JACET Journal of Advances in Computer Engineering and Technology, 4(1) 2018

The Idea Of Using The Steganography As Encryption Tool

Ali Abed shilg[1]; Amer Saleem[2]

Received (2017-11-27)
Accepted (2018-02-10)

Abstract - **the increasing use of computers and the widespread use of networks, Social networking and use applications through the use of the Internet to make the spread images, which make it easy to be penetrated from the attacker and from everyone who try to change the information. So, the need arises to transmit the information securely through a secure manner . Steganography is the best solution to solve this Steganography may be characterized as the science of concealing or embedding "data" done a transmission medium. Its final objectives, which would undetectability, heartiness Furthermore ability of the stowed away data, are those principle Components that recognize it from cryptography. In this paper an investigation for advanced picture Cryptosystem with versatile Steganography need been exhibited. The issue from claiming information hidey need been struck starting with two directions. Those to start with methodology tries should succeed those focused on Steganalytic strike. The worth of effort keeps tabs basically on the 1st request facts built focused on strike. Two calculations bring been introduced which could preserve those primary request detail for a picture after embedding. The second methodology plans toward opposing visually impaired Steganalytic strike particularly the alignment built visually impaired strike which attempt should assess a model of the blanket picture starting with the stego picture.**

1- Student of ACRCE Khozestan (ar.habibi69@gmail.com)
2- Depatment of Computer, Central Tehran Branch, Islamic Azad University, Tehran, Iran.

1. INTRODUCTION

In this paper, we will explain the theoretical background of the proposed system which contain steganography and cryptography technique used on image and because of Since the ascent of the Web a standout amongst the most essential components of data innovation and correspondence has been the security of data. Ordinary huge amounts of information are exchanged through the Web through email, record sharing destinations, interpersonal interaction locales and so on to give some examples. As the quantity of internet clients rises, the idea of internet security has likewise pick up significance. The savagely focused nature of the PC business powers web administrations to the market dangerously fast, leaving almost no time for review of framework security, while the tight work advertise causes Web extend advancement to be staffed with less experienced faculty, who may have no preparation in security. This blend of market weight, low joblessness, and fast development makes a situation rich in machines to be misused, and pernicious clients to abuse those machines.

Because of the quick improvement of correspondence innovation, it is advantageous to procure sight and sound information. Unfortunately, the issue of illicit information get to happens each time and all around. Thus, it is imperative to ensure the substance and the approved utilization of interactive media information against the aggressors. Information encryption is a technique to make the information garbled, imperceptible or tremendous amid transmission by scrambling the substance of

information.

In a picture cryptosystem, it utilizes some solid encryption calculations or mystery keys to change or encode mystery pictures into figured pictures. Just the approved clients can decode mystery pictures from the figured pictures. The figured pictures are unimportant and non-unmistakable for any unapproved clients who get them without knowing the unscrambling calculations or the mystery keys as per (Bhattacharyya, Banerjee, & Sanyal, 2011) "Steganography's niche in security is to supplement cryptography, not replace it. If a hidden message is encrypted, it must also be decrypted if discovered, which provides another layer of protection."Disparately, steganographic systems allude to strategies for inserting mystery information into cover information such that individuals can't perceive the presence of the shrouded information. The picture steganographic strategies (or called virtual picture cryptosystems) are proposed to covering the mystery pictures into clear however non-basic cover pictures. They are intended to lessen the notice of illicit clients. Normal strategies for information stowing away can be arranged into spatial and change area techniques. In the spatial space, data stowing away is a developing exploration range, which includes applications, for example, copyright security for computerized media, watermarking, fingerprinting, and steganography. In watermarking applications, the message contains data, for example, proprietor ID and a computerized time stamp, which typically connected for copyright insurance. See Figure (1).

Unique mark, the proprietor of the informational index installs a serial number that remarkably distinguishes the client of the informational collection. This adds to copyright data to makes it conceivable to follow any unapproved utilization of the informational index back to the client. Steganography covering the mystery message inside the host informational index and nearness subtle and is to be dependably imparted to a recipient. The host informational index is intentionally undermined , however secretly, intended to be imperceptible to information analysis., in this chapter reviews the techniques of concealing the content of a massage by using steganography [10].

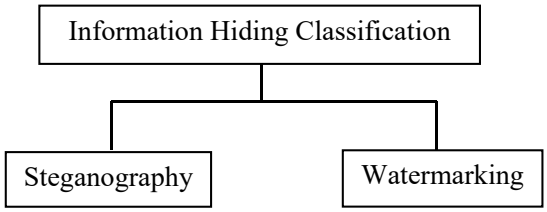

Figure (1) :Information Hiding Classification

2. STEGANOGRAPHY

The word steganography came from the an old Greek word **stegos** meaning the cover and **graphy** meaning, writing or and defining it as covered writing as appear in Table (1). Steganography is the art or the (technique) of secret communication. It is the act of encoding, installing (embedding) the secret data , for example, the presence of the data is imperceptible. The original files can refer to as cover text, cover image see **Figure (2)**.

The main purpose from Steganography is sending the important information or date in unsecure medium without detecting this information and also without any doubt or attention. If the secret information compromise to any one this means that the embedding process has been fail[1].

These points can be attributed to the renaissance of steganography[1]:

a. protecting the secret data .Government, companies and Individuals who look for privacy by using steganography, it is important to use both cryptography and steganography.

b. To ensure the protection of property rights, whereas the need to use the modern technique is to protect the rights of the owners by using (water mark).

Table(1): the original meaning of steganography

Greek word	English word	explanation
στεγανός	steganos	covered, concealed, or protected
γράφειν	graphein	Writing

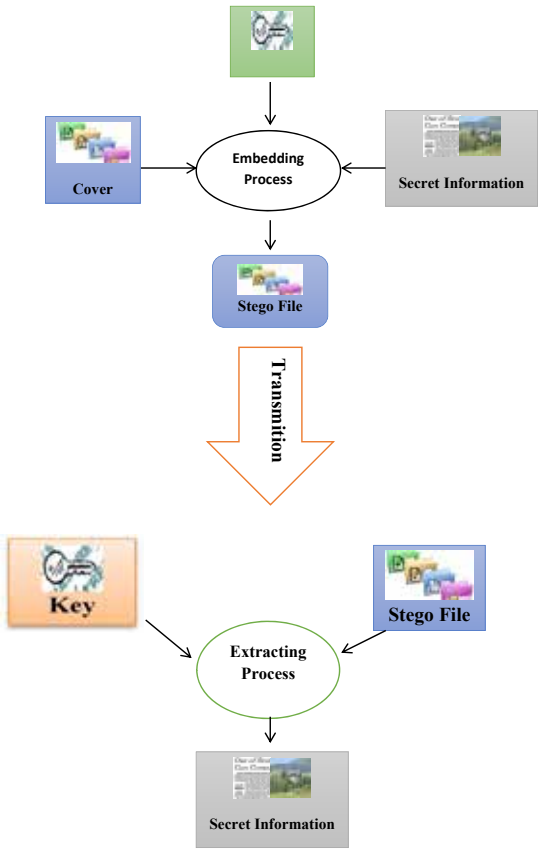

Figure (2) : Steganography Application Scenarios

2.1 STEGANOGRAPHY TECHNIQUES

The steganography techniques consist of two categories classification of Steganographic Categories and Classification of Steganographic Methods :

2.1.1 Classification of Steganographic Categories

Steganography could be divided to 2 types:

• Pure steganography with no stego key. It will be based on the assumption that is no one or third person is aware of the massage in general.

• Public key steganography where a is the public key and a the private key is used for to make safe communication[12].

2.1.2 Classification of Steganographic Methods

Steganography methods could be could be divided to 6 types, although in some cases exact classification it is impossible.

see **Figure 3**.

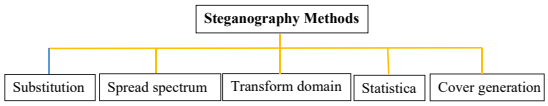

Figure 3 : Steganography Methods

• Substitution methods substitute the redundant parts of the cover with a hidden message (in the spatial domain).

• Transform domain techniques embed the hidden information in a transform space of the signal (in the frequency domain)

• Spread spectrum techniques adopt the thoughts from spread spectrum communication and transformation.

• Statistical methods encode the information by deform several statistical properties of a the cover and use hypothesis testing in the extraction process.

• Cover modeling methods encode the information in the same way that the cover for secret communication is created [12].

3. IMAGE FILE

Image is a portrait that is saved as a digital form (raster or vector). Raster means that the image consist of a set of pixel or points and this make the process of Enlargement and Reduction effecting the efficiency (quality)of the image for example (jpeg) .Raster is an image which is either as gray scale and consist of 8bits (0-265) or colored image that consist of 3 bit and consist of the main color (RGB)Red, Green and Blue , whereas the vector consist of a set of lines that is represented in an equation the image the quality of the image remain as it is with no distortion example(EPS) [11].

3.1. Image Compression

The data compression process becomes very important nowadays because of the urgent need to send and download the data for example (image)through the network whether it is Ethernets or internet in order to send the data quickly and without using large area for storing the data. Taking into consideration maintaining the efficiency of the image then using data compression process if the image in (gray scale) and the storage space will be more than (50,000) elements (256*256)pixel but if the image is colored image and its dimensions (480*640) the storage space will be (921,600) elements. Today

we have different methods of image compression available. These falls into two general categories: lossless and lossy image compression[12].

In the lossless compression, the data will remain as it is in the compression process and even after decompression this means that the data will be reduced in the compression process and because it is repeated all the data will be retrieved in the decompressing process for example Graphical Interchange Format GIF image and also bitmap file BMP [11].

In the lossycompression, the data compression process will affect the data and the data will be lost and the compression process will be applied by using (DCT)Discrete Cosine Transform equation through it the image will be divided in to blocks of frequency. In quantization stage the low frequencies will be neglected and the process of retrieving the image from frequencies in to pixel will be done by retrieving the high frequencies also the development of the efficiency of the data compression becomes very necessary because of its important role in the process of saving and sending[11].

3.1.1. JPEG Compression Techniques

Because of the redundancy between the components in the RGB image which requires storing much data and in order to reduce these components the image will be converted from RGB to YCbCr color model. In the YCbCr, (Y) represent the brightness,(Cb) its blueness and (Cr) its redness. Its values calculated in the equation below, after that using the sampling process (compressing the (Cb) and (Cr)) data.

c) Discrete Cosine Transform (DCT) is applied to each block by multiplying DCT matrix with the modified blockon the left and transpose of DCT matrix on its right.

d) Each block is then compressed through quantization.

e) By using Huffman encoding, Quantized matrixes are entropy encoded.

f) The Compressed image is reconstructed through reverse process.

g) InverseDiscrete Cosine Transform(IDCT) which is used for decompression.

Discrete cosine transform (DCT) equations are:

For a 1-D discrete signal with the length of N, DCT is expressed as [13]:

$$F(u) = C(u) \sum_{x=0}^{N-1} f(x) \cos\left[\frac{\pi(2x+1)u}{2N}\right]$$

Where $u = 0,1,\ldots,N-1$

$$C(u) = \sqrt{\frac{1}{N}} \text{ when } u = 0 \quad C(u) = \sqrt{\frac{2}{N}} \text{ when } u \neq 0 \tag{2}$$

for two-dimensional DCT is expressed as [13]:

$$F(u,v) = C(u)C(v)\sum_{x=0}^{n-1}\sum_{y=0}^{m-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right]$$

Where $u=0,1,\ldots N-1\ v=0,1,\ldots M-1$

$$C(u),\ C(v) = \sqrt{\frac{1}{N}} \text{ when } u,v = 0 \tag{3}$$

$$Cu), c(v) = \sqrt{\frac{2}{N}} \text{ when } u,v \neq 0$$

3.2. Huffman Encoding

This is very common technique for coding symbols established by their statistical appearance frequencies (probabilities). The pixels in the image are considered as symbols. The symbols that appear more than usual are assigned a smaller number of bits, while the symbols that appear less are assigned a relatively greeter number of bits. Huffman code is a prefix code. it mean that the (binary) code of any symbol is not the prefix of the code of any other symbol [14].

4. TRANSFORM DOMAIN

These techniques endeavor to encode message bits in the change area coefficients of the picture. Information implanting performed in the change space is generally utilized for strong watermarking. Comparative procedures can likewise acknowledge expansive limit inserting for steganography. Competitor changes incorporate discrete cosine Transform (DCT), discrete wavelet change (DWT), and discrete Fourier change (DFT).

By being implanted in the change space, the shrouded information dwells in more hearty ranges, spread over the whole picture, and gives better resistance against flag handling. For instance, we can play out a square DCT and, contingent upon pay-load and heartiness prerequisites, pick at least one segments in each piece to shape another information aggregate

that, thus, is pseudo haphazardly mixed and experiences a moment layer trans-development. Change is then done immediately change area coefficients utilizing different plans. These strategies have high inserting and extraction many-sided quality. As a result of the power properties of change space inserting, these systems are for the most part more relevant to the "Watermarking" part of information stowing away. Numerous steganographic methods in these spaces have been propelled from their watermarking partners.

Westfeld and Wolf (1998) utilizes the Discrete Cosine Transform coefficients of a picture for installing information bits. F5 installs information in the DCT coefficients by adjusting the quantized coefficients to the closest information bit. It likewise utilizes Matrix Encoding for lessening the installed commotion in the flag. F5 is one the most famous implanting plans in DCT area steganography, however it has been effectively softened up (Science and Goel, 2008).

The change area inserting does not really mean creating the change coefficients on pieces of size 8 × 8 as done in JPEG pressure procedures. It is conceivable to plan methods which take the changes in general picture. Other square based JPEG space and wavelet based installing calculations have been proposed in (Westfeld and Wolf, 1998).

5 . EXISTING ATTACKS

5.1. Steganalysis

Steganography is a session of find the stowaway. While steganography goes for concealing information with most extreme stealthiness, steganalysis intends to identify the nearness of any shrouded data in the stegomedia (in this proposal, JPEG pictures).

Previously, steganography kept away from any visual twists in the stego pictures. Henceforth, greater part of the stego pictures don't uncover any visual hints in the matter of whether a specific picture contains any concealed message or not. Current steganalysis expects to concentrate more on recognizing factual irregularities in the stego pictures which depend on the components removed from commonplace cover pictures with no adjustments. Cover pictures with no adjustment or bending contain an anticipated factual connection which when altered in a shape will bring about twists to that relationship. These incorporate worldwide histograms, bury and intra square conditions and other first and second request measurements of the picture. Most steganalysis calculations depend on abusing these solid conditions which are normal of regular pictures.

The steganalytic assaults created till date can be ordered into visual and factual assaults. The measurable assaults can additionally be delegated;-

1. Directed Attacks
2. Daze Attacks

Each of these classes of assault is canvassed in detail in the following two subsections alongside a few cases of every classification.

5.1.1 Targeted Attacks

These assaults are composed remembering a specific steganographic calculation. These assaults depend on the picture highlights which get changed by a specific sort of steganographic inserting. A specific steganographic calculation forces a particular sort of conduct on the picture highlights. This particular sort of conduct of the picture measurements is abused by the focused on assaults.

A portion of the focused on assaults are as per the following:

1.Histogram Analysis: The histogram investigation technique abuses the asymmetry presented by LSB substitution. The fundamental thought is to search for measurable antiquities of installing in the histogram of a given picture. It has been observed statistically that in natural images . **see Figure: 4.**

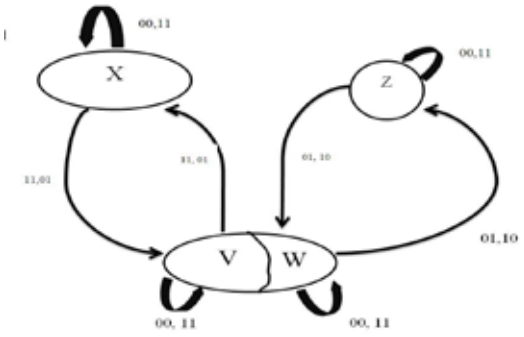

Figure : 4 The histogram investigation technique

(Cover images), the number of odd pixels and the number of even pixels are not equal. For greater than embedding rates of LSB Replacement these amount resort to be equal. So, instituted by this artifact a statistical attack instituted by the Chi-Square Hypothesis Testing is advanced to probabilistically propose one of the following two hypotheses:

Null Hypothesis H0: The image already include steganographic embedding.

Alternative Hypothesis H1: The image does not include steganographic embedding.

The decision to accept or reject the Null Hypothesis H0 is made on basis of the observed confidence value p. A more detailed discussion on Histogram Analysis can be found in (Ã et al., 2010).

Sample Pair Analysis: Sample Pair Analysis is another LSB steganalysis strategy that can recognize the presence of shrouded messages that are haphazardly inserted at all critical bits of characteristic ceaseless tone pictures. It can exactly gauge the length of the installed message, notwithstanding when the concealed message is short with respect to the picture estimate. The way to this techniques achievement is the development of 4 subsets of pixels (X, Y , U, and V) whose cardinalities change with LSB inserting (as appeared in Figure 2.1), and such changes can be definitely measured under the suspicion that the installed bits are arbitrarily scattered. An itemized investigation on Sample Pair method can be found in (Petitcolas, Anderson, and Kuhn, 1999). Another assault called RS Steganalysis in light of a similar idea has been autonomously proposed by (Kodovský and Fridrich, 2009).

From Equations 2.1 and 2.2, a dimensionless discriminator for grouping can be acquired as C (HS) C (HS) of preparing information, a picture can be characterized either as cover or stego. An itemized overview can be found in (Kodovský and Fridrich, 2009).

5.1.2 Blind Attacks

The visually impaired way to deal with steganalysis is like the example grouping issue. The example classifier, for our situation a Binary Classifier, is prepared on an arrangement of preparing information. The preparation information includes some high request measurements of the change area of an arrangement of cover and stego pictures and on the premise of this prepared dataset the classifier is given pictures for characterization as a non-inserted or an installed picture. A hefty portion of the visually impaired steganalytic systems regularly endeavor to gauge the cover picture insights from stego picture by attempting to limit the impact of installing in the stego picture. This estimation is in some cases alluded to as “Cover Image Prediction”. Probably the most well-known visually impaired assaults are characterized next. **See Figure 5** .

Wavelet Moment Analysis (WAM): Wavelet Moment Analyzer (WAM) is the most mainstream Blind Steganalyzer for Spatial Domain Embedding. It has been proposed by (Goljan, Fridrich, and Holotyak, 2011). WAM utilizes a de-noising channel to expel Gaussian clamor from pictures under the suspicion that the stego picture is an added substance blend of a non-stationary Gaussian flag and a stationary Gaussian flag with a known difference.

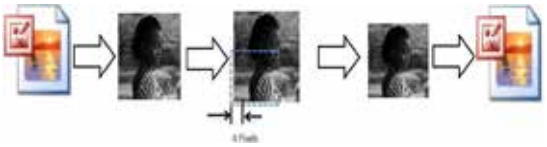

Figure 5: Calibration of the stego image for cover statistics estimation

As the examining is performed in the wavelet area, every one of the components (measurable minutes) are figured as higher request snapshots of the commotion lingering in the wavelet space. The gritty technique for computing the WAM includes in a dim scale picture can be found in (Goljan et al., 2011). WAM depends on a 27 measurement include space. It at that point utilizes a Fisher Linear Discriminant (FLD) as a classifier. It must be noticed that WAM is a best in class steganalyzer for Spatial Domain Embedding and no other visually impaired assault has been accounted for which performs superior to WAM.

1.Calibration Based Attacks: The adjustment based assaults gauge the cover picture insights by invalidating the effect of implanting in the cover picture. These assaults were first proposed by (Fridrich, 2012) and are intended for JPEG area steganographic plans. They evaluate the cover picture measurements by a procedure named as

Self Calibration. The steganalysis calculations in light of this self-alignment process can identify the nearness of steganographic clamor with just about 100% exactness notwithstanding for low inserting rates (Ã et al., 2010). This adjustment is finished by decompressing the stego JPEG picture to spatial space and editing 4 lines from the best and 4 sections from the left and recompressing the trimmed picture as appeared in Figure 2.2. The trimming and resulting recompression creates an "aligned" picture with most naturally visible elements like the first cover picture. The way toward editing by 4 pixels is a vital stride on the grounds that the 8 × 8 network of recompression "does not see" the past JPEG pressure and in this way got DCT coefficients are not impacted by past quantization (and installing) in the DCT space.

2.Farid's Wavelet Based Attack: This assault was one of the main visually impaired assaults to be star postured in steganographic examine (Lyu and Farid, n.d.) for JPEG space steganography. It depends on the components drawn from the wavelet coefficients of a picture. This assault initially makes a n level wavelet disintegration of a picture and registers four insights specifically Mean, Variance, Skewness and Kurtosis for each arrangement of coefficients yielding an aggregate of 12 × (n −1) coefficients. The second arrangement of measurements depends on the mistakes in an ideal direct indicator of coefficient size. It is from this blunder extra insights i.e. the mean, difference, skewness, and kurtosis are separated in this way framing a 24×(n−1) dimensional component vector. For usage purposes, n is set to 4 i.e. four level deterioration on the picture is performed for extraction of components. The source code of this assault is accessible at (FARID). After extraction of elements, a Support Vector Machine (SVM) is utilized for characterization.

6. STATISTICAL RESTORATION

Factual imperceptibility is one of the fundamental parts of any steganographic calculation. To keep up measurable imperceptibility, the steganographic methods are outlined with the point of limiting the antiquities presented in the cover motion by the inserting procedure. The primary accentuation is for the most part on limiting the commotion included by inserting while at the same time expanding the compensation stack. This is an essential thought in the outline of installing calculations, since the clamor included impacts the measurable properties of a medium. As of now specified beforehand, the calculation which rolls out less inserting improvements or includes less added substance clamor by and large gives preferable security over the calculation which rolls out moderately more improvements or includes higher added substance commotion (Kumar, 2011). From the perspective of the steganalyst, the assaults are intended to analyze a flag and search for measurements which get mutilated because of inserting. These insights run from minimal measurements of first and second request if there should be an occurrence of focused assaults and up to ninth request measurements for dazzle assaults (Goljan et al., 2011). Along these lines, with a specific end goal to vanquish these steganalytic assaults, there has been a move from the previously mentioned information concealing worldview. Calculations have been proposed which attempt to reestablish the insights which get mutilated amid the inserting methodology and are utilized for steganalysis.

7. IMAGE FILE FORMATS

Some of the Image File Formats are listed below [16]:

7.1 BMP format

This format consist of two main fields header and data the header Consists of 54 byte which contain the information of the image (height, width, file type ,number of band and the number of bit in each pixel), data includes the color palette or the color map in image .This format consider one of the format that is used in operating systems for example (windows) .

7.2 JPEG (Joint photo Graphic Experts Group):

It is simply images compressed algorithms which make it easy to be used in many different computer platforms. JPEG images compression is used extensively on the (WWW). It is flexible, therefore it can create large files with excellent image equality[15].

8 . CRYPTOGRAPHY

It is the art of writing in a secret codes and it has a lot of shapes. The first time the cryptography has been used in writing back to 1800 B.C. when an Egyptian used the hieroglyphs in writing whereas the new forms of cryptography came after the wide-spread and the evolution of computer Networks and communications system around the world. , crypto is the secure communication in the presence of third parties (antagonist). That's mean the main goal from it is security Related to various aspects in information security like data confidentiality, data integrity and authentication [7].

- Authentication: is the process of confirm one's identity.
- Confidentiality: is to ensure that no one especially (un authorized person) can read the secret message.
- Integrity: ensuring not to change the secret message during the process of sending .
- Non-repudiation: is to ensure that the sender really sent the secret message and to prove the identity of the sender.

There are some different between steganography and cryptography and table(2.3) show the most important difference between them [9].

Table(2) : The difference between steganography and cryptography

No.	The Steganography	The Cryptography
1	It is all about hiding the existence of the actual message	It is about hiding the content of the of the message
2	the cover doesn't trying to hide the fact that a message already there.	obscures the integrity of the massage so that it doesn't be understandable to anyone but the creator and the target.
3	stego image is not attracting any attention but stall visible and don't arouse suspicion	protect the information, when steganography protect both messages and communicating parties.

8.1 Components of a Cryptosystem

The following are the components of a cryptosystem:

- Plaintext: the original information or text is called plaintext.
- Ciphertext: it is created by using a certain encryption algorithm and the encryption key on the plaintext. During sending the message to the second party, the channel that is used to send through it is Possible tobeunprotected which make it possible to be reached from a third party and causing damage to the message.
- Encryption Key: it is the value that has been used in the encryption algorithm by the sender to produce the encrypted text ,and this can be used from the sender and the receiver in a prior agreement between them.
- Decryption Key: it is the value that has been used in the decryption algorithm in order to display the plain text which is known from the receiver and has been used with the ciphertext and decryption algorithm.
- Encryption algorithm: it is required at the side of the sender for changing the original message (Plaintext) to unreadable format (Ciphertext) to protect the information from other non-valid receivers.
- Decryption algorithm: it's required at receivers side to retrieve the original message that is to change the ciphertext to plaintext[12].

8.2 Encryption Techniques

The two basic building blocks of all encryption techniques are substitution and transposition. We examine these in the next two sections.

8.2.1 Substitution Technique

Substitution technique means changing the character instead of another character which lead to change bit with another bit. The value of the plaintext will change by another one by using mathematical equations.

ways of Substitution encryption:

- Playfair Cipher
- Hill Cipher
- Monoalphabetic Ciphers
- One-Time Pad
- Caesar Cipher
- Polyalphabetic Ciphers

8.2.2 Transposition cipher

A transposition cipher is rearranging the plaintext symbols ,by using the substitution process changing the place of the character of the message by using mathematical equations ,I will mention later the message will be encrypted in away that make it difficult to be understand and by using this equations inverse the message will change from the encryption to plaintext. This process will make the original character remain as it is without any change but changing only the place of the character and in order to decrypt the message this require rearranging the character. In this research one of these techniques will be used [14].

The Following are some transposition cipher techniques:

a. Columnar transposition
b. Rail Fence cipher
c. Myszkowski transposition
d. Route cipher
e. Disrupted transposition
f. Columnar Transposition

a. Columnar transposition

In this technique , the plaintext is written in rows of the same length, after that again read the message column by column, then we select the columns chosen in unordered way by using keyword and this keyword must be known from both the sender and the receiver [11].

b. Rail Fence Cipher

The Rail Fence cipher is a form of transposition cipher that gets its name from the method in which it is encoded. When the plaintext is written downwards on successive "rails" of an imaginary fence, then moving forward when we get to the end. The message is then read off in rows [13].

c. Myszkowski transposition

A different form of columnar transposition, Suggested by Emile Victor and Theodore Myszkowski in the year of 1902, demands a keyword with recurrent letters. When the subsequent occurrences of a keyword letter are treated as if the next letter in alphabetical order [14].

d. Route cipher

In a route cipher, the plaintext is first written out in a grid of given overall dimensions, then read off in a modality given in the key, In fact, for messages of sensible longitude, the number of possible keys is potentially very big to be calculated even by advanced machinery. But , not all keys are equally fine. Badly chosen routes will leave exaggerated chunks of plaintext, or text simply reversed, and this will give cryptanalysts a proof.

9. REFRENCES

[1] B. Mahalakshmiand Ch. Sravan Kumar, " An Overview on Disrupted Transposition Cipher for Security Enhancement", International Journal of Computer Applications, 2016.

[2] C. Chen, Y.Q. Shi,W. Chen, and G. Xuan, "Statistical moments based universal steganalysis using JPEG-2D array and 2-D characteristic function", in Proc. Int. Conf. on Image Processing, Atlanta, GA, USA, 8-11 Oct., 2006, pp. 105-108.

[3] Er. Reema Gupta Dr. Sukhvir Singh PardeepMaan,"Efficient Encryption Techniques In Cryptography Better Security Enhancement", International Journal of Advanced Research in Computer Science and Software Engineering, 2014.

[4] J. Fridrich, (2012)." Modern Steganalysis Can Detect YASS", 350.

[5] Harmsen, J. J., & Pearlman, W. A. (n.d.). Steganalysis of additive noise modelable information hiding.

[6] H. Farid, "http://www.cs.dartmouth.edu/farid/research/stegm" (Code for generating wavelet-based feature vectors)

[7] J. Fridrich, T. Pevny, and J. Kodovsky, "Statistically Undetectable JPEG Steganography: Dead Ends, Challenges, and Opportunities", in Proc. ACM Multimedia and Security Workshop, Dallas, TX, 20-21 Sept. 2007, pp. 3-14.

[8] J. Fridrich, M. Goljan, and T. Holotyak, "New Blind Steganalysis and its Implications", in Proc. SPIE Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072, pp. 607201, Jan. 2006.

[9] Nitesh Kumar More, Sipi Dubey, "JPEG Picture Compression Using Discrete Cosine Transform", in International Journal of Science and Research (IJSR), 2013.

[10] Rahul Shuklaand Narender Kumar Gupta, "Image Compression through DCT and Huffman Coding Technique", International Journal of Current Engineering and Technology, 2015.

[11] Gaurav Kumar, Er. Sukhreet Singh Brar, Rajeev Kumar, Ashok Kumar, "DWT-DCT Technique and Arithmetic-Huffman Coding based Image Compression", Published Online in MECS, 2015.

[12] Scott E Umbaugh, Ph.D, "Computer Vision and Image Processing", Prentice Hall PTR 1998.

[13] WILLIAM STALLINGS, "Cryptography and Network Security", THE WILLIAM STALLINGS BOOKS ON COMPUTER, fifth edition,2011.

[14] Rajkumar Yadav, " Study of Information Hiding Techniques and their Counterattacks", Rajkumar Yadav, International Journal of Computer Science & Communication Networks, 2011.

[15] Jawad Ahmad Dar, Sandeep Sharma, "Implementation of One Time Pad Cipher with Rail Fence and Simple Columnar Transposition Cipher, for Achieving Data security", International Journal of Science and Research (IJSR), 2014.