and some image of confidential projects.

The main objective of image encryption algorithm provides the three most important components are following confidentiality, integrity and authentication for image transmission over the public network. The primary objective of this algorithm to provide that high speed encryption and decryption of the digital image as compared than normal AES image encryption algorithm.

Table of Contents

List of Figures and Table

List of Abbreviations

AES	Advance Encryption Standards
DES	Data Encryption Standards
BMP	Bitmap Image
MAES	Modified Advance Encryption Standard
ECB	Electronic Codebook Cipher
CBC	Cipher Block Chaining
CFB	Cipher Feedback
JPEG	Joint Photography Expert Group
GIF	Graphics Interchange Format
TIFF	Tagged Image file Format
PNG	Portable Network Graphics

Chapter 1

Introduction

The exponential growth of image application in computer technology has made image processing a critical task in cryptography. Computer data are easy to access, stolen and copy ,use of Image Application in this exponentially growing multimedia world leads security threats, today a lot people, organizations, industries are using Multimedia application for their daily operations. So their sensitive information like images, projects, documents related to defense, industries and medical fields are travelling via internet are unsafe and prone to unauthorized and illegal access The digital image is stunning data type with a wide range of use in internet technology. So many users want to implement content, privacy method for them to keep from the preview, copyrights and modified. In widespread application like medical imaging system, military image database, video conferencing system, online or offline personal photograph storage, security is very necessary. Also, various application of image in official point of view resource and asset, Access control and physical security are the way of protection but this is not proper and appropriate solution to secure the data, we need a more secure technique to keep them safe. So there is requirement of a strong security policy.

Cryptography is a method of transforming an intelligible (plain text) data to an unintelligible (cipher text) and transforming that data in original format. In recent times, cryptography considers mathematics as well as computer science. The three main goals of cryptography are given below.

- Confidently: confidently refers to protecting the data from unauthorized client.
- Data integrity: data integrity shows that information or data has not been changed or modified in unauthorized ways.
- Authentication: There is two ways of authentication one is Message authentication and second one is entity authentication. Message-authentication confirms the identity of the sender of a message. Entity authentication provides ensure the receiver of message of both identities of the sender as well as active participation.

1.1 Fundamental of Image

Image is a function of f (x, y), from R^2 to R. F(x, y) gives the intensity of pixel value at coordinates (x, y). Image show over a rectangle with a finite area with have thousands number of pixels. The digital image is a numeric presentation of two dimensional images. It depend image resolution is fixed; it may be vector and roster type. The meaning of digital image refers to raster image or bitmap image. The digital image has a fixed number of rows and column of pixels. Pixels are smallest value in the image, having quantized value that shows the brightness of color at that point.

The pixel (picture element) is a fundamental unit of programmable color in an image. The size of particular pixel depend how to fix the resolution or intensity of the display image. If we fixed image to maximum resolution than physical size of a pixel will equal to physical size of dot pitch.

The every color of the pixel is a combination of three different color combinations which is called RGB color combination. The three bytes of data are used for a particular pixel value, one byte for each major color component. 24-bit color system uses all three color combinations.

A digital image is a combination of three functions given below.

$$\mathbf{F(x, y) = f(r(x, y), g(x, y), b(x, y))}$$

RGB (red, green, blue) with the help of these color lights we can produce any other color. The RGB color model having Red, Green, and Blue are taken together in many ways to reproduce a broad array of color. The RGB color model is device dependent, it means different device reproduce a given RGB value differently.

1.2 Type of Image

The most common image file format listed given below:

- Joint photography expert Group (JPEG or JPG)
- Graphics interchange format (GIF)
- Tagged Image File Format (TIFF)
- Portable Network Graphics (PNG)

- Bitmap Image (BMP)

- **Joint photography expert Group (JPEG or JPG)**

The Joint Photographic Experts Group, (JPEG) organization, is a standout amongst the most well-known groups for web design. It has 24 bit color information. The JPEG document Organization stores all color information in a RGB picture, and afterward it compress the file size to spare storage space, or it spares just the color information that is Crucial to the picture. Dissimilar to GIF, JPEG does not support transparency.

The compression technique utilized as a part of JPEG is normally lossy compression, implying that some visual quality is lost simultaneously. JPEGs can be spared in an assortment of lossy compression levels. This implies pretty much compression can be connected to the image, contingent on which looks best. JPEG can be used by any browsers. Since JPEG is an image compressor, it is best utilized for photographic quality pictures what's more, itemized representations with numerous colors. (Tom Lane, 2008).

The advantage of JPEG is that it is an exceptionally compress file format. Hence, the images can be packed while the quality is kept up. JPEG shortcoming is that lossy compression may bring about low quality illustrations. Another shortcoming noted in JPEG organizations is that there is no backing for pixel transparency. JPEGs lose quality each time they are opened, altered and spared. It is vital to minimize the number of altering sessions between the introductory and last form of a JPEG image (Sharon Wheeler, 2000), (CIMC, 2006), (Graphics Academy, 1998).

- **Graphics interchange format (GIF)**

The Graphics Interchange Format (GIF) was initially grown by CompuServe in 1987. It is a standout amongst the most mainstream document groups for web design and trading representation records between PCs. The GIF organization support 8 bits of color information that is constrained to 8 bits palette and 256 colors. Along these lines, just 256 distinctive colors are accessible to represent the image. It can be seen by all basic programs. GIF file format support animation, transparency and interlacing (Betcher and Gardner, 2006), (Robert Fry, 2006).

GIF pictures are consequently compressed when they are spared utilizing a lossless compression system known presently (Ziv-Welch) that does not debase the image quality. GIF organization gives four fundamental elements: interlacing, transparency, document compression, and primitive movement. The interlacing element permits the program to showcase segments of the picture right now. The first picture begins off with poor quality however improves right now the joining parts are upgraded. Joined GIF files permit clients to view a segment of the picture right now is stacking (Seeram and Radiography, 2006)

One of GIF's shortcomings is that GIF pictures are restricted to a most extreme of 256 colors. The nature of the image endures if the color depth is decreased to not exactly the shading profundity of the first image. GIF documents can store any of the 16.8 million colors yet just a most extreme 256 color in each GIF file. Subsequently, when changing over an image to GIF, the system store the record by diminishing the quantity of colors in the image from 24-bit (a huge number of colors) to 8-bit (256 colors). Notwithstanding, the GIF file arrangement can store different images in a solitary document and play the pictures in a circle, in this way giving the presence of animation (CIMC, 2006), (Sharon Wheeler, 2000).

- **Tagged Image File Format (TIFF)**

TIFF was made by Aldus for 'desktop distributed', and by 2009 it was exchanged to the control of Adobe Systems. TIFF is prevalent among regular clients, however has picked up acknowledgment in the visual depiction, distributed and photography industry. It is likewise main stream among Apple clients.

The Tag Interchange File Format (TIFF) is a tag-based universal standard for putting away and trading bitmaps in the middle of application and hardware platform. It is good with an extensive variety of programming applications and can be utilized crosswise over platform, for example, Macintosh, Windows, and UNIX. The TIFF organization is complex; in this manner TIFF documents are by and large bigger than GIF or JPEG records. TIFF support loss-less LZW compression. Nonetheless, compress TIFF takes more time to open. The organization comprises of things called tags which are characterized by the standard. Every tag is taken after by a tags subordinate information structure (Graphics Academy, 1998).

- **Portable Network Graphics (PNG)**

PNG or (Portable Network Graphics) is an as of late presented configuration, so not everybody acquainted with it. However, PNG has been sanction as a standard since 1996. It is an image arrange particularly intended for the web. PNG is, in all viewpoints, the predominant form of the GIF. Much the same as the GIF form, the PNG is spared with 256 color most extreme however it spares the shading data all the more effectively. It additionally supports an 8 bit transparency.

The Portable Network Graphics (PNG) arrangement is a bitmapped picture design that utilizes lossless information compression. It will probably be the successor to the GIF file format. PNG is required to turn into a standard configuration for web pictures and could supplant GIF completely. It is stage free and ought to be utilized for single images just (not animation). Contrasted and GIF, PNG offers more noteworthy shading bolster and better compression, gamma correction for shine control crosswise over stages, better backing for straightforwardness, and a superior system for showing dynamic pictures (Sharon Wheeler, 2000), (Fulton, 2005).

- **Bitmap Image (BMP)**

The Windows Bitmap or BMP documents are picture records inside of the Microsoft Windows working framework. Indeed, it was at one point one of only a handful few image designs. These records are substantial and uncompressed, yet the image are rich in colors, high in quality, straightforward and good in all Windows OS and projects. BMP documents are additionally called raster or paint pictures.BMP records are made of millions and a large number of dabs called 'pixels', with diverse hues and courses of action to concoct a picture or example. It may a 8-bit, 16-bit or 24-bit picture. Accordingly when you make a BMP picture bigger or littler, you are making the individual pixels bigger, and hence making the shapes look fuzzy and jagged.

Bitmap Image file format

The meaning of Bitmap is a mapping from some domain to bits. That means value zero or one.in general way we can say that bitmap refers to map of pixels. The BMP file format also knows as bitmap image file format or system independent bitmap file format.BMP file format are historic file format. It has black and white (1 bit per pixel) up to 24 bit color.

BMP file Structure

A BMP file has 3 to 4 blocks as shown in figure.

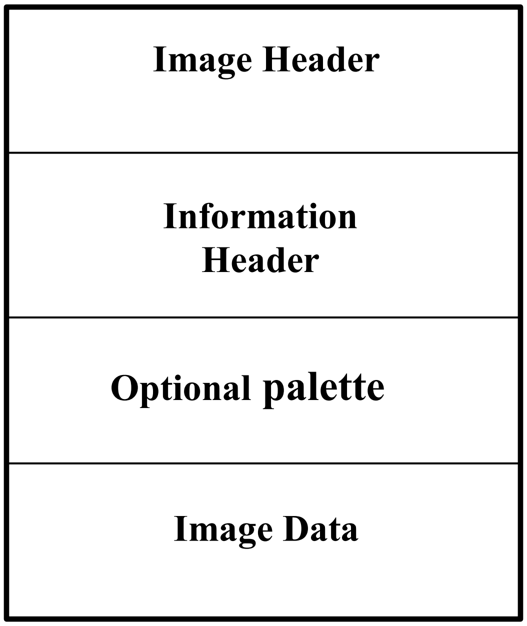


Figure 1.1: Bmp File Structure [1]

The first block is image header followed by information header. BMP image has indexed color than palette has information about pixel. In image data block having information about images like height, width, what method used for compression, the number of colors have information.

- **Image Header**
  Image header consists of, short in 2 bytes, it for 4 byte and long it for 8 bytes. For typical machine (like Intel machine) the header length consist 14 byte length.[1]

```
Typedef struct {

Unsigned short int type;
Unsigned int size;
Unsigned short int reversed1, reversed2;
Unsigned int offset;
}
Header
```

The main field in structure is type field, simply check that is likely to be a legitimate BMP file. Offset block contains number of byte before actual pixel data.

- **Information Header**

  The image information header has 40 byte in length. The field most involves in height and width of image the number of bits per pixel.

```
Typedef struct{
Unsigned int size;
In height, width;
Unsigned short in planes;
Unsigned short into bits;
Unsigned in compression;
Unsigned int image size;
int x-resolution, y-resolution;
Unsigned in colors;
Unsigned in important color;
}
Info header
```

Here many compression technique in the BMP image file format given below.

- 0 – no compression in file.
- 1- 8 bit run length encoding.
- 2- 4 bit run length encoding.
- 3-RGB bitmap with mask.

24 Bit Image Data: bmp file having 24bit image data. Its means image data flow immediately after information header that means no color palette. Its have 3byte per pixel in b, g, r order respectively .BMP file 0 show for black color and 1 for white color.

1.3 Research motivation

The most of algorithm specially designed for digital image to produce to encrypted digital images were given in 1990s. There are two major algorithms for digital image given by Maniccam and Bourbiks in 2004. First algorithm based on Non chaos selective method and another based on chaos selective based. These two algorithms mainly suitable for some specific type of image like compress and uncompressed image. This method is light encryption while another algorithm offers strong encryption.

According to Borko (2005) user have to rights to choose the encryption algorithm based on specific properties of algorithm. A most common application of image encryption like in internet communication, multimedia, medical and military system for protects the image information over the network. Different type of multimedia having its own properties like high correlation among the pixels and high image entropy and encryption and decryption speed, so we need different type of encryption algorithm for protect the confidential image from illegal access and all type attacks (Hossam , 2006).

The objective of this research is the ever increasing need for harder break encryption and decryption. One more constraint that reduces to time takes in encryption and decryption of image. We proposed block based encryption and decryption algorithm for image so it will reduce the relation of image element and algorithm will increase the entropy information and decrease the correlation among the pixels. Here we proposed algorithm for symmetric key encryption algorithm its means encryption of image and decryption of image the key will be same in both process. In our research mainly focused on the changes image properties will changed after the process the encryption of image.

This proposed model of algorithm based on Simple AES algorithm modified with some another approach having the high speed encryption and decryption and increase the entropy information of image.

1.4 Symmetric key Algorithm

The shared secret key is the single key which is used in Encryption-Decryption process. This is the fundamental concept of symmetric key algorithm in cryptography. In symmetric key algorithm the same key will be used for encryption and decryption process. Here two type of symmetric algorithm, block and stream cipher. A block cipher used encrypt the image into cipher image has same size of image after encryption. For example we take the size to 1024x1024 bmp image or size of bmp image is 2.5 MB as an input for encryption than cross ponding output must be same size. Blowfish, Data Encryption Standards (DES), Triple DES, and IDEA are example of symmetric block cipher. The symmetric key algorithm uses a single key for encryption and decryption process.

The blowfish algorithm was designed in 1993 by bruce Schneier is one symmetric block cipher algorithm. Whereby it can be used changed of Data Encryption Standard (DES) and International data encryption algorithm (IDEA).the blowfish algorithm having two part first one a key expansion part and second one is data encryption part. In this algorithm encrypt the data using block cipher method means image breaks into block having size of block is 64 bit block. It takes a range of key from 32 bits to 448 bits length, which shows flexibility in its security strength.

1.5 Asymmetric Key Algorithm

The issue with secret keys is trading them over the Internet or a vast system while keeping them from falling into the wrong hands. Any individual who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys - a key pair. A public key is made unreservedly accessible to any individual who may need to send you a message. A second, private key is kept secret, so that just you know it.

Any message (text, binary files, or documents) that are encrypted by utilizing people in public key must be decrypt by applying the same algorithm, yet by utilizing the coordinating private key. Any message that is encrypting by utilizing the private key must be decoded by utilizing the coordinating public key.

This implies that you don't need to stress over ignoring public keys the Internet (the keys should be public). An issue with asymmetric encryption, in any case, is that it is slower than symmetric encryption. It requires significantly additionally handling energy to both encryption and decryption the substance of the message.

1.6 Image Encryption

Today, most of encryption algorithm based on textual data. But the image is different from text format. An approach for image encryption 2D image consider as 1D data stream, and encryption, this stream with any encryption algorithm. This simple technique called nave method.in this method we can encrypt the text and some small bitrate audio, video. This algorithm is not suitable for different type of image format like JPG, PNG and BMP. Although we can use traditional cryptography to encrypt the image, but this approach is not very good to encrypt the image due to some reason like image is not like text, image size is much greater than text. Because of large data set and real time constraints, the traditional cryptography takes more time to encrypt the image. The other problem is decrypt text must be equal to plain text. However, this condition is not necessary in image due to an image encryption some distortion which is acceptable.

1.7 Goal, Scope and Objective of Research

The goal of this research to reduce the time of encryption and decryption using proposed algorithm. The scope is limited to bitmap image encryption using combined method Advance Encryption Standard and proposed algorithm. Main objective of thesis is reducing the time of encryption decryption ratio. Algorithm is related the row are break into block having size of 128 bits. Encryption of bitmap image using XOR operation and encrypt the block with ASE encryption Algorithm. Furthermore, the research related to after encryption what’s changes in the image behavior like image correlation, image entropy, image Histogram.

To achieve the above goal, the main objective of this research will be as follow:

- To Deployed the new encryption approach for Bitmap image and testing of encryption and evaluate it.
- To determine the result and compare different properties of image like correlation, entropy, histogram of different size of bitmap images with AES algorithm and Proposed Algorithm.
- Analysis the security level of encrypted bitmap images generated by proposed algorithm and Advance Encryption Standard (AES).
- Compute the time for encryption decryption and compare the time between AES Algorithm and Proposed Algorithm.

1.8 Thesis Structure

The thesis contains six chapters. Chapter one describes the introduction of image, type of image and format of image. This chapter also explains the motivation of Research and focus on important goal, scope and objective of study. Here describe the symmetric key algorithm and image encryption of image than most important aspect of AES algorithm.

Chapter 2 describes the digital image encryption and digital image and the fundamental of digital image and file format of Bitmap image. In this chapter also describe about the cryptography and some encryption algorithm like Advance encryption Standard, Data Encryption standard and blowfish algorithm.

Chapter 3 describes the proposed work of encryption and decryption with every step. In this chapter give the block diagram of Encryption and decryption process.

Chapter 4 thesis contains output of encryption and decryption of image. Also mention the histogram, entropy and correlation of image. This chapter contains the simulation of result and analysis of result.

Chapter 5, describe the conclusion and future work.

Chapter 02

Literature Survey on Image Encryption

2.1 Introduction

This chapter describes the full information of the cryptography system which is used in research Section 2.2 related to basic information of digital image.

Section 2.3 characterizes some imperative symmetric key algorithm, for example, block cipher and stream cipher algorithms are additionally presented in this segment. Besides, we will experience methods of operation; Electronic Code Book Cipher (ECB), Cipher Block Chaining (CBC), and Cipher Feedback (CFB).

Section 2.4 proposed a percentage of the as of late created or surely understood encryption and decryption algorithm in cryptography system, for example, DES, Blowfish, Rijndael-AES and IDEA. These algorithms characterize and take after the tenets of encryption and decryption that are utilized to give security in image encryption.

Section 2.7 characterizes the image security measurement; the relationship among image components, image entropy information, image histogram, and image correlation coefficient in a certain level of subtle element. These security estimations will be utilized as a part of this evaluate to process and assess the encrypted image delivered by the combined method.

2.2 Digital Images

The definition of a digital computerized image is an array of individual pixels and each pixel having its own value. The array, and thus the set of pixels, is called a bitmap. If we accept a digital image of 1024 pixels × 1024pixels, it means that the data for the image must contain information about pixels 1048576(Steinmetz and Nahrstedt, 2002), (Kristian Sandberg, 2000).

Digital pictures are delivered through a procedure of two stages: sampling and quantization. Sampling is the procedure of separating the first image into little areas called pixels, while quantization is the procedure of allotting a integer number worth (i.e. shading) to every pixel (David Salomon, 2007). The quantity of colors (i.e. color space) that can be appointed to any image component or pixel is an element of the quantity of bits, which is at times alluded to presently profundity or bits determination. This idea is otherwise called bits per pixel (bpp) that show to the colors for every quality. The color space is figured utilizing the accompanying comparison:

$$\textbf{Color space} = \mathbf{2^b}$$

Where b is bit depth.

The color values utilized as a part of every bitmap rely on upon the particular bitmap position. This implies that every pixel in a bitmap contains certain information, normally translated presently. The information content is dependably the same for every one of the pixels in a specific bitmap. Accordingly, every color depth in a bitmap is a twofold number. A binary number is a series of binary digits that can be either 0 or 1 and called bits. This binary number in a given configuration will vary long contingent upon the color profundity of the bitmap, where the color profundity of a bitmap decides the scope of conceivable shading values that can be utilized as a part of every pixel. For instance, every pixel in a 24-bit image can be one of approximately 16.8 million hues. This implies that every pixel in a bitmap has three color values somewhere around 0 and 255 and afterward those hues are shaped by combining fluctuating amounts of three essential colors: red, green and blue (Vaughan, 2004), (Rafael and Richard, 2002), (Sander, 2000).

Serial No	**Image Property**	**Color Space**	**Bit Resolution**
1.	Binary Image	2 Color	1
2.	Gray Scale	256 Gray levels	8
3.	Colored Image	256 Color	8
4.	Colored Image	65536 Color	16
5.	True Color(RGB)	16,777,216 Color	24

Figure 2.1: Table of Image Properties [1]

Table 2.1, as the numbers of bits increase, the image quality is additionally expanded. Notwithstanding, stockpiling necessities will expand, bringing about an immediate relationship between the image store size and the bits determination. Image storage size for an uncompressed image is processed utilizing the accompanying comparison:

$$\boldsymbol{IMGSS = IMGR \times BR}$$

Where: *IMGSS*: Image storage- size

IMGR: Image- resolution (i.e. image width × image height)

BR: Bits- resolution (bits depth)

2.2.1 Electronic Code Book Cipher (ECB)

Electronic Code Book (ECB) is a method of operation for a block cipher, with the trademark that every conceivable block of plaintext has a characterized comparing cipher-text quality and the other way around. At the end of the day, the same plaintext worth will dependably bring about the same cipher-text esteem. Electronic Code Book is utilized when a volume of plaintext is isolated into a few blocks of information, each of which is then encrypted autonomously of different block. Truth be told, Electronic Code Book can bolster a different encryption key for every block.

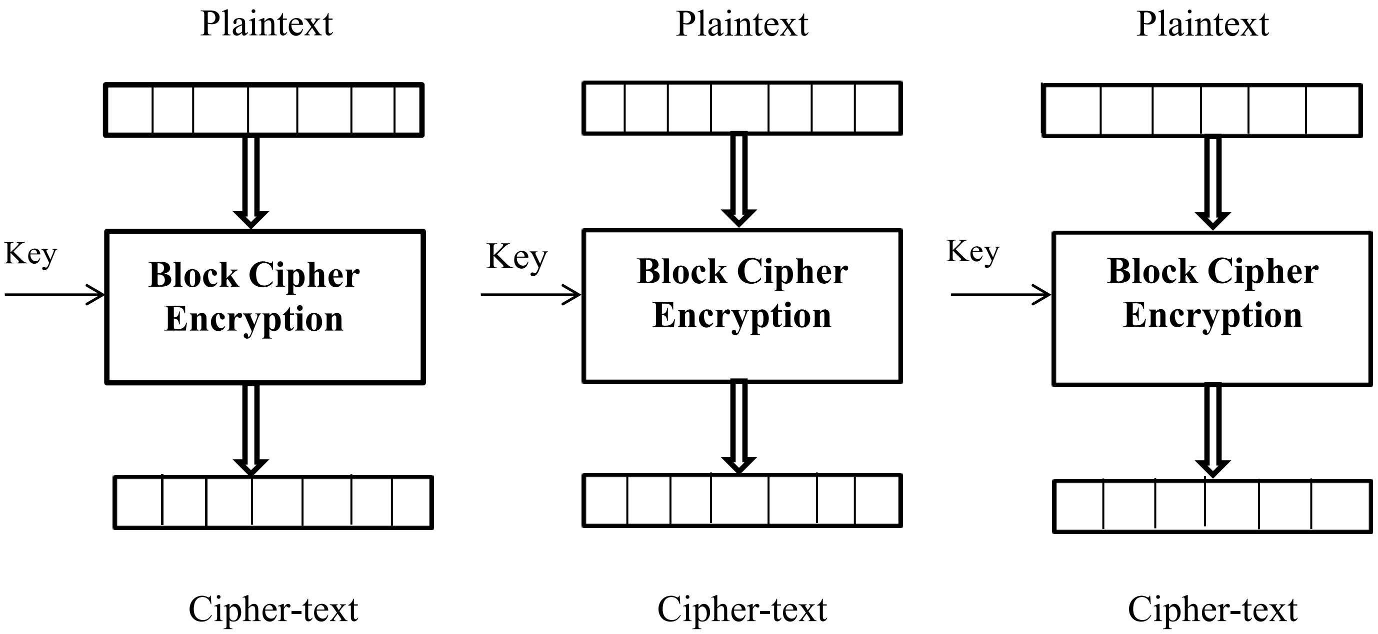


Figure 2.2: Block Diagram of Electronic Code Book (ECB) [2]

In any case, Electronic Code Book is not a decent framework to use with small block sizes (for instance, smaller than 40 bits) and indistinguishable encryption modes. This is on the grounds that a few words and expressions may be reused frequently enough so that the same dull part-pieces of cipher-text can rise, laying the foundation for a codebook assault where the plaintext examples are genuinely self-evident. Notwithstanding, security may be enhanced if arbitrary cushion bits are added to every block. Then again, 64-bit or larger block ought to contain enough one of a kind quality (entropy) to make a codebook assault unrealistic to succeed.

As far as blunder rectification, any bit mistakes in a cipher-text block influence decoding of that piece just. Affixing reliance is not an issue in that reordering of the cipher-text blocks will just reorder the comparing plaintext blocks, however not influence encryption.

2.2.2 Cipher Block Chaining (CBC)

Cipher block chaining (CBC) is a method of operation for a block cipher (one in which a succession of bits are encrypted presently unit or block with a figure key connected to the whole blocks). Figure piece tying uses what is known at this very moment vector (IV) of a certain length. One of its key attributes is that it utilizes a fastening component that causes the decryption of a block of cipher-text to rely on upon the entire first cipher-text block. Right now, the whole legitimacy of every first square is contained in the quickly past cipher-text block. A solitary bit slip in a cipher-text block influences the decoding of every single resulting block. Improvement of the request of the cipher-text blocks causes decrypted to wind up debased. Fundamentally, in figure block fastening, each plaintext square is XOR with the quickly past cipher-text block, and afterward encoded.

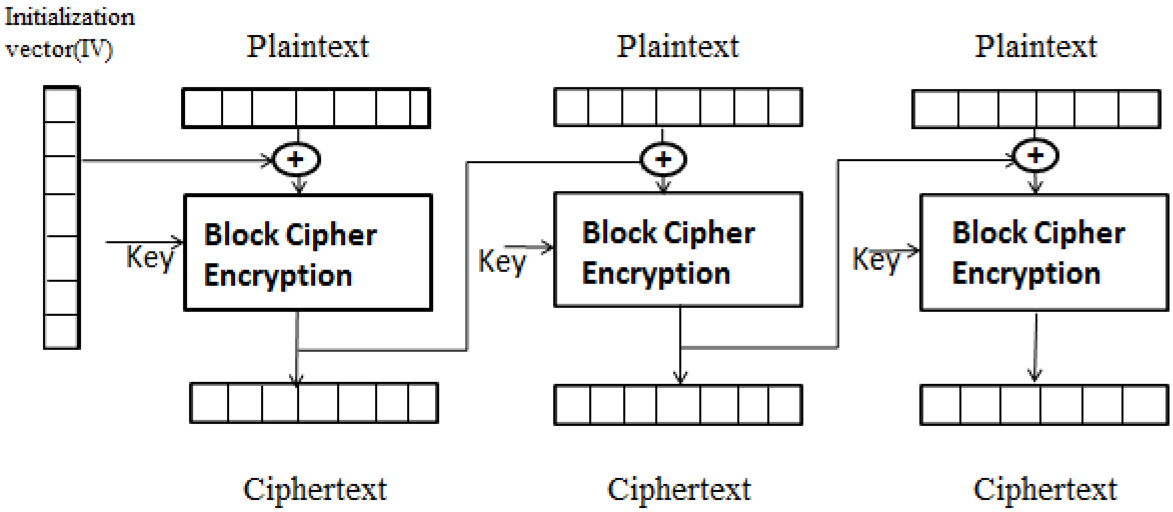


Figure 2.3: Block Diagram of Cipher Block chaining [2]

2.2.3 Cipher Feedback (CFB)

Cipher-text feedback (CFB) is a method of operation for a block cipher. Rather than the figure piece binding (CBC) mode, which encodes a set number of bits of plaintext at once, it is now and again alluring to encode and exchange some plaintext values immediately each one in turn, for which cipher-text input is a system. Like figure piece tying, cipher-text criticism likewise makes utilization of an introduction vector (IV). CFB utilizes a block figure as a part of an arbitrary number generator. In CFB mode, the past cipher-text piece is encoded and the yield is XOR with the current plaintext square to make the current cipher-text block. The XOR operation hides plaintext designs. Plaintext can't be specifically chipped away at unless there is recovery of blocks from either the starting or end of the cipher-text.

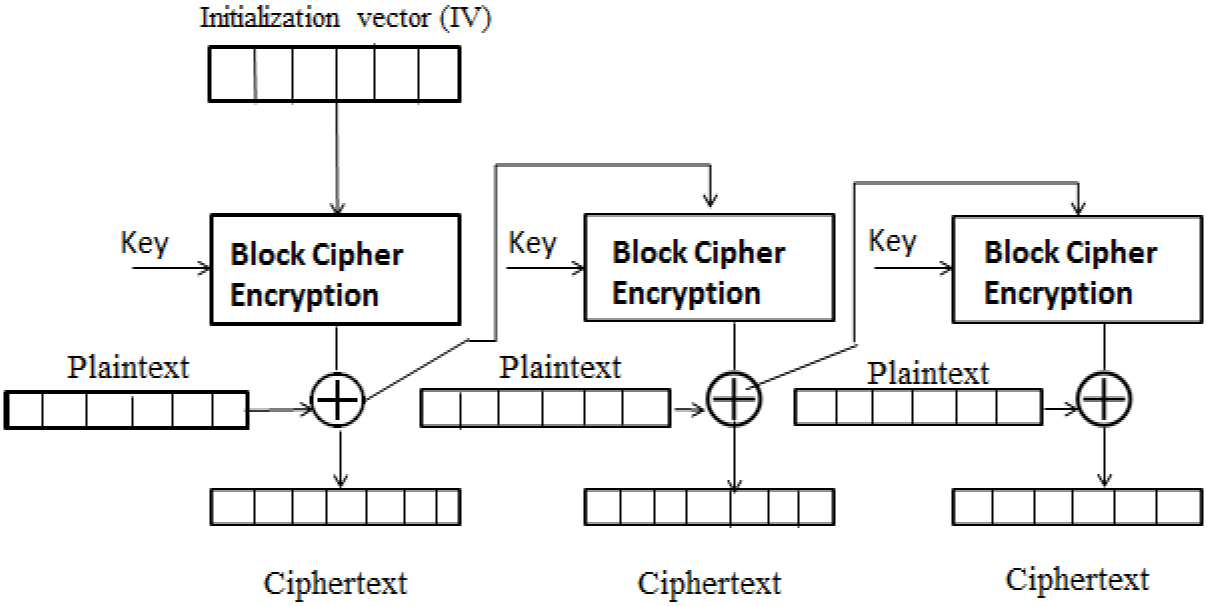


Figure 2.4: Block Diagram of Cipher Feedback(CFB) [2]

2.3 Cryptography System

Until advanced times cryptography referred almost to encryption, which is the procedure of changing over converting ordinary information (called plaintext) into unintelligible text (called cipher text). Decryption is the reverse, as it were, moving from the unintelligible cipher text back to plain text. Formally, a "cryptosystem" is the requested rundown of components of limited conceivable plaintexts, limited conceivable cypher texts, limited conceivable keys, and the encryption and unscrambling calculations which compare to every key.

2.4 Encryption Algorithm

2.4.1 Advance Encryption Standard

AES block cipher developed by the Jon Daeman and Vicent Rijmen. Advance encryption standard (AES) support the any combination of image with key size 128, 192 and 256 bits. In AES algorithm 128 bit data divided into four basic operation block. This block are maintain by 4x4 matrices for the decryption process these 128 bit data passed through different number of round like 10,12,14. This round maintains by following transformation:

2.4.1.2 Sub Byte Transformation:

Sub byte Transformation is S Substation table (S box) having properties of nonlinear substitution which is made by multiplicative inverse and affine transformation. The figure show that sub byte transformation.[3]

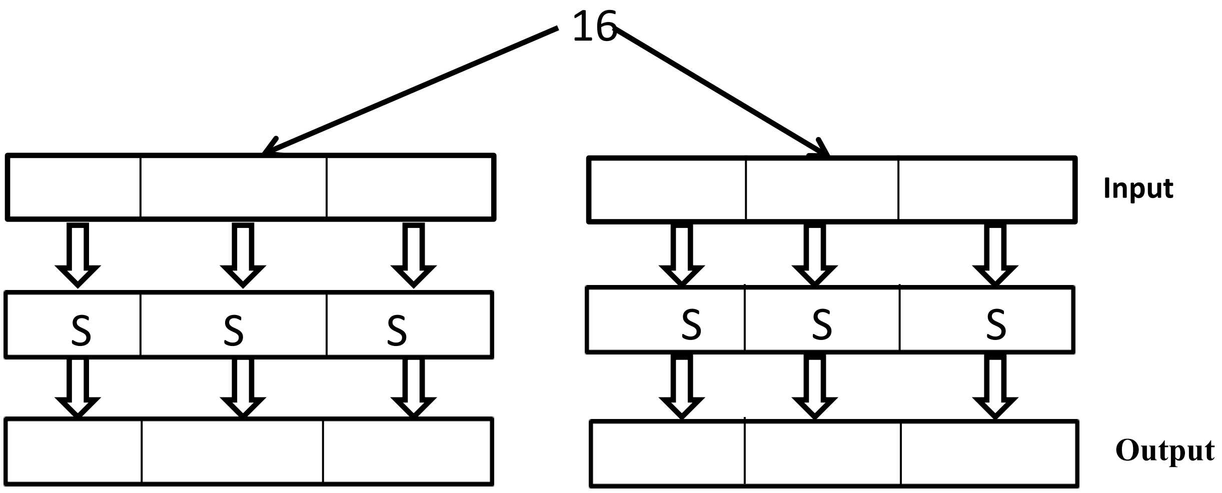


Figure 2.5: Block Diagram Substitution [3]

2.4.1.3 Sift row Transformation:

The Shift Rows step works on the lines of the state; it consistently moves the bytes in every line by a certain offset. For AES, the first column is left unaltered. Every bytes of the second line is moved one to one side. Likewise, the third and fourth columns are moved by counterbalances of two and three separately. For squares of sizes 128 bits and 192 bits, the moving example is the same. Column n is moved left round by n-1 bytes. Along these lines, every section of the yield condition of the Shift Rows step is made out of bytes from every segment of the information state. (Rijndael variations with a bigger piece size have marginally distinctive balances). For a 256-bit hinder, the first line is unaltered and the moving for the second, third and fourth column is 1 byte, 3 bytes and 4 bytes separately—this change applies for the Rijndael figure when utilized with a 256-bit obstruct, as AES does not utilize 256-bit piece.

2.4.1.4 Mix columns Transformation:

This is process of matrix multiplication of the states. Every Colum multiplied by the constant matrix. It means bytes are treated as polynomial instead of a number. This stage (known as Mix Column) is fundamentally a substitution however it makes utilization of mathematics of GF(28).

Every segment is worked on independently. Each byte of a section is mapped into another quality that is an element of every one of the four bytes in the section. The change can be controlled by the accompanying lattice increase on state.

Every component of the item matrix is the whole of results of components of one line and one segment. For this situation the individual augmentations and increases are performed in GF (28). The Mix Columns change of a solitary segment j (0 ≤ j ≤ 3) of state can be communicated right.

2.4.1.5 Add round Transformation:

This is process of XOR operation of round state and round key. This transformation having the property of own inverse. In this stage (known presently) 128 bits of state are bitwise XORed with the 128 bits of the round key. The operation is seen presently operation between the 4 bytes of a state segment and single word of the round key. This change is presently conceivable which helps in proficiency however it additionally impacts all of state.

2.4.1.6 AES Key Expansion

The AES key expansion takes right now 4-word key and produces a linear array of 44 words. Every round uses 4 of these words right. Each word contains 32 bytes which implies each sub key is 128 bits in length**.**

The function g consists of the following sub functions Rot Word performs a one-byte circular left shift on a word. This means that an input word [b0, b1, b2, b3] is transformed into [b1, b2, b3, b0]. SubWord performs a byte substitution on each byte of its input word, using this-box described earlier. The result of steps 1 and 2 is XORed with round constant, Rcon[j].

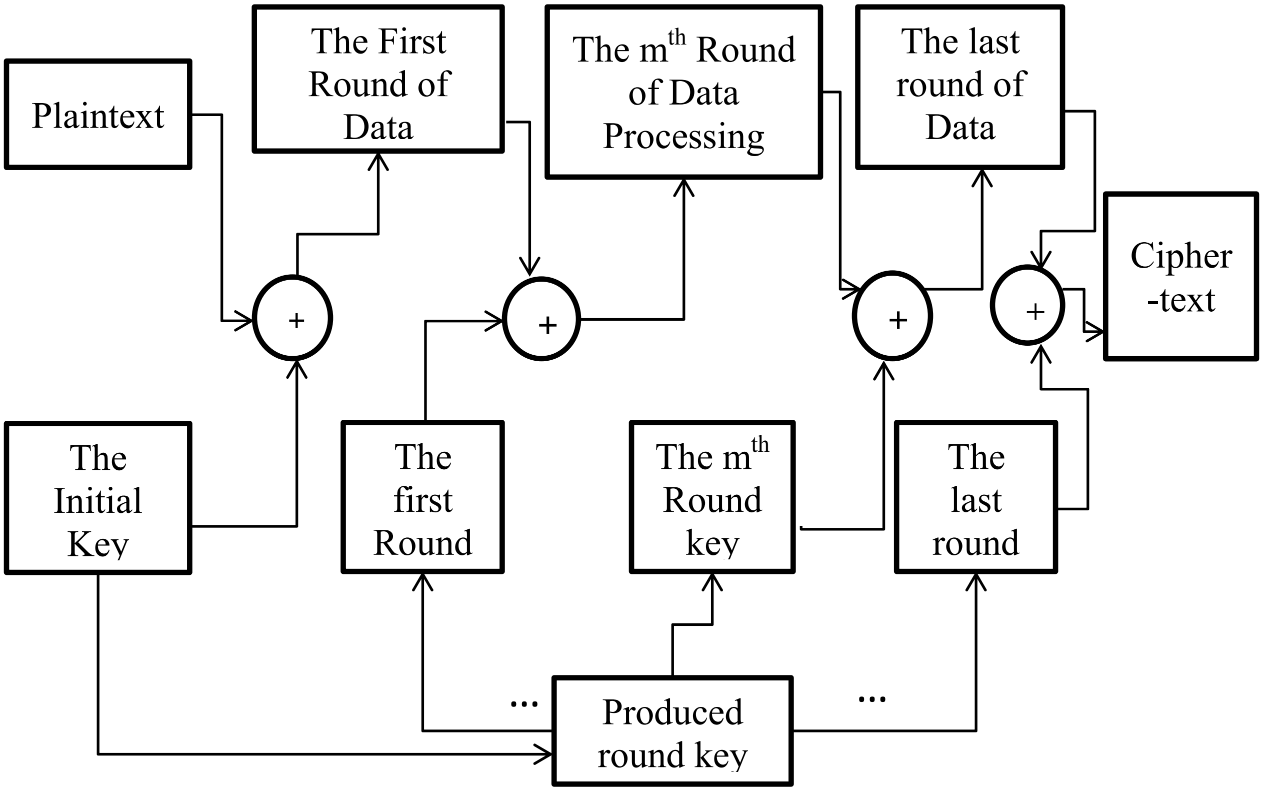


Figure 2.6 : Encryption Process of Advance Encryption Standard(AES) [3]

The encryption and decryption have several steps. First add round, a round function work on data block related all sub operation like sub bytes, shift row, mix column and add round key will be perform. This operation will perform many times which is depending on key length. The decryption step same as perform encryption in reverse order. This Advance encryption algorithm has key size 128 bits.

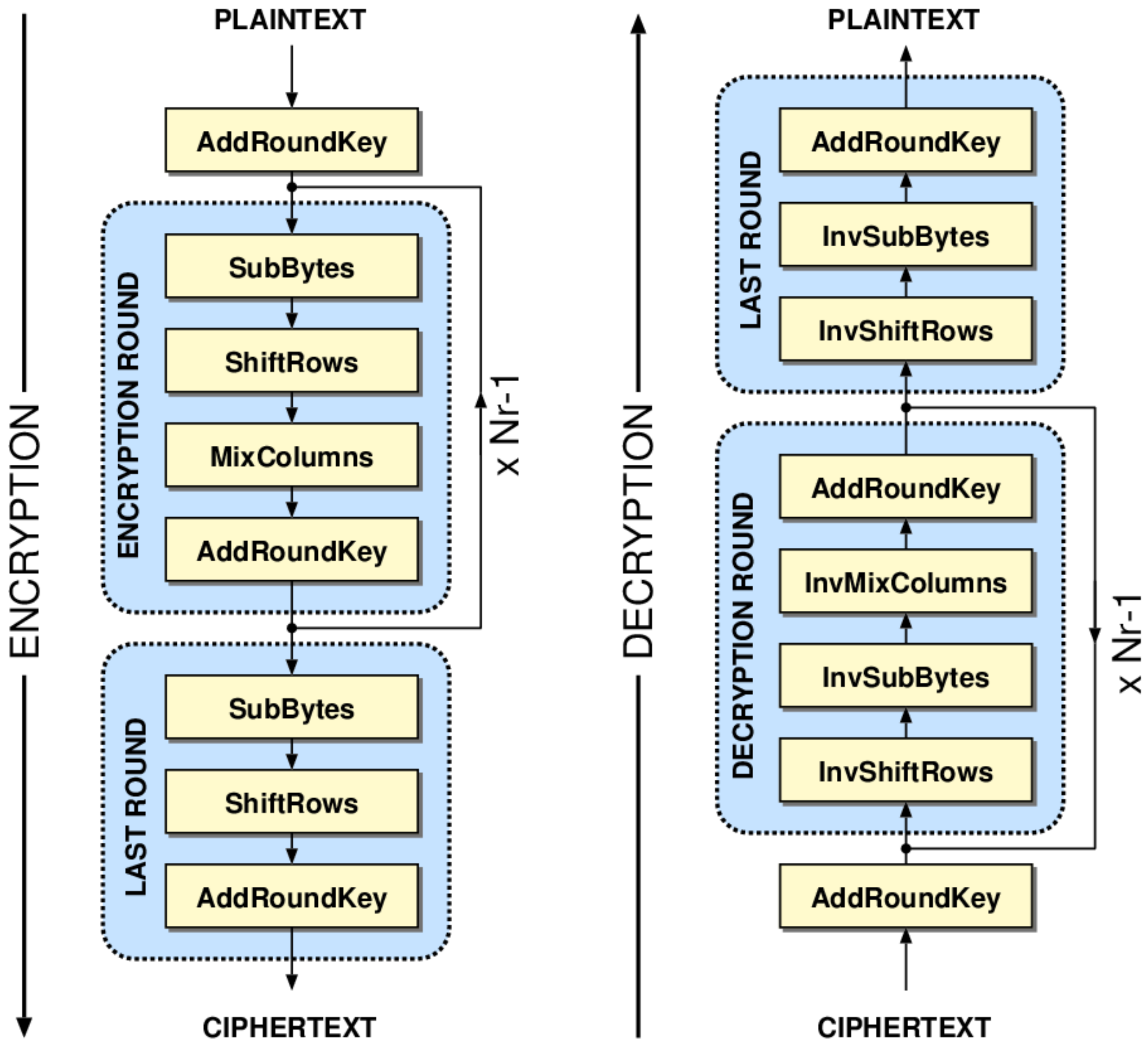


Figure 2.7: Block Diagram of Advance Encryption Standard (AES) [4]

2.4.1 Data Encryption Standard (DES)

There are two functions in DES cryptography system. First confusion and second one is diffusion. DES has 16 number of operation. A round is combined step of confusion and diffusion step, the process of diffusion to obtain the relation between original image and cipher image. The process of confusion to make the relationship encrypted image and key to reduce the predictability of discovering the key. DES used the 56 bit of key for 64 bit of data. The rest of 8 bit used for parity checking. The encryption process has two permutations, intimal and final permutations. In every round different 48 bits is used to produce the cipher image.

The 64 bit key of DES reduces the size of 56 bit just left every 8 bit for parity checking. The main function of parity checking to ensure that key is free from bugs. The next step is from 56 bit every 48 bits generated for each round of Des function. After that DES algorithm is computation of DSE function. This DES function applied on 48 bits key to right most 32 bits. P expansion box use for the expand 32 bit to 48 bits. 4 bit become 6 bit with repeating first and fourth bit. S box performed the compress key and expandable block. The s box has property nonlinear and gives the maximum security for DES algorithm. In decryption process all step will perform in reverse order.

- **Encryption Process in DES**

  Encryption process having two input first one image (plain image) and second one is encryption key. The encryption key select randomly form function generate secret (). It is very common that the size of image is larger than text. Now here the first step is image convert into byte of array and byte array convert into string object. The second step is defined the method for encryption and decryption and key by some awt classes. Next step is array byte of image convert into string for input as a DES algorithm. DES takes only 64 bit length of data for encryption so rest of string will pass by loop for encryption. The header of image is excludes from encryption process. Only which element start from next of header will be encrypted.

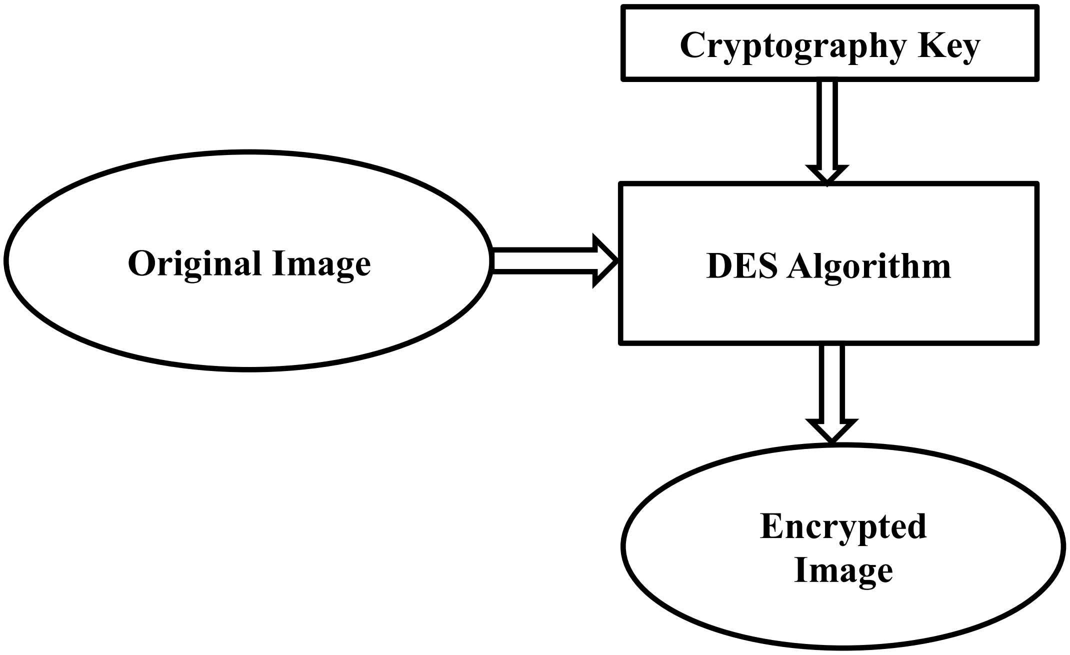


Figure 2.8: Encryption Process of Data Encryption Standard (DES) [5]

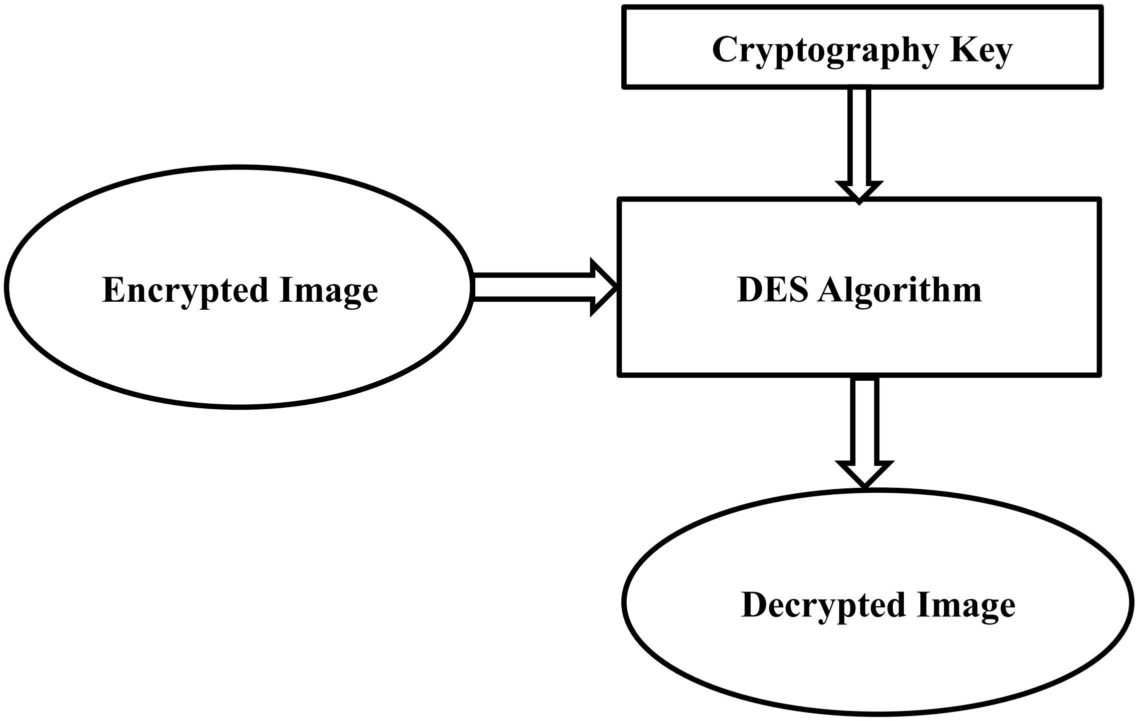


Figure 2.9: Encryption Process of Data Encryption Standard (DES)[5]

- **Decryption process in DES**

The encrypted image divides into same block length of DES algorithm, First of 64 bit block and same key used for decryption process with reverse order of encryption algorithm. The next step decrypted text convert into same string and this string convert into byte array. By help of byte array we can get the original image.

2.4.3 Blow fish Algorithm

The blowfish algorithm is a symmetric block cipher having variable length key from 32 bits to 448 bits. This is necessary to make tradeoff between speed and size of message. In blowfish encryption algorithm required the very high speed operation and small size of hardware. The blowfish algorithm designed in 1993 by Bruce Schneir. The blowfish algorithm is suitable for hardware implementation. The basic operation in blowfish is lookup, XOR and addition. The table contains four s box (56x32) and p array (18x32). DES is festival type and provides the same security with high speed and efficiency in software.

Here some specification of blowfish as following.

- Symmetric block cipher
- 64 bit Block
- Algorithm having variable length of key from 32 bits to 448 bits.
- Algorithm run at defined clock time.
- Suitable and simple for hardware implementation.

The blowfish algorithm has two step processes. First one is key expansion and second one is data encryption .the function of key expansion convert the key 448 bits to 4168 bytes. Data encryption has 16 festal rounds, each round the operation of permutation of key and data dependent. The operation of XOR and addition will be done on 32 bits words. The mainly addition operation have four index array data lookup. In blowfish algorithm the sub key calculated by following sequence.

- First step is Initialization of p array and s box.
- Perform the XOR operation with p array and key bits.
- Perform above step to encrypt the all zero string.
- Here we get new output P1, P2.
- Do encrypt the P1, P2 with modified key.
- Here get the output P3, P4.
- Repeat the process 521 times and determined sub key for p array and four s box.

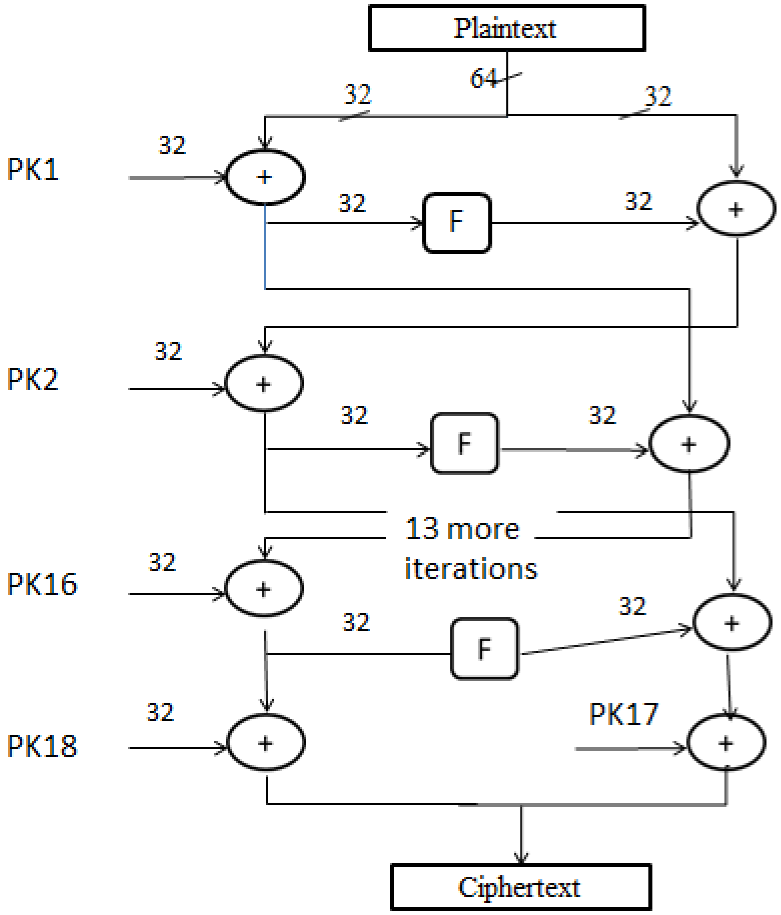


Figure 2.10: Data Flow Graph of Blowfish Cipher [6]

The blowfish uses the four S Box with having 256 entries and each entry having the size 32 bits. For determined F function use first byte of 32 bit of entries, the second bytes find the entries in second s box. First dividing XL into 4 bit quarter than determined F(XL) as given by equation.

$$F\ (XL) = ((Sl[boxl] + S2[box2]) + XOR\ S3[box3]) + S4[box4]$$

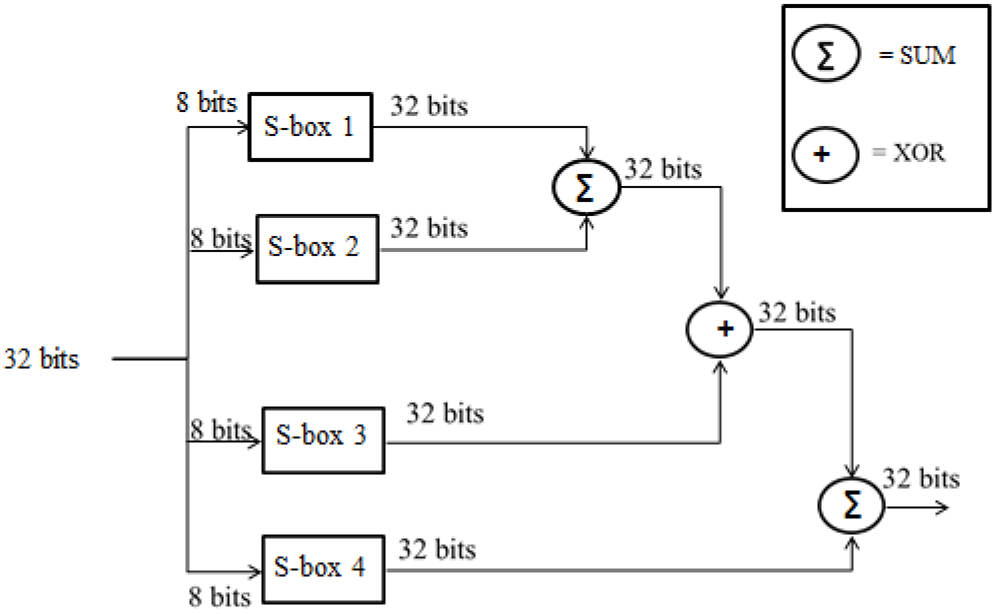


Figure 2.11 : Function Block of Blowfish [6]

At the start algorithm sub key 1 to 18 followed by element zero to 255 for first s box and next element zero to 255 for second s box and so on or 4 s box with fractional part of p. the most significant bit of p will assign for first sub key. Key may be having length of 72 bytes and repeat the same process entire array of 16 sub key. Execution of blowfish to repeat same process for 64 bit Block size. After each execution replace part of sub key in same order digit of p from where place them. For the first iteration replace sub key 1 and 2 and after 10 iterations replace first two entries and this process will goes so on for entire image.

2.5 Related Research in Image encryption

2.5.1 Classic image encryption

Advance encryption standard (AES) is symmetric cryptography system, discovered by Daemen and Rijmen in 1990.this algorithm is also famous by another name is Rijndael Algorithm. This algorithm applied for image encryption with some modification in key generation and some other specific properties. Zeghid proposed an algorithm based on AES for image encryption by adding a key stream generator to ensure encryption performance.

A second algorithm gives by Subramanyan which is based on AES key expansion. In this algorithm bit wise operation XOR of a group of image pixel having 128 bit key which change for every group of pixel? .The key produce different for sender and receiver side based on the AES key generator. AES key expansion routine generate the round key word by word, where a word having size of four byte the routine generate total number of round 4*[N_r+1].cipher key are made from first four word, key having array of 16byte.

2.5.2 Public key Image Encryption

In some specific application, we don’t transmit the private key in communication on a secure channel.so we have required the public key cryptography. First public key encryption method proposed by Diffie and Hellman in 1976. In this algorithm we use the key exchange method for generating a secret shared key for the authenticated communication channel, some research done on public key encryption, one method given by shuihua. In this algorithm plain text of image break into block by matrix transformation and set of all pixels in per block transferred to DCT domain. the process like encryption, decryption, public key and private key based on DCT coefficients. The results show that it is robust against JPEG image lossy compression and another some specific attack.

Second public key encryption given by K.Ganesan which having the concept of chaos map. This algorithm designed for audio and video file.

In this section I go through many research papers based on image encryption and decryption algorithm and performance parameter which have important role in algorithm. In [1] combined study of three block cipher (Rijndael, RC6, and MRC6) algorithm. In approach author done encrypted different type of bitmap image file using above three algorithms and calculated the much deviation between original image and encrypted image, the correlation factor among the original and encrypted image, analysis the pixel values, how much time take for encryption and decryption of image.

In [2] the author proposed a block based transformation algorithm for combination of image transformation combined with encryption decryption algorithm, Blowfish. Now the plain image divided into random number of block and block transformed into transformed image. Now transformed image encrypted with blowfish encryption algorithm. The output showed that correlation will be decrease between pixels. Using on small block show that low correlation and high entropy. Thus we can say that combination of transformation and encryption algorithm will give the high level security for encrypted image.

[3] S.S Maniccam & N.G Bourbakis proposed new approach for image encryption having two step algorithms: lossless compression and encryption of image have some specific property.
The algorithm mainly based on SCAN pattern. The SCAN method describes the presentation of 2D spatial accessing method.

[4] The author proposed method for image encryption based on digital signature. In this technique digital signature added encoded form in image and encrypts the image. At the side of receiver the image will verify based on digital signature. The main function of digital signature provides the authentication of image.

[5] Algorithm for image encryption using image divided and multi-level approach: Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha Wmn Lee, and SmJmng Kim [7] proposed the encryption algorithm based on XOR operation and image blocking technique. Image having properties same gray multilevel divide into binary image. Then binary image will regenerate the binary phase encoding and these images will encrypted with binary random phase image and XOR operation.

[6] A novel image encryption based on hash function, in this algorithm author proposed a novel approach based on SHA 512 encryption algorithm. This algorithm will be executed in two steps.

First step is preprocessing operation to shuffle half of image than hash number generates a random number mask. The mask parts of image will XOR operation with first part of image.[11] This algorithm mainly based on substitution diffusion of image. Here four step in SHA-2 based image cryptosystem, first two step of substitution of image means one four of image pixel will be replace with respect S-Box of AES. Diffusion step to modify to pixel value so that a small change in one pixel value is effect of other pixels. Suppose if image size is larger than we can convert image into block and perform the same substitution diffusion on block of image.

[7] Kamli,shakerian proposed an image encryption algorithm which is modification of AES encryption algorithm. New technique is called modified Advance encryption standard (MAES) this algorithm better than AES as compare in security and faster image encryption. In modified AES algorithm we modified in original shift row transformation. First we examine the value in first row and first Colom. If it is odd, than shift row perform on rows of state. It is circularly shifts the byte in each row by a particular value. In modified AES first and third row will remains same and each byte of second row will shift to one to left. Like that same operation performs on fourth row. If it is even the shift rows operation perform on rows of state. First and fourth rows will remain same and second row of each byte will circularly shifted three to right, similarly third row will perform same operation. Due to some modification in shift rows operation, the encryption decryption speed will faster as compared than normal AES encryption algorithm.

[8] Image encryption based affine transformation and XOR operation: authors proposed the new technique which is based on affine transformation and shuffling of pixels. It is two stage of algorithm .first one XOR operation on image its means the image will encrypted once time. Resulting image uses affine transformation, the shuffling of pixels with different location having 4 bit key. The transformation image converts in (2x2) pixel block than perform the XOR operation on each block to encrypt by four 8 bit key. The encrypted image show that the correlation between pixels will be reduces after affine transformation.

[9] Image encryption using bit plane decomposition and random scrambling: Wenxin, Jiangwei,Qiudong proposed that general method for scrambling is more stable as compared classical Arnold transformation. The first stage of the algorithm a gray scale image converts into

many number of bit plane images. Than start the process of shuffling by a random scrambling algorithm and after that start the process of merge of scramble image with respect to their original level of bit plane than output image will encrypted. Because of each of bit plane image scramble using different random sequence, the location of bit position will change with respect their original position. So our algorithm will do both position exchanges as well as gray level change scrambling at same time. This is advantage of algorithm that no need of other algorithm of two different tasks.

[10] A new method of scrambling of digital image using Fibonacci number: the researcher proposed the new algorithm for encryption of digital image using the Fibonacci number. The scrambling transformation having two advantages: decoding and Encoding. Both process encoding and decoding can be applied in real time situation. In scrambling data of image will redistribution the whole image.

[11] “A symmetric encryption scheme for color BMP image” this is new image encryption technique using predefined secret key of 120 bit. first step, image break into block(P1,P2,P3…) sub sequentially into color compoents.by the help of bitwise operation will modified color component according to secret key used in algorithm. Process will complete in three rounds. To provide cipher image more robust we need feedback mechanism applied by modified secret key for each block when encrypted. This is simple and very fast technique for image encryption as well as provides more security level as compared than normal AES. Because of using high number of substitution common attack will infeasible.

Forward key mixing (FKM) and backward key mixing (BKM), two type of key mixing are used in proposed algorithm. In both type of mixing, block divide into sub block and it will be modified by sub key. Another process is substitution; simply bit wise operation will perform on pixels of sub block.

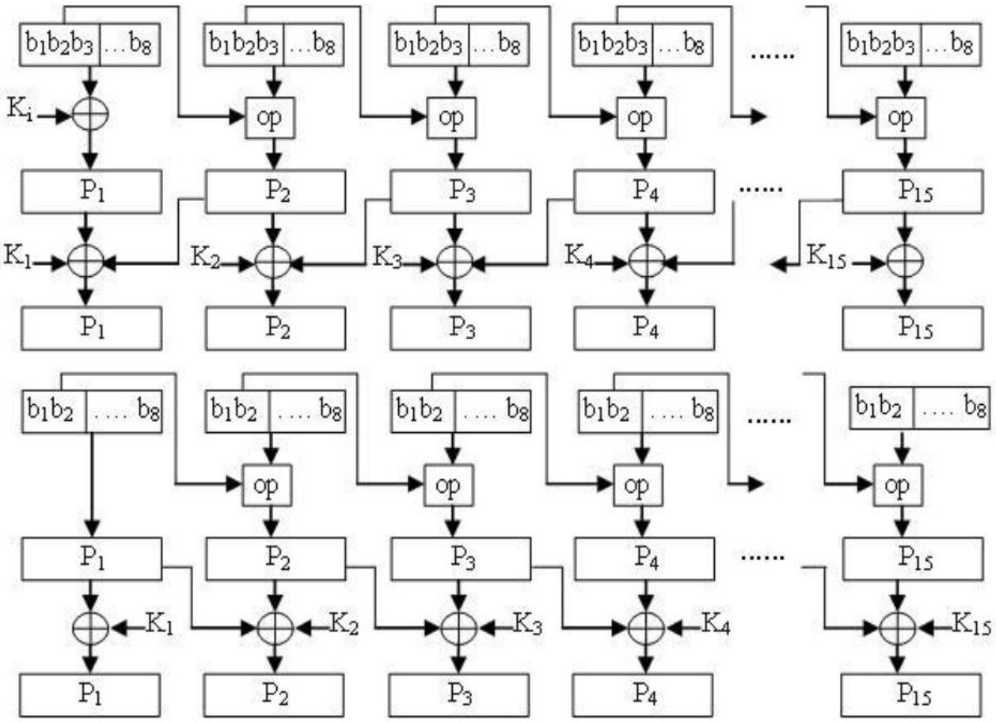


Figure 2.12 Blocks Divide into Sub Block and Modified by Key [13]

In the substitution process first step image block divided in to 15(p1, p2, p3…) sub block and each sub block having the 8 (b1, b2, b3...) bit. Each sub block having two step operation, first block(p1) modified by XOR with first sub key and reaming sub block will modified according operation show in table.

Bit value	**Operation on Sub block for encryption**
0	P_i=NOT(p_i) XOR (K_i mod 15)
1	P_i=NOT(p_i XOR (K_i mod 15))
2	P_i=(p_i) XOR (K_i mod 15)
3	Invert all bit p_i= NOT(p_i)
4	Circular left shift by one position(p_i=p_i<<1)
5	Circular left shift by one position(p_i=p_i>>1)
6	P_i= NOT(circular left shift by one position)
7	P_i= NOT(circular right shift by one position

Figure: 2.13: Table of Operation on Sub Block for Encryption [13]

The operation on each sub block depend on first most significant three bit of sub key of their previous block .suppose , the value of first two sub block p1 and p2 are 225 ,173 respectively . The value of p2 after applied XOR operation on its cross ponding bit value 7 change of its previous sub block change to 41.in step second backward key mixing the remaining block will modified according to given table [1].

[12]" A modified AES based Algorithm for image encryption'' author analyzed the AES algorithm for image encryption and modified with add a key generator (A5/1, W7) to AES purpose to improve the encryption process. Main motive of this encryption algorithm to reduces the entropy information of image. The new image encryption techniques based on modified AES algorithm with add a key generator. Here author using two type generators, A5/1 and W7 key stream generator. Block diagram of algorithm shown in figure [2].

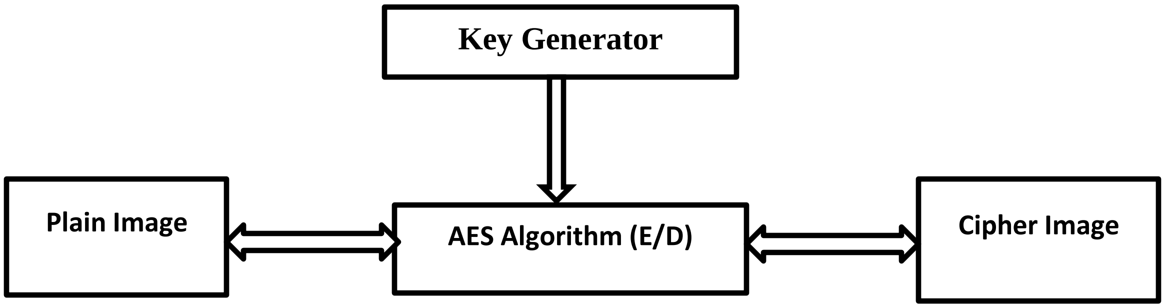


Figure 2.14: Block Diagram of Image encryption based on AES [13]

The first key generator A5/1 cipher is made by three linear feedback shift regesters,R1,R2,R3 having the length 19,22,23 respectively .Each register shifted by specific clock cycle which is determined by some majority function. Three bits C1, C2, C3 uses by majority function. The 64 bits of the key map in register with initial state after each clock cycle last bit of register XORed to produce one output bit.

Second one is W7 key stream generator, W7 algorithm is byte wide it is process the synchronous of cipher optimized for efficient hardware implementation with very speed data rate. W7 algorithm is symmetric key algorithm having the key size 128 bit. W7 having 8 similar block (c1c2c3c4…) and each model contain three LFSRs registers and one majority function. Here author used concept of control unit and function unit. Main objective of function unit to generated the key stream.

2.6 Image Security Measurement

2.6.1 Image correlation coefficient:

Image correlation is defined the relations between the neighboring pixel after the encryption the bit map images. Correlation is measurements the accurate changes in 2D or 3D images. Digital image correlation is rapidly popular for imaging technology. The main function of correlation coefficients to calculate that shifted in pixel to their position. Now days all application of image like image compression, image analysis using the image correlation. To calculate for image correlation formula is given below.

$$Rn = \frac{\sum_{i=t-n+1}^{t}(xi - xi')(yi - yi')}{\sqrt{\sum_{i=t-n+1}^{t}(xi - xi')^2 . \sum_{i=t-n+1}^{t}(yi - yi')^2}}$$

Where X'= mean2(X) and Y'=mean2(Y)

2.6.2 Image Histogram

Image histogram is graphical representation of pixel distribution among the images. Each shows the number of pixel in each particular value. Any person can observe the image with seen the histogram of image. Horizontal axis show the tonal and vertical axis shows the total number of pixel that tonal. The horizontal axis Left side show the black or dark and middle show the medium gray and right show the light and pure white area.

Syntax of histogram in mat lab given as follow:

Imhist= (bitmap Image)

2.6.3 Entropy Information of Image

The entropy information of image was discovered by C.E Shanon in 1949. Entropy of image gives the measurement of change in image with actual image. Its means how much plain image changes to encrypted image? It concerns about the error, image compression and all about changes in image Entropy determined by the Shannon formula.to calculate entropy H (m) of image m.

$$H = -\sum p(x) \log p\ (x)$$

Where p(x) show the probability of function p, however the image is encrypted their entropy should be 8. If encrypted image entropy is less than 8 it may be possible to encrypted image may be decrypted. But when entropy is 8 than its predictability is very tough. Its means the image encrypted with the very strong encryption algorithm.

2.6.4 Key Space Analysis

Key space size is total number of possible key to that can be used in algorithm .for the security purpose the key should be large too unpredictable to brute force attack. The proposed algorithm has the 2^{128} possible combination of key. In this algorithm we are using the symmetric key. So all possible combination key is sufficient for secure transmission of image.

Chapter 3

Proposed Work

3.1 Problem Statement

Let there be big size of bitmap image (size in MB) than AES, blowfish algorithm takes more time to encrypted the image so encryption –decryption time ratio will be high.

The objective of encryption -decryption algorithm to make more efficient following constraints:

- To reduce the encryption and decryption time.
- Image Histogram
- Image Entropy
- Image Correlation
- Security analysis

The main objective of work to reduces the time of encryption and decryption. Image histogram is technique to plot the pixel values of image (vertical axis) with corresponding brightness value (horizontal axis). Image entropy is quantity which shows the characteristics of image that is amount of information which is coded by encryption algorithm. The value of low entropy image show that a lot of black sky, having very little contrast .an encrypted image having the entropy value very close to 8, But in most of case encrypted image having entropy approximate the 7.9999. Image correlation defined that what relation between the neighboring pixels is. Image correlation value must be close to zero to show used good encryption algorithm.

3.2 PROPOSED SOLUTION

Let we have taken bitmap image (1024x1024) where the 1024 rows and 1024 column.

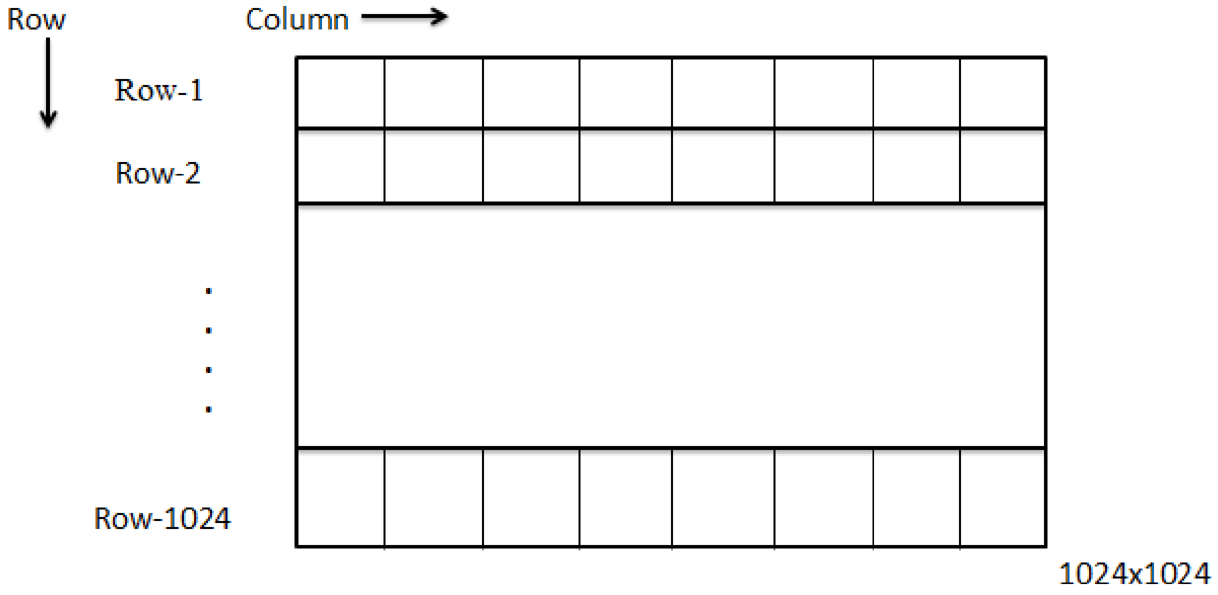
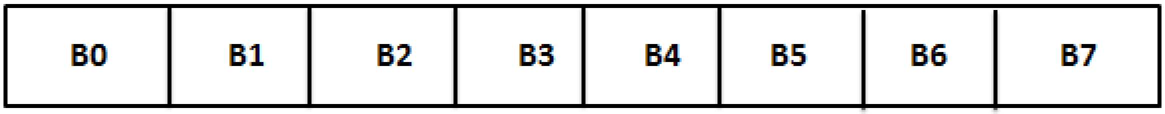


Figure 3.1: Bitmap Image (1024x1024) converts into row and column

Encryption process:

The encryption process for the bitmap image with uses Advance encryption Standard (AES) having symmetric key 128 bits. Same key will be uses in the encryption and decryption process for enhancement of algorithm.

Here the first step that row1 break into block having the size of 128 bits each block than total number of block will be 8 in row1.same process do repeat for row no 2.

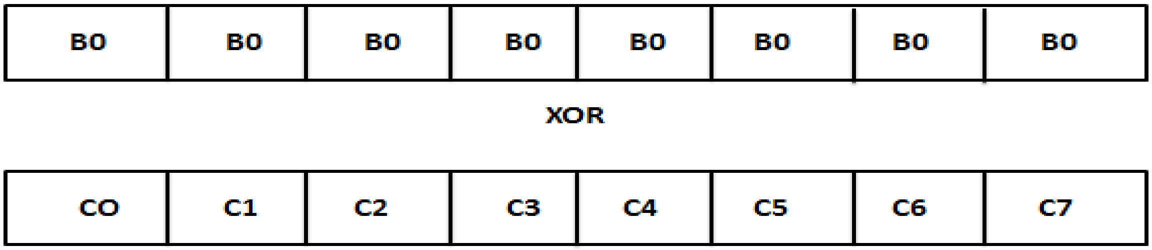


Row :1

Take the first block B0 (128 bit) encrypted with Advance encryption Standard (AES)

E= Encrypt AES (B0)…………………………………. (1)

Encrypted B0 block expand up to size of 1024 bit. It means make the duplicate copy of B0 up to size of image. The expandable B0 is shown in figure.



Now row-2 breaks into blocks (C0, C1, C2, C3, C4, C5, C6, C7) having each block size 128 bits. Now perform the XOR operation between row-1 and row-2 and get the result of Encrypt_row-2

Encrypt_row-2= Expand (B0) XOR row-2…………….. (2)

Now second step is take next block B1 (128 bits) and encrypt with Advance encryption standards (AES)

E= Encrypt_ AES (B1)………………………………. (3)

Encrypted B1 block expand up to size of 1024 bit and perform the XOR operation with row-3 and get the result Encrypt row-3. The same step will be repeat for the block B2,B3,B4,B5,B6,B7 and perform XOR operation with row-3,row-4,row-5,row-6,row-7, row-8 and get the result encrypted row-3,row-4,row-5,row-6,row-7, row-8 . Now row-1 encrypt with Advance Encryption Standard (AES).

E= Encrypt_ AES (row-1)…………………………….. (4)

Next step of encryption algorithm is going through row-9 and row-9 will break into blocks having size of each block 128 bits. The total number of block in row-9 will be 8.

The same process of encryption will repeat for the row-9 and so on. The process do until that all rows have been encrypted.

Decryption Process

The processes of decryption of encrypted image have following steps. At the time of decryption same key will be used for decrypt the image. Its means it is symmetric encryption decryption algorithm.

Let take the encrypted bitmap image and decrypt the first row (row-1) with Advance encryption Standard (AES) and we get the row-1.

Row-1= Decrypt- AES (row-1)…………………………. (1)

Second step decrypt the block B0 with AES and get the Expand Block B0.

Expand B0= Decrypt-AES (block B0)…………………… (2)

Third step is Do the XOR operation between Expand B0 and row-2 and get the original row-2.

Encrypted –row-2 XOR Expand B0= Row2…………..... (3)

The same process repeat for Encrypted row-3 and expand block B1 and get cross ponding original row.

Encrypted –row-3 XOR Expand B1= Row3…………… (4)

Repeat the process for row-9 and expand block B8 and get cross ponding original row-9.

Encrypted –row-9 XOR Expand B8= Row9………….... (5)

When the row-1 to row -9 decrypted, than go for row no 10 and repeat same step from1 to 5.

3.3 Flow chart of Encryption Process

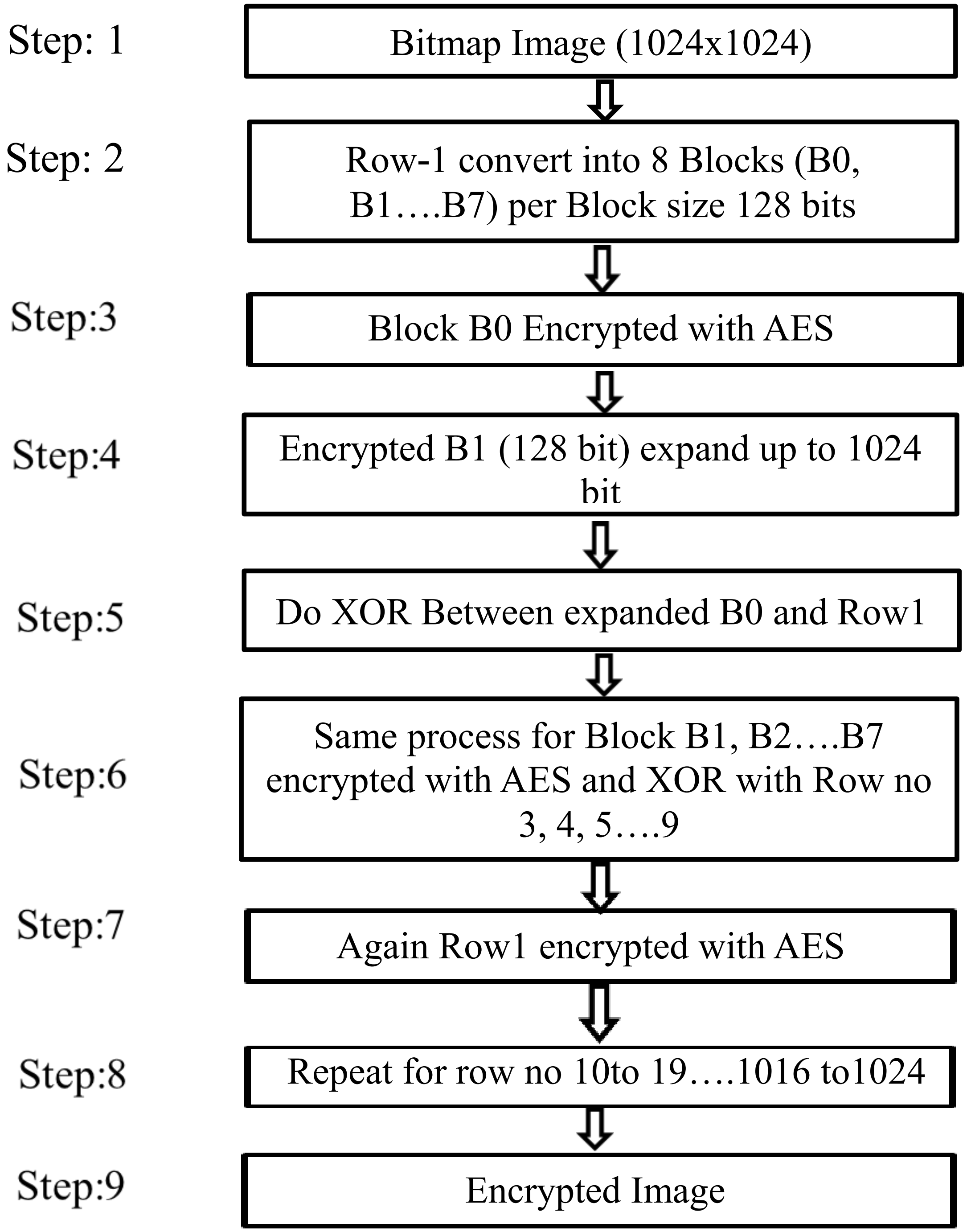

Step: 1
Bitmap Image (1024x1024)
Step: 2
Row-1 convert into 8 Blocks (B0, B1….B7) per Block size 128 bits
Step:3
Block B0 Encrypted with AES
Step:4
Encrypted B1 (128 bit) expand up to 1024 bit
Step:5
Do XOR Between expanded B0 and Row1
Step:6
Same process for Block B1, B2….B7 encrypted with AES and XOR with Row no 3, 4, 5….9
Step:7
Again Row1 encrypted with AES
Step:8
Repeat for row no 10to 19….1016 to1024
Step:9
Encrypted Image

Figure 3.2: Flow Chart of Proposed Encryption Algorithm

3.4 Flow chart of Decryption Process

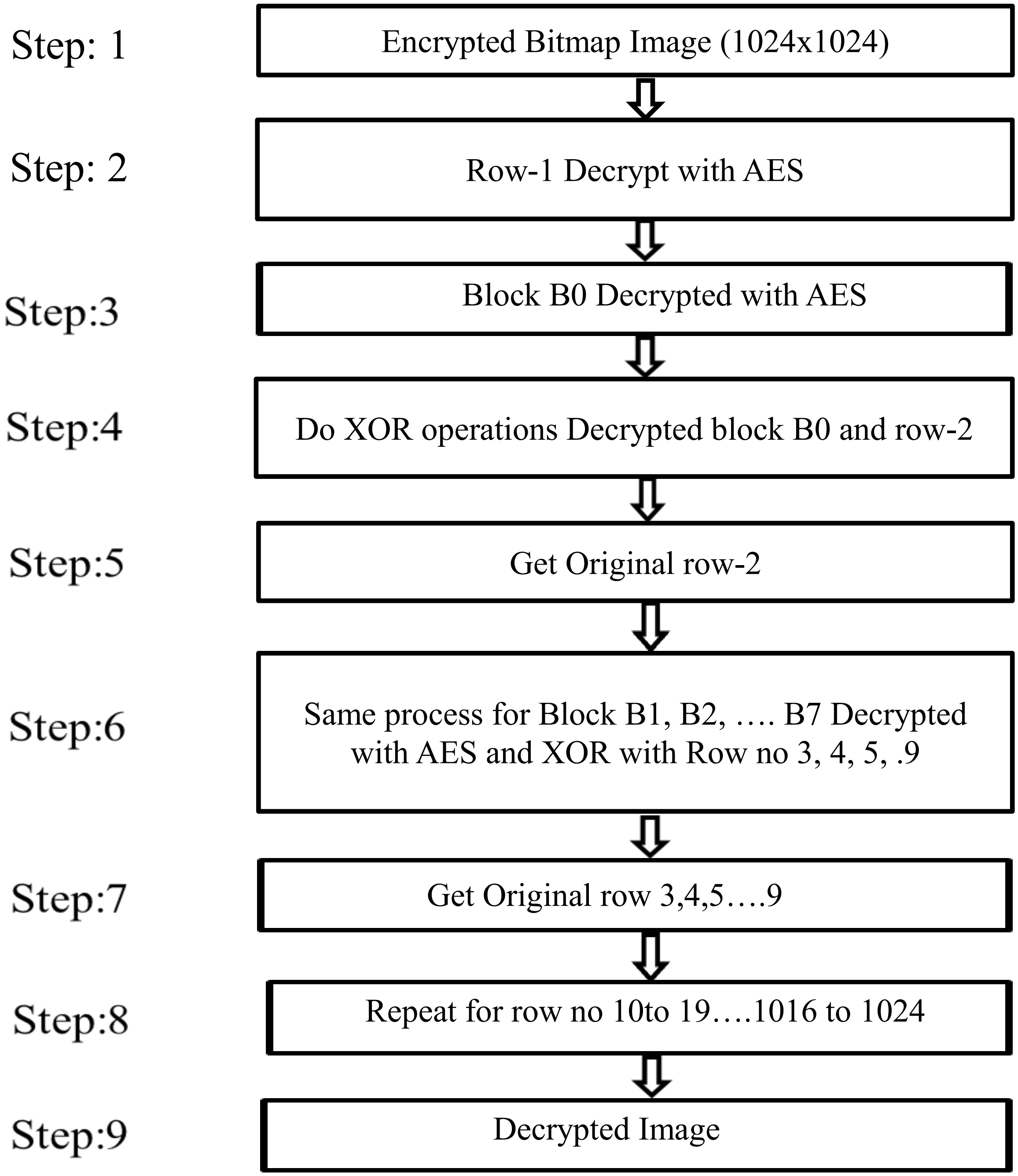

Step: 1
Encrypted Bitmap Image (1024x1024)
Step: 2
Row-1 Decrypt with AES
Step:3
Block B0 Decrypted with AES
Step:4
Do XOR operations Decrypted block B0 and row-2
Step:5
Get Original row-2
Step:6
Same process for Block B1, B2, …. B7 Decrypted with AES and XOR with Row no 3, 4, 5, .9
Step:7
Get Original row 3,4,5….9
Step:8
Repeat for row no 10to 19….1016 to 1024
Step:9
Decrypted Image

Figure 3.3: Flow Chart of Proposed Decryption Algorithm

3.5 Architecture Model of Proposed Algorithm

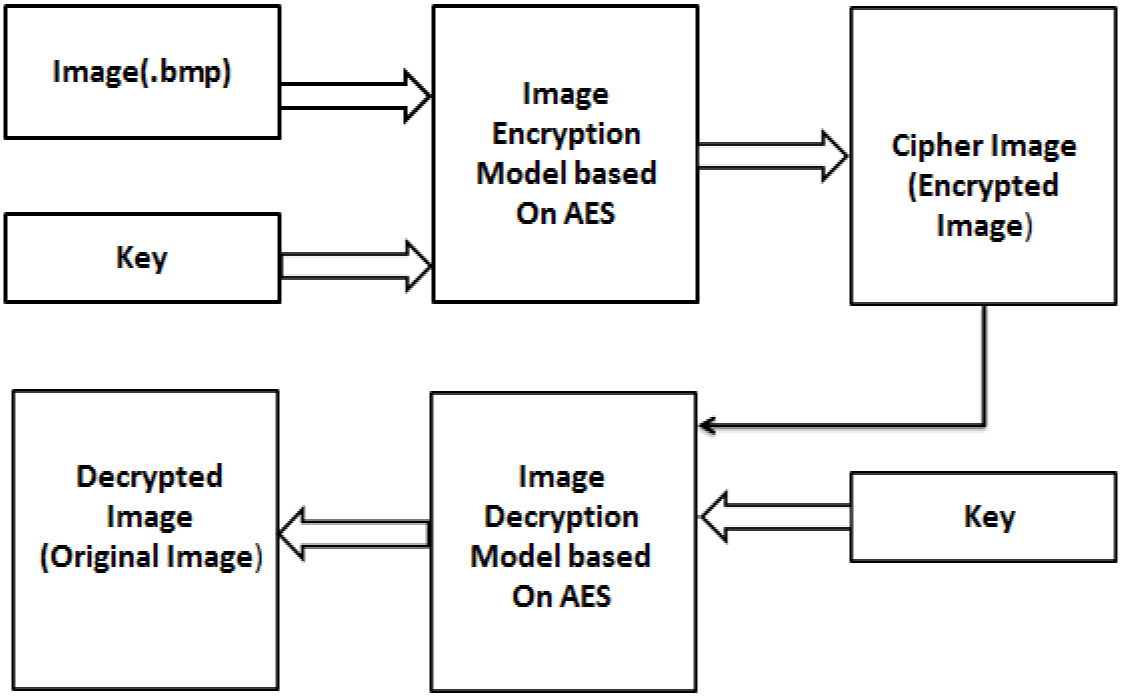

Image(.bmp)
Key
Image Encryption Model based On AES
Cipher Image (Encrypted Image)
Decrypted Image (Original Image)
Image Decryption Model based On AES
Key

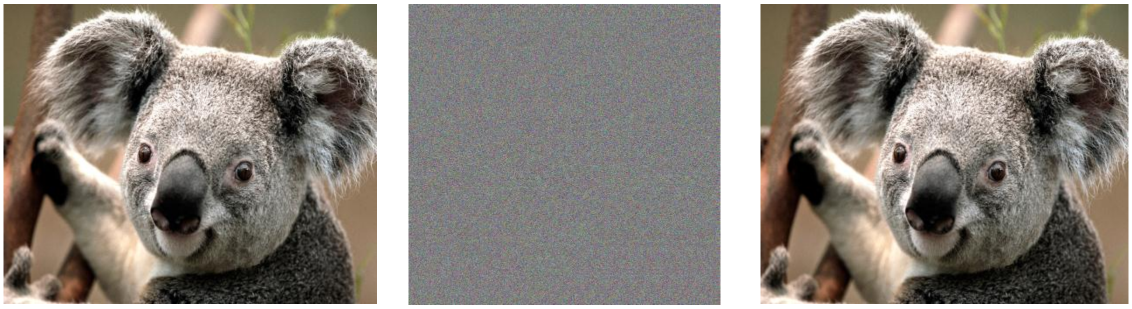
Figure 3.4: Arcitecture Model of Proposed Encryption Decryption Method

Chapter 4

Implementation, Testing and Results Analysis

We take the intinal bitmap image size 2.25 MB (cat image) now scaling this image with 25% and store all images in input file. First bitmap image 2.25, MB apply encryption algorithm to encrypt that image. The encryption-decryption code done in Java and Image entropy , Histogram and correlation calculate in Matlab.

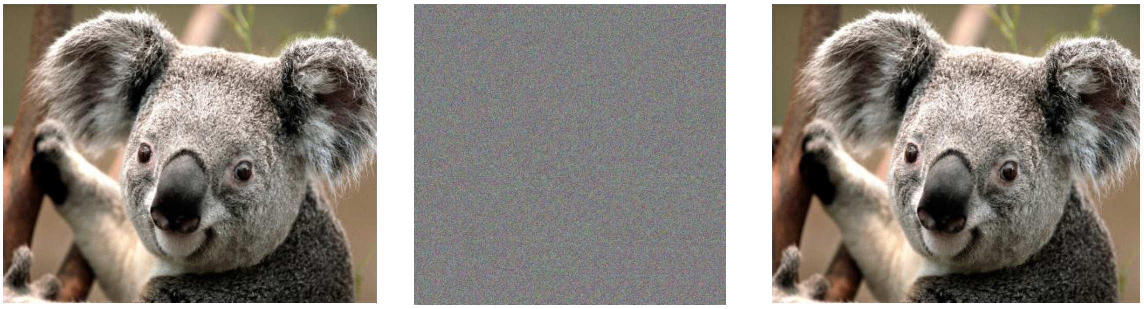
Image-1(size 2.25 MB)



Original image Encrypted image Decrypted image

Figure 4.1

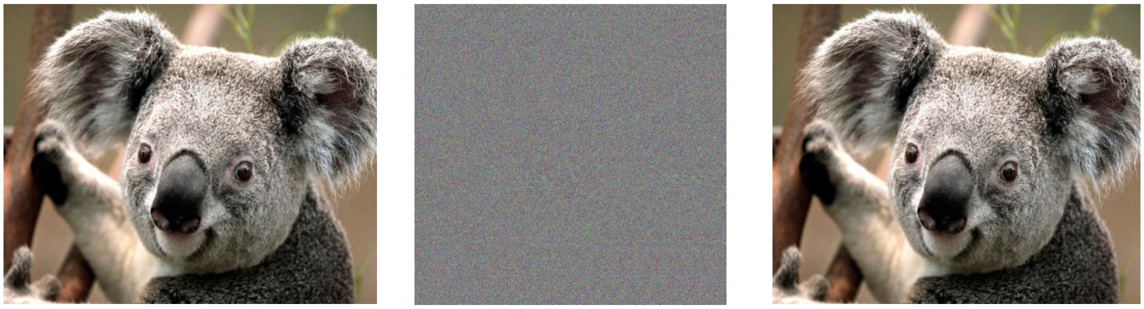
Image-2(size 3.51 MB)



Original image Encrypted image Decrypted image

Figure 4.2

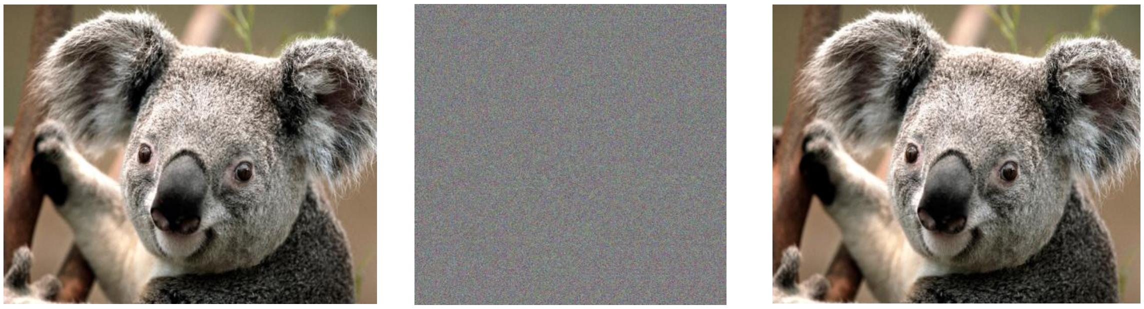
Image-3(size5.49 MB)



Original image Encrypted image Decrypted image

Figure 4.2

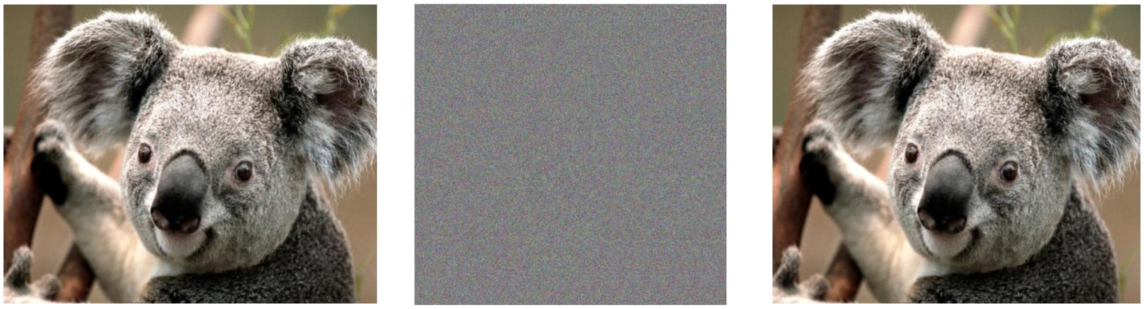
Image-4(size8.58 MB)



Original image Encrypted image Decrypted image

Figure 4.4

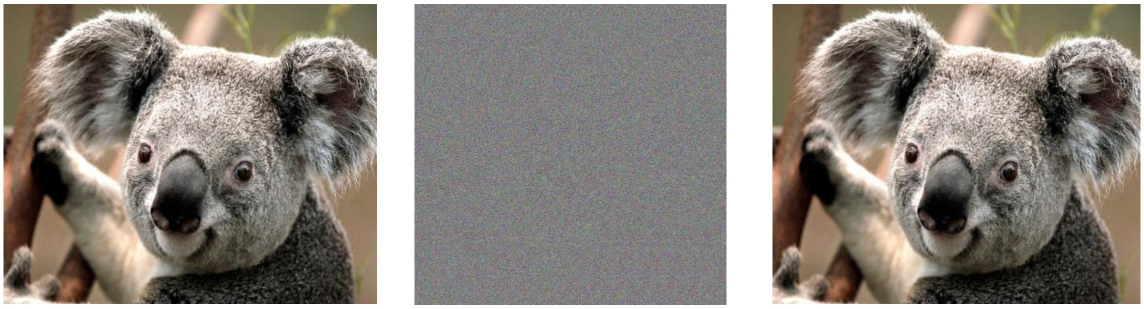
Image-5(size 13.4 MB)



Original image Encrypted image Decrypted image

Figure 4.5

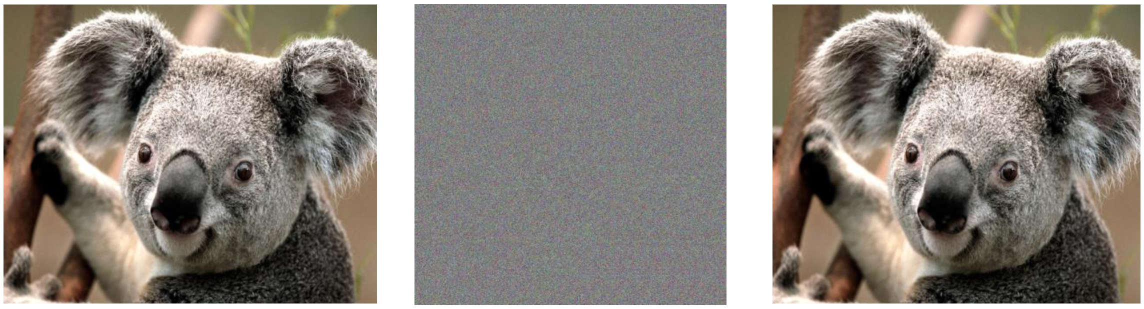
Image-6(size 20.9 MB)



Original image Encrypted image Decrypted image

Figure 4.6

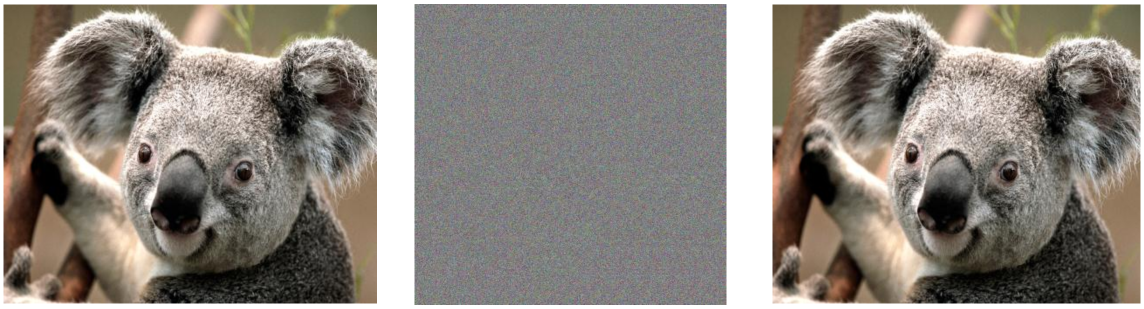
Image-7(size 32.7 MB)



Original image Encrypted image Decrypted image

Figure 4.7

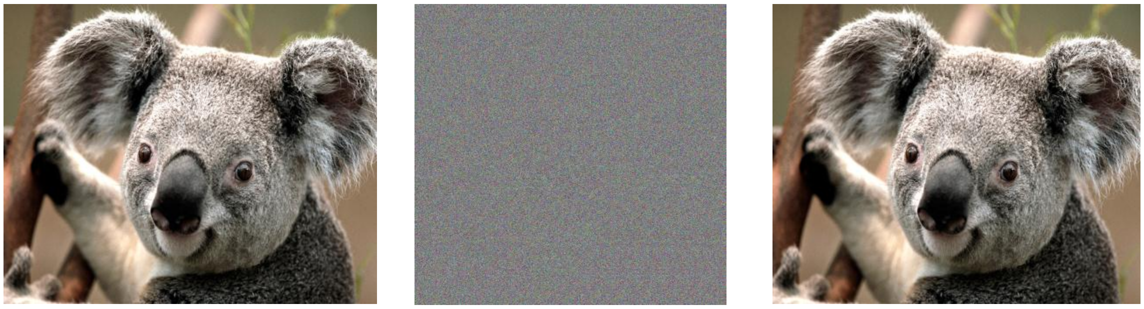
Image-8(size 51.1 MB)



Original image Encrypted image Decrypted image

Figure 4.8

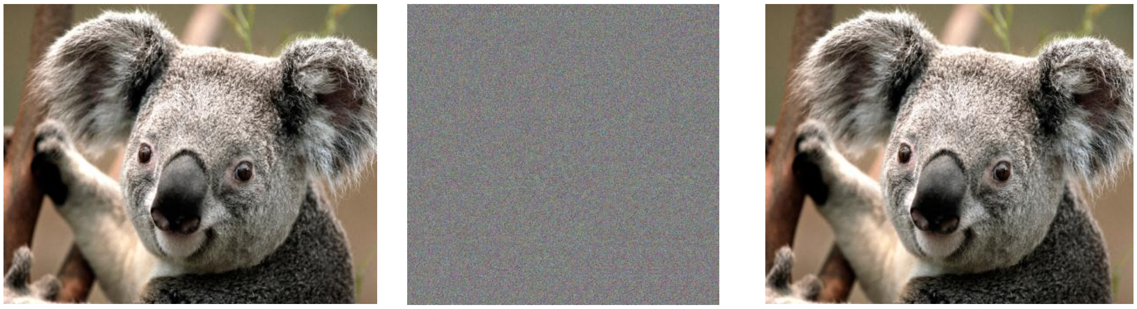
Image-9(size 79.9MB)



Original image Encrypted image Decrypted image

Figure 4.9

Image-10(size 124 MB)



Original image Encrypted image Decrypted image

Figure 4.10

Here take the 10 bitmap image with having different size and encrypt all image with consider the encryption and decryption time. The main objective of encryption algorithm to reduces the time of encryption and decryption.

In the table shows the size if bmp image and cross ponding time taken in encryption -decryption with Advance encryption Standard (ASE) and modified encryption decryption algorithm.

Image(Size in MB)	Encryption decryption time by AES(second)	Encryption decryption time by Proposed Algorithm(second)
2.25	0.595	0.542
3.51	0.712	0.592
5.49	0.894	0.699
8.58	1.19	0.828
13.4	2.253	0.998
20.9	3.407	1.247
32.7	5.229	1.584
51.1	7.522	2.107
79.9	9.468	2.934
124	17.924	4.529

Figure 4.11: Table of Encryption Decryption Time

All images have been encrypted with Advance encryption standard (AES) and proposed algorithm. Here shown in graph about the time take by both algorithms.

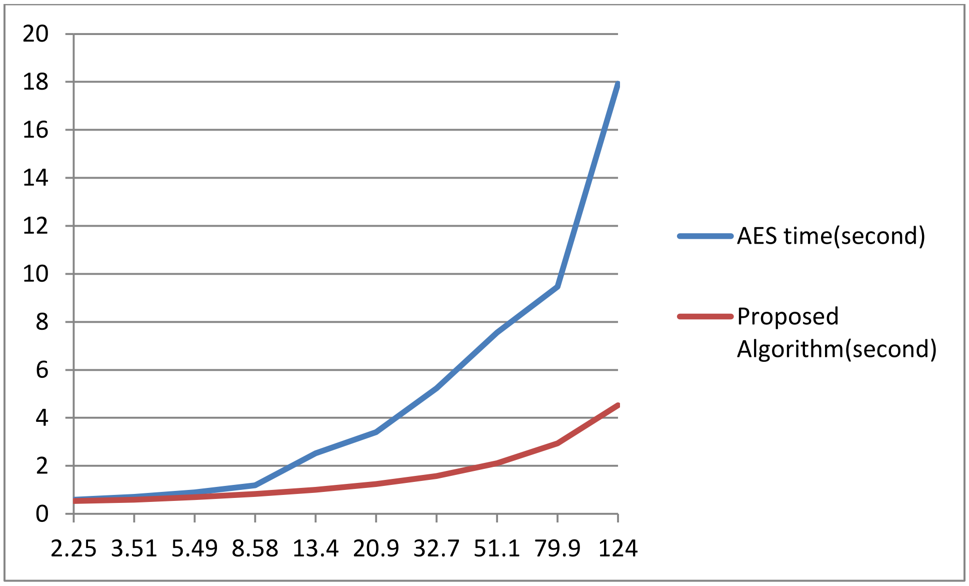
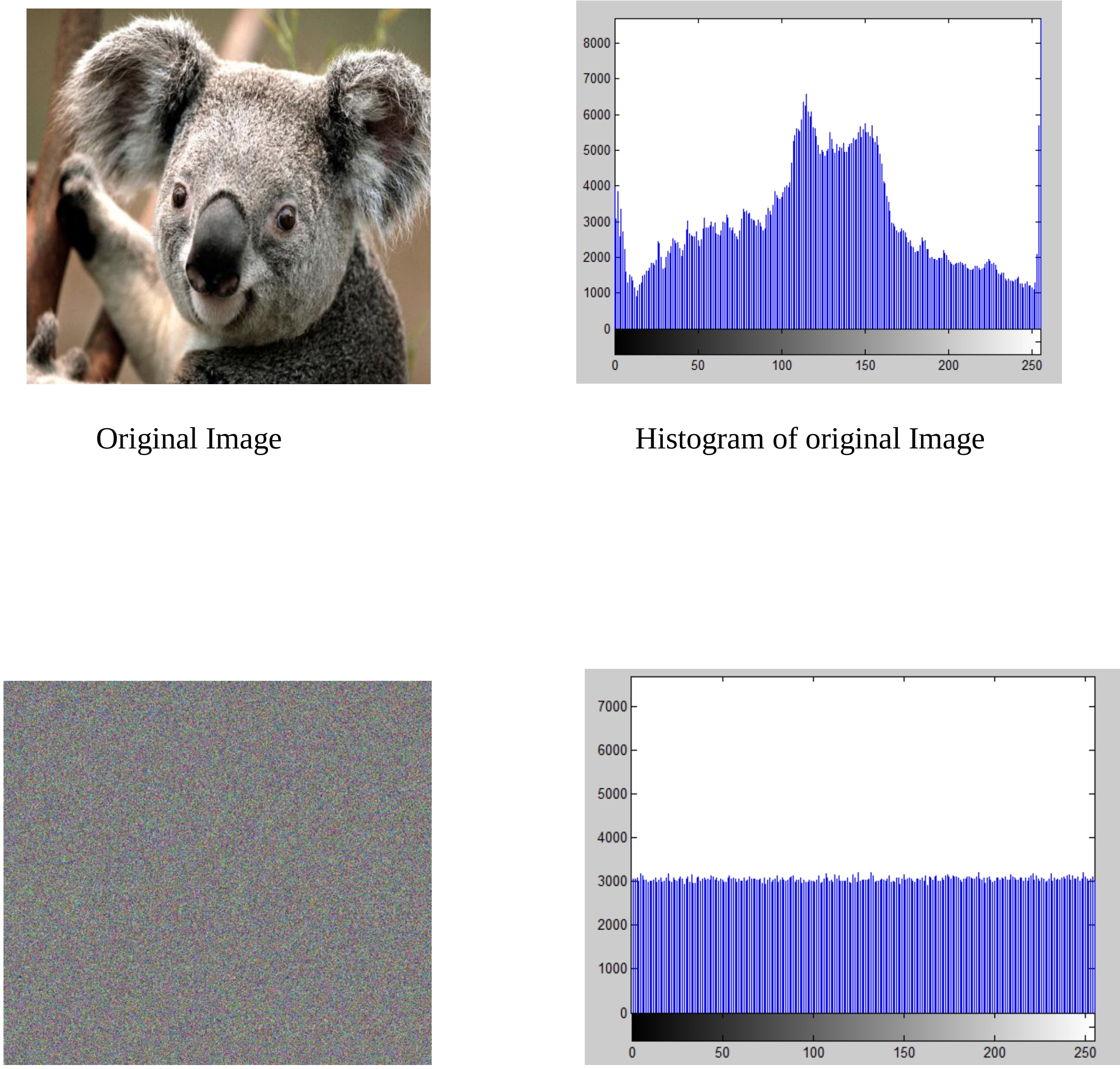


Figure 4.12: Graph of Encryption Decryption Time

2. Image histogram

Image-1(size 2.25 MB)



Original Image

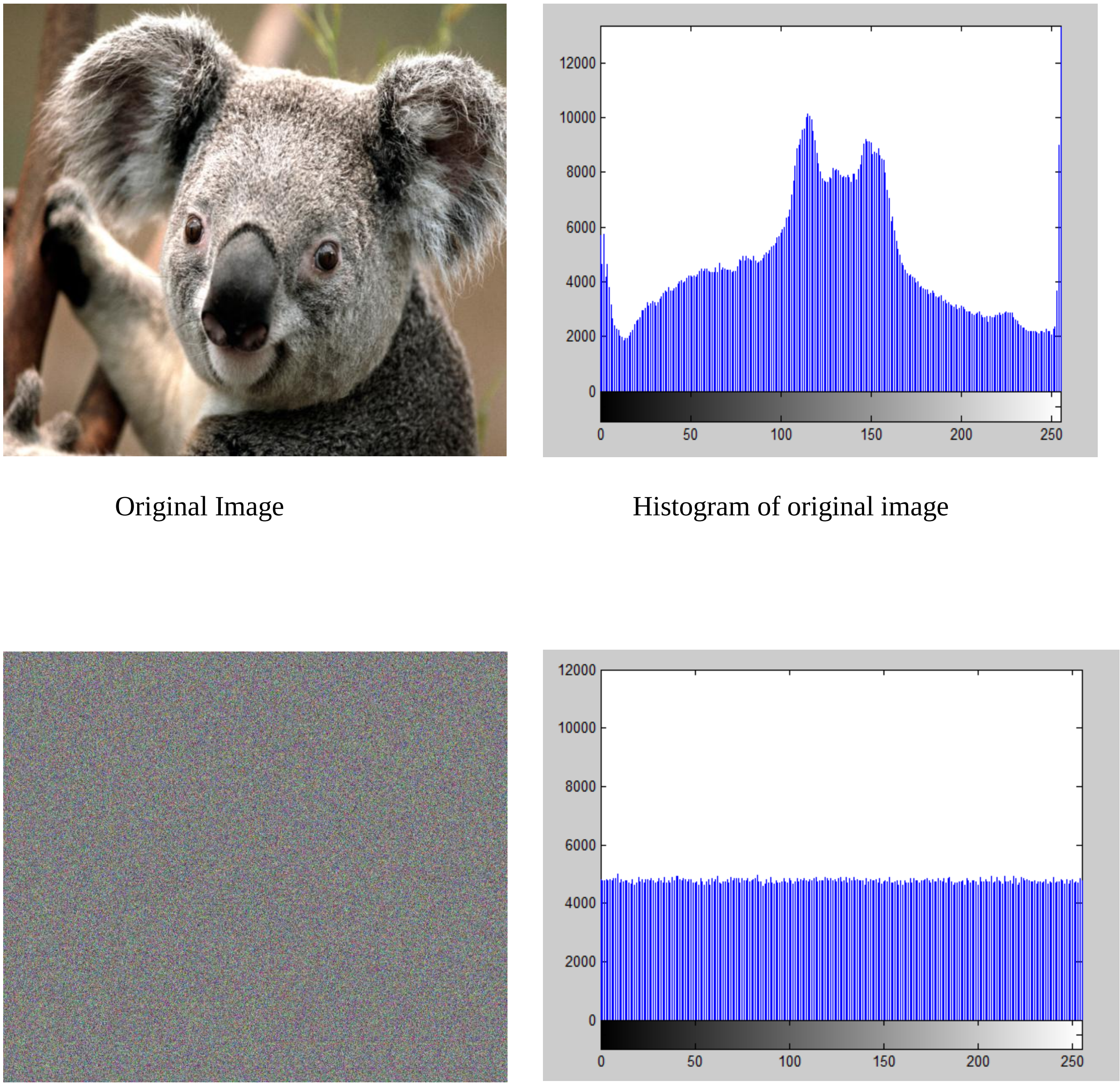
Histogram of original Image

Encrypted Image

Histogram of Encrypted image

Figure 4.13

Image-2(size 3.51 MB)



Original Image

Histogram of original image

Encrypted Image

Histogram of encrypted Image

Figure 4.14

3.1 Image Entropy of proposed Algorithm

Bitmap Image	Entropy of plain image	Entropy of Encrypted Image
Image-1(size 2.25MB)	7.8254	7.9999
Image-2(size 3.51MB)	7.8429	7.9999
Image-3(size 5.49MB)	7.8408	8.0000
Image-4(size 8.58MB)	7.8408	8.0000
Image-5(size 13.4MB)	7.8408	8.0000

Figure 4.15: Table of Image Entropy of proposed Algorithm

3.2 Image Entropy of Advance Encryption standards (AES).

Bitmap Image	Entropy of plain image	Entropy of Encrypted Image
Image-1(size 2.25MB)	7.8254	7.8987
Image-2(size 3.51MB)	7.8429	7.9123
Image-3(size 5.49MB)	7.8408	7.9432
Image-4(size 8.58MB)	7.8408	7.9569
Image-5(size 13.4MB)	7.8408	7.9889

Figure 4.16: Table of Image Entropy of AES Algorithm

4.1 Image correlation coefficient of Proposed Algorithm

Direction	Plain Image	Cipher Image
Horizontal	0.9728	-8.8776e^{-05}
Vertical	0.9692	-.0014
Diagonal	0.9660	0.0008

Figure 4.17: Table of Image correlation coefficient of Proposed Algorithm

Chapter 5

Conclusion and Future Work

Today the world of multimedia, the security of images is very necessary to communicated over the network. In this research we proposed a new encryption for bitmap image which is based on AES algorithm. The main objective thesis that designed very fast image encryption algorithm, that provides good security from unauthorized person. Some confidential image needs the security to transmit over the network. We have studies all method of image encryption and got all technique have own way to encrypt the image. Advance Encryption Algorithm, Data encryption standard and blowfish is real time encryption techniques which have covered in my research. Each method may be possible for different application, some algorithm giving fast encryption and some give the high security level.

In this research we proposed encryption algorithm for bit map provide the faster encryption method as compare than Advance Encryption Standard. Propose algorithm also provide a good security level because it’s double encryption by AES Limitation of Proposed scheme that designed for only bitmap images. Here the encryption decryption ratios will less compare than AES. Proposed method mainly useful for when the size of bitmap images in Mb. Its means when the size of bitmap high its will give good throughput. The future work of research to deploy the encryption of thousands bit map image, so this algorithm is very useful for parallel encryption algorithm.

References

[1] Bourke, P. (2011). BMP Image Format, (July 1998), 3–5.

[2] https:// upload.wikimedia.org/wikipedia/commons/thumb/d/d6/ECB_encryption.svg/1280px-ECB_encryption.svg.png.

[3] Zeghid, M., Machhout, M., Khriji, L., Baganne, a, & Tourki, R. (2007). A Modified AES Based Algorithm for Image Encryption. International Journal of Computer Science & Engineering, 1(1), 70–75. Retrieved from http://scholar.google.com/scholar?

[4] Radhadevi, P., & Kalpana, P. (2012). SECURE IMAGE ENCRYPTION USING AES, 115 117.

[5] Brindha, K., Sharma, R., & Saini, S. (2014). Use of Symmetric Algorithm for Image, 4401–4407.

[6] Moussa, a. (2005). Data encryption performance based on Blowfish. 47th International Symposium ELMAR, 2005., (June), 131–134. http://doi.org/10.1109/ELMAR.2005.193660

[7] Subramanyan, B., Chhabria, V. M., & Sankar Babu, T. G. (2011). Image encryption based on AES Key Expansion. Proceedings - 2nd International Conference on Emerging Applications.

[8] Kamali, S., & Shakerian, R. (2010). A new modified version of Advanced Encryption Standard based algorithm for image encryption. 2010 International Conference on Electronics and Information Engineering (ICEIE 2010), 1(Iceie), 141–145.Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5559902.

[9] Younes, M. A. B., & Jantan, A. (2008). Image Encryption Using Block-Based Transformation Algorithm. International Journal of Computer Science, 35(1), 407–415.

[10] Techniques, D. (2013). A Survey On Different Image Encryption and, 4(1), 113–116.

[11] Zeghid, M., Machhout, M., & Khriji, L. (2007). A modified AES based algorithm for image encryption. World Academy of Science, Engineering and Technology, 1(1), 70–75.

[12] Pareek, Narendra K, Vinod Patidar, K. K. S. (2011). A Symmetric Encryption Scheme for Colour BMP Images. IJCA Special Issue on “Network Security and Cryptography”", 42–46.

[13] Moussa, a. (2005). Data encryption performance based on Blowfish. 47th International Symposium ELMAR, 2005., (June), 131–134. http://doi.org/10.1109/ELMAR.2005.193660.

[14] Soleymani, A. (2012). Transmission, 6(6), 225–232.

[15] Brindha, K., Sharma, R., & Saini, S. (2014). Use of Symmetric Algorithm for Image, 4401–4407.

[16] Seyedzade, S. (2010). A novel image encryption algorithm based on hash function. … Vision and Image …, 1–6. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5941167.

[17] Li, S., & Zheng, X. (2002). On the security of an image encryption method.pdf. 2002 IEEE International Symposium on Circuits and Systems, 2(01010101), II–708 – II–711.

[18] Li, X., Knipe, J., & Cheng, H. (1997). Image compression and encryption using tree structures.

[19] Notice of Violation of IEEE Publication Principles “ Enhanced Blowfish algorithm using bitmap image pixel plotting for security improvisation ” by Nirmala Palaniswamy , Dipesh Dugar , Dinesh Kumar Jain , Raaja Sarabhoje in the 2010 2 nd International Conference on Education Technology and Computer (ICETC).

[20] Logeshwari, A. S. R. (2010). A Secure PMS based on Fingerprint Authentication and Blowfish Cryptographic Algorithm, 424–429.

[21] Alabaichi, A., & Ahmad, F. (2013). Security Analysis of Blowfish algorithm, 12–18.

[22] Kamali, S., & Shakerian, R. (2010). A new modified version of Advanced Encryption Standard based algorithm for image encryption. 2010 International Conference on Electronics and Information Engineering (ICEIE 2010), 1(Iceie), 141–145. Retrieved from http://ieeexplore.ieee.org /xpls/abs_all.jsp? arnumber=555990.

[23] Encrypted, I. (2005). Quality for Bitmap, (Nrsc).

[24] Munir, R. (2012). Security analysis of selective image encryption algorithm based on chaos and CBC-like mode. 2012 7th International Conference on Telecommunication Systems, Services ,and Applications (TSSA), (2), 142–146. http://doi.org/10.1109/TSSA.2012.6366039.