Enhanced Steganography by using Symmetric Cryptography

Manoj Kumar Ramaiya [1], Nirupma Tiwari [2], Naveen Hemrajani[3], Pragya Sharma[4]
Suresh Gyanvihar University, Jaipur, India [12]
JECRC University ,Jaipur , India[3]
Shriram College of Engineering & Management, Gwalior, India[4]

Abstract: **In a digital world, Steganography and Cryptography are both projected to guard information from unnecessary parties. Both Cryptography and Steganography are superb means by which to achieve this but neither technique or technology alone is ideal and both can be out of order losing. It is for this cause that the majority professional would put forward using both to add several layers of security. Presented research work concentrated on the security of the information (image) by using a common technique steganography. To improve the level of security in steganography proposed work adds cryptography technique. So that overall proposed concept is enhancing the information (image) security. Initially cryptography work on confidential information and followed by steganography technique. Overall performance of the proposed technique is proving the effectiveness and security.**

Key Word: - Steganography, Security, Encryption, Decryption, Internet

I. INTRODUCTION

Steganography transmits secrets from end to end apparently harmless covers in an effort to cover the existence of a furtive. Digital image steganography and its derivatives are increasing in use and relevance. In areas where cryptography and strong encryption are being proscribed, people are looking at steganography to outwit such policies and go by communication secretly. Further huge innovations of the digital era: the battle between security experts and hackers, cryptographers and cryptanalysis, steganography and Steganalysis, record companies and pirates, will frequently build up new techniques or method to counter every other. In the coming future, the mainly significant use of steganography techniques will probably belie in the area of digital watermarking. Content providers are enthusiastic to defend their copyrighted mechanism against prohibited sharing and digital watermarks provide a way of tracking the uesr of these resources. Steganography may also turn into limited below laws. The possible use of steganography technique are

- defeat data on the network in case of a contravene
- Peer to Peer secretive communications.
- Posting top secret interactions on the Web to pass up communication.
- Embedding corrective audio or image information in case decay occurs from a poor link or communication

Those users who look for the definitive in personal communication can merge Cryptography and steganography. Encrypted data is more complicated to distinguish from obviously happening phenomena than plain text is in the carrier medium. There are various tools and technique by which they can encrypt data earlier than hiding it in the selected medium. In several situations, sending an encrypted significance will across distrust while an undetectable significance will not do so. Both techniques can be collective to generate better guard of the significance. The purpose of proposed technique provide perfect and risk free security technique.

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data [9].

In [1] the presents 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.

In [2] we have analyzed that a method for image steganography based on Huffman Encoding is presented. In which two 8 bit gray level image of size M X N and P X Q are using as a cover image and secret image respectively. Huffman Encoding is performing over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedding inside the cover image.
In [3] we have observed that authors propose an approach for Image steganography based on LSB using X-box mapping where they have used several Xboxes having unique data. The embedding component is completed by Steganography algorithm where they use four unique X-boxes with sixteen different values (represented by 4-bits) and every value is mapped to the four LSBs of the cover image.

In [4] a tutorial review of the steganography techniques appeared. Various image steganography techniques have been proposed. In this we investigate of founded steganography techniques and steganalysis techniques. we state a set of criteria to analyze and evaluate the strengths and weaknesses of the previous techniques. The least-significant bit (LSB) placing technique is the most frequent and easiest technique for embedding communication in an image with high ability, while it is quantifiable by statistical analysis for example RS and Chi-square analyses.

In [5] 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 [5].

In [6] we have analyzed that author proposes three indigenous methods as a variant of Cipher Block Chaining (CBC) mode for image encryption via considering three dissimilar traversing path (Horizontal, Vertical and Diagonal). In method one easy Raster Scan has been in use to scramble the secret Image called Horizontal Image Scrambling (HIS). technique two is a variation of technique one called Vertical Image Scrambling (VIS), here traversing trail would be peak to base and left to Right. Third technique employs diagonal traversing path called Diagonal Image Scrambling (DIS). Afterward Image Steganography has been personalized to send these Scrambled Images in an invisible manner.

In [7] focused on the combination of cryptography and steganography methods and a new technique – Metamorphic Cryptography has suggested. The message is changed into a cipher image through a key, covered into another image through steganography by converting it into an intermediate text and at last changed once again into an image. The difficulty of cryptography does not permit lots of users to really recognize the motivations and consequently available for enthusiastic safety cryptography. Cryptography procedure seeks to allocate an opinion of basic cryptographic primitives around a number of confluences in sequence to decrease safety assumptions on individual system, which set up a level of fault-tolerance conflicting to the system alteration. In a increasingly networked and scattered communications environment, there are other and more useful situations where the capability to share out a estimation between a number of unlike network intersections is needed. The cause back to the effectiveness, fault-tolerance and security that order in a different way.

Hence, in [8] described and reviewed the different research that has done toward text encryption and description in the block cipher. Moreover, in this suggests a cryptography model in the block cipher. There are many security issues in data communication. Cryptography is a substantially safe method to provide protection in data receiving and sending.

In [9] expressed a novel algorithm of data hiding using cryptography named as ASK algorithm. Sensitive data is hided in a color image using cryptography. This shows how data can be send using a color image without ignorance of third party. Algorithm described a method for vanishing data in a color image.

II. PROPOSED WORK

Reason behind choosing this model is the security and efficiency. Most interesting thing in this technique is the combination of two different techniques. Basically this technique is a method of encryption that combines two or more encryption technique and usually includes a combination of symmetric and steganography to take benefit of the strengths of each type of encryption. Symmetric encryption technique has the advantage of performance and therefore is the normal answer for encrypting/decrypting presentation-insightful data, for example an online information stream. On the other hand, steganography provides better security in that the cryptographic key required for decrypting data does not have to be shared with other parties. Figure 1 is showing the general architecture of proposed technique at sender end. This architecture start with "S" function, initially it take a secrete image "SI" which is passed to proposed encryption "PE" technique, this proposed encryption technique encrypt "SI" through a private key "K" value. After completing encryption process a new encrypted value produced and formed encrypted image "EI". This encrypted image which is secreting image hides within cover image "CI" through proposed steganography technique "PS". This proposed steganography technique use least significant bit "LSB" technique. In this technique encrypted image value "EI" replacing LSB value from cover image "CI" and formed stego image "SI" , at last whole technique ended with end "E" function. Similarly figure 2 is showing the general architecture at receiver end. These architecture starts with "S" function. Initially it takes stego image "ST" as an input; pass this image into steganography technique "PS". This technique read and excludes encrypted value "EI" and rest of the value is form cover image "CI". Select all "EI" value and pass to proposed decryption technique

"PD". Proposed decryption technique decrypted "EI" value through private key "K" value to produce secrete image "SI". At last whole technique ended with end "E" function.

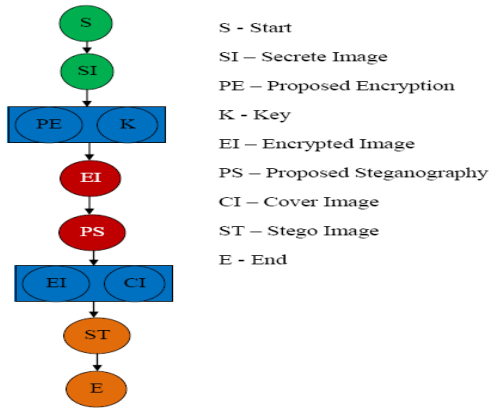


Figure 1: Architecture of Proposed Concept at First End

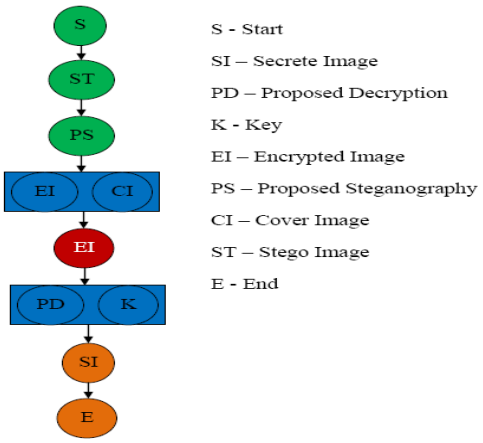


Figure 2 Architecture of Proposed Concept at Second End

Proposed Encryption Architecture: Figure 3 is showing the architecture of proposed encryption process. Initially this architecture read a block of 128 bits from number of bits value in secrete image "I", then these 128 bits block divided into four equals sub parts of 32 bits each (I_1, I_2, I_3, I_4). Similar this architecture used a special value know as key value "K" of same size 128 bits, which is also divided into four equal sub key (K_1, K_2, K_3, K_4), these sub key value are performing XOR operation with sub parts (I_1, I_2, I_3, I_4) of information respectively. During process thses sub parts of information one more operation is performed known as circular shift operation (Left, right) with number of bits (See figure 3). one whole process completed then 128 bits cipher value is produced, these cipher value pass an input to the next round. This process will continue up to eight rounds. After completing eight rounds final cipher value produced.

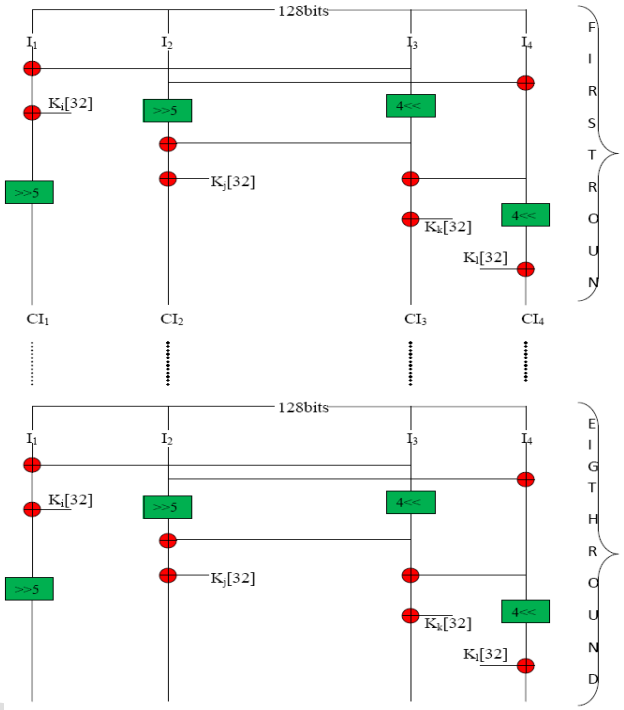


Figure 3: Architecture of Proposed Encryption

Proposed Encryption Algorithm

Input Secrete Image (SI)

Input Private Key (K) of 128 bits

Divide K For I = 1 to 4

K_1 [32]

K_2 [32]

K_3 [32]

K_4 [32]

End Loop

Select Secrete Image (SI)

Read Binary Value of SI

BV = Binary (SI)

Loop I = 1 to N

If (A [i] == 128 bits)

Then

Divide A[i] For j = 1 to 4

AI_1 [32]

AI_2 [32]

AI_3 [32]

AI_4 [32]

End Loop

End If

Loop K = 1 to 8

For first 4 Loop K will K_i K_j K_k K_l

For Last 4 Loop K will K_l K_k K_j K_i

$AI_1[32] = AI_1[32] \oplus AI_3[32]$

$AI_4[32] = AI_2[32] \oplus AI_4[32]$

$AI_2[32] = AI_2[32] >> 5$

$AI_3[32] = AI_3[32] << 4$

$AI_1[32] = AI_1[32] \oplus K_i[32]$

$AI_1[32] = AI_1[32] >> 5$

$CI_1 = AI_1[32]$

$AI_2[32] = AI_2[32] \oplus AI_3[32]$

$AI_2[32] = AI_2[32] \oplus K_j[32]$

$CI_2 = AI_2[32]$

$AI_3[32] = AI_3[32] \oplus AI_4[32]$

$AI_2[32] = AI_4[32] \oplus K_k[32]$

$CI_3 = AI_3[32]$

$AI_4[32] = AI_4[32] << 4$

$AI_4[32] = AI_4[32] \oplus K_l[32]$

$CI_4 = AI_4[32]$

K = K+1

End Loop

End Loop

Proposed Decryption Architecture: Figure 4 is showing the architecture of proposed decryption process. Initially this architecture read a block of 128 bits from number of bits value in cipher image "CI", then these 128 bits block divided into four equals sub parts of 32 bits each (CI_1, CI_2, CI_3, CI_4). Similar this architecture used a special value know as key value "K" of same size 128 bits, which is also divided into four equal sub key (K_1, K_2, K_3, K_4), these sub key value are performing XOR operation with sub parts (CI_1, CI_2, CI_3, CI_4) of information respectively. During process these sub parts of information one more operation is performed known as circular shift operation (Left, right) with number of bits (See figure 4). One whole process completed then 128 bits cipher value is produced, these cipher value pass an input to the next round. This process will continue up to eight rounds. After completing eight rounds final secrete value produced.

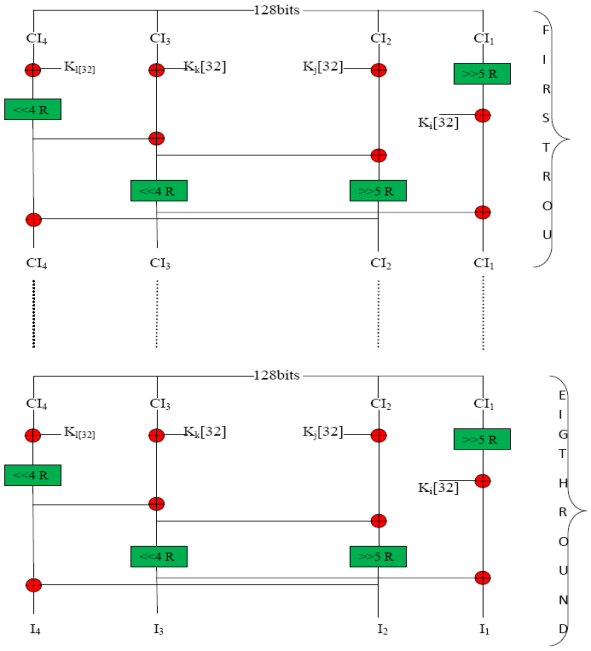


Figure 4: Architecture of Proposed Decryption

Proposed Decryption Algorithm

Input Encrypted Image (EI)

Input Private Key (K) of 128 bits

Divide K For I = 1 to 4

K_1 [32]

K_2 [32]

K_3 [32]

K_4 [32]

End Loop

Select Encrypted Image (EI)

Read Binary Value of EI

BV = Binary (EI)

Loop I = 1 to N

If (CAI [i] == 128 bits)

Then

Divide A[i] For j = 1 to 4

CAI_1 [32]

CAI_2 [32]

CAI_3 [32]

CAI_4 [32]

End Loop

End If

Loop K = 1 to 8

For first 4 Loop K will K_i K_j K_k K_l

For Last 4 Loop K will K_l K_k K_j K_i

$CAI_4[32] = CAI_4[32] \oplus K_l[32]$

$CAI_3[32] = CAI_4[32] \oplus K_k[32]$

$CAI_2[32] = CAI_2[32] \oplus K_j[32]$

$CAI_1[32] = CAI_1[32] >> 5\ R$

$CAI_4[32] = CAI_4[32] << 4\ R$

$CAI_3[32] = CAI_3[32] \oplus CAI_4[32]$

$CAI_2[32] = CAI_2[32] \oplus CAI_3[32]$

$CAI_3[32] = CAI_3[32] << 4\ R$

$CAI_2[32] = CAI_2[32] >> 5\ R$

$CAI_1[32] = CAI_1[32] \oplus K_i[32]$

$CAI_1[32] = CAI_1[32] \oplus CAI_3[32]$

$CAI_4[32] = CAI_4[32] \oplus CAI_2[32]$

K = K+1

End Loop

End Loop

$CAI_4[32] \rightarrow I_4$

$CAI_3[32] \rightarrow I_3$

$CAI_2[32] \rightarrow I_2$

$CAI_1[32] \rightarrow I_1$

Sub Key Selection Process: Figure 4.5 is showing the sub key selection during encryption and decryption. Basically encryption and decryption process having eight round and each round required a key value which is divide into group of four sub key like (K_1, K_2, K_3, K_4) and sequence of each sub key is differed in each round. So that selection of os sub key sequence is very important in encryption/decryption process. Initially total 8^{th} round is divide into two group of four-four sub key. In first group of round, sequence of sub key started with 1→2→3→4 and it will increase by one in circular manner like 2→3→4→1 for second round similarly for next two round see figure 5. After completing first group of round sequence of sub key started with 4→3→2→1 first round (actually 5^{th} round) and will decrease by one in circular manner like 3→2→1→4 for second round (actually 6^{th} round) similarly for next two rounds third (actually 7th round) and fourth (actually 8^{th} round) round see figure 4.5 second part.

Sequence of Sub Key for First Four Round Will Follows

K_1	K_2	K_3	K_4
K_2	K_3	K_4	K_1
K_3	K_4	K_1	K_2
K_4	K_1	K_2	K_3

Sequence of Sub Key for Next Four Round Will Follows

K_4	K_3	K_2	K_1
K_3	K_2	K_1	K_4
K_2	K_1	K_4	K_3
K_1	K_4	K_3	K_2

Figure 5: Figure Selection Sequence of Sub Key

Block Diagram of Proposed Steganography: Figure 6 is showing the general architecture of proposed steganography technique. Initially in this architecture two images pass as an input one for secrete image and another for cover image at sender side. Secrete image worked with encryption on process and produced cipher image after this proposed steganography technique worked with cover image and cipher image and produced stego image. Similarly at receiver end one image pass as an input called stego image, apply reverse steganography on stego image and produced cipher image and cover image. Now select cipher image and applied decryption process to produced original secrete image.

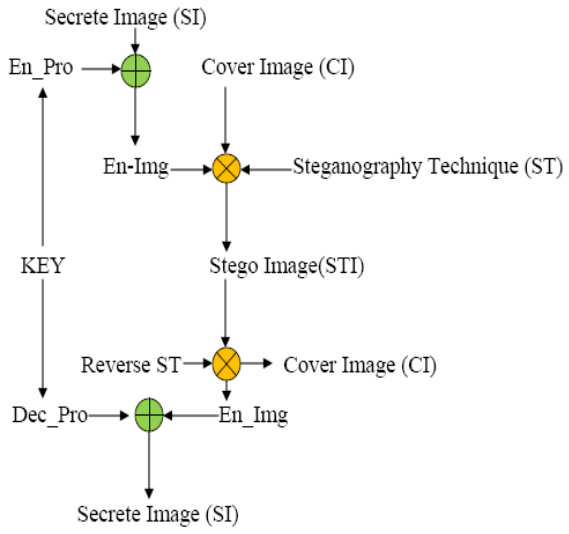


Figure 6: Architecture of Proposed Steganography

III. RESULTS

This Evaluated results through Existing as well as proposed technique by using some selected performance parameters. Selected performance parameters are Peek Signal to Noise Ratio (PSNR), Correlation and Entropy of the image which is described below.

- **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 [2,3 ,4]

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

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

Where L is the number of discrete gray levels
The value of PSNR should be greater for the better of the output image quality

- **Correlation:** Digital image correlation (DIC) techniques is predicated on the correlation coefficient maximization that is resolute by investigative pixel strength array subsets on two or additional consequent images and extracting the warp mapping function that relates the images. An iterative method which used to minimize the 2D correlation coefficient through nonlinear optimization techniques. The cross correlation coefficient r_{ij} is defined as [18, 17, 19]

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

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

- **Entropy:** For a given Entropy Ent[P] is computed as [3, 4,6,7]-

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

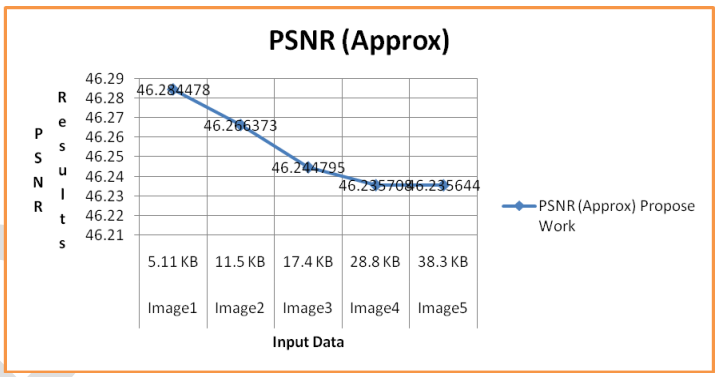
The Entropy is a used to measure the prosperity of the particulars in the output image.

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 proposed concept over various secrete image

Table 1: PSNR performance

Input		PSNR (Approx)
Input Data	**Size**	**Propose Work**
Image1	5.11 KB	46.284478
Image2	11.5 KB	46.266373
Image3	17.4 KB	46.244795
Image4	28.8 KB	46.235708
Image5	38.3 KB	46.235644

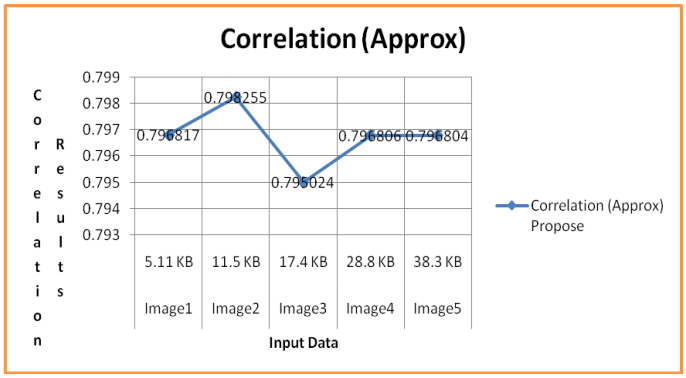


Graph 1: PSNR Graphical Analysis of Image Secrete

Table2 is showing the Correlation performances proposed concept over image of various size.

Table 2: Correlation Performance

Input		Correlation (Approx)
Input Data	**Size**	**Propose**
Image1	5.11 KB	0.796817
Image2	11.5 KB	0.798255
Image3	17.4 KB	0.795024
Image4	28.8 KB	0.796806
Image5	38.3 KB	0.796804

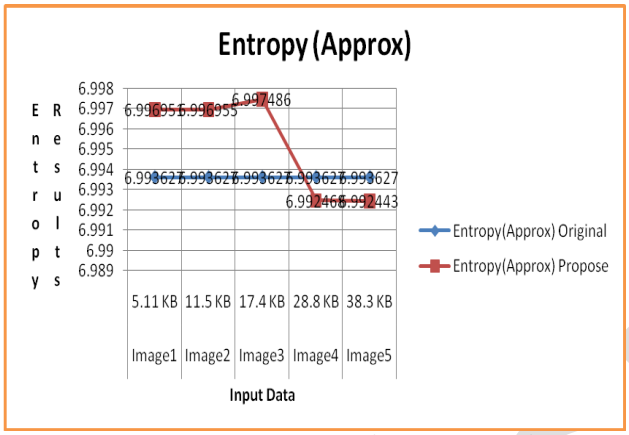


Graph 2: Correlation Graphical Analysis of Secrete Image

Table 3 showing the Entropy performances proposed concept over image of various size.

Table 3: Entropy Performance

Input		Entropy(Approx)	
Input Data	**Size**	**Original**	**Propose**
Image1	5.11 KB	6.993627	6.99695
Image2	11.5 KB	6.993627	6.99696
Image3	17.4 KB	6.993627	6.99749
Image4	28.8 KB	6.993627	6.99247
Image5	38.3 KB	6.993627	6.99244



Graph 3: Entropy Graphical Analysis of Image Secrete Information

Results Summary: From the outcome study it has been experiential the performance of proposed concept in all facets has batter then existing concept. By the LSB steganography, embedding hug amount of confidential information is not easy. Concept of the proposed work is to embed hug amount of confidential information ie image using LSB steganography. 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 for image where five inputs confidential images with one cover image is noted. In this for image of 5.11 KB is producing 46.284478 PSNR through proposed concept producing good results. Correlation of stego image had shown in table 2 for image. In this for image of 5.11 KB producing 0.796817, entropy through proposed concept respectively over image secrete information which proposed concept producing good results. Similarly Entropy of stego image had shown in table 3 for image. In this for image of 5.11KB producing 6.996951, entropy through proposed respectively over image secrete which proposed concept producing good results. Graph 1 ,2 ,3 is also showing the graphical analysis of proposed concept on selected parameters (PSNR, Correlation, Entropy) on various size of secrete Image.

CONCLUSION

Unlike the existing cryptographic systems, where only the cryptographic or steganography techniques are explored, the proposed concept approach explores the techniques in both cryptography and steganography. Any type of format is used to save the images. From the results comparison it is analyzed that efficiency of the proposed algorithm is very high as compare existing algorithm. It is already known that security of the algorithm is depended on the length of the key that mean longer key length will always support to good security feature and proposed hybrid crypto system have used 128 bits key length which is provided too much security for the proposed system. To access original key or crypto analysis of the proposed key is required 2^{128} time to break the key which is almost impossible for any hacker. There is no chance to generate floating point error because no such types of mathematical formula have applied on the proposed algorithm, this is also provided efficiency.

REFERENCES

[1] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena "Security Improvisation in Image Steganography using DES" IEEE 3rd International Advance Computing Conference (IACC), 22-23 Feb. 2013 PP 1094 - 1099

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

[3] Nirupma Tiwari ,Monika Sharma, Manoj Kumar Ramaiya, *"Digital Watermarking using DWT and DES "* ,3rd IEEE International Advance Computing Conference (IACC - 2013) ,Jan 2013, Gaziabad New Delhi , India ,pp1088 – 1091.

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

[5] L.Jani Anbarasi and S.Kannan "Secured Secret Color Image Sharing With Steganography" IEEE 2012

[6] 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

[7] 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

[8] 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

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

[10] Guy-Armand Yandji, Lui Lian Hao, Amir-Eddine Youssouf and Jules Ehoussou research on a normal file encryption and decryption" IEEE 2011

[11] Akhil Kaushik, AnantKumar and Manoj Bamela " Block Encryption Standard for Transfer of Data " IEEE International Conference on Networking and Information Technology 2010

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

[13] danah boyd and Alice Marwick "Social Steganography: Privacy in Networked Publics" ICA 2011