Dedicated

To

My Parents

&

My Family

A Contribution to Text Embedding into Image Encryption Algorithm

By

MAHWISH BANO

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2016

A Contribution to Text Embedding into Image Encryption Algorithm

By

MAHWISH BANO

Supervised By

PROF. TARIQ SHAH

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2016

A Contribution to Text Embedding into Image Encryption Algorithm

By

MAHWISH BANO

A Thesis Submitted in the Partial Fulfillment of the requirement for the Degree of

DOCTOR OF PHILOSOPHY

In

Mathematics

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2016

Introduction

The concept of text embedding into images was first introduced by Trithmious in his book on magic [1] and thereafter a number of researchers embedded text into the famous images. With the ushers of modern computers and fast electronics machines, text embedding has become a well-established branch of cryptology. These techniques have extensive applications in various branches of information science, business and system engineering, medical sciences, retrieval of ancient's heritage photographs. Later on researchers have developed fast and secure algorithms using various embedding techniques and inherited capabilities of pixels manipulations. Many books and a large number of research publications have been done and they mostly focused on the development of algorithms [2, 3, 4, 5].

The first documented use of such field was in 440 BC by Herodotus in his famous book in "The histories of Herodotus" where he used wax tablets for writing secret messages. Another one was writing messages on bare head and then waited for the hair to grown up. Apart from these famous methods people were in use of various other techniques to hide secret messages. In modern era the concealment of information was done into digital software files.

In [6], an algorithm was proposed based on lossless packing and encryption of parallel and gray scale images. A vector quantization for designing better crypto system for images was then developed in [7]. Researchers first time proposed an algorithm in which they used binary phase exclusive OR and image dividing technique [8]. The chaotic map with some initial key was first introduced in [9]. The chaotic map was generated with some initial parameters to get a non-periodic sequence in binary images. This work was extended and proposed chaos-based stream

cipher which composed of two chaotic logistic and external secret key of various lengths was developed in [10]. Another algorithm [11] was developed in which two chaotic frameworks (Lorenz and Rosseler) were used. These systems used large key space with high level security and speed. A wavelet technique was developed by using Discrete Cosine Transformation which compressed the image and separated into little squares together with rotation matrix for encryption [12]. The widely recognized system was developed in [13] in which the LSB were used for text embedding. Further to this an algorithm was developed by combining LSB with DCT to insert the text messages into digital image [14]. An analysis was carried out and rectified this method to use of DCT with base mutilation of image quality [15]. Edges of images were also utilized to conceal instant message in steganography [16]. Information concealing strategy was presented in the dark area of the image using LSB [17]. A novel lossless or reversible information concealing plan for binary images was developed useful for binary images not for gray or RGB images [18]. In [19], authors proposed LSB based image hiding method, the LSB were chosen by comparing the intensity based pixels of neighboring pixels which enhance the capacity of embedding area of the image. In the last decades tremendous use of steganography methods were done for text embedding in text to text, text to video, text to audio, text to images with latest technique of Graph Cut method.

Most of the researchers have done with the emphases to implementation of algorithms only without thorough analyses which have made the technique optimal. There were few important aspect of implementation, the strength of the algorithm in terms of attack and robustness of the algorithms. In the present thesis we have not only developed new algorithm using existing embedding techniques [25] but also employed the robustness of the algorithm in terms of computing time and security. In the earlier works [35, 36, 40, 41, 42, 43] the emphasis was on

the implementation of an algorithm for text embedding only. In the present analysis we developed an algorithm on image encryption coupled with Genetic Algorithm. This gives the strength to the algorithm and randomness placing the text into image by appropriate application of genetic algorithm. To make algorithm more secure, we further improved our algorithm by introducing modern encryption technique like DES in combination with MPWLCM for text encryption and then used encrypted text into our proposed algorithm. The MPWLCM used with DES gave the strength in developing non periodic chaotic linear sequence. It has a double security as we used DES with MPWLCM.

Graph cut technique is a technique which splits graph into two detached subsets. In this procedure the image is constructed in form of graph that contains nodes and vertices. Each node represents a single pixel. The problems are solved in vision using this technique. It is an idea implemented here, to use this graph cut technique for encrypted text embedding into our proposed algorithm. The graph cut technique is first time reported here together with GA-MPWLCM in our proposed algorithm on symmetric key cryptographic system blend of DES, PWLCM, MPWLCM and Genetic algorithm. Further to our proposed composite algorithm, which consists of graph cut combined with GA-MPWLCM, an additional effort is made to use SCAN pattern with XOR in image reconstruction which made our entire system highly secure and unbreakable by the intruder. Analysis is also carried out to show the strength of our proposed algorithm.

The chapter-wise breakdown of the thesis is as follows: In chapter 1, we have described the most ancient methods of text hiding inclusive Galois field. In Chapter 2, we described the complete history of how steganography evolved. Chapter 3 is based on Linear Chaotic Map coupled with advanced technique like genetic algorithm. In Chapter 4 we further extended modern encryption

technique coupled with GA and modified Chaotic Map techniques. A new strategy named Graph Cut technique is implemented couple with modern encryption technique for text hiding randomly (chapter 5). And finally we extended our work with the use of XOR coupled with Graph cut technique (chapter 6).

Chapter1

Preliminaries

1.0. Cryptography

Cryptology is a combination of Greek word Kryptos meaning hidden and logo stands for words or study, respectively. Study and drill of procedures for protected and reliable communication in existence of adversaries complies the field of cryptography. More generally, cryptologist constructs and analyzes protocols that prevent third parties interference or intrusion from reading the information shared and transferred privately or secretly. In present modern era, ATM cards, computer passwords, data integrity etc are some applications of cryptography. The two foremost characteristics of cryptology are symmetric and asymmetric key encryption-decryption.

1.1. Attributes of Cryptography

1.1.1 Keys

In cryptography, some of the shared secret information is termed as keys which are shared between the sender and receiver.

1.1.2 Symmetric Encryption

When the same key is shared between the sender and receiver such system is called symmetric

encryption.

1.1.3 Cipher

Algorithms dealing with symmetric encryption are known as ciphers. Ciphers are generally classified into two major categories

(i) Block ciphers

(ii) Stream ciphers

1.1.4 Block Cipher

Cipher consisting of between 2 to 5 features of statement is known as Block cipher. They are inappropriate when large message is to be transferred because of weak security protocols.

1.1.5. Stream Cipher

Stream ciphers are made of simple text digits mingled with a pseudo random cipher digit stream. It can cope with large messages.

1.1.6 Shift Register

Digital memory circuit set up in calculators, computers and data processing systems is termed as Shift Register. Binary digit enters shift register from one side and emerges from other side. Mostly applied scheme for stream cipher is Linear Shit Register. It is helpful in generating especially extensive sequences. They are easily executed in hardware or software. They are exploit in global system mobile (GSM), blue-tooth and wireless security. Prime factorization

numbers primarily play part in length of a shift register. It is worth mentioning here that employing polynomials for linear shift register is significant as they are irreducible.

1.1.7 Initialization vector

The additional key employ in stream ciphers is message key known to be initialization vector. This is not clandestine; however it must not be used twice.

1.1.8 Modulo Operation

It is a computing operation to find the remainder of a number say a when divided by another number say b. It is also known as modulus and is abbreviated as $\boldsymbol{a \bmod n}$.

1.2. Useful Algebraic Topology

1.2.1 Ring

Ring is described as an algebraic structure defined over two binary operations. All the abelian group properties are satisfied by the first operation while closure and associative properties holds for the latter operator.

1.2.2. Division Ring

If in a nonzero ring, multiplicative inverse exists for every nonzero element a i.e.,

$$a * x = x * a = 1$$

Then such ring is termed division ring or skew field.

1.2.3. Field

Field is one of crucial arithmetical structures utilized in abstract algebra. It is nonzero commutative division ring. It is an algebraic structure with concept of addition, subtraction, multiplication and division fulfilling abelian group conditions and distributive law. Field of real and complex numbers are most usually utilized fields; however there are likewise finite fields, algebraic function fields.

The hypothesis of field extension which embraces Galois Theory includes the roots of polynomial with coefficient in a field. In cutting edge arithmetic, the theory of fields assumes a vital part in number theory and algebraic geometry. As an algebraic edifice, each field is a ring, however not every ring is a field. The distinction is that field takes into account division (though not division by zero), while a ring need not have multiplicative converse.

1.2.3.1. Galois Field

A finite field is a field with finite field order (i.e. number of components) additionally called Galois field. The order of finite field is dependably a prime or power of prime. If for a ring the latter binary operator follows all the characteristics of an abelian group then the ring is named as Galois Field (GF). It has finite number of elements so it falls in the category of finite field. Generally, it is denoted by, $GF(p^n)$. Categorization of Galois Field counting on values of p and n can be made as follows:

i. $GF(p)$: This field includes maximum p elements for example

$Z_p = \{0,1, \dots, p-1\}$,

ii. $GF(2^n)$: This field consists of maximum 2^n elements. Generally value of n is 8,16,32

iii. $GF(p^n)$: This field has maximum p^nelements where p is prime.

1.3. Irreducible Polynomials

An irreducible polynomial is a non-consistent polynomial that cannot be figured into result of two non-consistent polynomials. The property of irreducibility relies on field or ring to which coefficients are considered to belong. Here polynomials are considered over $GF(2)$ Galois field. Polynomials are presented through n bit words having coefficients from $GF(2)$. When two polynomials of degree $(0 < degree \leq n-1)$ are multiplied the resultant polynomial is of degree $> n-1$ which does not belong to the same field. To conquer this hurdle, prime or irreducible polynomials are considered. For instance $x+1$ and x^3+x+1 are irreducible polynomials.

1.4 Residue Number System (RNS)

A residue number framework displays large integers utilizing an arrangement of smaller integers, so that the calculation might be performed all more proficiently. It depends on Chinese remainder theorem of particular arithmetic for its operation. Consider an integer z whose residue representation in RNS arithmetic is $z = (x_1, x_2, \dots, x_n)$ i.e., for some integer x_i,

$x_i = x_i \, mod \, m_i \;\; for \; all \; i = 1,2, \dots n$ and $0 < x_i < m_i$ (1.1)

x_i's are called residues and m_i , $i = 1,2, \dots n$ are moduli of residue number system.

1.5. Asymmetric Encryption

A system in which both sender and receiver may have their own covert key is termed as asymmetric encryption system. This is based on two key structures. Encryption is done by one

key while other key is utilized for decryption. In general, mathematical relation holds within these keys. Receiver's key is kept public maintaining algorithm security and the other key is kept private. Notably, no one can consequently establish deciphering key recognizing enciphering key.

Several ciphers are available for encryption and decryption. Some are described here

1.6. Exponentiation Cipher

In this cipher, encryption / decryption procedure slot in plane and cipher text message to explicit powers such as Pohlig-Hellman, RSA.

By description, public key cipher is a one direction crypto scheme. Hence, all exponentiation ciphers are public key crypto scheme.

General course of action ensures for most of exponentiation technique is as follows:

By utilizing modular arithmetic, establish a relation as:

$$a^{k\phi(p)+1} = a \; mod \; p \tag{1.2}$$

Or

$$a^{E*D} = a \; mod \; p \tag{1.3}$$

Where

$$E * D = k\phi(p) + 1 \tag{1.4}$$

Or

$$E * D = mod \; \phi(p) = 1 \tag{1.5}$$

Here p and a denotes any prime number and an integer not divisible by p. E and D are the inverse or multiplicative inverse of each other. Generally, E is selected and associated D is extracted out. Exponentiation cipher also holds the modular arithmetic property which leads to

(1.6)

the fact that E and D are commutative as well so,

$$a^{E*D} mod\ p = [a^E mod\ p]^D\ mod\ p$$

The message block is encrypted by computing exponentiation as indicated in Eq. (1.2). If a number M is divisible by p i.e.,

$$M^{E*D} mod\ p = M \tag{1.7}$$

Then by Eq. (1.6),

$$[M^E mod\ p]^D = mod\ p = M \tag{1.8}$$

From Eqs. (1.7) and (1.8), it is revealed that if M the plain text cipher is enciphered with $\{(plain\ text)^E (mod\ p)\}$ algorithm and produce a cipher text which at the receiver end is deciphered by $\{(cipher\ text)^D (mod\ p)\}$, same plain text M will be acquired. Thus, it can be expressed as,

$$C = M^E mod\ p\ and\ M = C^D\ mod\ p\ , \tag{1.9}$$

here M denotes plaintext, C stands for cipher text, E and D are encryption and decryption keys, respectively.

1.7. Pohlig-Hellman Algorithm

Here all arithmetic is executed over Galois filed $GF(n)$. Moreover, largest available prime number is chosen for modulo. The encryption/ decryption are done by following the procedure explained in Eqs. (1.8) and (1.9). However, in Pohlig-Hellman algorithm, Keys obey the following relation,

$$E * D = 1\ mod\ \phi(p) = 1\ mod\ (p-1) \tag{1.10}$$

Where

$$\phi(p) = p - 1 \tag{1.11}$$

1.7.1. The RSA Algorithm

It is a modified scheme of exponentiation cipher. The scheme is modified by taking modulo n originated on two significant prime numbers say p and q. Subsequent course of action is pursued to pick communal and clandestine keys in RSA algorithm,

i. Selection of two prime numbers p and q is done randomly.

ii. $modulo\ n = pq$ is established

iii. Euler function $\phi(n) = \phi(pq) = (p-1)(q-1)$ is computed

iv. Selection of public number comparatively prime to $\phi(n)$ is made.

v. Private number is searched so that it obeys

$$public * private = 1\ mod\ \phi(n).$$

vi. n and communal key are disclosed while $\phi(n)$ and confidential key are kept furtive.

1.7.2. Substitution

Method of substitution is considered to be one of the oldest techniques used for encryption. Here the plain text units are switched with cipher text. Note that units can be consisting of single letter, pairs of letters or their combination. Many other permutation based algorithms have been exploited for encryption. Mostly $GF(p), GF(2^n), \ldots., GF(p^n)$ and finite rings in residue number system $modulo\ (p_1 p_2)$ are taken as the field over which cipher matrix for encryption is executed.

1.8. Lossless Compression

It is a collection of data compression algorithms that compress original data in such a manner that data can be perfectly reconstructed from the compressed data. This algorithm usually improves compression rates and consequently file sizes reduces. Lossless data compression is employed in ZIP format and in GNU tool gzip. Moreover, it is used in some image files formats like PNG or Gif.

1.8.1. Scanning

It is a bijective function of two dimensional arrays $P_{m\times n} = P(i,j)$ where $1 \leq i \leq m$ and $1 \leq j \leq n$ into set $\{1,2,\dots, mn-1, mn\}$. Process consists of ordering two dimensional arrays in a manner that each element of array is accessed precisely one time.

1.8.2. SCAN

Language based two-dimensional spatial-accessing methodology which can characterize and fabricate large number of wide assortment of scanning paths easily termed as SCAN. It belongs to class of formal languages such as Simple SCAN, Extended SCAN, and Generalized SCAN, each of which can embody and create a specific set of scanning paths.

1.9. Vector Quantization of Images

It is a scheme where data is divided into non overlapping vectors, each vector contains n elements. For each image vector a closest vector is located in codebook and its index is generated and encoded. In order to reconstruct image, entropy decode is implemented to lookup

in codebook for each index and repossess vector. These retrieved vectors are then combined to reconstruct image.

1.10. Chaotic Map

In mathematics, a chaotic map is a guide that shows some kind of confused trend. Maps might be parameterized by discrete-time or consistent time parameter. Confused maps regularly happen amid investigation of dynamical framework. Tumultuous maps are nonlinear maps implanting initial conditions with property of affectability.

CHAPTER 2

STEGANOGRAPHY

2. 0. Introduction

The combination of ancient Greek words steganos stands for protected and graphein stands for writing is termed as steganography. It is a technique of concealed communication having applications in encoding embedding camouflaged data in such a way that secret data presence is under cover.

In this technique information embedded bits is transformed into unused bits in regular html and graphics files in computer. This invisible information is revealed by incorporating stego medium which translate it into encrypted data. To control inclusion or extraction of hidden information a stego key method is used in encoding process. Information encryption main purpose is to secure such information from third party.

A succinct disparity among steganography and cryptography is illustrated in following section.

2.1. Steganography VS Cryptography

Steganography differs from cryptography in a manner that it conceal information file into computer regular files unlike cryptography whose core is to convert readable data into unintelligible form. Steganalysis is the detection of hidden files via stegnography where as *cryptanalysis* is a process in which plain text is accessed without using the secret key. Concept of cryptography is well known to technology while steganography is relatively less exposed.

2.1.2. Watermarking

It is a procedure used to protect documents. Mostly, it is custom to protect intellectual property. In this process, hidden information is transformed into hauler wave. A digital watermark is a sort of marker which is secretly clandestine in a carrier signal spate i.e. audio, video, text, 3D models or in pictures. In general it is exercised to concede proprietorship of exclusive rights of such signal. The patent security is made sure by encoding facts in water marked file where mark or sign indicate proprietorship of arrest order.

Fig. 2.1 Watermarked image

2.1.3. Fingerprinting

An impersonation left through friction edges of a human finger is a fingerprint. In this procedure, numerous consumers are presumed to make sure through some exclusive marks interleaved in document copy. This procedure is useful for in securing belonging properties to avoid violation of agreement rules, illegal activities and transfer of property or copy to other groups.

2.2. Conventional Approach of Steganography

J. Trithmious introduced crypto and steganogrpahy in his book on magic[1]. However, this word is implemented differently in ancient and present age.

2.2.1. Steganography in Past

Back in 440 B.C, Herodotus decribed two incidents of history setting an evidence of seganographic field usage. He revealed few samples of steganography utilization in his work entitled "*The history of Herodotus*". Dermaratuis informed Greece about an upcoming assault by writing this message on wooden wax tablet prior to smearing honey comb surface. Later on, these wax tablets became common usage as refillable writing surface and shorthand.

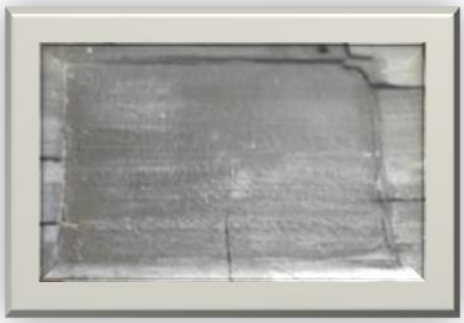


Fig. 2.2 Wax Tablet; ancient writing material

Greek history also exposes another well renowned established sample of steganography. Leader of Miletus, Histaeus tattooed furtive memo on shaved head of one of his most entrusted slaves. When slave's hairs were grown back, he was sent to Aristagorous, where the message that ordered a revolt against the Persians was revealed by shaving his hairs.

In this scenario, slave has been deployed as transported of the secret information, throwing dust in eyes of every individual who saw the slave being sent to Aristagorous. As a consequence, the message arrived at beneficiary with no suspicion of secret correspondence perpetually being raised.

2.2.2. Steganography in Present

In present age, steganography applications are witnessed in diverse disciplines such as modern printers, scanners, detecting terrorist activities and in intelligence services. Now adays, steganography employs vision of conceal information at net packet level and in digital software records

2.3. Image Encryption Existing Approaches

2.3.1. SCAN Utilization for Lossless Image Compression and Encryption

Here binary and grey scale images are initially encrypted, then lossless compressed. Compression and encryption routines are performed under SCAN approach.

2.3.2. Vector Quantization for Image Cryptosystems

Here images are encrypted and decrypted based on vector quantization. This is done in three major steps. Step one is the reorientation of image into vector quantization, step two is to perform compression of these quantized vectors and in last step the compressed data is encoded vector by vector. At this stage routine cryptosystems are utilized.

2.3.3. Implementation of Multi-level and Image Dividing Techniques on Image Encryption

This technique principle is based on binary phase cliquey OR operation and image isolating method. Binary images are generated by detaching same gray level and multi level images. At this stage, pair stage encoding is done by deploying recovered two fold images. Subsequently, these images are jumbled with binary capricious phase images by double stage XOR operation.

2.4. Image Encryption using 1D Chaotic Map

Here the image encryption is carried out by embedding sensitivity property to initial condition. Several 1D Chaotic maps are available in literature incorporated in image encryption.

2.4.1. Composition of Two Chaotic Logistic Maps as Basis for Image Encryption

In this, snarled and plain images are extracted out by means of an exterior furtive input of 104 bit and two chaotic logistic maps. Further, encoded image are made more secure by adjusting secret key in wake of encoding of each pixel of plain image. An estimation process is exploited to enhance effectiveness of system.

2.4.2. Image Encryption Based on the General Approach for Multiple Chaotic Systems

This encryption scheme is based on combination of two chaotic frameworks: Lorenz and

Rosslere systems. The security level of this scheme is up to six parameters.

2.4.3. Image Encryption and Compression Method based on Independent Component Analysis

Here Discrete Cosine Transformation (DCT) is incorporated to endow compression. This is done by separating the image into little squares obstructs by applying DCT and obtaining DCT parts. The DCT greater part has high energy in low frequency cluster; low frequency segments are utilized through a low pass filter.

Once the compression is done, small pieces are rotated randomly and obtained rotation matrix as a key. Visually blighted partition source is used to revive encryption system. Coated and revolved DCT fragments are merged. It is examined that best implementation is achieved for compression ratio from 0.1 to 0.5. Furthermore, quick and secure image transmission was attaining by utilizing this technique [12].

2.5. Text Steganography Existing Approaches

2.5.1. Least Significant Bit (LSB) Matching Revisited Image Steganography

The most widely acknowledged system developed by Chandramouli et al.[13] is employed to bury message. This system includes the implementation of LSB, by manipulating sieving, covering and alteration on cover media. LSB matching reverted to image steganography and edge flexible plan was proposed by Weiqi [2]. It can select embedding locales as revealed by coverage of clandestine message. Smooth edge districts are deployed for huge inserting rates while more hone areas are exploited for lower installing rate.

2.5.2. LSB and DCT Techniques

Ekta Walia et al. [14] give analysis of Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) based steganography. LSB based steganography inserts the text message into digital image. Changing over an image from a format like BMP or GIF which recreates first message precisely to a JPEG which does not and afterward back could crush the data covered up in LSBs. Text message is embedded into LSB bits of discrete cosine coefficient of digital image by using DCT based steganography. At the point when data is concealed inside video, the process concealing the data typically performs the DCT. It slightly changes each of the images in the video. A usage of both these techniques and their execution observation has been carried out for LSB based and DCT based stego images utilizing PSNR proportion demonstrates that PSNR degree of DCT based steganography plan is high as contrasted with LSB based steganography plan for numerous types of images. DCT based steganography works up to expectations efficiently with insignificant mutilation of the image quality as contrasted with LSB based. Anyway DCT based steganography plan is suggested as a result of the base mutilation of image quality. [15].

2.5.3. Hide Data into Edges of Image

Nitin Jain [16] demonstrated how the edges of images can be utilized to conceal instant message in steganography. It gives profound perspective of image steganography and edge detection filter methods. The system computes binary value of each one character of instant message and after that attempted to discover dull spots of light black image (black) by changing over actual image to binary image. At that point these images are changed over to RGB image to discover dark places. Each one succession of gray color transforms into RGB shade and dark level of gray

image is found along these lines. In last stage every 8 pixels of dark spots are considered as a byte and parallel binary value of each one character is placed in low bit of each one byte that is made manually by dark spots pixels for expanding security of fundamental method for LSB bit steganography. Steganalysis then used to assess concealing methodology to guarantee the information can be covered up in best conceivable way. This methodology conceals content in close dark places. However, information is not placed in direct way in those pixels and put in low bits of every eight bit pixel.

2.5.4. Hiding Data using Dark Region

In [17], an information concealing strategy was presented where it was fathomed to utilize murky area of image to shroud information by means of LSB. It changes over to binary image and names each one article exploiting 8 pixel integration plans to conceal information bits. The strategy obliged elevated calculation to detect murky areas in its network. It was not tried on high surface sort of image. Concealing limit completely relies upon image composition.

2.5.5. Reversible Data Hiding

Innovative lossless or reversible information covering up plan for binary pictures was presented [18]. In this system bit depth of quantized coefficients are implanted in some code square by employing JPEG2000 compacted information. It is beneficiary for binary images.

2.5.6. DCT based Data Hiding

DCT based data hiding method was proposed in [20]. Embedding system based on DCT information mantled color data in clamp grey level. Image steganography was attained by

considering shade quantization, color sorting and veil information stages. The motivation behind this technique was to provide free approach towards gray level image for everybody excluding restricted entrance of same color images to individuals who have its stego-key. It has high PSNR in addition to with observable antique inserting information.

2.5.7. Common Pattern Bits

Anthers [19] proposed LSB based image burying scheme. A proposal of LSB based image concealing technique includes basic example of using bits (stego-key) to shroud information. The LSB's of pixel are altered relying on stego-key design bits and clandestine memo bits. Design bits are mixed of $L = M \times N$ size rows and columns (of a piece) and with random key value. Every example bit is matched with message bit, if accomplished it adjusts second LSB bits of hidden image overall persists as before. This method focuses to attain collateral of concealed memo in stego-photograph utilizing typical example key. The suggested system has minimal shrouded limit in light of the fact that solitary secret bit obliged a block of $L = M \times N$ pixels.

2.6. Mechanism of Steganograhy

At the point when a steganographic framework is produced, it is imperative to consider what the most fitting cover work ought to be, furthermore how the stego-gramme is to be achieved its beneficiary. With the Internet offering such a great amount of usefulness, there are numerous distinctive approaches for sending information to individuals without anybody knowing they subsist. For instance, it is conceivable that a picture stegogramme could be sent to a beneficiary by means of email. Then again it may be posted on a web gathering for all to see, and beneficiary

could log onto the discussion furthermore download picture to peruse message. Obviously, in spite of the fact that everybody can see stegogramme, they will have no motivation to expect that it is much else besides simply an image. As far as advancement, Steganography is involved two algorithms, one for implanting and one for concentrating. The implanting methodology is concerned with concealing a secret message inside a spread work, and is most deliberately built methodology of two. A lot of consideration is paid to guaranteeing that secret message goes unnoticed if an outsider was to capture spread work. The concentrating methodology is generally a much easier handle as it is just an opposite of installing procedure, where secret message is uncovered at end. The whole methodology of steganography for images can be exhibited graphically as:

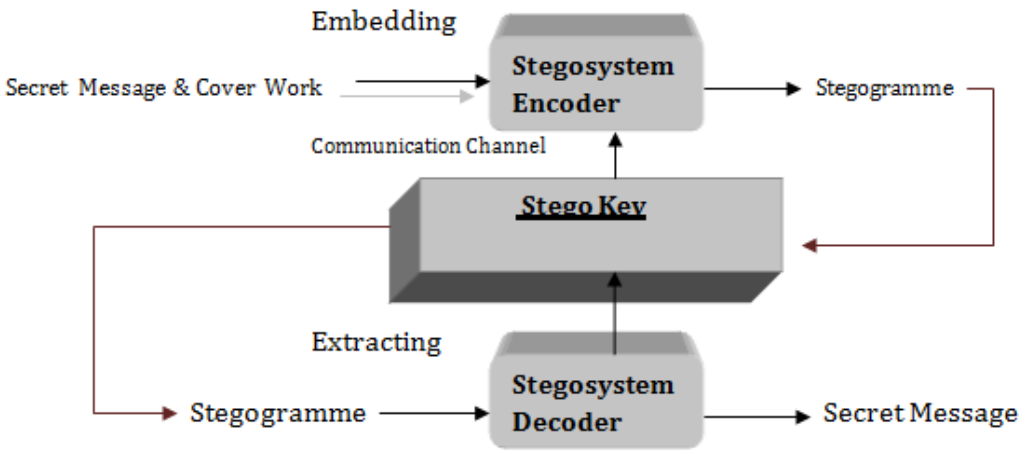


Fig. 2.3 The Mechanism of Steganography

2.7. Steganography in Modern Approach

Steganography can be classified into five categories:

(i) Text (ii) Video, (iii) Image, (iv) Audio and (v) Protocol Steganography.

2.7.1. Text Steganography

It is operated into digital make up such as PDF, digital watermarking and information concealing. Message hidden based on text is more intricately apprehend. Simplest scheme of data veiling is to firstly masquerade then adopt given rules to add phrase logical or spelling errors or replace with synonyms terms [21].

2.7.1.1. Text Steganography Methods

Following are few steganography methods in used:

- Text steganography in Markup Languages (HTML)
- Line Shifting Method
- Word Shifting
- Open Spacing
- Semantic Methods
- Character Encoding

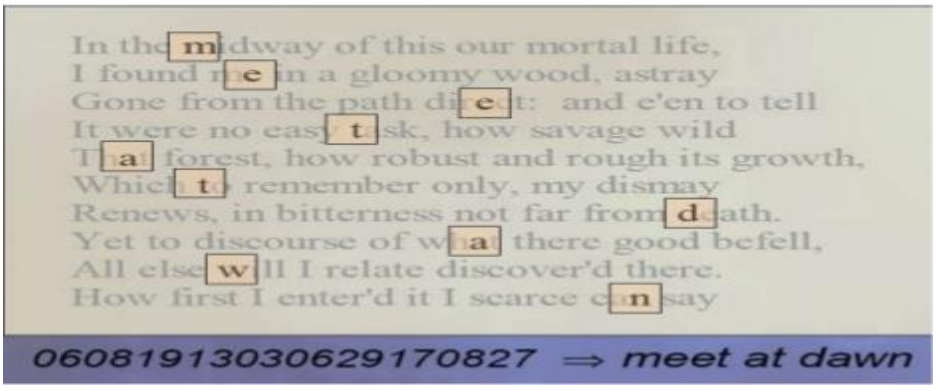


Fig. 2.4.Text Steganography

2.7.2 Image Steganography

This procedure also known as spatial domain technique works on principle of embedding messages in intensity of pixels directly, while for transform also known as frequency domain, images are first transformed and then message is embedded in image.

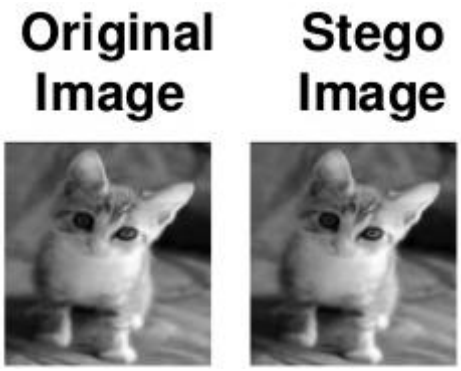


Fig.2.5. Image Steganography

2.7.3 Audio Steganography

The process of implanted secret messages into digital sound is acknowledged as audio steganography. It can embed messages in WAVE, Volume unit (VU) and even MP3 sound files. The entrance of data secretly onto digital audio file there are few techniques introduced:

(i) LSB

(ii) Parity

(iii) Phase coding

(iv) Spread spectrum

(v) Echo hiding

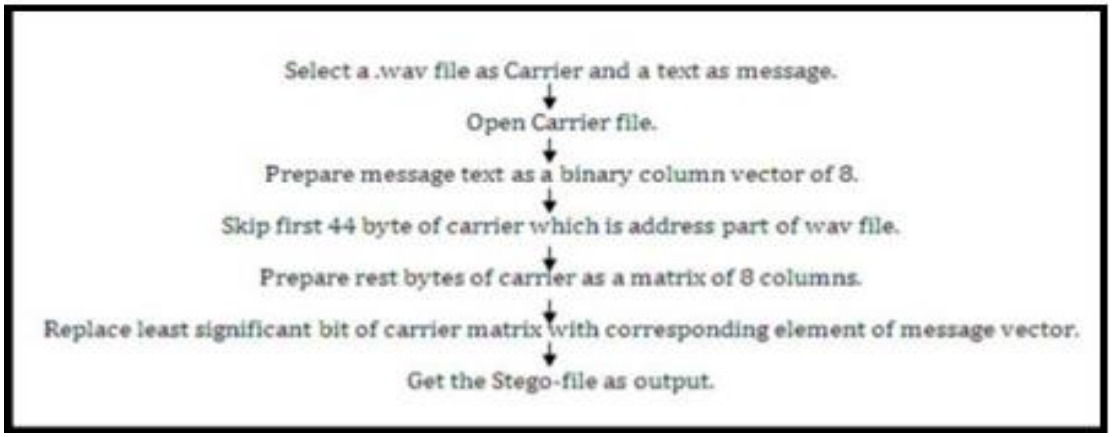


Fig. 2.6. Flowchart of Audio Steganography

2.7.4 Video Steganography

Video Steganography is a technique to hide any kind of files in any extension lead into a carrying video file.

2.7.5 Protocol Steganography

Embed information within messages and network control protocols used by common applications [1].

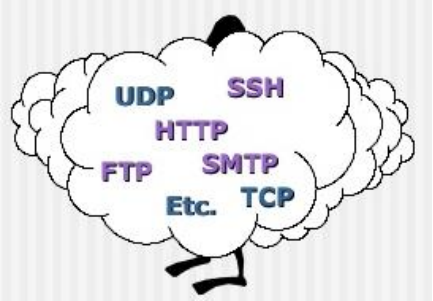


Fig. 2.7. Different Protocol

2.7.6 Protocol Steganography Framework

Sender sends message ‘m’

Alice intercepts m, hide some information on it and sends m’

Bob received m, and sends either m or m’

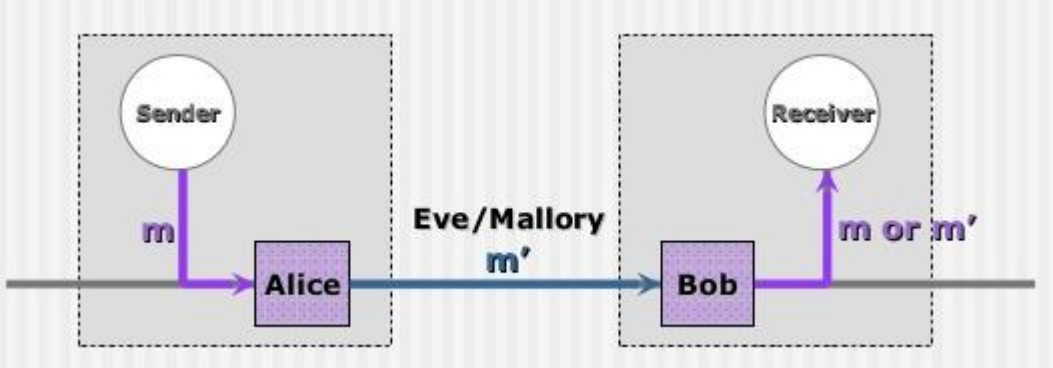


Fig. 2.8. Protocol Steganography Framework

2.8 Applications of Steganography

Steganography have many generic kind of application, including copyright, Feature Tagging, and secret communication etc. [22,23]

- **Copyright Protection**

  To identify image intellectual property, a secret copyright notice or watermark can be embedded inside image. This is called watermark process. Watermark process can also be used to check whether image has been modified or not.

- **Feature Tagging**

  Descriptive elements like Captions, Comments etc. are embedded inside an image. The entire embedded feature also copied while receiver copying the stego image and to extract and view the feature receiver must have decoding stego key.

- **Secret Communication**

  Sometimes, in the phase of transmitting a cryptographic message draws useless and unwanted attention. It happened because of cryptographic technique might be restricted by law. However, in steganography by analysis of sender activity, message and recipient, this situation is not occurred.

- **Digital Watermark**

  The purpose of a digital watermark is to leave a permanent mark on image. This mark can be used as a source of tracing the distribution of images for internet news services and also for photographers who are advertising their work for digital publication. A digital camera developed which place a watermark on all photographs. This watermark would give help photographers to employ "web-searching agent" to search where their images appear.

2.9. What is an Image

An image is visual representation that has been made or replicated and put away in electronic structure. It could be portrayed regarding vector illustrations or advanced design. An image put away in advanced structure is at times called a bitmap. An image guide is a document containing data that partners distinctive areas on a pointed out image with hypertext joins. An image is an accumulation of numbers that make diverse light intensities in distinctive regions of the image. This numeric representation structures a lattice and individual focuses are expressed to as pixels (image component). Grayscale images utilize 8 bits for every pixel and can show 256 separate colors or shades of light black. Digital color images are ordinarily put away in 24-bit records and utilize RGB shade model, otherwise called true color [5]. All shade refinements for pixels of a

24-bit image are determined from three essential shades: red, green and blue, and every essential color are spoken to be 8 bits [4]. Consequently in one given pixel, there might be 256 separate amounts of red, green and blue [5].

2.9.1. Digital Image Representation

An image may be characterized as a two-dimensional function $f\ (x, y)$, where x and y are spatial (plane) coordinates, and sufficiency of f at any pair of coordinates is known as intensity of image. The term light black level is utilized regularly to allude to power of monochrome images. Color images are framed by a synthesis of individual images. Case in point, in RGB color framework a shade image comprises of three individual monochrome images, alluded to as red (R), green (G), and blue (B) essential (or part) images. Hence, a large portion of systems created for monochrome images might be ex-had a tendency to color images by transforming three segment images separately. [10]

An image may be consistent as for x and $y-$facilitates, furthermore in adequacy. Changing over such an image to computerized structure obliges that directions, and also amplitude, be digitized. Digitizing direction qualities is called *sampling*; digitizing adequacy qualities is called *quantization*. In this manner, when $x,\ y,$ and adequacy values of f are all limited, discrete amounts, image is termed as digital image.

An advanced digital image could be considered as substantial show of discrete specks, each of which has a splendor connected with it. These specks are called *image components*, or *pixels*. The pixels encompassing a given pixel constitute its neighborhood. An area might be described by its shape in same route as a matrix. We can talk about a 3x3 area, or of a 5 x 7 area. As show in Fig.2.9

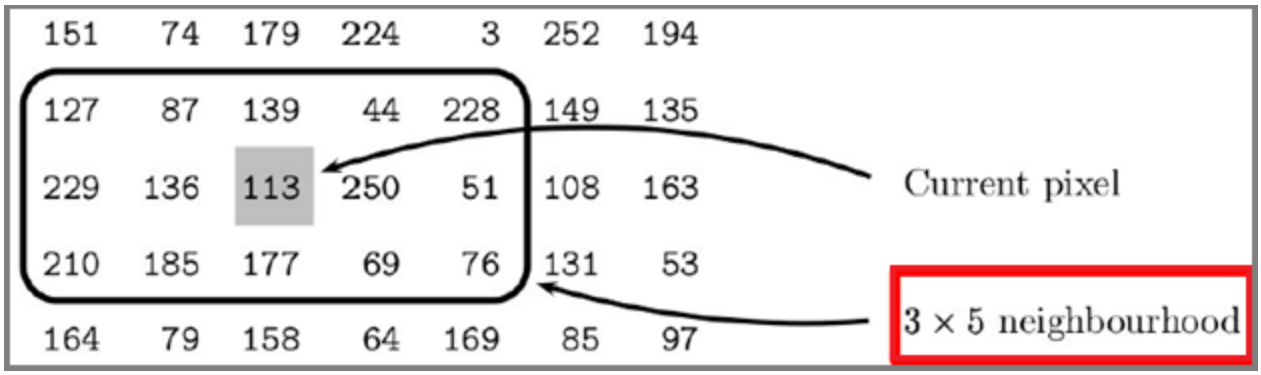


Fig. 2.9 Pixel Locations

2.9.2. Images as Matrices

This is representation of an image in matrix form:

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \cdots & f(0,N-1) \\ f(1,0) & f(1,1) & \cdots & f(1,N-1) \\ \vdots & \vdots & & \vdots \\ f(M-1,0) & f(M-1,1) & \cdots & f(M-1,N-1) \end{bmatrix}$$

By definition, right side of this equation is digital image whose each element is termed as an image element, picture element, or pixel.

A digital image can be represented in MATLAB matrix as:

$$\mathtt{f} = \begin{bmatrix} \mathtt{f(1,1)} & \mathtt{f(1,2)} & \cdots & \mathtt{f(1,N)} \\ \mathtt{f(2,1)} & \mathtt{f(2,2)} & \cdots & \mathtt{f(2,N)} \\ \vdots & \vdots & & \vdots \\ \mathtt{f(M,1)} & \mathtt{f(M,2)} & \cdots & \mathtt{f(M,N)} \end{bmatrix}$$

Where $f\ (1,1)\ = f\ (0,0)$, $c$learly, two representations are identical, except for shift in origin. The notation $f\ (p,q)$ denotes the element located in row p and column q. For example, $f\ (6,2)$ is element in sixth row and second column of matrix$f$. Typically, we use the letters M and N,

respectively, to denote number of rows and columns in a matrix. $A\ (1, N)$ matrix is called a row vector, whereas an $(M, 1)$ matrix is called a column vector. $A\ (1, 1)$ matrix is a scalar [10].

2.10. Features of Image Processing

2.10.1. Image Enhancement

The procedure through which an image specific attributes are improved for a specific application is known as image enhancement. Hoeing or refining a blur picture, emphasizing edges, enhancing photograph contrast, or brightening an image and diminishing noise are few examples.

2.10.2. Image Restoration

Overturning destruction done to a picture due to a recognized reason such as amputating blur because of hand or equipment movement or removal of optical falsifications is termed as image restoration.

2.10.3. Image Segmentation

Slicing a picture into integral pieces or separating particular feature of an image is known as image segmentation. Locating lines, ring, or specific silhouette in an image or aerial shoot, recognizing cars, trees, buildings, or roads are some examples.

2.11. Types of Digital Image

2.11.1. Grayscale

Normally, from 0 (black) to 255 (white) is available range of gray. Each pixel is a tint of gray. Thus, each pixel using this range can be represented by eight bits or exactly one byte. Other gray scales employed are generally a power of two.

A data matrix whose values represent shades of gray is a gray scale image. When elements of a gray-scale image are of class `uint8` or `uint16`, they have integer values in range [0, 255] or [0, 65535], respectively. If image is of class `double` or `single`, values are floating-point numbers. Values of double and single gray-scale images normally are scaled in range [0, 1], although other ranges can be used. [10]

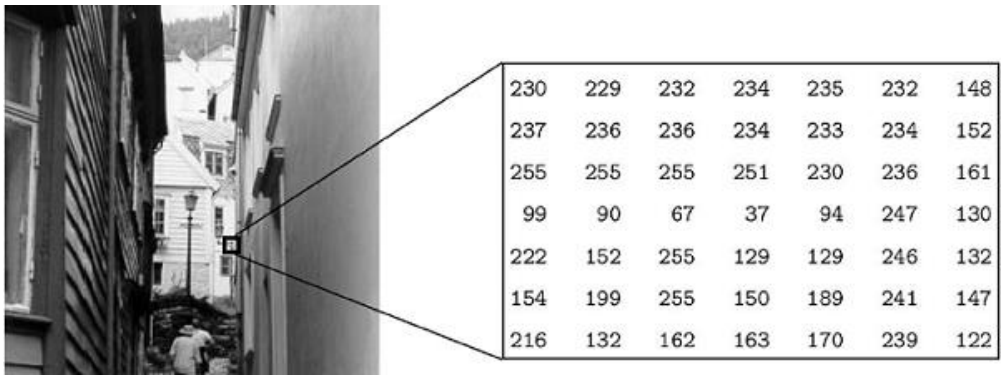


Fig. 2.10. Grayscale Image

2.11.2. Binary Image

A logical array of zeros and ones constructs a binary image. Thus, in MATLAB an array of zeros and ones whose values are of data class say, unit 8 is not a binary image. Function logical is applied to convert a numeric array into binary. Thus, a logical array B from a numeric array A consisting of zeros and ones is created by using the statement

B = logical (A)

Logical function converts all nonzero elements in A to ones and all zero entries in A transform to logical zeros. Thus, in binary image each pixel is either black or white corresponding to two possible values for each pixel (0, 1) and one bit per pixel is required [10].

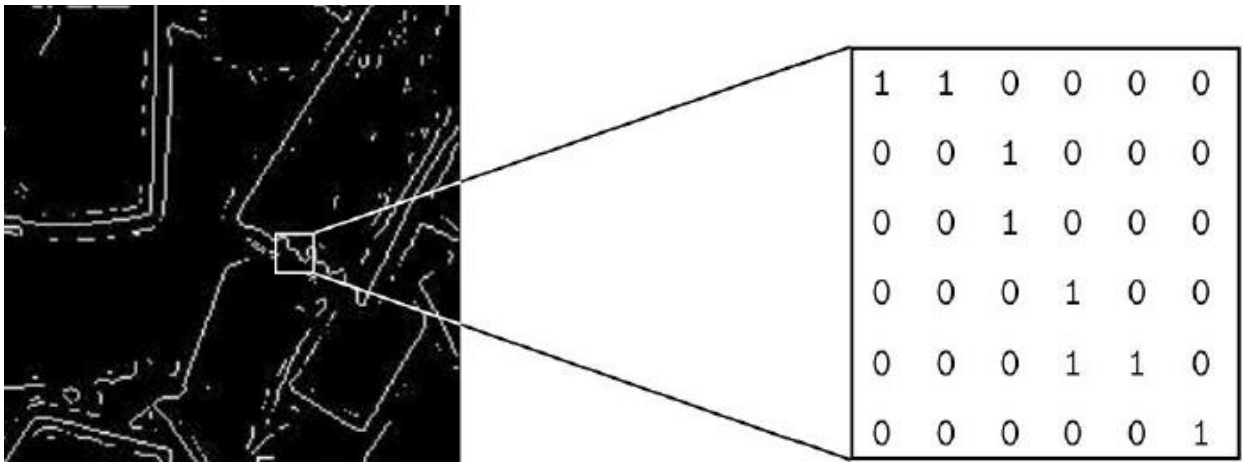


Fig. 2.11 Binary Image

2.11.3. RGB

Amount of red, green and blue in a pixel describes the particular color of a pixel. A total of 2563 distinct possible colors are created if each of these components has a range from 0 to 255. Thus, three matrices representing red, green and blue values for each pixel build a stack for an image. It reveals that three values correspond to every pixel [10].

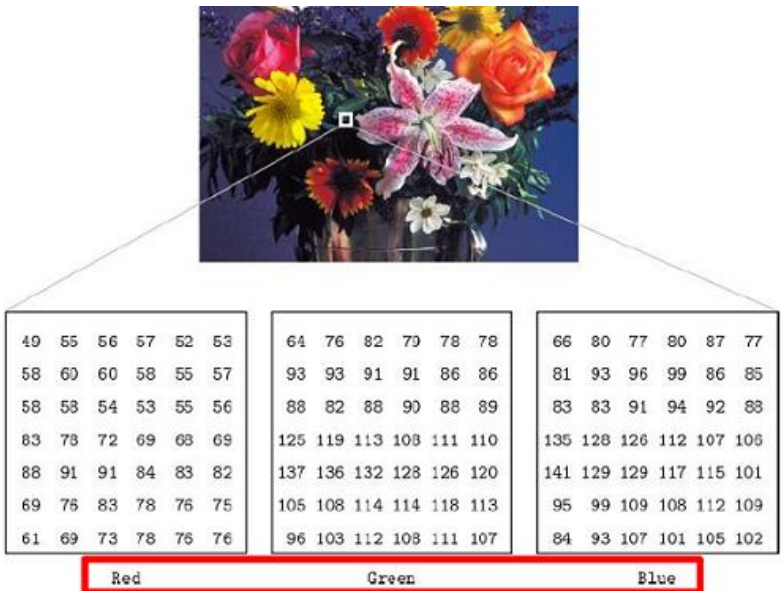


Fig. 2.12. RGB Image

2.12. Change the Intensity of Pixels by Applying Arithmetic Functions

2.12.1. Addition

Here each pixel is added up by a constant $y = J + C$ (imadd). Each gray value in image is operated by utilizing a simple function of addition.

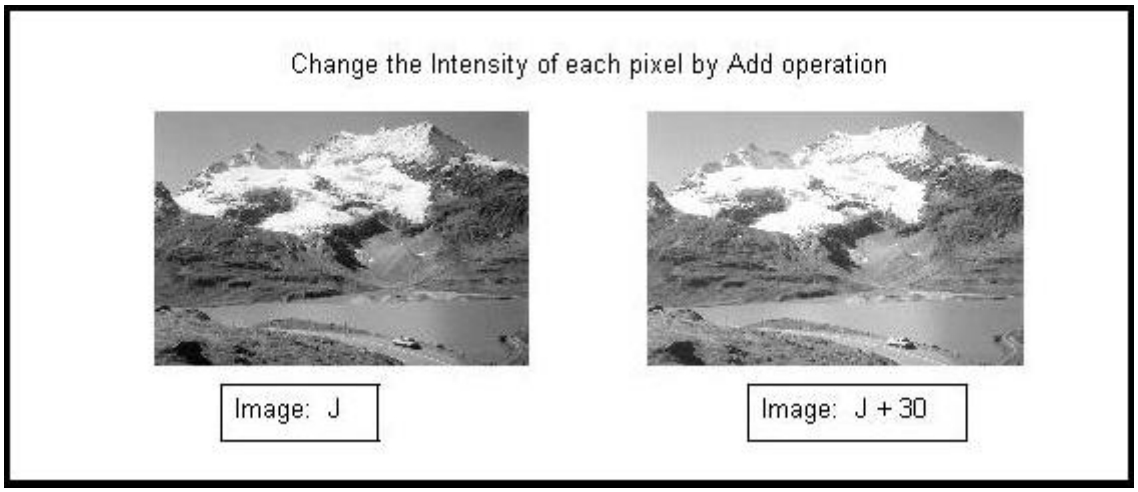


Fig. 2.13. Add a constant value to each pixel

2.12.2. Subtraction

Each pixel of image is deducted by a constant $y = J - C$ (imsubtract).

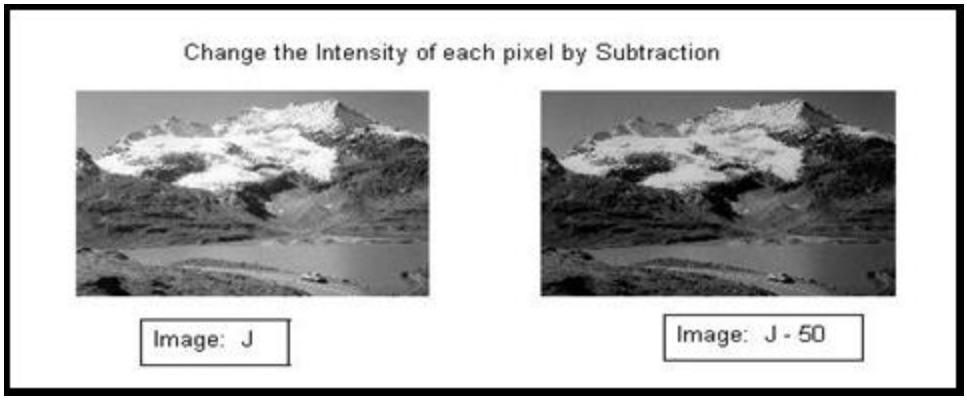


Fig. 2.14 Subtract a constant value to each pixel of Image J

2.12.3. Multiplication

Every pixel is proliferated by a constant $y = C \cdot J$ (immultiply).

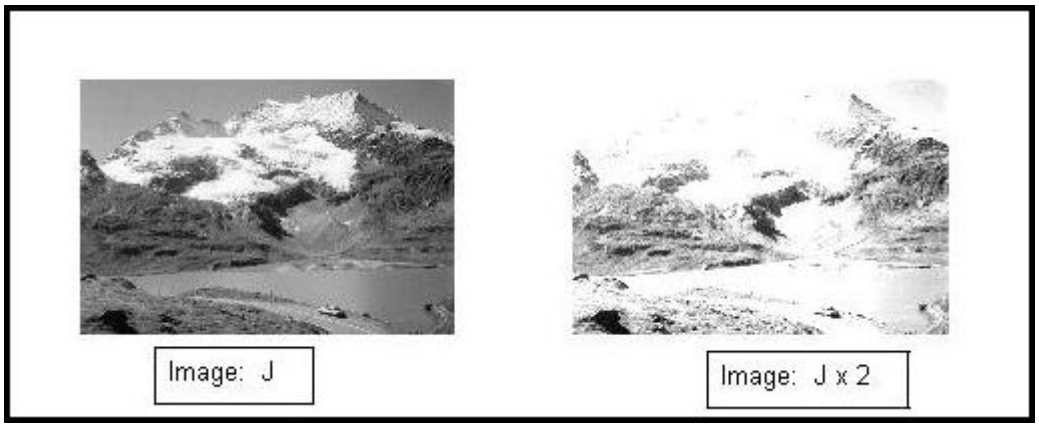


Fig. 2.15 a constant value multiplied with each pixel

2.12.4. Complement

In complement of a binary picture, zeros get to be ones and ones get to be zeros; highly contrasting is swapped (white and black). For an intensity or RGB image complement, each pixel

value is deducted from the most extreme pixel quality along with class and peculiarity. These are exploited as pixel esteem within yield image. Thus, dull zones get lighter and lighter regions get darker.

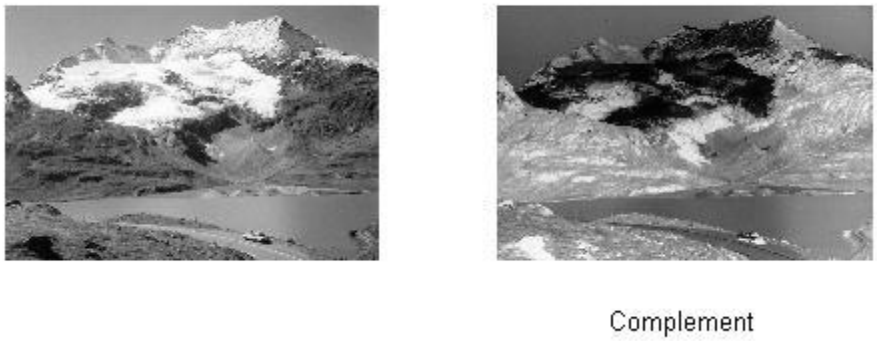


Fig. 2.16 Complement of an Image

2.13. Image Processing using MATLAB

2.13.1. Imagery in MATLAB

ARRAY is basic data formation in MATLAB; it is an ordered set of real or composite components. ARRAY is appropriate for exhibition of IMAGES, true sets of colors or intensity of pixel value.

In MATLAB, pictures are mostly accumulated in two dimensional array i.e. matrices, in which every value or component of matrix correlates to a Pixel value of picture. Pixel is PICTURE COMPONENT. It is generally represented by only a dot on a computer demonstrates.

Consider a picture which is comprised on 100 rows and 200 columns of unusual shades dots will be mounted up in MATLAB like a 100 x 300 matrix. Three dimensional array is

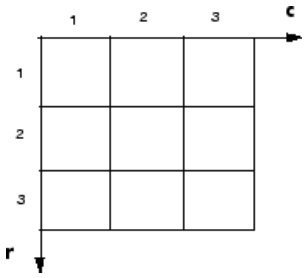
required for RGB images, in which first array demonstrate Red, second array reveal Green and third represent Blue pixels. Such type of resolution gives help in working with images in MATLAB and provides full command on image processing.

2.13.2. Expressing Image Locations

2.13.2.1. Pixel Indices

Position in a picture is usually represented by pixel indices. A picture or an image is considered to be trellis of discrete components sequence, from top to bottom and left to right as expressed in following figure

Pixel Indices



For pixel records in sequence, row expands descending, while column increments to right. Pixel lists or indices are in number or digit, and reach from 1 to length of column or segment.

In MATLAB a balanced correspondence exist between pixel indices and subscripts for two initial matrix measurements. For example, information for pixel in second row, fifth column is put in matrix component (2, 5). Ordinary MATLAB lattice subscripting is used to get to

estimations of individual pixels. For instance, MATLAB code I (12, 5) gives back information for pixel at row 12, column 5 of picture I. Similarly, MATLAB code RGB (5, 3) displays RGB values at row 5 and column 3.

An association among picture information and method used to display image is evident in MATLAB through balance between pixel record in sequence or indices and subscription for two matrix dimension.

2.14. Image Representation in MATLAB

RAND command is used to create a matrix and IMAGESC command is incorporated to scale the image information, color map and then show image as output.

```
n = 100;

a = rand(n);

imagesc(a);
Colormap(hot);
axis square;
```

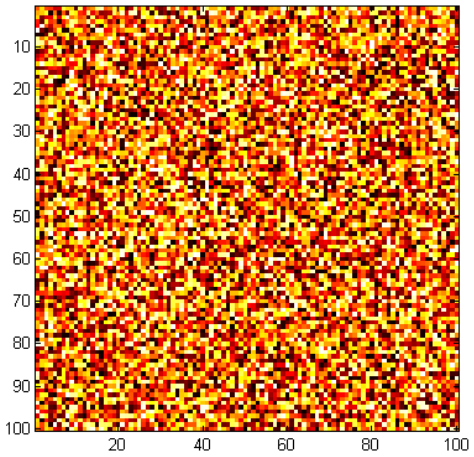


Fig. 2.17 Image in MATLAB

This is an inverse of that matrix representation.

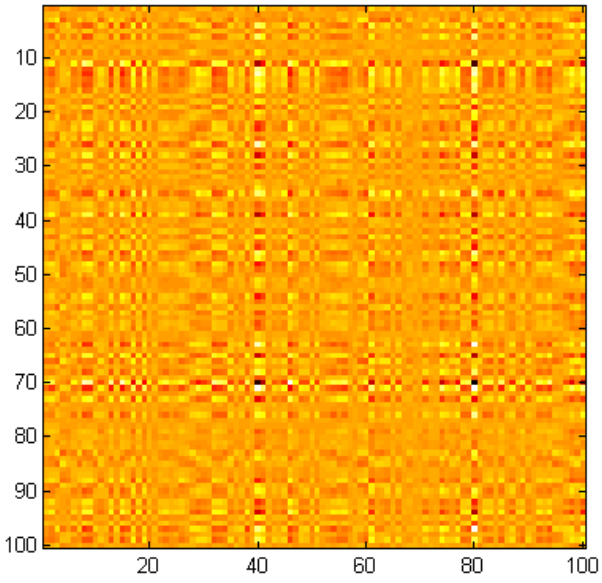


Fig. 2.18 Inverse of a Matrix

The correctness of the inverse matrix is ensured by multiplying it with the original matrix. If the outcome gets 1, then inverse is correct as $a * inv\,(a) = I$ where I stand for identity matrix. This matrix is just similar to a number one matrix. All elements are zeros except diagonal consisted on ones.

Imagesc (a*b);

axis square;

Following image illustrates multiplication of two matrices

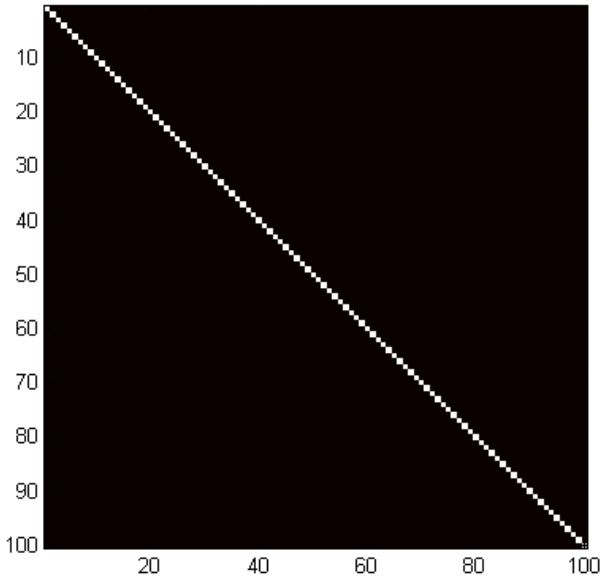


Fig. 2.19 Multiplication of two matrixes

2.14.1. Image Processing Example

Step 1: Read the Image

```
I = imread('austroner.png');

figure;

subplot(1,2,1);

imshow(I);

title('ORIGINAL IMAGE');
```

Fig. 2.20 Image read by MATLAB

Step 2: Simulate a Blur

In daily life, it often happens that image after being captured could be blurred because of camera or hand movement. Image can be blurred in MATLAB by running a GAUSSIAN filter together with original image. Gaussian filter embodies point spread function PSF.

```
PSF = fspecial('gaussian',7,10);
Blurred = imfilter(I,PSF,'symmetric','conv');
figure;
subplot(1,2,2);
imshow(Blurred);
title('Blurred Image');
```

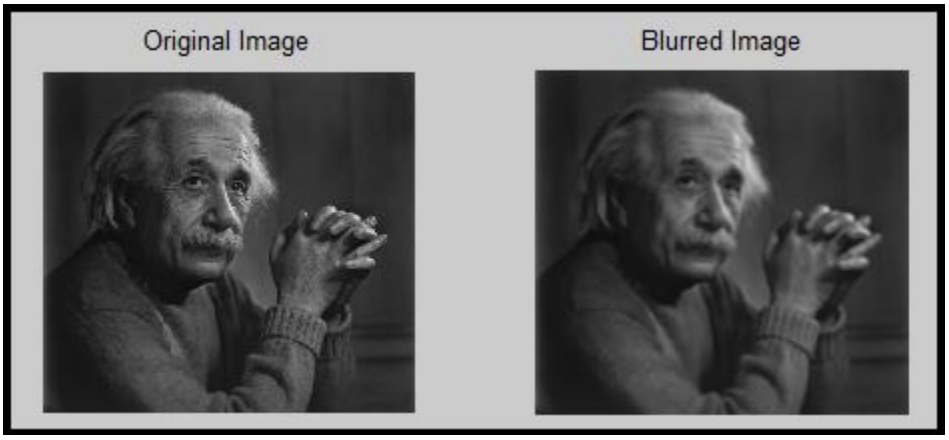


Fig. 2.21 Original Image and Blurred Image

Step 3: Enhance Grayscale Images

Following techniques based on built in settings are used for a comparison of efficiency:

Imadjust: It would improve the diversity of photograph by transforming values of input dilution picture to upcoming new outcomes. Typically, original image data is blended at low and high intensities by one per cent.

Histeq, Histogram equalization is executed by this function. The disparity of pictures is raised by altering picture intensity values. As a consequence, resulted histogram is almost similar to a specific histogram.

Adapthisteq, implements discrepancy limited adaptive histogram equalization. It executes on tiny regions unlike Histeq. Thus, each section disparity is amplified and hence resulted histogram of every tile get almost equivalent to uniform distribution histogram which is done by default. The difference increment should be restricted because it would raise noise in image.

```
imgadjust = imadjust(I);
imghisteq = histeq(I);
imgadapthisteq = adapthisteq(I);
subplot(1,2,2), imshow(imgadjust);
```

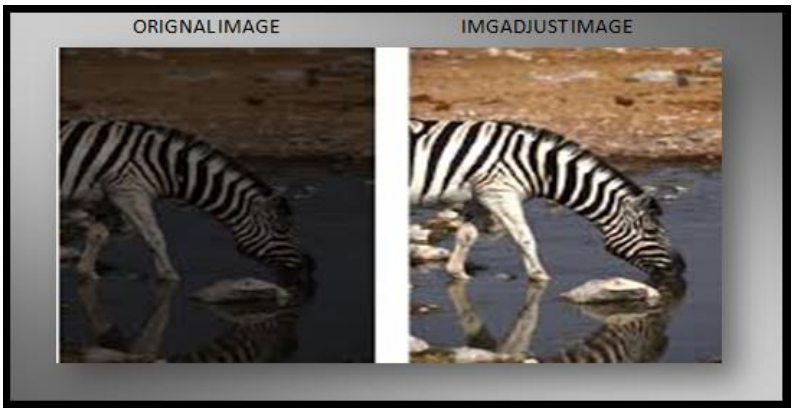


Fig. 2.22 Shows that imadjust Adjust image contrast intensity values

```
imshow(imghisteq);
```

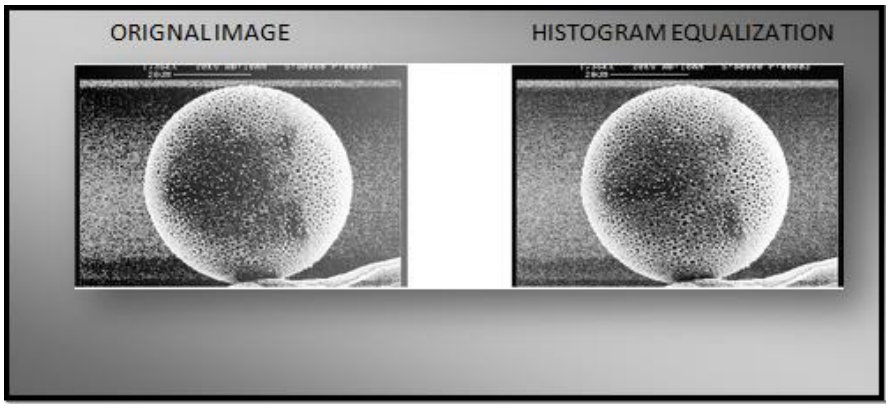
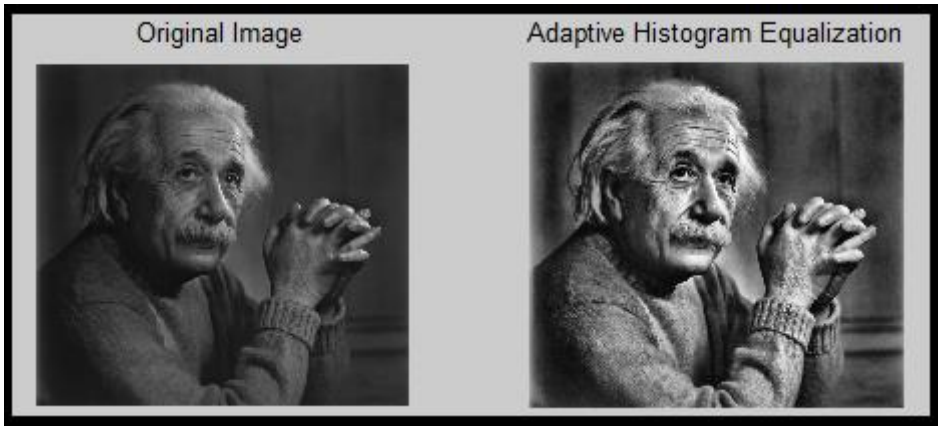


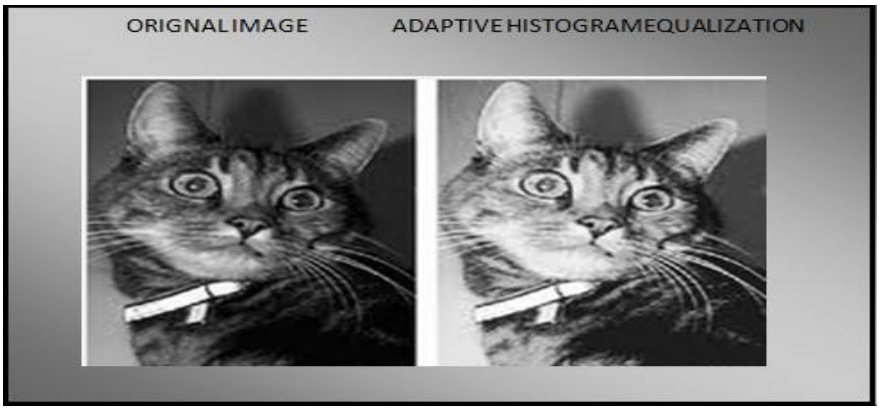
Fig. 2.23 Histogram Equalization

```
imshow(imgadapthisteq);

title('Adaptive Histogram Equalization');
```



(a)



(b)

Fig. 2.24 (a) and (b) Adaptive Histogram Equalization

Histogram:

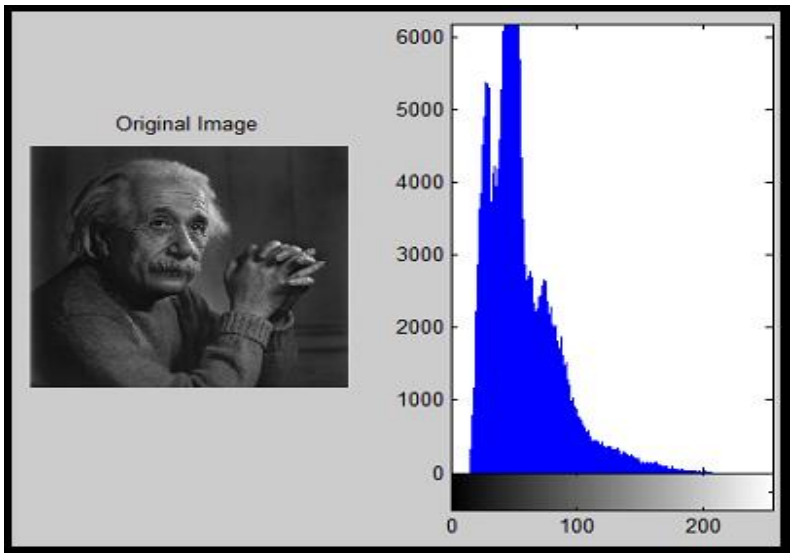


Fig. 2.25 Image with Histogram

2.15. Segmentation

It is creation of an image composed of set of pixels and partitioning of pixels on basis of identical attributes such as texture, color or intensity. Purpose of segmentation is to obtain an improved representation of an image in a sense of significance and lighter to examine. To place objects and boundaries such as lines, a curve etc in an image, segmentation is applied. Image segmentation is performed under many techniques.

It is very beneficial in medical imaging as it is used to identify some disease. Some of its applications include face detection, iris detection, fingerprint recognition etc.

Intensity values on which are building blocks for image segmentation algorithms are as follows:

2.15.1. Discontinuity based

In this methodology partition are performed on basis of some spiky variations in imitation gray level dilution.

(i) Detection of Isolated Points

(ii) Lines detection

(iii) Edge detection

2.15.2. Similarity based

Here fragmentation is attained on pixels grouping established characteristics listed as follows:

(i) Thresholding

(ii) Region growing

(iii) Merging and splitting of region

(iv) Clustering

(v) K-Means Clustering

(vi) Fuzzy C Means Clustering

2.16. Graph Cut

According to graph theory cut is partition of the nodes which splits graph into two detached subsets. In graph cut procedure, the image is constituted in form of graph that contains nodes and vertices. Nodes represent pixels and edges are the distance between these nodes.

Chapter 3

Image Encryption using Coupled advanced Techniques

3.0 Introduction

With the ushers of network communication of third and fourth generation technologies, the digital images are commonly transmitted on public communication networks. It is, therefore, crucial to prevent images piracy, most importantly; the medical images must be saved from forging that is why, the image encryption technology has become a powerful tool for information security. The images are of two types: The heavy data capacity pixels and the strong correlation with the neighboring pixels. Therefore, the conventional encryption algorithms are not suitable for such types of image encryption. Recently [24, 26, 27, 28, 29, 30], researchers have used chaotic cryptography as it has ergodicity and sensitive dependence on initial conditions and high efficiency in image encryption. There are many rooms to improve the strength of the algorithm such as optimal randomness in placing the pixels or acquiring genetic algorithmic properties for optimally placement of pixels in the process of confusion and diffusion.

The confusion and diffusion processes based on Shannon theory [31] are applied in image encryption successfully. These processes have used a permutation diffusion structure and

others have used chaotic image encryption systems. Both of them have shuffled the position of pixels by confusing phases and separating the two processes.

These are weak algorithms and periodic state appeared after little iteration [32]. Other problems are the size of a picture, that is, height and width of the processed images must be the same for permutation processes and the pixel position of different images in same size is fixed. These weaknesses are not acceptable in practical applications in the chaotic cryptography. Separation of confusion and diffusion processes has reduced the efficiency of an encryption algorithm. A different mapping scheme has been used to confuse the plain images and then to diffuse with a piece-wise linear chaotic map [33]. In this chapter, an improved PWLCM model based on random selection of pixels and the pixel's fitness of plain images is proposed. The pixel's fitness is selected by a simple use of genetic algorithm. We use this model to shuffle pixel's position and diffuse values in plain image simultaneously. Test results and security analysis are carried out and the strength of algorithm has achieved to resist against brute force attack.

Motivation behind this work is to develop a comprehensive algorithm which is robust, secure and simple to encode image encryption techniques for hiding important classified pictures or medical images which should not be traceable by any means except the authorized person. The developed technique must be feasible from computational complexity and storage point of view. The technique must also be protected against brute force attack. In the following sections, we describe the basic genetic algorithm and PWLCM.

3.1 Genetic Algorithm

In general the genetic algorithm was developed for optimization problem and implemented on genes for the population growth. The basic algorithm is consisting of selection of the

chromosomes, crossover for population growth and finally mutation which resulted in an optimal chromosome for further population growth. There after this algorithm was used mostly in optimization problems. In current research, genetic algorithm section is applied to pick two pixels as an initial population from a target image and find fitness near-global optimal pixel for numerous objective functions. The procedure is described as follows:

- Initialize operators and parameters of GA
- While (Termination condition = FALSE)do
- Begin Population initialization
- Selection
- Crossover
- Mutation
- Replacement
- End
- Set chromosome structure and assign sub-goal weighting by the process parameter controller.
- Refine GA operators and parameters by the GA manager.

3.2 Piecewise Linear Chaotic Map(PWLCM)

Linear Chaotic map is a map in which pixels do not behave periodicity. Any piecewise linear functions which behaves non periodicity in pixels sequence are called piecewise linear chaotic function. One of the PWLCM is defined as follows

$$x_{n+1} = \begin{cases} x_n/q & \text{for} \quad 0 \le x_n < q \\ (x_n - q)/(0.5 - q) & \text{for} \quad q \le x_n < 0.5 \\ F(1 - x_n, q) & \text{for} \quad 0.5 < x_n < 1 \end{cases}$$

where $x_n \in (0, 1)$, and the control parameter which is so called secret key $q \in (0, 0.5)$, evolved into a chaotic state. This system has been provided excellent profile due to randomness; it is widely used for image encryption.

3.3 The Modified Piecewise Linear Chaotic Map (MPWLCM)

The PWLCM described in section 3.2 is now modified with inserting a different non-linear function given below.

$$x_{n+1} = \frac{x_n - \left\lfloor x_n/q \right\rfloor \times q}{q} \qquad (3.1)$$

Equation (3.1) is a non-linear sequence with different fixed values of q. For the purpose of encryption, the one which is non repeating and fairly random sequence is the best for image encryption.

Figure (3.1) and Figure (3.2) show the state sequences of PWLCM and MPWLCM respectively. It is shown that the randomness of MPWLCM is better for the image encryption. In the following section, we describe a crypto system based on these two mappings but selection of pixels is done by the genetic algorithm.

3.4 The proposed Algorithm for encryption

Based on PWLCM and MPWLCM, we have calculated the sequence x_{n+1}, converted this

sequence into a binary sequence s_{n+1} and then applied genetic algorithm on binary sequence to obtain best fit pixel to use them for linear chaotic function for encryption. Fitness of binary sequence is based on intensity of each pixel compared with neighboring pixels, if the intensity of the target pixel is close to the average intensity of the neighboring pixels it is taken otherwise choose another one. Having done the fitness of the pixel, we perform the confusion, diffusion and optimization of the plain images given below:

- Calculate the sequence x_{n+1}, from PWLCM algorithm
- Re-calculate the updated sequence x_{n+1}, using MPWLCM algorithm.
- Convert the latest calculated sequence x_{n+1}, into binary sequence, s_{n+1}, to use for further encryption processes.
- Use genetic algorithm to retain the most fit pixel using fitness of the individual pixels intensity compared with neighboring pixels and obtained the sequence s'_{n+1} . This sequence is now prepared for using encryption process.
- Convert the binary sequence s'_{n+1} into decimal values as y_{n+1}.

The algorithm after applying genetic on MPWLCM was given the name GA-MPWLCM. The proposed GA-MPWLCM has better performance in randomness and achieved good secured system for encryption.

3.5 The Cryptosystem based on GA-MPWLCM

Consider a gray scale image of size $L = M \times N$, where M, N are rows and columns matrix and values of each element are ranged from 0 to 255. This data is treated as one-dimensional array, $P = (p(1), p(2), \ldots, , p(L))$, in which, $p(i)$ denotes gray level of image pixels at $\lceil (i/n) \rceil, [\lceil (i/n) \rceil - (i - 1) \times n]$.

3.5.1 Permutation sequence through Genetic Algorithm

Consider one-dimensional array $\boldsymbol{P}$ described in section 3.5 with size L. To generate a permutation sequence, we choose an initial value, x_0 and an array $\boldsymbol{P}$, then calculate one-dimensional array, $T(i)$, as $T = [t(1), t(2), \ldots, t(L)]$ is an ergodic matrix of size $1 \times L$, where $t(i)$ are integers so

$t(i) \in [1, L]$,

And

$t(i) \neq t(j)$ if $i \neq j$.

The scheme is described as follows:

- Iterate the PWLCM sequence , $x_{i+1} = F(x_i)$ for maximum time iteration to make the sequence steady state; set a one-dimensional matrix A, with zero elements of length L; initialize permutation sequence $T = [t(1), t(2), \ldots, t(L)] : T = A$
- Let $i = 1$;
- Iterate MPWLCM to calculate a new $\boldsymbol{x}$, compute an integer, j using current value of $\boldsymbol{x}$ as follows:
- $j = |(\lfloor (x \times 1015) \rfloor, L)| + 1$
- Check values of j and $A(j)$, if $(j == i)$, or $(A(j) == 1)$ then repeat the previous step; else move to next step.
- $A(j) = 1;\ t(i) = j$
- Increase, i by one and repeat the whole process until $i = L$.

3.5.2 Diffusion Sequence through GA-Algorithm

Before we use the sequence, $\boldsymbol{T}$, for the encryption process, we further use diffusion on sequence $\boldsymbol{T}$ to make the sequence more confuse.

Following are steps to generate diffusion sequence are as follows:

- The diffusion sequence is denoted by $K = [k(1), k(2), \dots, k(L)]$, $k(i) = 0, i = 1, 2, \dots, L$
- Let $i = 1$
- Compute a new x, by iterating PWLCM using the current x as follows:

$$k(i) = |(\lfloor(x \times 102 - \lfloor(x \times 102)\rfloor) \times 103\rfloor, 256)|.$$

- Check for $k(i)$, if $k(i) < 3$, then $k(i) = k(i) + 3$
- Increase, i by one and repeat the whole process until, $i = L$.

  Finally, obtained sequence is diffused completely.

3.5.3 Encryption Algorithm

The encryption process use both permutation sequence $\boldsymbol{T}$ to shuffle position of image pixels and the diffusion sequence K to diffuse the values of image pixels simultaneously. The encryption algorithm is described as follows:

- Move the pixel position, i in plain image to the position, j in the cipher image, where $j = t(i)$.
- Simultaneously the pixel value of position i in plain image is altered by using diffusion key $k(i)$ and previously encrypted pixel value.
- The swapping of pixel values position is done randomly by selecting two positions of

plain image and encrypted image. This algorithm is distinct from usual algorithms and has more strength to the security.

- The permutation and diffusion processes may be repeated R rounds

$$(r = 1\ to\ R, R \geq 1).$$

- The encryption formula is the same as given in [25], except the selection of plain and cipher pixels is done randomly as follows;

$$c(j) = |(p(i) + c_1, 256)| \bigoplus k(i) \text{ if } r = 1$$
$$c(j) = |(c(i) + c_1, 256)| \bigoplus k(i) \text{ if } r > 1$$
$$\text{where } i = 1, 2, ..., L \text{ and } j = 1, 2, ..., L$$

Where c is for encryption

The encryption algorithm is described as follows:

- Set $n = 1$
- If n is even, then $i = \lceil (n/2) \rceil$; otherwise $i = (RanL - n/2 + 1)$
- Obtain $j = t(i)$
- Use the above mentioned formulas to permute and diffuse the current pixel simultaneously.
- Upgrade $n = n + 1$
- If $n < L$ then repeat the whole steps, otherwise one round is completed.

3.6 Results and Analysis

Consider an 8-bit gray scale image of size 256×256 with parameters $q = 0.3$, $x_0 = 0.27, max - time = 200, c_0 = 150$ and $R = 2$. Having run the program with different x_0 values we concluded that the best results in terms of periodicity of the sequence was obtained

for $x_0 = 0.27$. Results obtained and presented in figures (3.1-3.10). Figure 3.1 shows non repeating periodicity obtained by MPWLCM with $q = 0.3$ whereas figure 3.2 shows repeating behavior of the sequence obtained by PWLCM with $q = 0.3$. Figures (3.3, 3.4, 3.7 and 3.8) are obtained plain image and cipher image of rice and cameraman respectively using sequence of MPWLCM. The rest of the figures are the histograms of rice and cameraman and their encrypted images respectively.

In this chapter we proposed a symmetric key cryptographic system using PWLCM, MPWLCM and the genetic algorithm to encrypt plain images. This system use genetic algorithm for the selection of pixel's position and provide strong cryptographic security. Texts would also be embedded into images and the same equally employed to RGB images. Due to the random approach, it has ability to resist any kind of attacks.

3.6.1 Key Space Analysis

Sample images of size 256×256 with 8 bit grayscale are normally used for testing. In this chapter, we assumed the same system parameters as in the case of MPWLCM given in [25]. The total number of keys used for encryption procedures give Key space size. Since we are using the MPWLCM scheme, therefore it is guaranteed that total size of keys is much more than, 2^{124} due to genetic algorithm. Thus, key space size for present algorithm is large enough to defy all kinds of assaults.

3.6.2 Statistical Analysis

Generally the confusion and diffusion processes are known as statistical analysis. This analysis has been done for MPWLCM with genetic algorithm. Results are shown in terms of histograms

and correlations in figures (3.5, 3. 6, 3. 9 and 3.10) and (Table 3.1) respectively.

3.6.3 Histograms of Encrypted Images

To demonstrate the histograms, we have selected 256 gray level images with size of 256×256 and calculated their histograms (figures (3.5 and 3.9)). The histograms of encrypted images are quite uniform and different from the original images figures (3.6 and 3.10). Correlation coefficient of two adjacent pixels of both plain image and encrypted image gives a fair comparison of all other algorithms. The comparison is carried out in vertical, horizontal and diagonal directions using the given formulas:

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i$$

$$D(x) = \frac{1}{L}\sum_{i=1}^{L} [x_i - E(x)]$$

$$Conv(x, y) = \frac{1}{L}\sum_{i=1}^{L} [x_i - E(x)]\,[y_i - E(y)]$$

$$\gamma_{xy} = \frac{Conv(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

Where x and y are gray-scale values of two-adjacent pixels in the image and γ_{xy} is the correlation coefficient of two adjacent pixels. The test results are given in Table 3.1. The calculated SNR values using the proposed algorithm are given in Table.3.2.

Table 3.1. Correlation of two adjacent pixels

Correlation	Horizontal	Vertical	Diagonal
Pepper	0.942848	0.945174	0.897210
Encrypted Pepper	-0.000182	0.000357	0.004215
Cameraman	0.933475	0.959223	0.908663
Encrypted Cameraman	-0.000090	-0.007362	0.003039
Rice	0.933471	0.959124	0.908666
Encrypted Rice	0.000012	0.000321	0.003452
Lena	0.904267	0.906432	0.875651
Encrypted Lena	-0.000167	0.000342	0.004875
Jelly beans	0.863571	0.866551	0.824165
Encrypted Jelly beans	-0.000159	0.000332	0.003452
Baboon	0.986453	0.988587	0.93129
Encrypted Baboon	-0.000220	0.000339	0.004876

Table.3.2. SNR value of different Images

Plain Image	256x256
Cameraman	0.4361
Rice	0.3621
Lena	0.4798
Tree	0.3123
APC	0.4291
Test Park	0.3982
Elain	0.4853
Truck	0.4663
Tiffany	0.4781
Ruler	0.2216
Couple	0.3672
Aerial	0.3144
Chemical Plant	0.4462
Moon Surface	0.3698

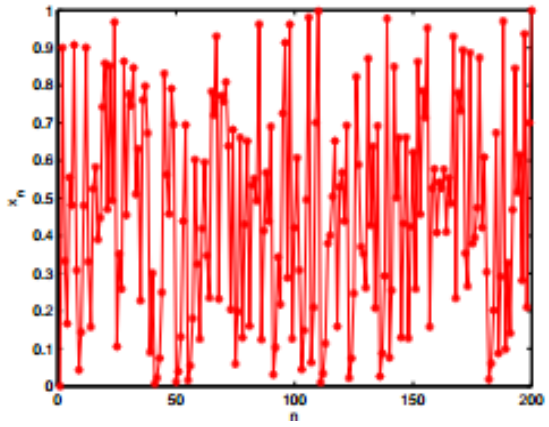


Figure 3.1: The state sequences of MPWLCM (q=0.3)

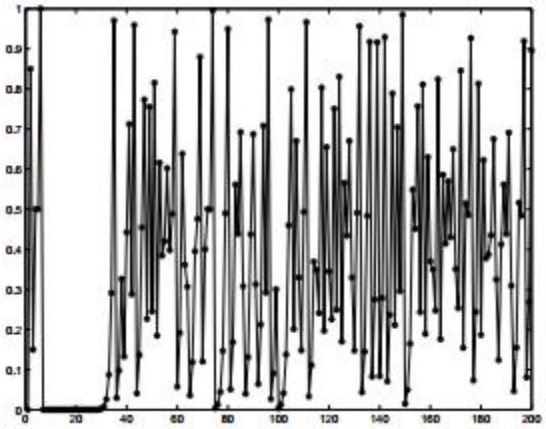


Figure 3.2: The state sequences of PWLCM (q=0.3)

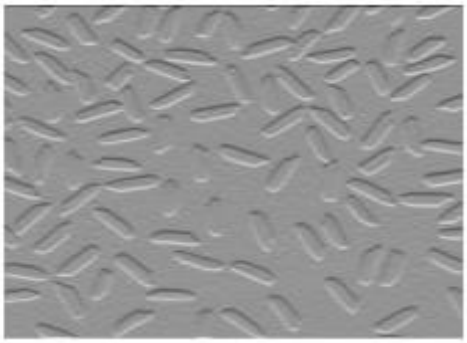


Figure 3.3: The Plain Image of Rice

Figure 3.4: The Cipher Image

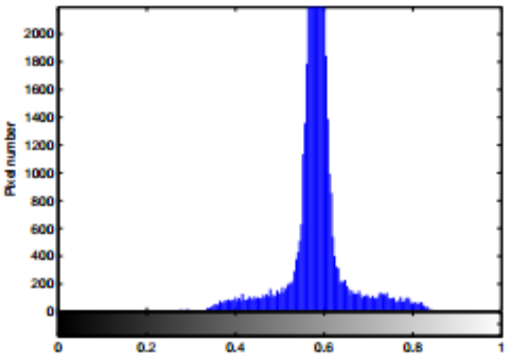


Figure 3.5: Histogram of Plain Image

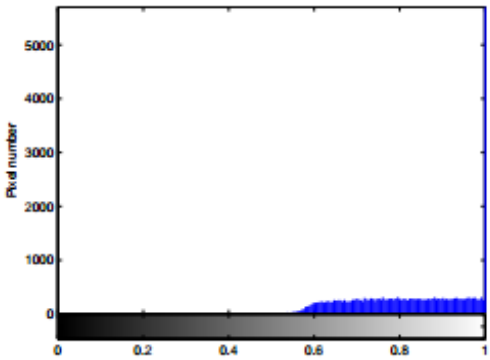


Figure 3.6: Histogram of Cipher Image

Figure 3.7: The Plain Image of Camera man

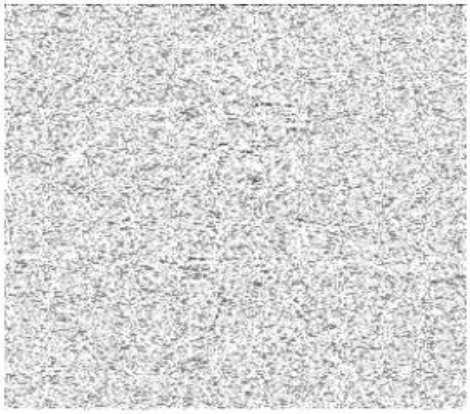


Figure 3.8: The Cipher Image

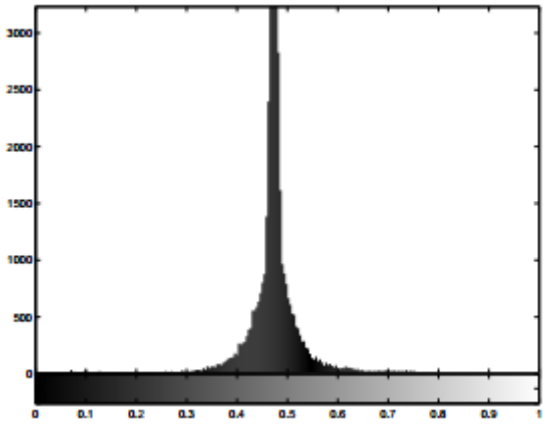


Figure 3.9: Histogram of Plain Image

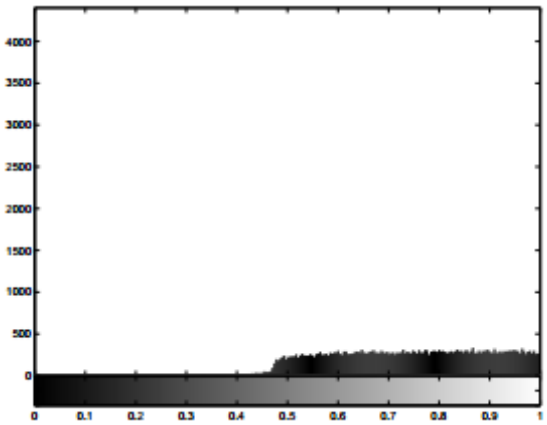


Figure 3.10: Histogram of Cipher Image

Chapter 4

Text Embedding using Modern Encryption Techniques with GA and MPWLCM

4.0 Introduction

In Chapter 3 we have developed a coupled system based on genetic algorithm and PWLCM. A detailed analysis has been carried out which has shown a strong security and easy to implement for text embedding. It is therefore, GA-PWLCM can easily be used for text embedding and medical images. The conventional encryption algorithms are not suitable for such kind of image encryption/text encryption. Unless and until chaotic cryptography be implemented. There are many rooms to improve the strength of the algorithm defined in the previous chapter such as optimal randomness and placing the pixels or acquiring the genetic algorithm properties together with modern encryption techniques like DES for optimally placement of pixels with text embedded in the process of confusion and diffusion. Despite of confusion and diffusion processes the strength of the algorithm is not that stronge for text embedding. It is therefore, a combination of modern encryption techniques together with GA-PWLCM is employed. Having done coupling of two made the algorithm strong and periodic state did not appear even after large iteration. Encrypted text embedding into a picture creates many problems like size height and width of the processed images. These problems can be solved by taking a carefull permutation processes.

4.1 Genetic Algorithm for PWLCM

In previous chapter, we developed an improve PWLCM model based on random selection of pixels and the pixels fitness of plain images. The fitness may be selected by a simple use of genetic algorithm. We used this model to shuffle positions and diffuse values of pixels in plain image simultaneously. Test results and security analysis were carried out and the strength of the algorithm achieved to resist against brute force attack.

4.1.1 Text embedding using PWLCM with genetic algorithm

This section is an addition to our earlier work by introducing technique to embed text into the encrypted images. The researchers [25**, 26**] have implemented this idea of embedding text into image without taking or analyzing the strength of security. The only security was the hiding text into images. This could only be secured till the retrieval of the images. We proposed an idea that first encrypt the text and image both using conventional text encryption technique and encrypt the image using the genetic algorithm. Then randomly place the encrypted text into encrypted images. This is called the double encryption techniques. Results are obtained and carried out time analysis for the retrieval of text. Further this technique can be used into medical images where the patient's history could also be placed into their encrypted bio-logical images.

4.2 Algorithm for text embedding

The MPWLCM described in the chapter 3 with operating parameters $x_N \in (0,1)$, and secret key, $q \in (0, 0.5)$, are now used together with modern encryption techniques DES. DES is first used to convert the target text into encrypted text. The encrypted text is then passing through periodicity test using MPWLCM. Having checked the periodicity the encrypted text is then placed randomly into image. The image has already passed through GA-MPWLCM. The

embedded encrypted text has tested permutation and diffusion for the security analysis. In the following section we describe how the original text is encrypted through DES and then embed into images.

4.3 Implementation of DES

4.3.1 DES Algorithm

The well known modern encryption techniques DES is briefly described in figure (4.1)

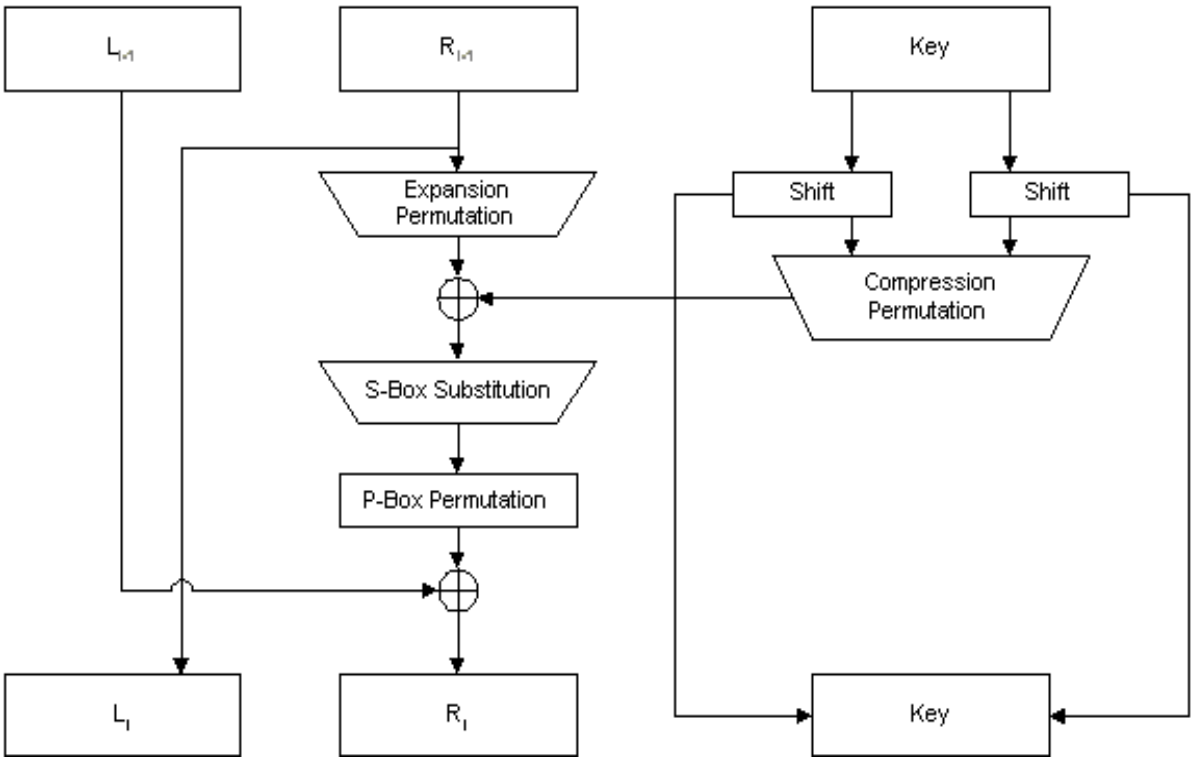


Fig. 4.1. A single round of DES algorithm

Figure (4.1) shows the internal structure of a single round. The left hand side of the figure is considered for encryption, 64 bits intermediate value treated as separate 32 bits

quantities, labeled L(left) and R(right). The overall processing of DES at each round can be summarized as follows.

$$L_i = R_i - 1$$

$$R_i = L_i - 1 \times F(R_i - 1, K_i)$$

The round key K_i is the 48 bits. R input is 32 bits, expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits. The resulting 48 bits are XORed with K_i. The 48-bit result passes through a substitution function which produces a 32 bit output which is then permutated again. The role of S-boxes accepts 6 bits as inputs and produces 4 bits as outputs through a prescribed transformation. After passing through S-boxes 32 bits output is then permuted and taken XOR with 32 bits Li and resulted 32 bit R_i. The 32 bits R_{i-1} is transformed into 32 bits L_i. First round of DES is now completed. In general, DES consists of 16 such rounds for encryption.

4.4 Embedding Phase

To insert the text into the least significant bits of image, the algorithm is as follows:

Inputs: An image in which secret text is to be embedded.

Output: An image in which text is embedded

Procedure:

Step 1: Take out all the pixels in the target image and accumulate it in the array which is called pixel array.

Step 2: Take all the characters from the secret text and put it in the array which is called character array.

Step 3: Take all the Stego-key characters and put it in the array, called Key array.

Step 4: Select first pixel location and take a character from key array and put it in the first section of pixel, if key array contains more character then put remaining characters in the first section of upcoming pixel, or else follow step (e), e has been utilized as an end mark.

Step 5: Put a few ending symbol which point out closing tags of the key. In this algorithm '0' has been utilized as an ending mark.

Step 6: The component of character array which are characters, substitute these characters in every first section of upcoming next pixels.

Step 7: Reiterate the previous step, unless all the characters have been replaced with each pixel of the target image.

Step 8: Here must be given any mark which point out that data has finished.

Step 9: Output, An image in which all the secret text character has embedded.

4.4.1 Extraction Phase

To retrieve the secret message or text; from a steganograph image follow the procedure given below

Step 1: Take character array, key array, and pixel array.

Step 2: Take out all pixels from the steganographed image and put it in the pixel array.

Step 3: Examine the pixels and take out key characters from first section of pixel and put it in the key array. Repeat this step, till the ending mark, or else go next step.

Step 4: Now, after saving the key array, if the retrieved key is equal or similar with the sender key then take step 5, or else stop the process by showing warning that key is not recognized or got similar.

Step 5: after validation of the key, again examine the next pixel and take out embedded text character from the first section of upcoming pixel and put it in the character array. Do this Step until the ending mark or else go to further step

Step 6: Take out all embedded text which is stored in character array.

4.5 PSNR of Algorithm

The most important task of this algorithm is to enhance the PSNR and utilize the logic gates to achieve this goal.

Step 1: Take the target or secret image

Step 2: Take the cover or wrap image

Step 3: Put the number of significant bits i.e. n; where n=1,2,3,4,5,6,7,8

Step 4: Set the size_secret image= size(secret) and size_cover image= size(Cover Image)

Step 5: Put the number of significant bits *"n"* significant bits of every byte of wrap image to zero by utilizing bit through AND logic gate process on wrap image and size_secret image matrix

Step 6: Fixed or inserted the MSB of target image to make steganographed image by utilizing Steganographed_img = (coverzero_secret) $/2^{8-n}$

Step 7: Retrieve the coded or secret image

Step 8: Show steganographed image and embedded image

Step 9: End

Reminder: When the value of n is increased the worth of both images would be decreased.

This algorithm is applicable for 24 bit color and 8 bit grayscale images.4.6 Results

After the experiment, outcomes have shown the strength of this algorithm as compare to the others [26, 27, 36]. We embedded and hide the text in actual or targeted image and got steganographed image. The peak signal to noise ratio (PSNR) of steganographed image is analyzed, the PSNR increased in this algorithm and visually, one cannot differentiate between original image or wrap image and steganographed image. This algorithm is implemented in Net beans Java. See Figure (4.2).

4.5.1 Security Analysis

Experiment was performed using 256×256 images with 8-bit gray scale, with parameters, $q = 0.3, x_0 = 0.27, nmax = 200, c_0 = 150,$ and $R = 2$, results were presented in Figures (4.1 to 4.10). Key space size for encryption algorithm is large enough to oppose possible types of brute force violations.

4.5.2 Key Space analysis:

In this chapter, test sample images are taken as 256×256 with 8 bit grayscale. We assumed similar system parameters as in the case of MPWLCM given in chapter **3**. Total number of keys used for encryption processes gives Key space size. Since we are using the MPWLCM scheme, therefore it is guaranteed that the total size of the key is more than 2^{124} due to the genetic algorithm. Thus, for present algorithm key space size is large enough to withstand all kinds of confrontations.

4.5.3 Statistical Analysis

Generally the confusion and diffusion processes are known statistical analysis. This analysis has been done for MPWLCM and for the genetic algorithm also. These are shown on histograms

(figures 4.7, 4.8, 4.11 and 4.12) and the correlations of adjacent pixel in encrypted images in Table (4.2).

4.5.4 Histograms of Encrypted Images

Histogram is calculated for 256 gray level images. It has been found that encrypted image is quite uniform and different from the cover images. As calculated in the last chapter the correlation coefficient of two adjacent pixels of both plain and encrypted image have a fair comparison of all other algorithms.

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i$$

$$D(x) = \frac{1}{L}\sum_{i=1}^{L} [x_i - E(x)]$$

$$Conv(x, y) = \frac{1}{L}\sum_{i=1}^{L} [x_i - E(x)]\,[y_i - E(y)]$$

$$\gamma_{xy} = \frac{Conv(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

This has to be carried out in vertical, horizontal and diagonal directions using the above formulas.

Table 4.1. Correlation of two adjacent pixels

Correlation	Horizontal	Vertical	Diagonal
Pepper	0.942848	0.945174	0.897210
Encrypted Pepper	-0.000182	0.000357	0.004215
Cameraman	0.933475	0.959223	0.908663
Encrypted Cameraman	-0.000090	-0.007362	0.003039
Rice	0.933471	0.959124	0.908666
Encrypted Rice	0.000012	0.000321	0.003452
Lena	0.904267	0.906432	0.875651
Encrypted Lena	-0.000167	0.000342	0.004875
Jelly beans	0.863571	0.866551	0.824165
Encrypted Jelly beans	-0.000159	0.000332	0.003452
Baboon	0.986453	0.988587	0.93129
Encrypted Baboon	-0.000220	0.000339	0.004876

Table. 4.2. SNR value of different Images

Plain Image	256x256
Cameraman	0.4361
Rice	0.3621
Lena	0.4798
Tree	0.3123
APC	0.4291
Test Park	0.3982
Elain	0.4853
Truck	0.4663
Tiffany	0.4781
Ruler	0.2216
Couple	0.3672
Aerial	0.3144
Chemical Plant	0.4462
Moon Surface	0.3698

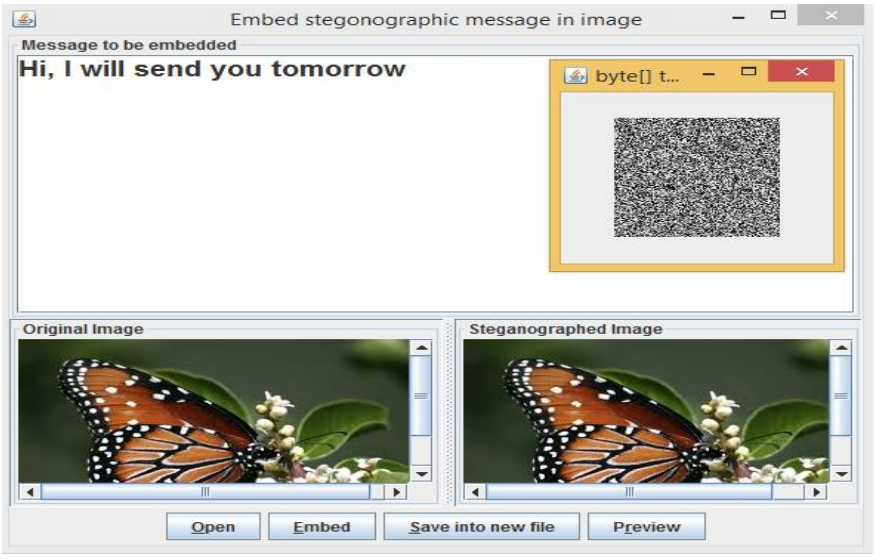


Figure 4.2(a) “Hi, I will send you tomorrow” Message is going to embed into an image (b) Selected Butterfly Image (c) After Embedding Steganographed Image (d) Encrypted Image

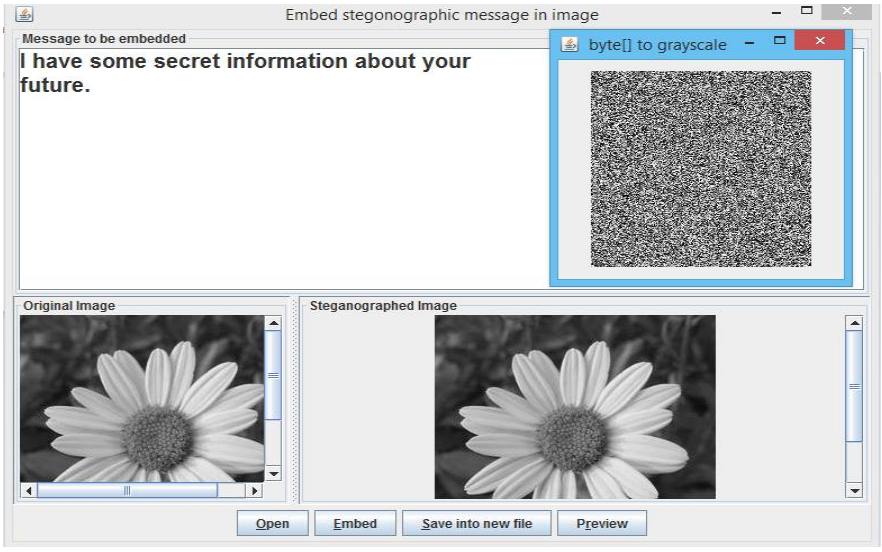


Figure. 4.2(b) “I have some secret information about future” Message is going to embed into an image (b) Selected flower Image (c) After Embedding Steganographed Image (d) Encrypted Image

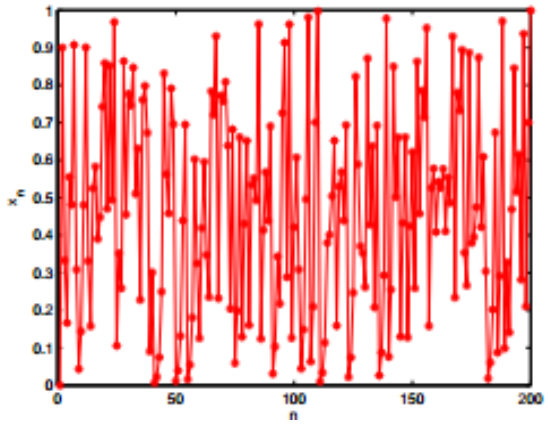


Figure 4.3: The state sequences of MPWLCM (q=0.3)

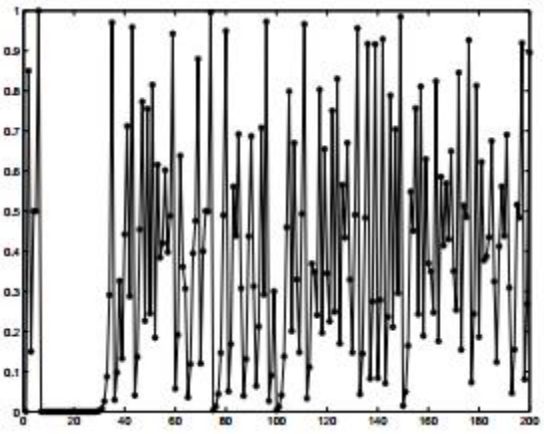


Figure 4.4: The state sequences of PWLCM (q=0.3)

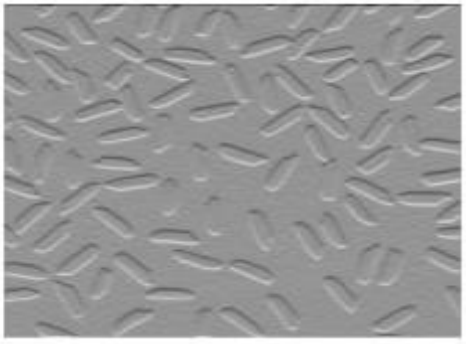


Figure 4.5: The Plain Image of Rice

Figure 4.6: The Cipher Image

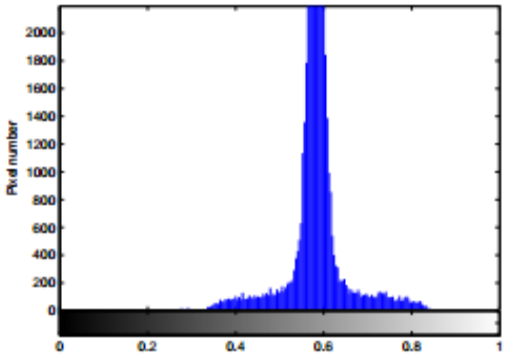


Figure 4.7: Histogram of Plain Image

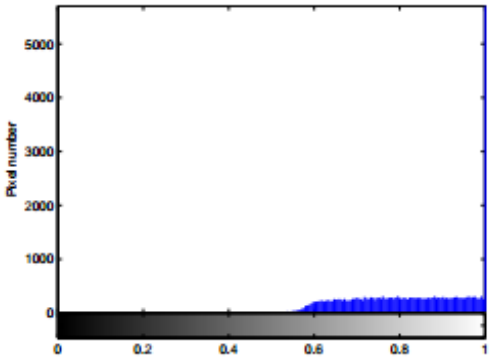


Figure 4.8: Histogram of Cipher Image

Figure 4.9: The Plain Image of cameraman

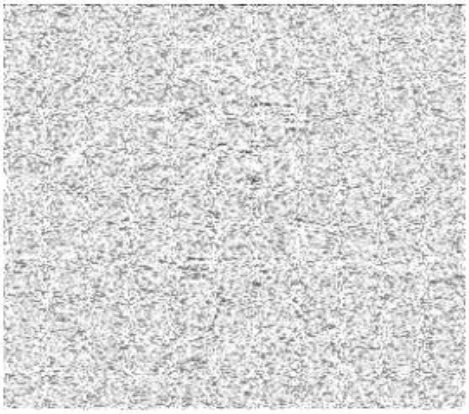


Figure 4.10: The Cipher Image of cameraman

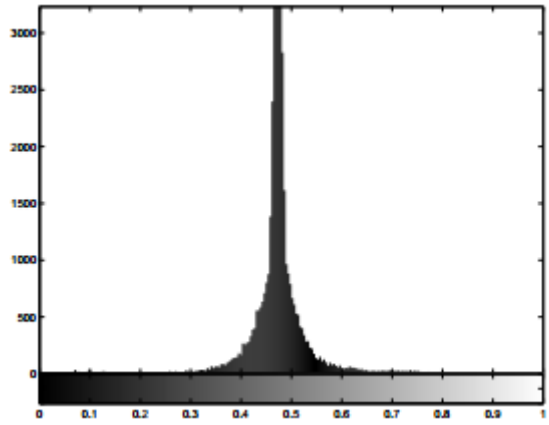


Figure 4.11: Histogram of Plain Image

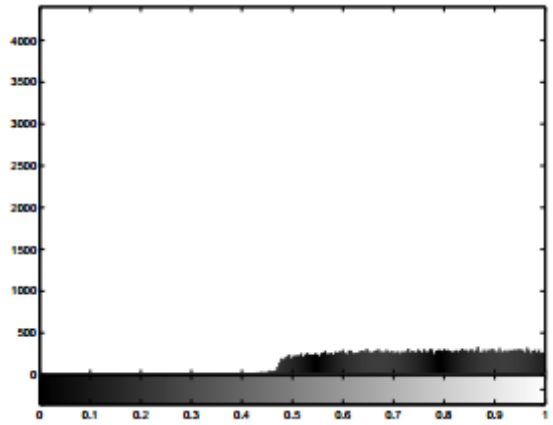


Figure 4.12: Histogram of Cipher Image

4.6 Conclusion

In this chapter, we embedded encrypted text using DES algorithm together with GA-MPWLCM. This work has proposed a strong algorithm on symmetric key cryptographic system blend of DES, PWLCM, MPWLCM and the Genetic Algorithm to embed plain text or images into images. This system, with the use of genetic algorithm for the selection of pixel's position is useful and provided strong cryptographic security. Texts could also be embedded into signals and the same has equally employed to RGB images.

Chapter 5

Image Reconstruction and Text Embedding using Graph Cut

5.0 Introduction

This chapter comprises of a new idea of text embedding into images by using a graph cut method. Patch is used for text embedding using conventional encryption algorithm. Generate a large pattern and one which is selected for proper patching, embed text into it. Image texture synthesis method based on sample is required to stimulate large realistic texture for rendering of complex graphic scenes. The concept of texture is defined as an infinite pattern that can be modeled by stationary stochastic processes. In this chapter, a new algorithm is presented which utilizes small quantity of trainee data employing petite example segment of texture; trainee data to engender an infinite precedent. In this algorithm initially an appropriate location for placement of patch is searched, followed by finding optimal region of patch embedded with text to transfer using graph cut technique to output. These approaches are not restricted to spatial (image) texture and embrace spatio-temporal (video) texture.

An engendered texture should be perceptually analogous to example texture. This notion of perceptual resemblance has been formulized as Markov Random Field (MRF). The output texture is represented as grids of nodes relied on similitude of their neighboring pixels in input textures. This input texture is used for text embedding. Goal of texture synthesis reaffirmed as solution for nodes of system. This formulation is known as machine learning. The basic

contribution of this chapter is an algorithm for texture synthesis with text embedded into it which after locating a good patch offset, compute best patch stratum. This algorithm works by reformulating as a minimum cost graph cut problem. Finally we have extended our previous text embedded into encrypted images based on graph cut algorithm. This graph cut technique is fairly used in image processing as a whole and synthesis specifically; First time we have introduced our text embedded into patterns which after synthesized would be placed in an output image. Further this technique can also be used in video synthesis technique.

5.1 Proposed Algorithm

An algorithm is developed to use the known graph cut technique for the purpose of text hiding. The algorithm is described as follows:

(i) Take a target matrix in terms of adjacency matrix of size 256 x 256. This is called target matrix to be restructured

(ii) Identify a cluster of pixels which is needed to be re-patched to get the target matrix repair.

(iii) Consider another objective matrix of the same size from where a patch is extracted using graph cut technique. This patch of objective matrix is being used to embed text in it.

(iv) The embedded text patch is placed in the target matrix to recover the original picture. This original picture is now embedded with text.

(v) To recover the text the patched portions remove from the original picture and text to be recovered.

(vi) Embedding of text into patch can be done with common text embedding

algorithm randomly.

(vii) The algorithm is implemented into a sample picture (figures 5.4-5.7), where figure (5.4) is a target picture to be synthesized, figure (5.5) is the mask of input image. The text is to be embedded in the mask. Figure (5.6) is obtained after placing the mask into target image through graph cut technique and figure (5.7) is spread after the use of graph cut technique.

5.2 Details of Algorithm

The main goal of the algorithm is the composition of the matching scene when place back to the target image. It has to recover the target image completely without superimposing pixels. The process of image composition is described in the following section.

5.2.1 Image Composition Using Graph Cut

Once the best patch was found, we place composite matching scene into incomplete image. The input mask covers the area of incomplete image that the user specified but edges of mask might not be best for stitching two images when gradient of both images are very different to each other. This can be reduced by refining the input mask, we allow mask to leave from its original path and find its best place so that subsequent blending looks more persuasive. Instead of copying and pasting matched patch into hole, stitch it together with original image so that seem between matching patch and original image is less noticeable. This can be done by finding maximum flow/minimum cut via graph cut, it has played very important role in solving certain problem in vision. Mounting number of publications in vision utilize graph-base energy

minimization techniques for application such as image segmentation, image restoration stereo, object recognition, Texture synthesis, shape reconstruction and others reveals its significance.

Graph we are building consider one node for each pixel that will be in final image. Each pixel is connected to its four neighbors. For solving graph cut problem, we need some quality measure for pixel from the original image and matched image. We assigned weights to all edges of pixel that is being considered the simplest measure is color difference flanked by pair of pixels where s and t be two contiguous pixels in overlap segment. These weights actually decide where the best cut will be. In order to create flow inside graph we need two terminal source and sink as shown figure 5.1, all pixels under mask are connected to sink while all pixel at the maximum border of local context are connected to source terminal so flow must go through the border of input mask. For calculating maximum flow/ minimum cut, we have used library implementing Max-Flow Algorithm [37].

5.2.2 Some Background of Graph Theory

A graph $G = \{V, E\}$ consists of set of nodes V and set of edges E. Each node represents a single pixel. In order to solve problems in vision using graph cut, we need two additional nodes source and sink are called terminals as shown figure 5.1. In the context of vision, terminals correspond to set of labels that can be assigned to each pixel that is being considered. George et al [39] were first to proposed max-flow/min-cut algorithms from combinatorial optimization exploited to minimize energy function. The energy function proposed by George et al and other graph-based methods can be represented as equation (5.1).

$$\boldsymbol{E(L) = \sum_{p \in P} D_{p(L_p)} + \sum_{p,q \in N} V_{p,q(L_p,L_q)}} \qquad (5.1)$$

Where $L = \{L_p | p \in P\}$ is a labeling of image P. $D_p(\cdot)$ is data penalty function that indicates label preference for pixel based on intensities. $V_{p,q}$ is an interaction potential that instigate spatial coherence by penalizing discontinuities between pixels. usually there are two form of edges N-links and T-links. N-links connect two some of pixel. Outlay of n-links refers to consequence for discontinuity amid pixels and this cost can be derived from the $V_{p,q}$ term from equation 5.1. T-links basically are used to connect pixel with terminal nodes called source and sink, cost of t-links refers to a penalty for assigning a specific label to the pixel. In the next section we will describe Min-cut/Max-flow problem briefly.

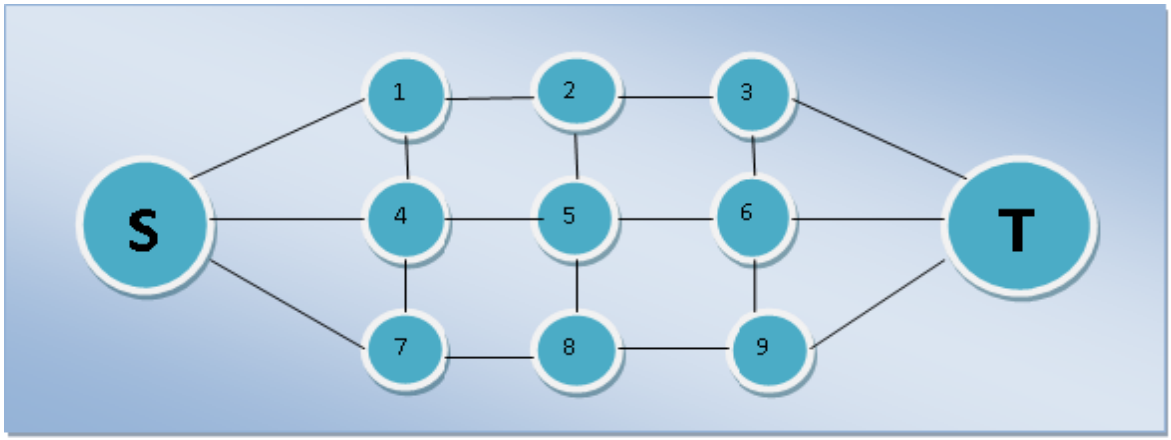


Figure 5.1: Example of graph with Source and Sink

5.2.3 Minimum-cut/Maximum- Flow Problem

A s/t cut CT with two terminals is partition of graph into subset $S1$ and $S2$ in such a way s belong to $S1$ and t belongs to $S2$. Figure 5.2 shows example of simple graph cut which show all nodes say Node1, Node2, Node4 and Node7 should belongs to subset $S1$ while Node3, Node5, Node6, Node8 and Node9 should belongs to subset $S2$. The cost of cut CT can be describes as

"Totting up of cost of all margin edges say $\{p, q\}$ where $p \in S1$ and $q \in S2$. Basic purpose of least cut is to find minimum cut among all cuts. It is done by locating maximum flow from source S to sink T. In other words, maximum flow is similar to water maximum amount that can flow from source to sink by using edges refers to as Pipes. This can be done using most commonly used algorithm Ford and Fulkerson [38] affirms that maximum flow from source to sink actually inundate edges that divide graph into two subset $S1$ and $S2$ corresponding to minimum-cut. Hence maximum-Flow and minimum-Cut are equivalent. In simple words cut CT divides the graph into disjoint subset $S1$ and $S2$ and each subset containing only one terminal. Therefore, any cut corresponds to assigning a label to a pixel (node).

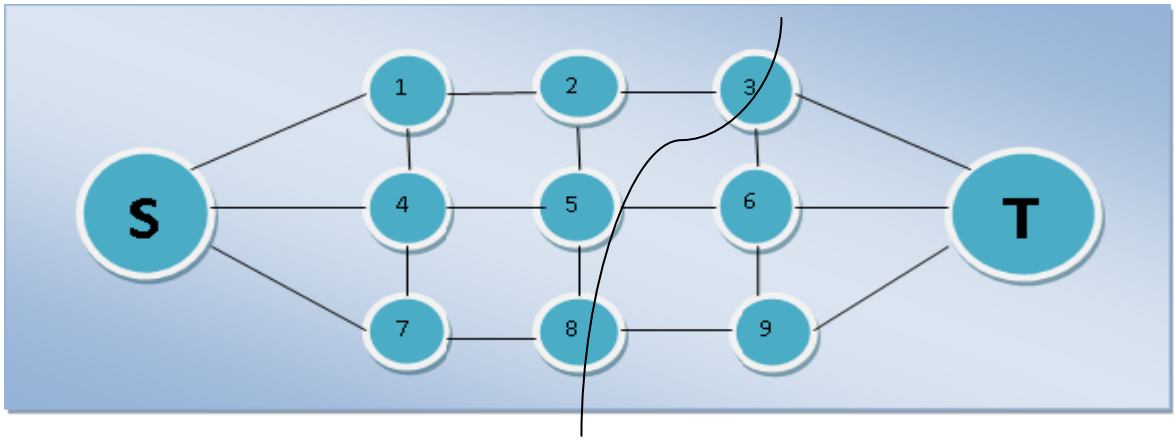


Figure 5.2: Example of cut on a Graph

5.2.4 Algorithm overview

Figure 5.3 shows basic terminology, there are two non-overlapping search trees $S1$ and $S2$ connected with parent/root at source S and sink T, respectively. In tree $S1$ and $S2$ all edges from its parent to children are non-saturated. The nodes that are not connected to any terminal node are called free nodes.

$$S1 \subset V, S \subset S1, S2 \subset V, T \subset S2, S1 \cap S2 = \emptyset$$

The nodes in tree $S1$ and $S2$ can b passive and active labeled as P and $A$and respectively, as shown in figure 5.3.The basic idea is active nodes allow to grow tree by getting new children from the free nodes. Active nodes are those which are on the border while passive nodes are internal nodes that cannot grow the tree because these nodes are completing blocked by other nodes. This algorithm is augmented –based, augmented path is found when an active node in one of the tree $S1$ or $S2$ finds a node that belongs to other tree. There are three stages that this algorithm iteratively repeats.

1. **Growth Stage:** In this stage search tree $S1$ and $S2$ grow by finding new children from set of free nodes until one node detects a node that belongs to other search tree and giving an $S - T$ path. At growth stage search trees $S1$ and $S2$ elaborated. The active nodes search for non-saturated adjacent nodes and get new children from set of free nodes as represented by black nodes in figure 5.3.These new children become active node of respective tree, all neighbor of given active node are explored then active nodes become passive node. Growth stage terminated when active node finds a node that belongs to other tree and we get a path from S to T.
2. **Augmentation Stage:** In this stage, a found path during growth stage is augmented that actually break search tree into forest. Augmentation stage augments the path by pushing maximum flow so that some edges in the path become saturated. Some of the nodes in this stage become "Stray" as edges linking Stray nodes to their parents becomes saturated (having maximum flow).

3. **Adoption Stage:** In this stage tree $S1$ and $S2$ are restored. The main purpose of this stage is to restore the single-tree structure of tree $S1$ and $S2$ with roots S and T. Adoption stage find parent of "Stray" that should be from same tree $S1$ or $S2$ and connected with non-saturated edge, if adoption stage fails to find valid parent of "Stray" node then this node is removed and becomes free node This stage terminates when there is no "Stray" node and tree S1 and S2 are restored.

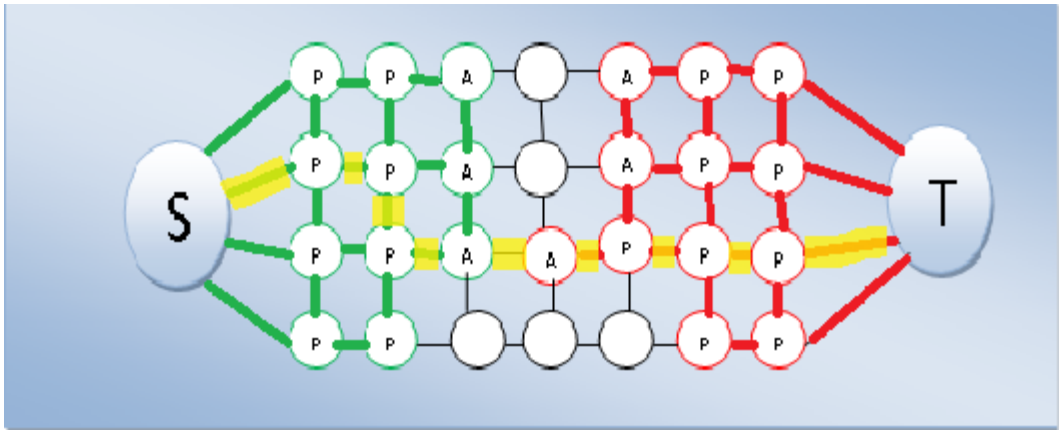


Figure 5.3: Example of search Tree ***S*1** (Green nodes) and ***S*2** (red nodes) after growth Stage when path is found from ***S*** to ***T*** .Free nodes are represented by black nodes. Active and passive nodes are labeled by ***A*** and ***P*** respectively.

5.3 Detail Implementation of Algorithm

For augmenting path algorithm, Flow f and residual graph G_f (Residual graph have same topology as original graph, it only reflects residual capacity of edge given the amount of flow in that edge) should maintain. Let we have a graph$G = \{V, E\}$. The detail of algorithm's stages Growth, Augmentation and Restore is described below.

Initialize: $S1 = \{S\}$ $S2 = \{T\}$ $A = \{S, T\}$ $Stray = \phi$

While True

Grow $S1$ or $S2$ to find Augmenting Path "P" from S to T

If $P = \phi$ terminates

Augment on PATH

Restore Stray

End while

It is very helpful to store content of search tree $S1$ and $S2$ using a flag that actually describe the relationship of each node q. so that

$$\text{flag(q)} = \begin{cases} \text{S1 if q} \in \text{S1} \\ \text{S2 if q} \in \text{S2} \\ \emptyset \text{ if q} \in \text{FreeNode} \end{cases}$$

If node q belongs to any tree then its content would be stored as Parent(q). It is very important to mention it roots of search trees say source and sink, Stray and all free nodes don't have any parent. All augmenting path algorithm must maintain residual graph so $\text{Res\_Cap(q} \rightarrow \text{r)}$ shows the residual capacity of edge (q, r) if $\text{flag(q)} = \text{S1}$ or edge (r, q) if $\text{flag(q)} = \text{S2}$. The point that is very important all these edges should be non-saturated for node q to be a valid parent for its child r.

5.3.1 Growth Stage Implementation

At this stage active node get new children from free nodes.

While $A \neq \emptyset$

Select an Active node $q \in A$

For every neighbor r such that $\text{Res\_Cap}(q \rightarrow r) > 0$

if $\text{flag}(r) = \emptyset$ Then add r to tree as an Active node

$\text{flag}(r) := \text{flag}(q)$

$\text{Parent}(r) := q$

$A := A \cup \{r\}$

If $\text{flag}(r) \neq \emptyset$ and $\text{flag}(r) \neq \text{flag}(q)$

Return P= path $S \rightarrow T$

End for

Remove q from A

End while

Return $P = \emptyset$

5.3.2 Augmentation Stage Implementation

During growth stage a path $S \rightarrow T$ has been found. The augmentation stage takes this path as an input and augments that path by pushing maximum flow from S to T so that some edges in path may become saturated. Initially, "Stray" is empty but at the end of this stage there may be some "stray "nodes because at least one edge become saturated in the given path.

Find the bottleneck capacity C on path P

Update the residual graph G_f by pushing flow f through path P

For each edge (q, r) in P that becomes saturated

If $flag(q) = flag(r) = S1$ then set

$Parent(r) := \emptyset$ and

$Stray := Stray \cup \{r\}$

If $flag(q) = flag(r) = S2$ then set

$Parent(q) := \emptyset$ and

$Stray := Stray \cup \{q\}$

End For

5.3.3 Adoption Stage Implementation

In this stage all stray nodes are processed .Each node q being processed find a new parent within same tree. If node q finds valid parent that node will remain in the same tree but with different parent and if it does not find a valid parent then this node will remove from Stray and becomes a free node. All its children nodes becomes Stray.

While $stray \neq \emptyset$

Select a Stray node $q \in Stray$ and remove it from stray

Process q

End while

The operation “Process q” contains following steps. First, find new valid parent of process q from all its neighbors. A parent r is valid parent if $\text{flag}(q) = \text{flag}(r), \text{Res\_Cap}(r \rightarrow q) > 0$ and origin of r should be source or sink because during adoption stage some node may come from Stray in the search tree S1 and S2. If node q catches the legal parent then we assign Parent(q) = r and status of node q remains the same but if it does not find valid parent then node q is treated as free node and some more operations are needed to perform

a. Scan all neighbor of node q such that flag(r)=flag(q)
    i. If Res Cap>0 add r to the active set
    ii. If Parent(r) = q add r to the set of Stray and set Parent(r):=0
b. Flag(q) :=null, A := A – {q}

5.4 Experimental Result

After the experiment, outcomes have shown the strength of this algorithm as compare to the others [25, 38, 39]. We embedded and hide the text in actual or targeted image and got steganographed image. The peak signal to noise ratio (PSNR) of steganographed image is analyzed, the PSNR increased in this algorithm and visually, one cannot differentiate between original image or wrap image and steganographed image. Having implemented the Graph cut technique on known test plain images, we obtained SNR value listed below for testing algorithm.

Table 5.1. Correlation of two adjacent pixels

Correlation	Horizontal	Vertical	Diagonal
Pepper	0.942848	0.945174	0.897210
Encrypted Pepper	-0.000162	0.000347	0.004215
Cameraman	0.933475	0.959223	0.908663
Encrypted Cameraman	-0.000091	-0.007362	0.003039
Rice	0.933471	0.959124	0.908666
Encrypted Rice	0.000014	0.000221	0.003452
Lena	0.904267	0.906432	0.875651
Encrypted Lena	-0.000167	0.000332	0.004876
Jelly beans	0.863571	0.866551	0.824165
Encrypted Jelly beans	-0.000159	0.000332	0.003452
Baboon	0.986453	0.988587	0.93129
Encrypted Baboon	-0.000230	0.000340	0.004878

Table.5.2. SNR value of different Images

Plain Image	256x256
Cameraman	0.4366
Rice	0.3921
Lena	0.4688
Tree	0.3333
APC	0.4169
Test Park	0.3982
Elain	0.4853
Truck	0.4663
Tiffany	0.4781
Ruler	0.2216
Couple	0.3672
Aerial	0.3145
Chemical Plant	0.4442
Moon Surface	0.3699

Figure 5.4:Input Image

Figure 5.5:Mask of input Image

Figure 5.6:Matching Image

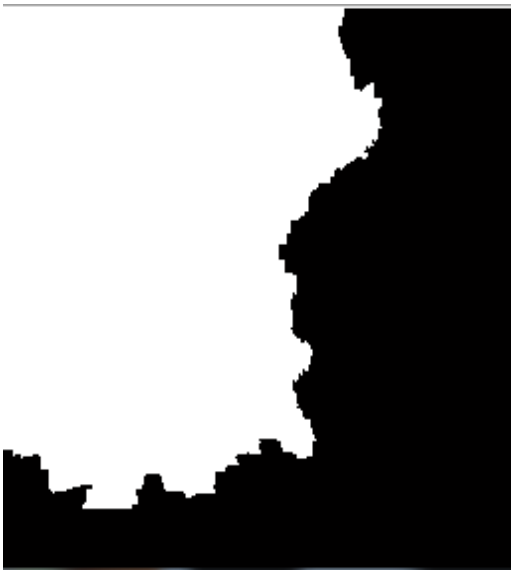


Figure 5.7: Mask After Graph cut

5.5 Conclusion

Finding is two-fold: one it has been described the details of graph cut technique to recover the original image with composing matches images and second the use of patch for the purpose of text hiding has been proposed. An example of using such algorithm has been demonstrated and analyses have also been carried out for a variety of known images and SNR were obtained.

Hiding text in such a manner is first time presented for a high quality security with double achievements. Further experiments would be done for saving space and cost effectiveness. Due to random security approach, it has ability to resist any kind of attacks. The scheme can be used on network communication.

Chapter 6

Image Reconstruction and Text Embedding using Scan Patterns with XOR in Graph Cut Technique

6.0 Introduction

In our earlier work, we have developed an algorithm where text embedded into patch regions using graph cut technique. In that work text embedding procedure was conventional. In present work we used a technique of scan pattern with XOR function [40] for text embedding into patching region. This made our previous algorithm more secure and strong confusion process. Our main focused is patching region where we are interested to embed text using scan pattern with XOR. Here we explained first usual graph cut technique and then idea of scan pattern with XOR.

The sample based image texture synthesis method was needed to generate large realistic texture for rendering of complex graphic scenes. Concept of texture was defined as an infinite pattern that can be modeled by stationary stochastic processes. In previous chapter we have presented algorithm which generated an infinite pattern from a small amount of trainee data using a small example patch embedded with text of the texture. We generated a large pattern with embedded text stochastically. The algorithm first searched for an appropriate location for placement of patch. It was then used a graph cut technique to find optimal region of patch embedded with text to transfer to output. These approaches were not limited to spatial (image) texture, and included spatio-temporal (video) texture.

A generated texture was perceptually similar to example texture. This concept of perceptual similarity has been formulized as a Markov Random Field (MRF). Output texture was represented as grids of nodes depended on similarity of their neighboring pixels in input textures. This input texture was used for text embedding. Goal of texture synthesis restated as solution for nodes of network. This formulation is known as machine learning. Primary contribution of our previous chapter was an algorithm for texture synthesis with text embedded into it which after finding a good patch offset, computed best patch seam. Algorithm worked by reformulating as a minimum cost graph cut problem. Finally, we have extended our previous text embedded into encrypted images based on graph cut algorithm. This graph cut technique was fairly used in image processing as a whole and synthesis specifically; First time we have introduced our text embedded into patterns which after synthesized placed in an output image. In present chapter we extended our work by exploiting scan pattern with XOR function for text embedding into patching regions. In following section we explain this idea in detail.

6.1 Scan Language and Proposed Method

SCAN language is an image preprocessing language, devoted to engender a family of 2D scanning patterns (or fractals). The scanning path of image is a random code form, and by enumerating pixels sequence along path. Note that scanning path of an image is merely an arrangement in which each pixel of image is accessed exactly once. Such encryption also involves specification of set of secret scanning paths. Therefore, encryption needs methodology to specify and generate larger number of wide assortments of scanning paths effectively. A scanning of a two dimensional array is a bijective function from A to B set. In other word, a scanning of a two dimensional array is an order in which each element of array is accessed

exactly once. Note that scanning function $P_{mxn} = \{ p(i,j)\ 1 < i < m, 1 < j < n\} \}$ is a bijective function from P_{mxn} to set $\{1,2, \dots , mn-1, mn\}$. The details of this technique can be found in [scan]. Proposed algorithm is described as follows:

(i) Take a target matrix in terms of adjacency matrix of size $256\ x\ 256$. This is called target matrix to be restructured

(ii) Identify a cluster of pixels which is needed to be re-patched to get the target matrix repair.

(iii) Consider another objective matrix of the same size from where a patch is extracted using graph cut technique. This patch of objective matrix is being used to embed text in it.

(iv) The embedded text patch is placed in the target matrix to recover the original picture. This original picture is now embedded with text.

(v) To recover the text the patched portions remove from the original picture and text to be recovered.

(vi) Embedding of text into patch is done with scan language technique described in [scan].

(vii) The algorithm is implemented into a sample picture (figures 6.3-6.6), where figure (6.3) is a target picture to be synthesized, figure (6.4) is the mask of input image. The text is to be embedded in the mask. Figure (6.5) is obtained after placing the mask into target image through graph cut technique and figure (6.6) is spread after the use of graph cut technique.

6.2 Details of Algorithm

This algorithm is an extension of our previous work described in the previous chapter where a composition of the matching scene when place back to the target image. The text embedding procedure is passed through by taking XOR with scan patterns; it has to recover the target image completely without superimposing pixels. The process of image composition is described in the following section. Before we describe the procedure of text embedding, we re-addressed the graph cut technique with image composition.

6.2.1. Composition of Image in Graph Cut

There are various compositions of an image while dealing with the graph cut technique. Among the various patches, one should identify the best patch to be placed composite matching scene into incomplete image. The selected mask covers the area of incomplete image that the user specified but edges of mask might not be best for stitching two images when gradient of both images are very different to each other. This can be reduced by refining the input mask, we allow mask to leave from its original path and find its best place so that subsequent blending looks more persuasive. Instead of copying and pasting matched patch into hole, stitch it together with original image so that seem between matching patch and original image is less noticeable. This can be done by finding maximum flow/minimum cut via graph cut, it has played very important role in solving certain problem in vision. The graph-base energy minimization techniques for application like image segmentation, image restoration stereo, object recognition, Texture synthesis, shape reconstruction and others are very common in use.

Consider one node for each pixel that will be in final image to be placed. That pixel is connected to its four neighbors. For solving graph cut problem, we need some quality measure

for pixel from the original image and matched image. We assigned weights to all edges of pixel that is being considered the simplest measure is color difference between pair of pixels where s and t be two adjacent pixels in the overlap region. These weights actually decide where the best cut will be. In order to create flow inside graph we need two terminal source and sink as shown figure 1, all pixels under mask are connected to sink while all pixel at the maximum border of local context are connected to source terminal so flow must go through the border of input mask. For calculating maximum flow/ minimum cut, we have used library implementing Max-Flow Algorithm [37].

6.2.2 Some preliminaries of Graph Theory

A graph $G = \{V, E\}$ consist of set of nodes V and set of edges E. Each node represent to a single pixel. In order to solve problems in vision using graph cut, we need two additional nodes source and sink are called terminals as shown figure 6.1. In the context of vision, terminals correspond to set of labels that can be assigned to each pixel that is being considered. George et al [39] were first to proposed the max-flow/min-cut algorithms from the combinatorial optimization can be used to minimize the energy function. The energy function proposed by George et al and other graph-based methods can be represented as equation 6.1.

$$\boldsymbol{E(L) = \sum_{p \in P} D_{p(L_p)} + \sum_{p,q \in N} V_{p,q(L_p,L_q)}} \quad (6.1)$$

Where $L = \{L_p | p \in P\}$ is a labeling of image P. $D_p(\cdot)$ is data penalty function that indicates label preference for pixel based on intensities. $V_{p,q}$ is an interaction potential that instigate spatial coherence by penalizing discontinuities between pixels. Normally there are two types of edges N-links and T-links. N-links connects pairs of pixel. Cost of n-links refers to a penalty for discontinuity between pixels and this cost can be derived from the $V_{p,q}$ term from equation 6.1.

T-links basically are used to connect pixel with terminal nodes called source and sink, cost of t-links refers to a penalty for assigning a specific label to the pixel. In the next section we will describe Min-cut/Max-flow problem briefly.

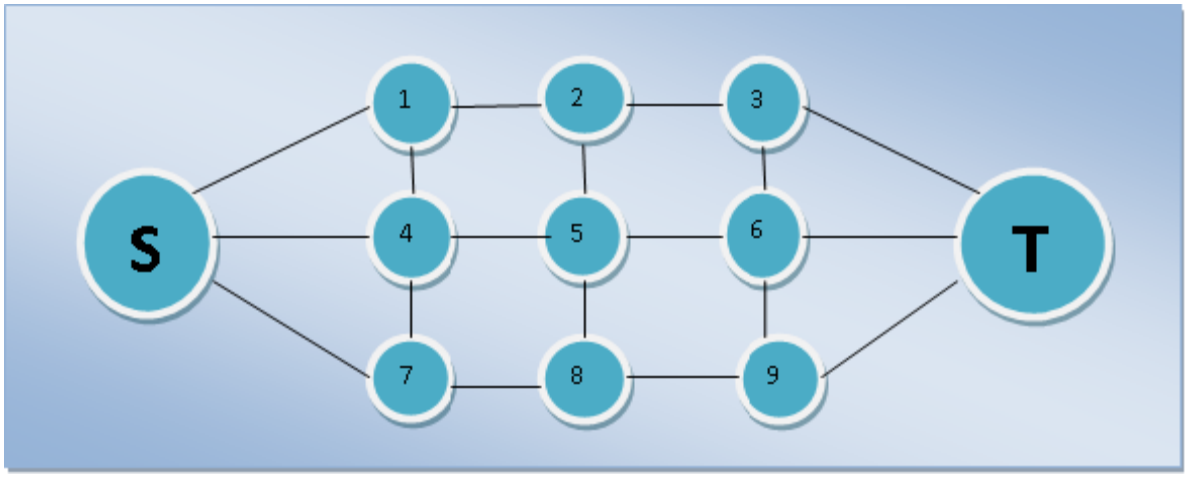


Figure 6.1. Example of graph with Source and Sink

6.2.3 Minimum-cut/Maximum- Flow Problem

A s/t cut CT with two terminals is partition of graph into subset $S1$ and $S2$ in such a way s belong to $S1$ and t belongs to $S2$. Figure 6.2 shows example of simple graph cut which show all nodes say Node1, Node2, Node4 and Node7 should belongs to subset $S1$ while Node3, Node5, Node6, Node8 and Node9 should belongs to subset $S2$. The cost of cut CT can be describes as "Totting up of cost of all margin edges say $\{p, q\}$ where $p \in S1$ and $q \in S2$. Basic purpose of least cut is to find minimum cut among all cuts. It is done by locating maximum flow from source S to sink T. In other words, maximum flow is similar to water maximum amount that can flow from source to sink by using edges refers to as Pipes. This can be done using most

commonly used algorithm Ford and Fulkerson [38] affirms that maximum flow from source to sink actually inundate edges that divide graph into two subset $S1$ and $S2$ corresponding to minimum-cut. Hence maximum-Flow and minimum-Cut are equivalent. In simple words cut CT divides the graph into disjoint subset $S1$ and $S2$ and each subset containing only one terminal. Therefore, any cut corresponds to assigning a label to a pixel (node).

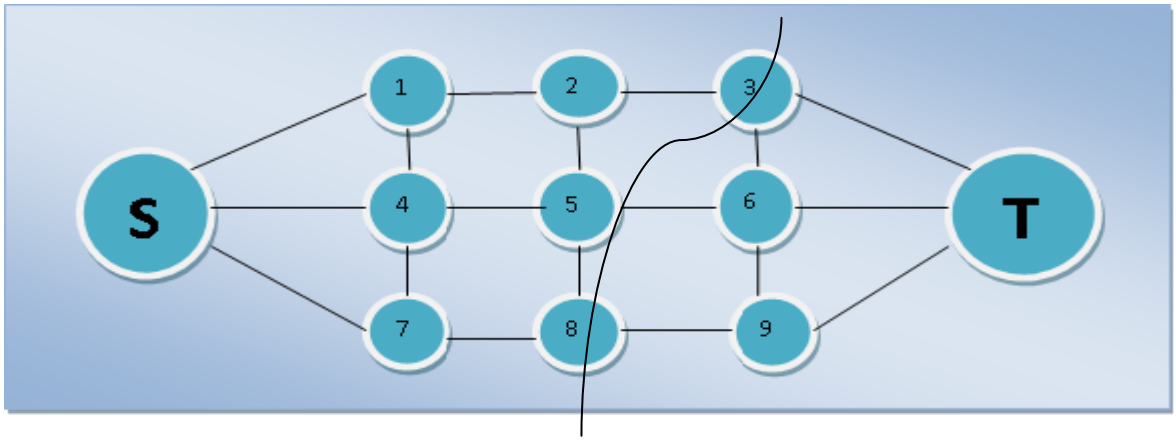


Figure 6.2. Example of cut on a Graph

6.3 Algorithm in used

The details of the algorithm has already described in chapter 5, where growth, augmentation and adoption stages are described. A pseudo code was also explained the procedure of graph cut technique and implementation of each stage. The procedure of text embedding is now described in the following section and the rest of embedding procedure is followed as in the previous chapter.

6.4 Text Embedding Procedure

Here a new algorithm for text embedding based on scan pattern with XOR and texture synthesis has been introduced. It explodes scan pattern and XOR function in three standalone steps to embed into patching regions from a sample image transformed and copied to output and then stitched together along optimal seams to generate a new output. The graph cut technique for seam optimization is applicable in two and three dimensions. This technique of patching into original picture is very much applicable in image processing. In this chapter, we have presented a new idea to embed text into patching seam using scan pattern with XOR and then placed in original images. In the subsequent section fallout for regular, random and natural images are obtained and presented. It is evitable to mention that this method can be used interactively.

6.5 Results

After the experiment, outcomes have shown the strength of this algorithm as compare to the others [26, 27]. We embedded and hide the text in actual or targeted image and got steganographed image. The peak signal to noise ratio (PSNR) of steganographed image is analyzed, the PSNR increased in this algorithm and visually, one cannot differentiate between original image or wrap image and steganographed image. Having implemented the Graph cut technique on known test plain images, we obtained SNR value listed below for testing algorithm.

Table 6.1. Correlation of two adjacent pixels

Correlation	Horizontal	Vertical	Diagonal
Pepper	0.942848	0.945174	0.897210
Encrypted Pepper	-0.000182	0.000357	0.004215
Cameraman	0.933475	0.959223	0.908663
Encrypted Cameraman	-0.000090	-0.007362	0.003039
Rice	0.933471	0.959124	0.908666
Encrypted Rice	0.000012	0.000321	0.003452
Lena	0.904267	0.906432	0.875651
Encrypted Lena	-0.000167	0.000342	0.004875
Jelly beans	0.863571	0.866551	0.824165
Encrypted Jelly beans	-0.000159	0.000332	0.003452
Baboon	0.986453	0.988587	0.93129
Encrypted Baboon	-0.000220	0.000339	0.004876

Table.6.2. SNR value of different Images

Plain Image	256x256
Cameraman	0.4961
Rice	0.3721
Lena	0.4888
Tree	0.2923
APC	0.4129
Test Park	0.4000
Elain	0.3853
Truck	0.4563
Tiffany	0.4681
Ruler	0.2316
Couple	0.3662
Aerial	0.3144
Chemical Plant	0.4462
Moon Surface	0.3698

Figure 6.3:Input Image

Figure 6.4:Mask of input Image

Figure 6.5:Matching Image

Figure 6.6:Mask after graph cut

6.6 Conclusion

This chapter is an extended version of our previous work in which we have introduced the graph cut technique to encrypt text into images. The patch for the purpose of text hiding has been used differently. The proven technique of SCAN language has been implemented for hiding text into patch portion and the rest of image construction was done similar to the graph cut techniques. An example of using such algorithm has been demonstrated and analyses have also been carried out for a variety of known images and SNR were obtained.

Hiding text in such a manner is first time presented for a high quality security with double achievements. Further experiments would be done for saving space and cost effectiveness. Due to random security approach, it has ability to resist any kind of attacks. The scheme can be used on network communications.

6.7 Future work

The scheme would be used on network communications while sending important and classified domain images. Such techniques would also be used for text embedding into images and in signals. The same would also be used in water marking processes. An effort would be made to use graph-cut technique for hiding texts into re-structured images. Selective image encryption using chaotic map and image encryption using Block Based Transformations are included in the future work.

Thesis Conclusion and Future Recommendations

There were two major achievements in the present thesis. The earlier text embedding techniques were based on chaotic maps obtained by various secret keys and parameters. Although these techniques were simple to implement but from secure algorithmic point of view it has flaws. The arrangement of pixels was non-periodic but text embedding is straight forward only the conventional diffusion and confusion processes were acquired. As a result, weaknesses were found from the security point of view. Algorithms were not found to be secured. In the present research this weakness was removed by introducing non-linear PWLCM together with Genetic Algorithm and text embedding was done randomly. The randomness was achieved through various processes. Not only the texts were embedded randomly but also a modern encryption is employed to convert the plain text into encrypted text and then placed into image randomly. To make algorithms more confused and secure, we further employed the graph cut techniques for embedding encrypted text in sample morphing pictures. The reconstruction of pictures was done by text embedded morphic samples. The analysis showed a strong secured and easy to implement image encryption techniques. The usual statistical analysis was carried out to show the strength of our algorithms. The graph cut technique was further modified by XOR function and then used for encrypted text through various modern encryption methods. Research publications were made out of the latest graph cut technique together with modern encryption methods.

A class of image encryption into signals or into frequency domains are in the process of our future work, it will be a classic work if we implement all techniques which we have

developed here. Moreover, image encryption with 2-D piece-wise linear map will also be considered in the future research work.

References

[1] J. Reeds, ``The Cipher in book III of Trithemius's steganographia", AT &T Labs-Research, Florham Park, New Jersey 07932, Draft: 26 March 1998

[2] R. Anderson and F. Petitcolas, ``On the limits of steganography", IEEE Journal of selected areas in communications, 16, (4), May 1998.

[3] K. B. Raja, K. R. Venugopal and L. M. Patnaik, "A Secure stegonographic algorithm using LSB, DCT and image compression on raw images", IEEE proceeding in the year 2005.

[4] R. Z. Wang, Chi-Fang Lin, J. C. Lin, "Hiding data in images by optimal moderately significant-bit replacement" IEE Electron, Lett. 36, (25), (2000), 2069-2070.

[5] C. K. Chan, L.M. Cheng. " Hiding data in images by simple LSB substitution", Pattern recognition, 37, 2004, 469-474.

[6] S. S. Maniccam, N. G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern recognition, 34, 2001, 1229-1245.

[7] C. C. Chang, M. S. Hwang, T. S. Chen, ``A new encryption algorithm for image crypto systems", The journal of systems and software, 58, 2001, 83-91.

[8] C. M. Shin, D. H. Seo, K. B. Chol, H. W. Lee, S. Kim, ``Multilevel image encryption by binary phase XOR operations", IEEE proceeding in the year 2003.

[9] F. Belkhouche, U. Qidwai, ``Binary image encoding using 1D chaotic maps", IEEE Proceeding in the year 2003, 39-43.

[10] I. A. Ismail, M. Amin, H. Diab, ``A digital image encryption algorithm based a composition of two chaotic logistic maps", International journal of network security, 11 (1), 2010, 1-10.

[11] Q. H. Alsafasfeh, A. A. Arfoa, ``Image encryption based on the general approach for multiple chaotic systems", Journal of signal and information processing, 2, 2011, 238-244.

[12] M. Ito, A. Alfaou, A. Mansour. ``New image encryption and compression method based on independent component analysis", 2003.

[13] N. F. Johnson, S. Jajodia, ``Exploring steganography, seeing the unseen", IEEE Computer, 31, (2), (1998), 26–34.

[14] J. C. Judge, ``Steganography, past, present, future", SANS Institute publication, 2001.

[15] E. Walia, P. Jainb, ``An Analysis of LSB & DCT based Steganography", Global journal of computer science and technology, 10(1), 2010, 4-8.

[16] S. N. Devi, P. L. Juliet, ``Survey on image steganography algorithm", International journal of communications and engineering, 4 (2), 2012.

[17] N. Jain, S. Meshram, S. Dubey, ``Image steganography using LSB and Edge – Detection technique", International journal of soft computing and engineering, 2 (3), 2012, 217-222.

[18] H. Motameni, M. Norouzi, M. Jahandar, A. Hatami, ``Labeling method in steganography", World academy of science, Engineering and Technology, 1 (6), 2007.

[19] M. Chaumont and W. Puech, ``DCT-based data hiding method to embed the color information in a JPEG grey level image", 14th European signal processing conference, 2006.

[20] S. Ohyama, M. Niimi, K. Yamawaki, H. Noda, ``Lossless data hiding using bit depth embedding for JPEG 2000 compressed bit-stream", Journal of communication and computer, 6 (2), 2009.

[21] E. T. Lin, E. J. Delp, ``A review of data hiding in digital images", Video and image processing laboratory, Indiana, 2009

[22] N. F. Johnson, S. Jajodia, Exploring stenography: ``Seeing the unseen", IEEE Computer, 31 (2), 1998, 26-34.

[23] W. Bender, D. Gruhl, N. Morimoto, A. Lu, ``Techniques for data hiding", IBM systems journal, 35 (3), 1996, 313-336.

[24] K. Zhang, J. Fang , ``Color image encryption algorithm based on TD-ERCS system and wavelet neural network", Mathematical problems in engineering, 2015,1-10.

[25] Y. Hu, C. Zhu, Z. Wang, ``An improved piecewise linear chaotic map based image encryption algorithm", The scientific world journal, volume 2, 2014, 1-7.

[26] H. Liu, X. Wang, ``Color image encryption based on one-time keys and robust chaotic maps", Computers and Mathematics with Applications, 59 (10), 2010, 3320-3327.

[27] X. Tong, M. Cui, ``Image encryption with compound chaotic sequence cipher shifting dynamically", Image and Vision Computing, 26 (6), 2008, 843-850.

[28] F. Sun, S. Liu, Z. Li, Z. Lu, ``A novel image encryption scheme based on spatial chaos map", Chaos, Solitons and fractals, 38 (3), 2008, 631-640.

[29] Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, S. Liu, ``Double image encryption by using iterative random binary encoding in gyrator domains", Optics express, 18 (11), 2010, 12033-12043.

[30] G. Zhang and Q. Liu, ``A novel image encryption method based on total shuffling scheme", Optics communications, 284 (12), 2011, 2775-2780.

[31] C. E. Shannon, ``Communication theory of secrecy systems", Bell system technical journal, 28 (4), 1949, 656-715.

[32] H. Liu and X. Wang, ``Color image encryption using spatial bit-level permutation and high dimension chaotic system", Optics communications, 284 (16), 2011, 3895-3903.

[33] X. Wang, C. Jin, ``Image encryption using game of life permutation and PWLCM chaotic system", Optics communications, 285 (4), 2012, 412-417.

[34] R. Vijayaraghavan, S. Sathya, N. R. Raajan, ``Security for an image using bit-slice rotation method-image encryption", Indian journal of science and technology, 7 (4), 2014, 1-7.

[35] R. Tamilselvi, G. Ravindran, ``Image encryption using pseudo random bit generator based on logistic maps with random transform", Indian journal of science and technology, 8 (11), 2015, 1-7.

[36] S. Indhumathi,D. Venkatesan , ``Improving coverage deployment for dynamic nodes using genetic algorithm in wireless sensor networks", Indian journal of science and technology,8 (16) 2015, 1-7.

[37] Y. Boykov, V. Kolmogorov. ``An experimental comparison of min-cut/max-flow algorithms for energy minimization in vision", Pattern Analysis and Machine

Intelligence, IEEE Transaction, 26 (9), 2004, 1121-1137.

[38] L.R. Ford, D. R. Fulkerson, ``Flows in networks". Princeton University Press: Princeton, 1962.

[39] D. M. Greig, B. T. Porteous, H. A. Seheult, ``Exact maximum a posteriori estimation for binary images". Journal of the Royal Statistical Society. Series B, 1989, 271-279.

[40] R. Moradi, R. A. Attar, and R. E. Atani, ``A new fast and simple image encryption algorithm using scan patterns and XOR". International journal of signal processing , Image processing and pattern recognition, 6 (5), 2013, 275-290.

[41] C. Fu, Z. Zhang, Y. Cao, ``An improved image encryption algorithm based on chaotic maps", Third international conference on natural computation, 3, 2007, 24-27.

[42] X. Wangn, L. Teng, X. Qin, ``A novel colour image encryption algorithm based on chaos signal processing", 92, 2012, 1101-1108.

[43] N. F. Elabady, H. M. Abdalkader, M. I. Moussa, S. F. Sabbeh, ``Image encryption based on new one dimensional chaotic map", Second international conference on engineering and technology, GUC, Egypt, 2013.