Volume 1, Issue 3, July 2014 ISSN: 2348-8565 (Online)

International Journal of Modern Engineering and Research Technology

Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

A Novel Steganography Approach using Cryptography

Megha Tiwari
M-Tech Scholar
CSE Department
Jai Narain College of Technology,
Bhopal (M.P.) [INDIA]
Email: er.meghatiwari@gmail.com

Dr. Mukta Bhatele
Prof. & Head
CSE Department
Jai Narain College of Technology,
Bhopal (M.P.) [INDIA]
Email:mukta_bhatele@rediffmail.com

Prof. Vigyan Sharma
Assistant Professor
CSE Department
Jai Narain College of Technology,
Bhopal (M.P.) [INDIA]
Email: vigyan.sharma@yahoo.co.in

ABSTRACT:

*Multimedia Information provides a robust and easy modification/editing in information. The Information can be transmitted over public networks without any error and often without interference. But unfortunately, digital media distribution raises a concern for digital content owners. Digital information could be copied without any loss in quality and content. This poses a big problem for the protection of intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data. Proposed work entitled "**Novel Steganography Approach using Cryptography**" is proposed by analyzing the principle of the image steganography technique with cryptography (Symmetric). Proposed approach support to basic security principal like integrity, authorization, and accuracy of confidential images in the network. It"s known that, lots of effort is required during steganography with image encryption/decryption. Overall performance of the proposed technique is proving the effectiveness and security.*

Keywords:—*Steganography, Security, Encryption, Decryption, Internet*

I. PROPOSED WORK

This proposed concept having three parts which is following.

1. Proposed Encryption and Decryption

2. Proposed Steganography

3. Randomization

Figure 1 showing the block diagram of the proposed technique at sender end. Basically this block diagram is divided into three parts. First part is encryption of secret image, second part is steganography of cipher image and third part is detailed description of encryption process. In the first part secret imag SI is passing to propose encryption PE then it will executed to produce cipher image CI. The detailed execution E processes are defined in third parts. In second part a steganography technique are executing. In this a cover image CovI passing to proposed steganography where

it is calling to least significant bits LSB technique, this LSB technique are calling to randomization function to select a LSB pixel value form cover image CovI and embedding cipher image CI to produced Stego Image STI. Now in third parts which is the execution part of encryption, here read the pixel value of secret image SI and again read the binary value of these pixels. After that arranging all these binary value in the form of matrix of M X M, then performing displacement process on the arranged matrix value, here two displacement process are adopted one is right displacement and second is up ward displacement where each displacement applying sequentially. Here randomization are also using during selection of pixel position. After completing this process perform XOR operation between displaced binary values and key value to produced encrypted image.

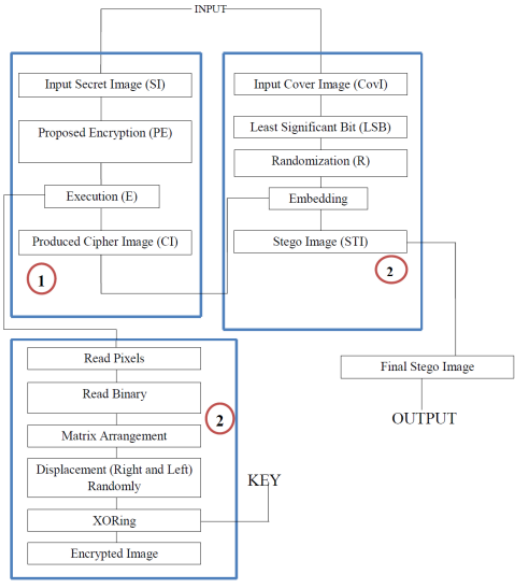


Figure 1: Block Diagram of Proposed Concept at Sender Side

Similar figure 2 is showing the block diagram of proposed concept at receiver end. This block diagram is also divided into three parts. First part is the steganography technique, second parts are proposed decryption technique and third parts are detailed description of decryption process during execution. Now in first part stego image STI" passing to proposed steganography PS where it is calling to LSB technique and this LSB technique are calling randomization R function to extract the cipher image CI and cover image CovI from stego image STI. Randomization function is just for the selection of pixel in sequentially where it will start to extract cipher image CI.

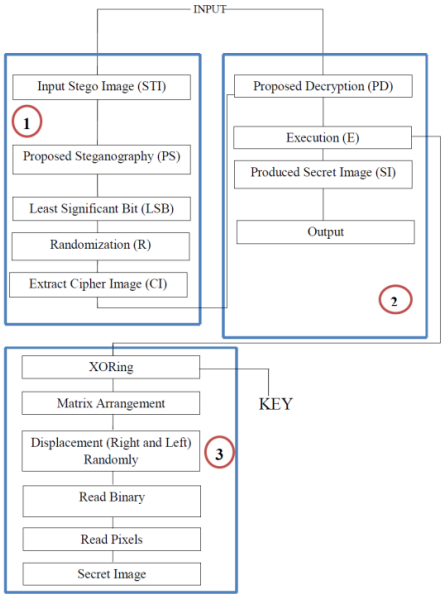


Figure 2: Block Diagram of Proposed Concept at Receiver Side

Once extraction is over and gets the cipher image proposed concept goes in second part of block diagram. In this proposed decryption PD algorithm, here cipher image are executed to gets original secret image SI. In third part which is providing the details description of proposed decryption process during execution. In this read pixel value then read binary value of these pixels and perform the XOR operation with key values. After that arrange these binary value in matrix form and apply displacement process in reverse direction as compare encryption process to produced original secret image SI.

First Part Proposed Encryption and Decryption: In this part architecture of proposed encryption and decryption are

defined with algorithm steps of encryption and decryption.

Architecture of Proposed Encryption Technique: Figure 3 is showing the architecture of proposed encryption process. In this architecture secret image "SI" of M X N pixels are converting in P X P pixels and dividing into four sub image like SI_1, SI_2, SI_3, and SI_4. After that

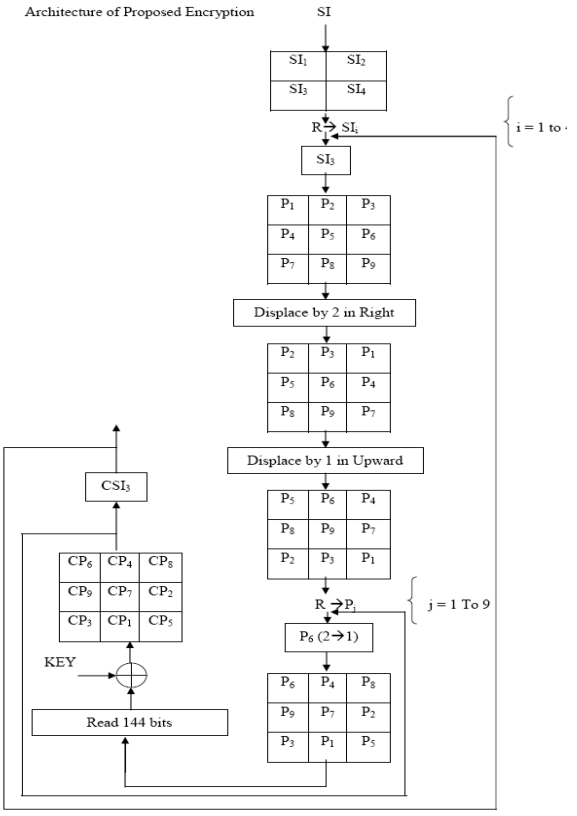


Figure 3: Architecture of Proposed Encryption

Select one block randomly (see randomization algorithm) and arrange pixels of this block in matrix of P X P. Than perform displacement process, that mean displace pixels in right direction by 2 and then perform displacement process in upward direction by 1 (see figure 4). once again call randomization function to select a pixel randomly and say it is the first pixel of matrix and arrange all the pixel according that selected pixel (see figure 4). And at last read binary value of the pixel and perform XOR operation with key value. In this concept the size of the key are

144 bits so the 144 binary values from secret image will read at a time. These process will continue till all the binary values of the selected block will not equals to null and all sub image block will not equals to null.

Algorithm Step of Proposed Encryption Algorithm:

1. Input Key K of 144 bits Size

2. Input Secret Image (SI) of P X Q Size

3. Reset SI of P X P Size

SI_1	SI_2
SI_3	SI_4

4. Divide SI in Four Block ie.

5. Select One Block Randomly

6. Arrange Pixels of Selected Block in Matrix Form

P_1	P_2	P_3	P_4
P_5	P_6	P_7	P_8
P_9	P_{10}	P_{11}	P_{12}
P_{13}	P_{14}	P_{15}	P_{16}

7. Apply Displacement in Right by 2

P_3	P_4	P_1	P_2
P_7	P_8	P_5	P_6
P_{11}	P_{12}	P_9	P_{10}
P_{15}	P_{16}	P_{13}	P_{14}

8. Apply Displacement in Upward by 1

P_7	P_8	P_5	P_6
P_{11}	P_{12}	P_9	P_{10}
P_{15}	P_{16}	P_{13}	P_{14}
P_3	P_4	P_1	P_2

ie.

9. Select one Pixel Randomly say X
10. Set as a Starting Pixel X = Starting Pixel
11. Read 144 bits Sequentially from First Pixel X
12. Perform XOR between K and Selected First 144 bits
13. Repeat Step 11 and 12 till all bits is not Equals NULL
14. Repeat Steps 5 till all Block is Not Equal NULL.
15. Produced Cipher Image (CI)
16. Exit

Architecture of Proposed Decryption Technique: Figure 4 is showing the architecture of proposed decryption process in this cipher image CI is dividing into four sub image block and then randomly selects one block. Arrange pixels of selected block in matrix form and read binary value to perform XOR operation with key value. It is already known that this decryption key are same as encryption key because symmetric in nature. Once again perform randomization for selection of a pixel randomly and arrange all the remaining pixels according to selected pixel in the form of matrix (See figure 4).

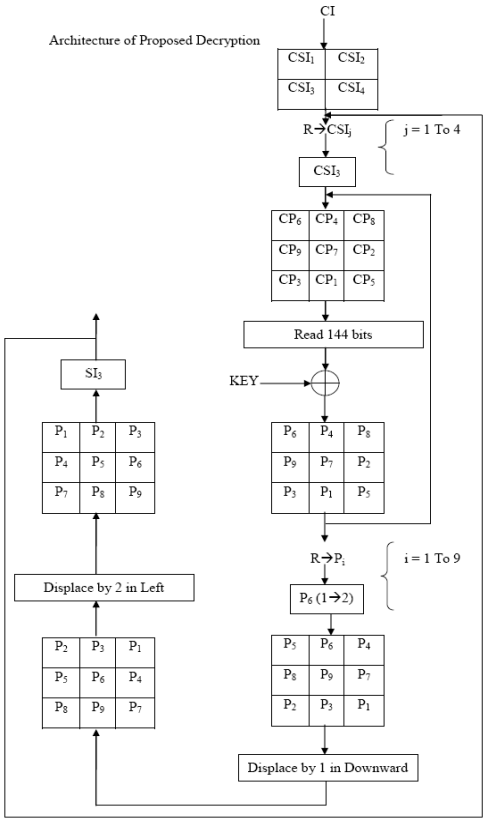


Figure 4: Architecture of Proposed Decryption

Now apply displacement process in reverse direction, first apply displacement in down ward direction by 1 and then apply displacement in left direction by 2. These processes will continue till original secret image are not produced.

Algorithm Step of Proposed Decryption Algorithm:

Steps of Proposed Decryption Algorithm

1. Input Key K of 144 bits in Size
2. Input Cipher Image CI
3. Divide CI into Four Block

CI_1	CI_2
CI_3	CI_4

4. Select on Block Randomly

5. Arrange Pixels of Selected Block in Matrix Form

CP_1	CP_2	CP_3	CP_4
CP_5	CP_6	CP_7	CP_8
CP_9	CP_{10}	CP_{11}	CP_{12}
CP_{13}	CP_{14}	CP_{15}	CP_{16}

6. Read 144 bits sequentially from first pixel
7. Perform XOR Between K and selected 144 bits
8. Repeat Step 6 and 7 till all bits is Not Equal NULL of Selected Block
9. Select One Pixel Randomly and its Position in matrix
10. Rearrange Matrix of pixels according the position of selected pixel
11. Apply Displacement by 2 in downward on pixels of Matrix
12. Apply Displacement by 2 in Left on Pixels of Matrix
13. Repeat Step 4 to 12 till all Block is not equal NULL.
14. Exit

Second Part is Proposed Steganography: In this part steps of proposed steganography for hiding the secret image behind the cover image and extracting secret image from the stego image are defined.

Steps of Hiding Algorithm (Proposed Steganography)

1. Input Cover Image (CovI)
2. Input Cipher Image (CI)
3. Apply Least Significant Bits (LSB)
4. Call Randomization for LSB Selection
5. Embedded CI in CovI
6. Produced Stego Image (SI)
7. Exit

Steps of Extraction Hidden Image (Proposed Steganography)

1. Inputs Stego Image (SI)
2. Apply Least Significant Bits (LSB)
3. Call Randomization for LSB Selection
4. Extract Cover Image (CovI) and Cipher Image (CI)
5. Exit

Third Part is Randomization: In this there are three randomization processes are defined for sub image block selection, pixel position selection and least significant bits selection.

Randomization for Encryption/Decryption of Secret Image during Block Selection

1. Enter a Random Key RK Value of Arbitrary Length
2. Read the ASCII value of RK and Summation of all ASCII value of RK say ARK
3. Perform Mode Operation (ARK, (Length P of Secrete Image) Mod 4 Say N
4. N is the Random Number

Randomization for Encryption/Decryption of Secret Image during Pixel Position Selection

1. Enter a Random Key RK Value of Arbitrary Length

2. Read the ASCII value of RK and Summation of all ASCII value of RK say ARK

3. Perform Mode Operation (ARK, (Length P of Secrete Image) Mod 2 Say N

4. N is the Random Number

Randomization for Steganography during Selection of Pixel Position in Cover Image

1. Enter a Random Key RK Value of Arbitrary Length

2. Read the ASCII value of RK and Summation of all ASCII value of RK say ARK

3. Perform Mode Operation (ARK, Min (Length/Width „P"of Cover Image)) Mod 2 Say N

4. N is the Random Number Characteristics **of the Proposed System:**

Strength: The strength of the proposed concept resides in the new concept of higher key value with removing some flaw. Involving 128 bit key value (the probably it will be able to change the whole text value randomly at the time of implementation of the proposed model. This opportunity does not give a Steganalysis tool the chance of searching for a predictable set of modifications. The proposed approach has many applications in hiding and coding messages within standard Medias, such as images or videos.

- ***Usability***: The Proposed concept is suitable for many different applications:
- ***Bulk encryption***. The proposed concept is efficient in encrypting image files or a continuous data stream.
- ***Random bit generation***. The proposed concept efficient in producing random number.

Packet encryption. The proposed concept is efficient in encrypting packet-sized data. It should implementable in an application where successive packets may be encrypted or decrypted with different keys.

II. RESULTS

Performance Analysis: This section presents the results of evaluating the efficiency of the proposed technique that is based on selected parameters. Selected parameter is entropy, histogram and Peek Signal to Noise Ration (PSNR) of the image which is describe below.

Entropy: Image entropy is a quantity which is used to describe the `business' of an image, i.e. the amount of information which must be coded for by a compression algorithm. Low entropy images, such as those containing a lot of black sky, have very little contrast and large runs of pixels with the same or similar DN values. An image that is perfectly flat will have entropy of zero. Consequently, they can be compressed to a relatively small size. On the other hand, high entropy images such as an image of heavily cratered areas on the moon have a great deal of contrast from one pixel to the next and consequently cannot be compressed as much as low entropy images [1].

$$H_e = -\sum_{k=0}^{G-1} P(k) \log_2 (P(k))$$

Where:

He: entropy.

G: gray value of input image (0... 255).

P(k): is the probability of the occurrence of symbol *k*.

Histogram: The Histogram shows the total tonal distribution in the image. It's a bar chart of the **count** of pixels of every tone of gray that occurs in the image. It helps us analyze, and more importantly, correct the contrast of

the image. Technically, the histogram maps Luminance, which is defined from the way the human eye, perceives the brightness of different colors. For example, our eyes are most sensitive to green; we see green as being brighter than we see blue. Luminance weighs the effect of this to indicate the actual perceived brightness of the image pixels due to the color components. The world won't end if you simply think of luminance as brightness, that's actually quite fine for our purpose (and it's really fun to watch the purists have a fit anyway <grin>). But luminance is weighted by color, and there is more detail and explanation about luminance in histograms if you're still curious. For now, luminance can be the "apparent brightness" of the RGB pixel tones in the image [38].

Peek Signal to Noise Ration: Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an *approximation* to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content.

PSNR is most easily defined via the mean squared error (MSE). Given a noise-free $m \times n$ monochrome image I and its noisy approximation K, MSE is defined as:

$$MSE = \frac{1}{m\,n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\ &= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \\ &= 20 \cdot \log_{10} (MAX_I) - 10 \cdot \log_{10} (MSE) \end{aligned}$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using linear PCM with B bits per sample, MAX_I is $2^B - 1$. For color images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. Alternately, for color images the image is converted to a different color space and PSNR is reported against each channel of that color space, e.g., YCbCr or HSL [32].

Execution Time: Execution Time is the time taken to complete an algorithm for encryption or decryption. It is possible that encryption time and decryption time can be differing for same algorithm on same data. So here proposed algorithm is consider only encryption time as an execution time.

Key Analysis: Key length of the proposed concept is also considered to evaluate the security and performance of the proposed algorithm. Security of the image is the prime concern of the proposed research. To achieved this by combining the slicing, displacement and encryption technique to increase security and performance of the proposed system.

The experiment show the superiority of the proposed concept as compare existing

concept in terms of entropy, correlation and histogram. Desktop machine has been used to calculate experimental results which has following configuration (See Table 1)

Table 1: Configuration

S. No.	Processor	Memory(Primary)	Platform	Software Application
1	Intel Pentium Dual Core E6700 3.20 GHz	2 GB of RAM	Window-XP SP2	Dot Net 2010

In the experiments, the system encrypts/ decrypt images. There are four parameters are calculating by the proposed system one is entropy, second is histogram, third is and important parameter is peek signal to noise ratio (PSNR), fourth is execution time in terms of encryption time and fifth is key size analysis. All the parameters are shown in table 4, 5,6, 7 and table 8. The proposed system has run hundred times approximately. In each time, same images are respectively encrypted by existing algorithm and ***"Proposed algorithm"***. Size of the selected key was same in each time. Finally, the outputs of the comparison system are entropy, histogram PSNR, execution time and length of Key value which is noted in numeric form. During experiment proposed system has four secret images of various sizes (see table 3) which is hiding behind four different cover images (see table 2).

Table 2: Cover Images

Cover Image -1  Animal.jpg	Cover Image -2  Lena.jpg
Cover Image - 3  Monaleesa.jpg	Cover Image -4  Vegitable.jpg

Table 3: Secret Image Images

Secret Image -1  50 X 50.jpg	Secret Image -2  90 X 90.jpg
Secret Image - 3  80 X 80.jpg	Secret Image -4  70 X 70.jpg

Tabular Analysis: **-** In this compared results present in the form of tables.

Encrypted Image Entropy: *"The Proposed Algorithm"* have been implemented on a number of images varying types of content and sizes of a wide range. Encrypted image entropy of various images comparisons shown in table 4.

Table 4: Entropy Analysis of Stego Images through Proposed Algorithm on Animal.jpg as a Cover Image

S.NO	Input Images	Pixel Size	Cover Image	Pixel Size	Proposed Algorithm
Stego Image Entropy (Approx)					
					Max
1	Se-Img-1	20 X 20	Animal.jpg	300 X 300	8.8795
2	Se-Img-2	25 X 25	Animal.jpg	300 X 300	9.1233
3	Se-Img-3	30 X 30	Animal.jpg	300 X 300	9.1233
4	Se-Img-4	35 X 35	Animal.jpg	300 X 300	9.1241

Histogram: - "The Proposed Algorithm" have been implemented on a number of image varying types of content and sizes of a wide range. Histogram of Various images comparisons shown in table 5.

Table 5: Histogram Analysis of Stego Images through Proposed Algorithm on Animal.jpg as a Cover Image

S.NO	Input Images	Pixel Size	Cover Image	Pixel Size	Proposed Algorithm	
Stego Image Histogram (Approx)						
					Mean	Sigma
1	Se-Img-1	20 X 20	Animal.jpg	300 X 300	136	40
2	Se-Img-2	25 X 25	Animal.jpg	300 X 300	150	42
3	Se-Img-3	30 X 30	Animal.jpg	300 X 300	150	42
4	Se-Img-4	35 X 35	Animal.jpg	300 X 300	150	42

Peek Signal to Noise Ration (PSNR): - "The Proposed Algorithm**"** have been implemented on a number of image varying types of content and sizes of a wide range. PSNR of Various images comparisons shown in table 6.

Table 6: PSNR Analysis of Stego Images through Proposed Algorithm on Animal.jpg as a Cover Image

S.NO	Input Images	Pixel Size	Cover Image	Pixel Size	Proposed Algorithm
Stego Image PSNR					
1	Se-Img-1	20 X 20	Animal.jpg	300 X 300	63.024
2	Se-Img-2	25 X 25	Animal.jpg	300 X 300	10.3544
3	Se-Img-3	30 X 30	Animal.jpg	300 X 300	10.3544
4	Se-Img-4	35 X 35	Animal.jpg	300 X 300	10.3544

Encrypted Image Execution Time: **"The** Proposed **Algorithm"** have been implemented on a number of images varying types of content and sizes of a wide range. Encrypted image execution time of various images comparisons shown in table 7.

Table7: Execution Time Analysis of Stego Images through Proposed Algorithm Algorithm on Animal.jpg as a Cover Image

S.NO	Input Images	Pixel Size	Cover Image	Pixel Size	Proposed Algorithm
Stego Image Execution Time (Approx in Milisecond)					
					Max
1	Se-Img-1	20 X 20	Animal.jpg	300 X 300	93
2	Se-Img-2	25 X 25	Animal.jpg	300 X 300	140
3	Se-Img-3	30 X 30	Animal.jpg	300 X 300	171

Key Analysis: **"The Proposed Algorithm"** have been implemented on a number of images varying types of content and sizes of a wide range. Key comparisons shown in table 8.

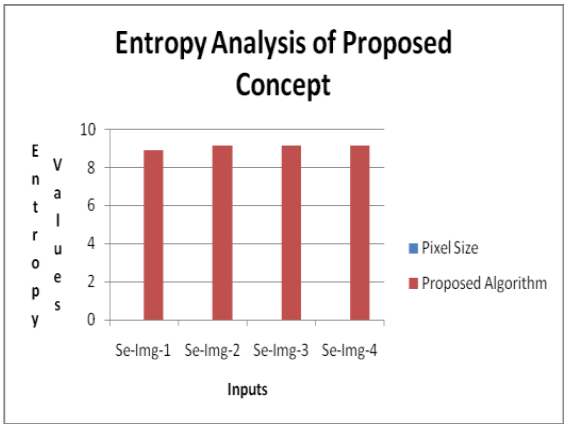
Table 8: Key Size Analysis of Stego Images through Proposed Algorithm

Parameters	Proposed Concept
Key Size	144 bits
Private Key	01
Random Key	01

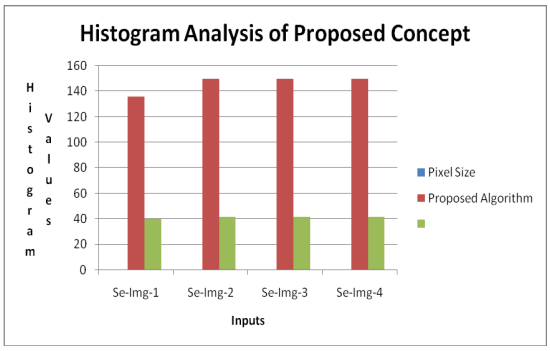
Graphical Analysis: In this compared results showing in the form of graphs.

Stego Image Entropy: A graphical representation for the table 4 is shown in graph 1 for entropy, similarly table 5 shown in

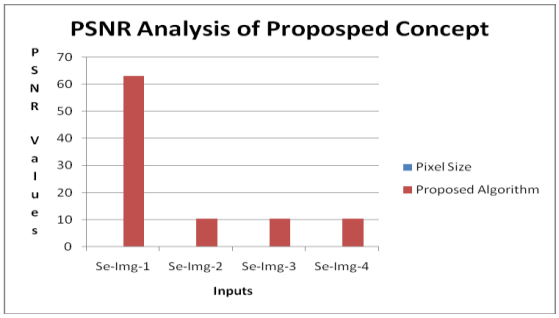
graph 2 for histogram, similarly table 6 shown in graph 3 for PSNR, similarly table 7 shown in graph 4 for execution time and similarly table 8 shown in graph 5 for Key Analysis, According to the graph, produced entropy, histogram, PSNR, Execution time and Key size all are producing good results.



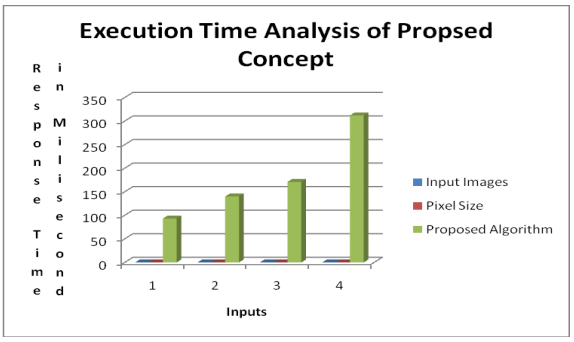
Graph 1: Graphical Representation of Entropy Analysis of Stego Images through Proposed Algorithm on Animal.jpg as a Cover Image



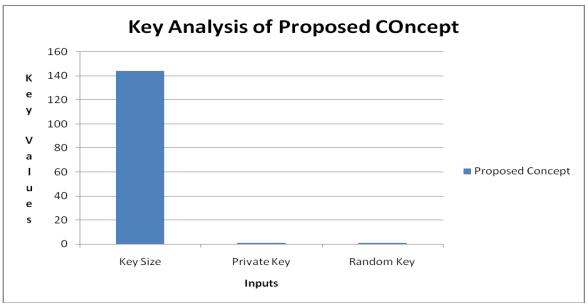
Graph 2: Graphical Representation of Histogram Analysis of Stego Images through Proposed Algorithm on Animal.jpg as a Cover Image-



Graph 3: Graphical Representation of PSNR Analysis of Stego Images through Proposed Algorithm on Animal.jpg as a Cover Image



Graph 4: Graphical Representation of Execution Time Analysis of Stego Images through Proposed Algorithm on Animal.jpg as a Cover Image



Graph 5: Graphical Representation of Key Analysis of

III PROPOSED ALGORITHM

Results Analysis: From table 4 its observed that entropy of stego image are evaluating through maximum entropy value of encrypted pixel, in all four secrete images of various size proposed algorithm producing higher value in terms of entropy. For example secret image-4 producing 9.1241 entropy value through proposed algorithm and For example secrete image-3 producing 9.123 entropy value through proposed algorithm For example input image-2 producing 9.123 entropy value through proposed algorithm on every secrete image our proposed algorithm will produce better results animal.jpg as a cover image.

From table 5 observed that histogram of stego image are evaluating through two parameters one is mean value (mean) of encrypted pixel and another is sigma value of encrypted pixel, in all four case proposed algorithm are producing higher histogram value in terms of

sigma parameters which is denoted the equal distribution of pixel. For example secret image -4 producing 150 histogram value through proposed algorithm and For example secrete image-3 producing 150 histogram value through proposed algorithm For example input image-2 producing 150 histogram value through proposed algorithm on every secrete image our proposed algorithm will produce better results when animal.jpg as a cover image.

The most important parameter of the proposed research is peek signal to noise ratio (PSNR) which is show in table 5.6 for various images. Through numeric value of table 6 it‟s easy analyzed that stego image of picture quality of proposed algorithm is batter then existing algorithm. For example secret image-4 producing 10.354 PSNR value through proposed algorithm and For example secrete image-3 producing 10.354 PSNR value through proposed algorithm For example input image-2 producing 0.354 PSNR value through proposed algorithm on every secrete image our proposed algorithm will produce better results when animal.jpg as a cover image.

Another most important parameter of the proposed research is execution time which is show in table 7 for various images. Through numeric value of table 7 it‟s easy analyzed that execution time in terms of encryption time of proposed algorithm is batter then existing algorithm. For example secret image-4 producing 312 ms execution time value through proposed algorithm and For example secrete image-3 producing 171 ms execution time value through proposed algorithm For example input image-2 producing 140 ms execution time value through proposed algorithm on every secrete image our proposed algorithm will produce better results when animal.jpg as a cover image.

And at last but not least important parameter of the proposed research is key analysis which is show in table 8. from the study of existing algorithm and proposed algorithm it is clearly seen that proposed algorithm having one private key for encryption and decryption of 144 bits which is far batter then existing algorithm and it is having another key known as random key of arbitrary length for steganography technique. So on the basis of these parameters comparison proposed concept has batter then existing in terms of security in terms of stego image quality and many more.

IV. CONCLUSION

For purposes of secret transmission and communication which is prim concern of the proposed concept proposes a concept which has combined effort of two different techniques like cryptography and steganography. Proposed Steganography process is improving image quality and security as compare to the earlier presented technique. Proposed cryptography is also increasing security in efficient manner. Our presented approach is better because there are separate key are using for separate process like displacement process are using randomization key similarly proposed encryption/decryption process are using 128 bits key and at last steganography is also using randomization key to hide secrete image. It is already known that without stego key and encryption/decryption key, no one can extract the original secrete information from the stego-image as e as cipher image, The results analysis have also confirmed our conclusions.

REFERENCES:

[1] 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

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

[3] 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

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

[6] 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

[7] 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

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

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

[10] AmrM. Riad, Amr H. Hussein and AtefAbou EI-Azm "A New Selective Image Encryption Approach using Hybrid Chaos and Block Cipher" The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May Computational Intelligence and Multimedia Computing Track

[11] Arun Raj R, Sudhish N George and Deepthi P. P. "An Expeditious Chaos Based Digital Image Encryption Algorithm" 1st Int"l Conf. on Recent Advances in Information Technology |RAIT-2012|

[12] Rithmi Mitter and M. Sridevi Sathya Priya "a highly secure cryptosystem for image encryption" IEEE Conferences 2012

[13] Somdip Dey, Kalyan Mondal, Joyshree Nath, Asoke Nath "Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm" I.J.Modern Education and Computer Science, 2012, 6, 59-67 Published Online June 2012 in MECS (http://www.mecs- press.org/) DOI:

10.5815/ijmecs.2012.06.08

[14] S.Premkumar, A.E.Narayanan "Steganography Scheme Using More Surrounding Pixels combined with Visual Cryptography for Secure Application" International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012

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

[16] 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

* * * * *