ISSN 2320-9984 04>
9 772320 998015

Volume 1, Issue 4, December 2013 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

New Approach of Information Security through Steganography by using Wavelet Transformation and Symmetric

Vigyan Sharma
M. Tech. Scholar
Department of Computer Science and Engineering
Patel Institute of Engineering and Science,
Bhopal, (M.P,) [INDIA]
Email: vigyan.sharma@yahoo.co.in

Prof. Hitesh Gupta
Asst. Professor
Department of Computer Science and Engineering
Patel Institute of Engineering and Science,
Bhopal, (M.P,) [INDIA]
Email: hitesh034@gmail.com

Abstract*—In this work a Steganography system, in which the data hiding (embedding) is realized in bit planes of encrypted text\image by using cryptography technique is implemented. To increase data hiding capacity while keeping the imperceptibility of the hidden data, cryptography technique and compression technique has. The proposed system shows a high data hiding capacity which is providing two layers of security first encoding of the information and second hiding of the information using LSB steganography. It known that all traditional steganography techniques work on limited information-hiding capacity. Our new Steganography system uses, an image as the visual data, initially it encoded to secrete information (text/image) with compressed manner through wavelet transform to reduced the size of secrete information (image) then this compressed information encoded through encoding technique with the help of symmetric of length of 128 bits, during mapping it create blocks of information of 128 bits in length so mapping should be linear to produced cipher secrete information in equally and at last it embed cipher secret text/image in the bit-planes of the image by using standard steganography technique (LSB Technique) through random number generation technique. During performance measurement proposed concept has set performance parameter like Peek signal to noise ration (PSNR), entropy and correlation. Based on these parameters performance through proposed concept which is show the superiority of its.*

Keywords:*—Internet, Steganography, Cryptography, Symmetric Key, Key, Algorithm, bit*

1. INTRODUCTION

The primary tool used in the research of steganography and cryptography is the Internet [11, 12]. The first thing was to understand the various terminologies related to the field. This was done through the previous research papers, books and the hyper dictionary websites. Additional technical details were obtained from various articles listed under the references section. The following points can be attributed to the renaissance of steganography:

- Government ban on digital cryptography, Individuals and companies who seek confidentiality look to steganography as an important complementary since combining cryptography and steganography can help in avoiding suspicion and protect privacy [8.9].
- The increased need to protect intellectual property rights by digital

content owners, using efficient watermarking [9, 10].

The trend towards electronic communications and humans desire to conceal messages from curious eyes. With rapid advancement in technology, steganographic software is becoming effective in hiding information in image, audio or text files [7]

The rest of the paper is structured as follows. Section II discuses the related work, Section III presents the proposed concept Section IV presents the performance parameter use proposed work and overall performance of proposed concept. Section V conclude and discuss the future directions of this work.

2. RELATED WORK

In [1] a multi secure and robustness of medical image based steganography scheme is proposed. This proposed technique provides an efficient and storage security mechanism for the protection of digital medical images. In this Integer Wavelet Transform (IWT) is used to protect the MRI medical image into a single container image. The container image was taken and flip left was applied and the dummy container image was obtained. Then the patient's medical diagnosis image was taken as secret image and Arnold transform was applied and scrambled secret image was obtained. In the first case, the scrambled secret image was embedded into the dummy container image and Inverse IWT was taken to get a dummy secret image. In the second case, the container image was taken and fused with the dummy secret image and stego image was obtained. In [2] is concerned with implementing Steganography for images, with an improvement in both security and image quality. The one that is implemented here is a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality is improved by using bit-inversion technique. In this technique, certain least significant bits of cover image are inverted after LSB steganography that co-occur with some pattern of other bits and that reduces the number of modified LSBs. Thus, less number of least significant bits of cover image is altered in comparison to plain LSB method, improving the PSNR of stegoimage. By storing the bit patterns for which LSBs are inverted, message image can be obtained correctly. To improve the robustness of steganography, RC4 algorithm has been used to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This process randomly disperses the bits of the message in the cover image and thus, making it harder for unauthorized people to extract the original message. To avoid the noise distortion in the image, the LSB insertion method is used to insert the bits in an image by using random number generators. In [3] presented technique before embedding the secret information into an image, the secret information has been compressed using the wavelet transform technique. The obtained bits after compression are encoded using quantum gates. In [4] the proposed work presents a unique technique for Image steganography based on the Data Encryption Standard (DES) using the strength of S-Box mapping & Secrete key. The preprocessing of secrete image is carried by embedding function of the steganography algorithm using two unique S-boxes. The preprocessing provide high level of security as extraction is not possible without the knowledge of mapping rules and secrete key of the function. Additionally the proposed scheme is capable of not just scrambling data but it also changes the intensity of the pixels which contributes to the safety of the encryption. In [5] I have analyzed that author proposes three indigenous methods as a variant of Cipher Block Chaining (CBC) mode for image encryption by considering three different traversing path (Horizontal, Vertical and Diagonal). In method one simple Raster Scan has been employed to scramble the confidential Image called Horizontal Image Scrambling (HIS). Method two is a variant of method one called Vertical Image Scrambling (VIS), here traversing path would be top to bottom left to Right. Third method employs diagonal traversing path called Diagonal Image Scrambling (DIS). Later

Image Steganography has been adapted to send these Scrambled Images in an unnoticeable manner. In [6] secret sharing refers to a method of distributing a secret among a group of participants, each of whom is allocated with a share of the secret. The participant's shares are used to reconstruct the secret. Single individual participants share is of no use. The reversible image sharing approach and threshold schemes are used achieve the novel secret color image sharing. The secret color image pixels will be transformed to m-ary notational system. The reversible polynomial function will be generated using (t-1) digits of secret color image pixels. Secret shares are generated with the help of reversible polynomial function and the participant's numerical key. The secret image and the cover image is embedded together to construct a stego image. The reversible image sharing process is used to reconstruct the secret image and cover image. The secret is obtained by the lagrange's formula generated from the sufficient secret shares. Quantization process is applied to improve the quality of the cover image. Peak signal to noise ratio is applied to analyze the quality of the stego images. The simulation results show that the secret and cover are reconstructed without loss [6]. Security, the most common word uttered by any man, any device, any peripheral since past two centuries. Protection from malicious sources has become a part of the invention or the discovery cycle. Myriad methods of protection are used ranging from a simple authentication password to most cryptography algorithms for protecting the extreme sensitive or confidential data. In [7] a tutorial review of the steganography techniques appeared. Various image steganography techniques have been proposed. In this I investigate of founded steganography techniques and steganalysis techniques. I state a set of criteria to analyze and evaluate the strengths and weaknesses of the previous techniques. The least-significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image with high capacity, while it is detectable by statistical analysis such as RS and Chi-square analyses. In [7] authors propose a novel LSB image steganography algorithm that can effectively resist image steganalysis based on statistical analysis

2.1 Wavelet Transformation:

Wavelet compressions are two types lossless or lossy. In lossless compression, the original data can be reconstructed from the compressed data, but in lossy compression the partial data can be reconstructed. Using wavelet transformation the data can be stored in less space, By doing so the memory space will be reduced and the data can be transferred easily [4]. Steps in wavelet compression: Load the image, perform wavelet decomposition of the image, and compress using fixed Threshold [3].

2.2 Random Number Generators:

Blum Blum Shub generator, is the pseudo random number generator. By using this random numbers are generated. The formula has shown below [3, 6],

$$Xi+1=(X/\text{mod } n$$

Where, Xi is the seed, and n be the range.

The pseudo random bit generator is used for generating random numbers in cryptography. Seed, two large prime numbers, and the range is the inputs for the pseudo random bit generators [3]. The mathematical formulae has shown below,

$$Xi+1= (PXi+Q) \text{ mod } n$$

Where P,Q are two large prime numbers, Xi is the seed. n be the range.

3. PROPOSED WORK

Proposed work entitled –Implementation of Steganography Technique (Layered Approach for Information Security) ‖ is proposed by the combination of the cryptography and steganography. Proposed

concept of information security fulfill basic security characteristic like authorization, accuracy of confidential information and integrity over network. Proposed concept proposes an encryption algorithm based on block cipher nature in symmetric cryptography. With the secrete information read ASCII value and convert it into binary value with divided into two equal parts, where binary value of each part of secrete information mapping (Circular shifting and XORing) with key value which is also equal with secret information. After completing mapping process (Circular shifting and XORing) produced encrypted information which is called cipher secrete information. The Proposed encryption/decryption algorithm used a private key value during process. This private key value is providing higher security for the proposed technique. Strength of the proposed symmetric encryption/decryption algorithm is that its take a block of 128 bits or 16 byte at a time for encryption/decryption which is highly secured and is suitable for practical use in the secure transmission of secured information over the public network. Furthermore produced ciphers secrete information embedded with cover image through standard steganography approach. Generated stego-image same in size as compare cover image after steganography process. The receiver ends the stego-image, produced encrypted information which is called cipher secret information, then apply decryption process on produced cipher secrete information to produced secrete information to get original secrete information. Figure 1 showing the block diagram of the proposed technique at sender side and Figure 2 showing the block diagram of the proposed technique at receiver side. If the secrete information is an image then proposed concept used a compression technique known wavelet transform technique to reduce the size of the image before apply mapping process. Similarly at receiver end receiver uncompressed image to get the original image after mapping process.

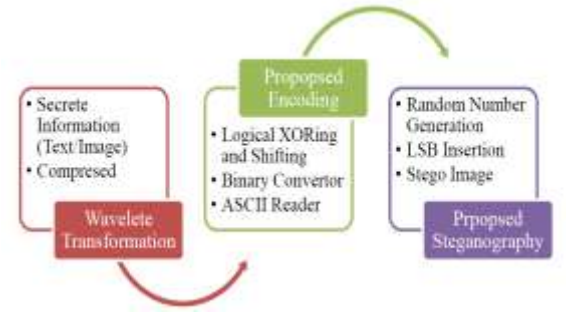


Figure 1: Block Diagram of Proposed Steganography at Encryption Side

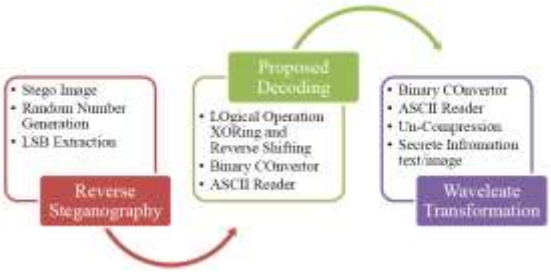


Figure 2: Block Diagram of Proposed Steganography at Decryption Side

3.1 Proposed Encryption Approach:

Figure 3 is showing the architecture of proposed encryption technique. In this initially secrete information ie. text/image converted into total number of binary value then read 128 bits at a time, these bits divided into two part. On each part of binary value perform circular shift operation then perform XORing operation with key (K) value 0f 128 bits binary which is also in two parts where sequence of key parts are inverted. Similarly this process repeat for whole binary value of 128 bits block. Step of encryption process is defined in section 3.3.1

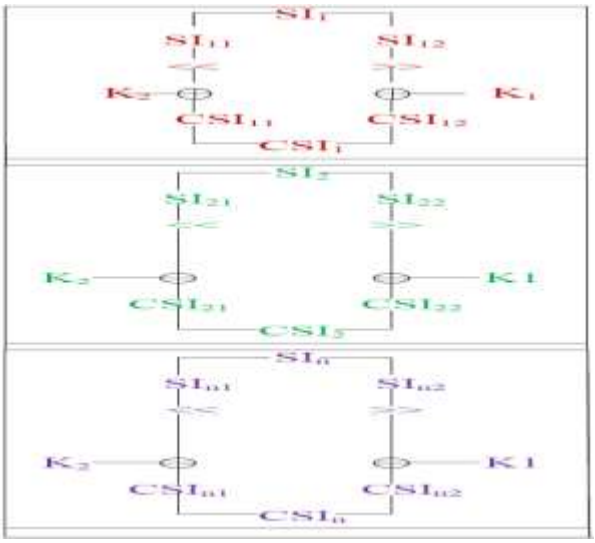


Figure 3: Architecture of Proposed Encryption

3.2 Proposed Decryption Approach:

Figure 4 is showing the architecture of proposed decryption technique. In this initially cipher secrete information i.e. text/ image converted into total number of binary value then read 128 bits at a time, these bits divided into two part. On each part of binary value perform circular shift operation then perform XORing operation with key (K) value of 128 bits binary which is also in two parts where sequence of key parts are inverted. Similarly this process repeat for whole binary value of 128 bits block. Step of encryption process is defined in section 3.3.1

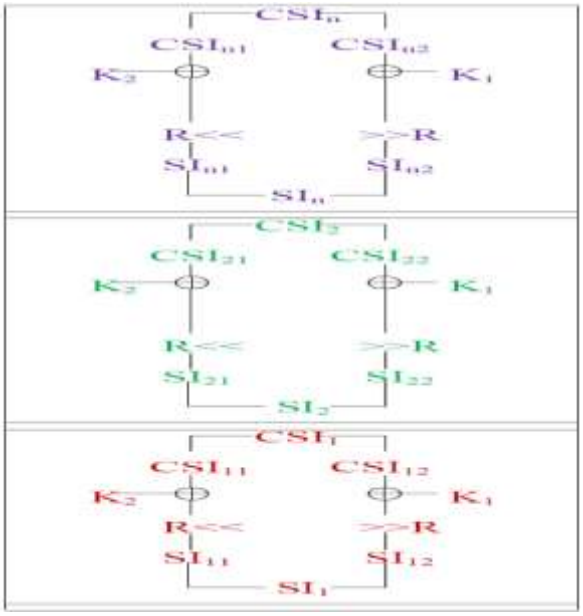


Figure 4: Architecture of Proposed Decryption

3.3 Algorithm Step: Proposed encryption algorithm Step are defining in section 3.3.1 and proposed decryption algorithm step are defining in section 3.3.2.

3.3.1 Algorithm of Proposed Encryption

1. Input Secrete Information SI ie. (Text/ Image)
2. Input Key (K) of 128 bits or 16 Bytes and Divide into K_1(64) and K_2(64) Bits
3. Read ASCII value of SI

   a. ASCII (SI)

4. Binary Convertor

   a. Bit = Binary (ASCII (SI))

5. Loop I = 1 to N
6. Loop J = 1 to N

   i. If ($Count_j$ (SI_i) == 128 Bits)

   Then

   $SI_i/2$ → (SI_{i1}(64)) & (SI_{i2}(64)) Go to Sept ii

   Else

   $Count_j$ (SI_i) ++

   ii. 2 bits Left and Right Circular Shifting

   1. << (SI_{i1})
   2. >> (SI_{i2})

   iii. XORing

   $CSI_{i1} = K_2 \oplus SI_{i1}$

   $CSI_{i2} = K_1 \oplus SI_{i2}$

   iv. $CS_i = CSI_{i1} \otimes CSI_{i2}$

   v. End Loop J

   vi. I = I+1

7. End Loop for I
8. Exit

3.3.2 Proposed Decryption Algorithm for Receiver Side:

1. Input Cipher Secrete Information CSI ie. (Text/Image)
2. Input Key (K) of 128 bits or 16 Bytes and Divide into K_1(64) and K_2(64) Bits
3. Read ASCII value of CSI

   a. ASCII (CSI)

4. Binary Convertor

   a. Bit = Binary (ASCII (CSI))

5. Loop I = 1 to N

6. Loop J = 1 to N

7. CASE -1 → For I = N to 1

i. If ($Count_j$ (CSI_i) == 128) Then

$CSI_i/2$ → (CSI_{i1}(64)) & (CSI_{i2}(64))

Go to Sept ii

Else

$Count_j$ (CSI_i) ++

ii. XORing

$SI_{i1} = K_2 \oplus CSI_{i1}$

$SI_{i2} = K_1 \oplus CSI_{i2}$

iii. 2 bits Left & Right Reverse Circular Shifting

SI_{i1} = (R<< (CSI_{i1})) SI_{i2} = (R>> (CSI_{i2}))

iv. $SI_i = SI_{i1} \otimes SI_{i2}$

v. End Loop J

vi. I = I-1

8. End Loop for I

9. Exit

3.4 Steganography Algorithm Steps:-

Steganography algorithm steps at sender end is in section 3.4.1 and steganography algorithm step at receiving end is in section 3.4.2.

3.4.1 Steganography Algorithm Steps at Sender Side:-

1. Input a Encrypted Information (EI) ie. Text/image and Cover Image (CI).
2. Read Binary of EI and CI.
3. Extract Least Significant Bit (LSB) from Cover (CI) by using Random Number Generation Technique
4. Swap LSB of CI with Binary Value of EI
5. Produced Stego-Image (SI)

3.4.2 Reverse Steganography Algorithm Steps at Sender Side:-

1. Select Stego Image (SI).
2. Read Least Significant Bit (LSB) from SI.
3. Collect all LSB value from SI by using Random Number Generation Technique.
4. Prepare Encrypted Image (EI) from LSB value.
5. Distinguish Cover Image (CI) and Encrypted Image (EI) from Stego Image (SI)

3.4.3 Strength of Proposed Approach:

Strengths of Proposed Approach is as follow:

1. Highly Efficient Encryption/ Decryption Algorithm Used.
2. 128 Key Value used.
3. Logical Operation uesd (XOR and Shift) to increage security.
4. Robustness
5. Reliable.
6. Consistency.

4. RESULTS ANALYSIS

4.1 Performance Analysis:

This section presents the Evaluated results through proposed conceptby using some selected performance parameters. Selected performance parameters are Peek Signal to Noise Ratio (PSNR), Entropy and Correlation to the stego image which is described below.

4.2 Peek Signal to Noise Ratio (PSNR):

PSNR is defined as assume that N is the total number of pixels in the input or output image, MSE (Mean Squared Error) is calculated as [13, 14] Where L is the number of discrete gray levels The value of PSNR should be greater for the better of the output image quality

***Entropy*:** For a given PDF *P*, Entropy Ent[P] is computed as [13, 14, 15]-

$$Ent[P] = -\sum_{k=0}^{L-1} P(k) log_2 P(k)$$

The Entropy is a used to measure the richness of the details in the output image.

***Correlation*:** The cross correlation coefficient r_{ij} is defined as [15]

$$r = \frac{n\sum(xy) - \sum x \sum y}{\sqrt{[n\sum(x^2) - (\sum x)^2][n\sum(y^2) - (\sum y)^2]}}$$

Where

r: correlation value

n: the number of pairs of data

$\sum xy$: sum of the products of paired data

$\sum x$: sum of *x* data

$\sum y$: sum of *y* data

$\sum x_2$: sum of squared *x* data

$\sum y_2$: sum of squared *y* data

The Calculated Results shows the batter performance of the proposed concept once. During Results Evaluation proposed system has used following configuration of hardware, platform and software.

***Hardware*:** Pentium Dual Core 3.67 GHz Processor, 2 GB of Ram as a Memory

***Platform*:** Window XP operating System

***Software*:** MAT LAB

Performance of the proposed system has measured on both (text & image) type of secrete information. During results evaluation proposed system has run on number of various size of text and image secrete information and captured overall performance on predefined parameters which is PSNR, Entropy, Correlation in numeric form and these values are shown in following table.

Table 1 is showing the PSNR performances through proposed concept over image and text of various sizes.

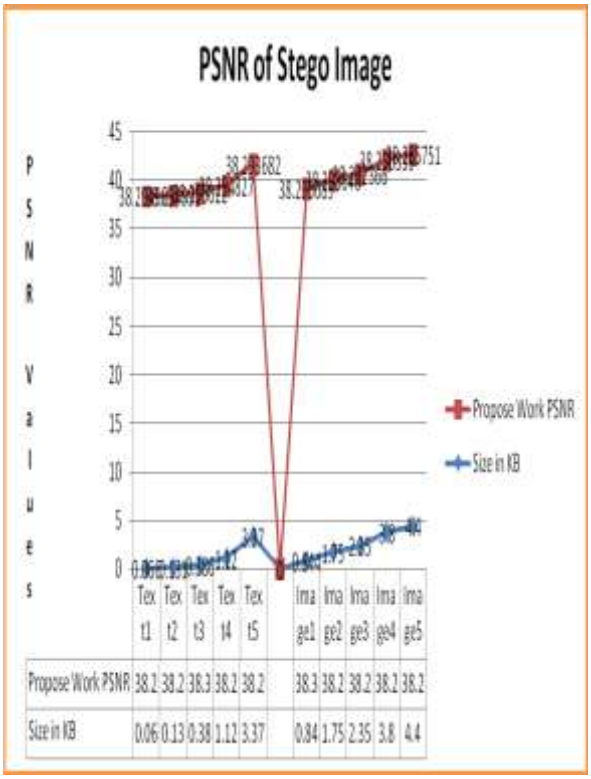
Table 1: PSNR performance through Proposed Concept over

Secrete Information	Size	Propose Con-cept
Text1	66 bytes	38.294965
Text2	130 Bytes	38.294991
Text3	386 Bytes KB	38.295022
Text4	1.12 KB	38.294827
Text5	3.37 KB	38.293682
Image1	844 Bytes	38.295089
Image2	1.75 KB	38.293646
Image3	2.35 KB	38.292366
Image4	3.8 KB	38.290339
Image5	4.4 KB	38.285751

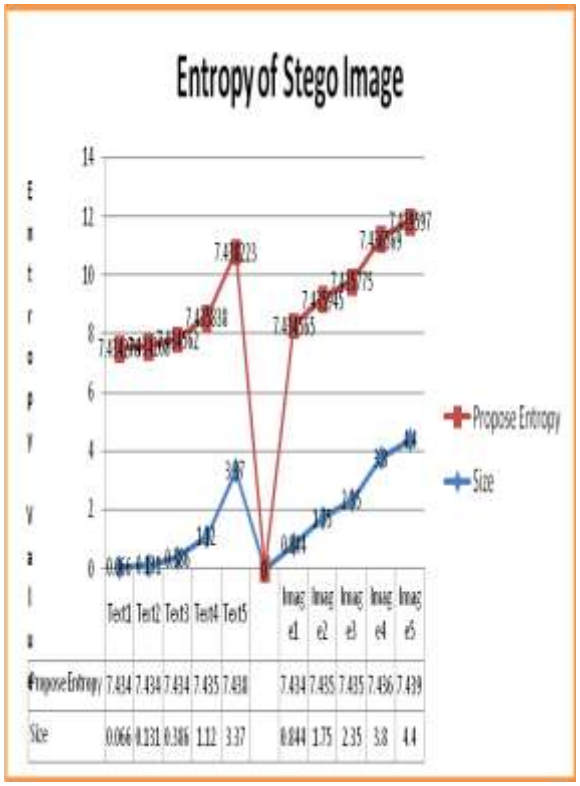
4.3 Text and Image Secret Information

$$PSNR = 10log_{10}\frac{(L-1)^2}{MSE}$$

$$MSE = \frac{\sum_i \sum_j |x(i,j) - y(i,j)|^2}{N}$$



Graph 1: Graphical Analysis of PSNR



Graph 2: Graphical Analysis of Entropy

Table 2 is showing the Entropy performances through proposed concept over text and image of various size.

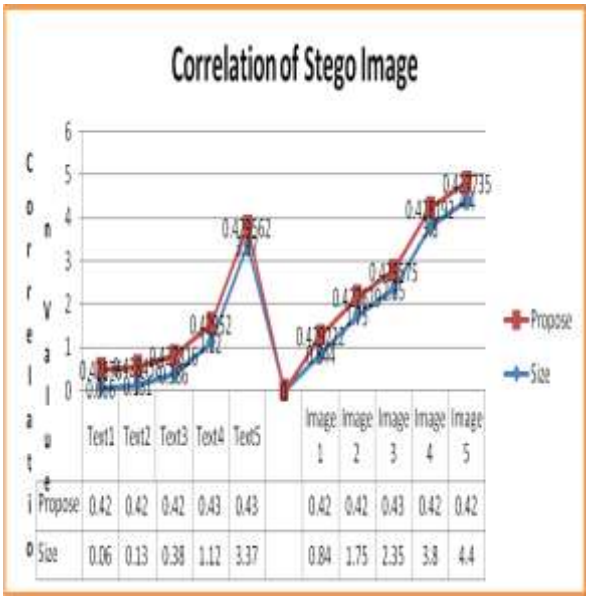
Secrete Information	Size	Propose Concept
Text1	66 bytes	7.434276
Text2	130 Bytes	7.434268
Text3	386 Bytes KB	7.434562
Text4	1.12 KB	7.435838
Text5	3.37 KB	7.438223
Image1	844 Bytes	7.434565
Image2	1.75 KB	7.435945
Image3	2.35 KB	7.435775
Image4	3.8 KB	7.436569
Image5	4.4 KB	7.439597

Table 2: Entropy Performance through Proposed Concept over text and Image Secret Information

Table 3 is showing the Correlation performances of proposed concept over text and image of various size.

Table 3: Correlation Performance through Proposed Concept over Text and Image Secret Information

Secrete Information	Size	Propose Concept
Text1	66 bytes	0.42876
Text2	130 Bytes	0.428458
Text3	386 Bytes KB	0.427816
Text4	1.12 KB	0.42952
Text5	3.37 KB	0.429562
Image1	844 Bytes	0.429222
Image2	1.75 KB	0.427629
Image3	2.35 KB	0.429575
Image4	3.8 KB	0.428192
Image5	4.4 KB	0.427735



Graph 3: Graphical Analysis of Correlation

5. RESULTS ANALYSIS

From the results analysis it has been observed the performance of proposed concept in all aspect has batter then traditional concept. Using LSB steganography technique, embedding large amount of secret information is not possible. Concept of the proposed work is to embed large amount of secret information ie image using LSB steganography technique by using compression through wavelet transforms technique and these compressed information bits are encoded using a proposed encoding technique. LSB Steganography technique is one of the best techniques when compared to transformation techniques, because it reduces lots of noise distortion. After LSB technique produced stego image quality shown in table 1 and graph 1 for text & image where five inputs (image/text) secrete information with one cover image is noted. In this for image of 844 Bytes is producing 38.295089 PSNR where text of 1.12 KB is producing 38.294827 PSNR of stego image. Entropy of stego image had shown in table 2 and graph 2 for text & image. In this for image of 844 Bytes producing 7.434565, where text of 1.12 KB is producing 7.435838 entropy of Stego Image. Similarly Correlation of stego image is shown in table 3 and graph 3 for text & image. In this for image of 844 Bytes producing 0.429222, where a text of 1.12 KB is producing 0.42952 correlation.

6. CONCLUSION

LSB technique of steganography technique is embedding large amount of confidential data in not possible generally. The general idea of this proposed concept is to embed large amount of confidential data using LSB technique by using compression of the data to reduce the original size with the help of wavelet transforms. After that the compressed bits are encoded using a proposed encoding/ decoding technique. Then these cipher bits are insertion in place of LSB in the cover image. It already known that LSB is the best/good techniques as compare transformation techniques, due to the reduction in noise distortion. With the help of proposed encoding/decoding technique, original confidential data is also encoded which is the second layer of the security where any attacker try to know the existence of the original data transferring. With the help of this process large amount of data can be transmitted in the covert channel and it's very hard to identify the existence of the original data. Proposed concept is providing ―text/ image‖ security which is one type of extension. But in digital world there are so many type of extension of the information which is travailing in the public network without any protection like audio, video etc.. So that in future proposed technique will include all other type of extension of the information and it will only for special type of extension and try to prove that proposed technique is batter among all other.

REFERENCES:

[1] G Prabakaran, R. Bhavani, P.S. Rajeswari, ―Multi secure and robustness for medical image based steganography scheme ‖ International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013, Page(s): 1188 –1193

[2] N. Akhtar, ; P. Johri, ; S Khan, –Enhancing the Security and Quality of LSB Based Image Steganography‖ 5th International Conference on Computational Intelligence and Communication Networks (CICN), Publication Year: 2013, Page(s): 385 – 390

[3] R.P Kumar, V. Hemanth, M –Securing Information Using Sterganoraphy ‖ International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013, Page(s): 1197 - 1200

[4] M.K Ramaiya. ; N.Hemrajani, A.K Saxena. ―Security improvisation in image steganography using DES‖ IEEE 3rd International on Advance Computing Conference (IACC), Publication Year: 2013, Page(s): 1094 - 1099

[5] Rengarajan Amirtharajan\ Anushiadevi .R2, Meena .y2, Kalpana. y2 and John Bosco Balaguru ―Seeable Visual But Not Sure of It ‖ IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[6] L.Jani Anbarasi and S.Kannan –Secured Secret Color Image Sharing With Steganography‖ IEEE 2012

[7] G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan –Steganography Using Edge Adaptive Image ‖ IEEE International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012

[8] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar ―An Image Steganography Technique using X-Box Mapping ‖ IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[9] RigDas and Themrichon Tuithung ‖ A Novel Steganography Method for Image Based on Huffman Encoding‖ IEEE 2012

[10] Abhishek Gupta, Sandeep Mahapatra and, Karanveer Singh –Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm‖ 2011 IEEE

[11] Thomas Leontin Philjon. and Venkateshvara Rao. –Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption ‖ IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011

[12] Ashwak M. AL-Abiachi, Faudziah Ahmad and Ku Ruhana –A Competitive Study of Cryptography Techniques over Block Cipher‖ UKSim 13th IEEE International Conference on Modelling and Simulation 2011

[13] Rosziati Ibrahim and Teoh Suk Kuan –Steganography Algorithm to Hide Secret Message inside an Image‖ Computer Technology and Application 2 (2011) 102-108

[14] Rosziati Ibrahim and Teoh Suk Kuan ―Steganography Algorithm to Hide Secret Message inside an Image‖ Computer Technology and Application 2 (2011) 102-108

[15] Danah Boyd and Alice Marwick –Social Steganography: Privacy in Networked Publics ‖ ICA 2011