Dynamic Key Based S-Box Expansion Method for Steganography

Ajay Kumar Raghuwanshi , Arun Jhapate

Dept. of Computer Science and Engineering SIRT Bhopal, INDIA

Abstract* - As with the merging trends of methodologies and the internet, the security of information considers as the most challenges in communication to protect information. A large variety of stenographic techniques are available for hiding the information within a proper carrier like image, text, audio, and protocol, which may be sent to a receiver secretly. The process of Steganography is an art of keeping a message within the cover media as secret like text, image, audio or signals in the form such that it is not accessed by anyone, only the required recipient may knows about the presence of data. Therefore the latest approach which is dependent over the combo of the cryptography approach and the Steganography approach both is described in this paper also represents how they overcome weaknesses of each other and build the system as complicated for the attackers in order to attack the personal information. In this paper discuss the fundamental features of the Steganography approach along with its comparison with the cryptography approach based on the existing analysis. This paper is all about this kind of new approach of Steganography which covers cryptography. This is implemented in MATALB.

Keywords—Steganography, Cryptography, Key Generation, LSB, PSNR, Correlation, Entropy.

I. INTRODUCTION

According to the current requirement of the security for the data over the network have been increasing so this may generate the requirement for an approach which may provide the way for providing the security to the data through applying some concept of hiding the message or sensitive information. So the major objective of concept of Steganography technique is for covering the details in order to prevent them from recognizing their presence. Hence this concept is implies the idea of covered-writing. Steganography may involve the transforming the communication in between the two different persons and the presence of those persons are not known to the attacker also their proper implementation is based on recognition of the presence of information [1].

In this concept the information, such as photos are decreases in size till it reach the size of the given period. This concept is also complicated in order to find out the hidden information, and the cover message have been transmit on the channel which is not secured along with any one periods embedded over the paper which is having the hidden information[3]. Recently the Steganography approach is extremely applied on the computers along with the digital data which is having the information along with the networks that are have the ability to providing channels a high speed for communication. Since it is associated with the cryptography approach, but both of these are not same. And Steganography process is used to wrap out the details or data, while in the process of cryptography the data or details may get coded to be not get understood [2]. Therefore these both approaches are used to secure the information from the unwanted parties where the technology only is efficient.

Since the digital information or data have got send over the network or the internet and this is securing the personal messages which are required to be find out and established frequently as done before, with the latest approaches for protecting and also securing the personal messages are required to understandand implemented.As the cryptography and the Steganography both the approaches have been presented towards the attacks through the Steganalysis, therefore in this constantly need to develop and look for new modes.Cryptography and Steganography are well-known and widely used techniques that handle information in order to cipher or hide their existence respectively [3].

Steganography techniques are used to secure the secret message transmitted over an open communication channel such as the internet. But message transmission over the internet is facing some problems. So securing communication
channel for transmitting data over the internet is needed. Two
schemes are used to protect secret messages against the attacks or getting stolen while sending. The first scheme is a cryptography which is a well-known method in which the information is encrypted by using a key and then sent over the channel and it is received by the authorized person only which is having the right key which may decode the actual message properly.

Basically the process of image-Steganographyis applied for wrapping the information within the cover-image then it is also produced one stego-image of it. This type of stego-image will get delivered to other person via a channel, in which other persons never knew about the presence of stego-image. And when this stego-image will get received then the information which is wrapped may get derived either by using the stego-key or not [4].

Steganography process have the main function for preventing from getting focus over the communication of the wrapped information in order to obtained the security whereas, in case the intruder may get find out any type of modification within the message which is delivered then the analyzer may find out that some information is present [2],[3].

II. STEGNOGRAPHY

This is the process of wrapping the secret information in any of the form like text, image, sound etc within the transmitting message. Major benefit of this process is that it may not enable the secret message to get attention during analysis. Usually various information that are able to see which are in encoded form are also not able to break have got the attention by those regions where the process of encryption is even not applied [4]. Hence,the process of cryptography may protect the contents only of message, while in the process of Steganography that secret information may get wrap during sending within other message or text which is used to wrap the contents of secret information [5][6].

For this process mainly four types of formats have been used in this approach for creating the Steganography like text, image, audio or signals. Provided here the description about digital-images that are used over the Internet and which may cause the huge volume of duplicate bits to be present within the digital form of the image which is mostly hidden objects for Steganography.

There are many reasons why Steganography is used. Mainly it insures the possibility of sending secret messages even under monitored conditions. There are many different ways of sending messages to people without anyone else knowing the message exist.

Major objective of the Steganography is to cover the secret information or message in a manner such that attackers are will never find out those hidden messages [1]. And in case any type of malignant data has been found, then the objective is not accomplished. And another objective of this approach is to interact within in a secured manner which is providing an undetectable environment.

2.1Various Types of Steganography

2.1.1Text-Steganography: This type is having process of hiding the information within the files of having type text. Here, information got wrapped by the nth letter of each word within the text. Several processes are present for wrapping the data within this type of text content. And these processes are like Random-and-Statistical process ,Linguistics process etc.

2.1.2 Image-Steganography:

In this process taken out the wrapped object for making the information to be hide in the form of image. Here the intensities of pixel are considered for wrapping of the information. In this type of digital-Steganography, the images have been used in large scale to cover the source as several bits have been available within the digital form of the image.

2.1.3 Audio-Steganography:

Here the information gets wrapped within the files of audio type. By using the methods like AU, WAV, and the MP3files. Several types of approaches are there for audio-Steganography in which implementing the Low-Bit-Encoding, Phase-Coding and Spread-Spectrum, etc.

2.1.4 Video-Steganography:

This process uses the digital formats of video for wrapping the data in order to hide it. For this video is considered as the medium for carrying the secret data.

III. STEGNOGRAPHY V/S CRYPTOGRAPHY

Since the users have to send, share or receive personal data on the internet more frequently [4]. And for this the Cryptography approach may consider the message unintelligible that targeted on the encryption of message but it is easy to detect the encrypted message through communication. For recovering the weak points of the cryptographic approaches, the Steganography approach is treated as the significant approach of wrapping the details which makes the process of communication to be not able to see by the intruders. In the processes of both the systems may enable the communications in the secret form. In case the attacker may be able to read the information within the process of cryptography so it may be got broken whereas, within the process of Steganography if the attackers may recognize the presence of secret message then it is consider as broken [5]. Process of Steganography is more easily get breakas compare to the process of cryptography systems in regards of the system-failure as in case the process of communication have been recognized, then process of Steganography becomes a failure [6].

3.1 Comparison of Steganography V/S Cryptography approaches:

3.1.1 Definition:

Steganography -According to definition it implies the hidden writing.

Cryptography - And it implies the secure writing.

3.1.2 Objective:

Steganography -Main objective is hiding the presence of the message.

Cryptography –Its objective is on maintaining the contents as secret of the message.

3.1.3 Key:

Steganography –It is Optional to use the key.

Cryptography - It is Necessary to use key for this process.

3.1.4 Carrier:

Steganography –This used any type of digital media

Cryptography –This is basically a text based approach

3.1.5 Visibility:

Steganography –It is never visible for anyone.

Cryptography –It is always visible.

3.1.6 Security Services Offered:

Steganography – It provides the feature of authentication and confidentiality of data

Cryptography - It provides the features of availability, confidentiality, integrity of data, and also provides non-repudiation.

3.1.7 Attacks:

Steganography - It got attacked if the attacker may find out that the Steganography is applied by the process as the Steganalysis

Cryptography –Whereas it will get attacked it the attacker may read the message which is secret, it is also referred as the Cryptanalysis process.

3.1.8 Result:

Steganography –It may generate the Stego-file as output

Cryptography - It may generate the Cipher text as a result

IV. LITERATURE REVIEW

In this paper [8]describes the analysis of Steganography process with in the audio formatas well as within the video format. Since this approach may be applied within the cloud-computing in a wide range, so few problems may also have required to be considered in regards of wrapping the secret data for providing protection.And several types of parameters which may enables the Steganography process to work efficiently are PNSR,MSE, SNR, and SC etc, and various different approaches have also been applied along with the audio type or the video type of Steganography process like the DCT, LSB, DWT, etc all these may enable enhanced security.

Within this suggested paper [9]represented a latest concept of the image Steganography which is dependent on the modified LSB technique. The proposed algorithm is based on the parity of LSBs of three color components that is R, G, B. The main goal of the proposed method is to increase the size of the message to be embedded with the image and also make the technique difficult to the unauthorized person to determine the presence of secret message.

[10] Here within this research analysis describes one of the steganographic techniques which may combined the steg and the outguess algorithms. The approach allowed us to benefit from the potential features and strengths of both algorithms and this added a significant level of protection to hidden images. In principle what happened in this suggested approach is that an image intended to be a secret image is first hidden in an image using steg algorithm and the resultant stego image is further hidden in another second image using outguess 0.1 algorithms to produce a final stego image.

According to this analysis [11] mentioned that the work which has been applied here for increase the efficiency of approach which is suggested in this paper of Steganography process which will do not affect the quality of image. So in this approach of DCT have been applied for the 32 x 32 blocks along with the RGB pixel of image may provides the effective results. This is summarized that by organizing the pixels at the lower level may raise the tendency of image to get wrapped the certain messages. The Neural Network has been found effective enough to find pixels to extract the data bits with least affecting the original pattern of the image.And the suggested approach may provide the better psnr, mse values, so results better image quality and better way of hiding messages. It has been also concluded that if we can encrypt the data up to some level before merging it to the image, it may enhance the chances of security while image embedding**.**

Within this paper [12] represented the analysis being performed the experiments by the use of ZOH, the four types of approaches in which the PSNR method’s values was higher than the suggested method of ZOH and the other methods, this implies that the method's PSNR stego quality of image is also enhances successfully. And for the future work, it is planned to enhance the Maximum-Hiding-Capacity through enhancing the message which is secret by the use of LSB raille-image-Steganography approach such as the “Image-Steganography Method by Using Braille-Method of Blind-People”. And through describing the characters of secret message through the use of Braille approach of writing and reading available for the blind people which may save extra space for embedding.

In this paper [13] it is presented that the ideal Steganography approach which merges both the DWT and ERBP algorithms. And the two main stages are included while Steganography technique that is the extraction and embedding phases .The system implemented using MATLAB software and the performance evaluated in terms of MSE and PSNR criteria in addition to histogram test for both embedding and extraction stages. The result ensured the effectiveness of the proposed scheme in terms of high values PSNR and very low value of MSE.

Here in this paper [14] provide a brief an alysison the latest trends of the Steganography process. And this approach is deployed properly in the medium that is not protected also this process is working for the intrusion which are causing the creation of unnecessary type of stego-images with to the lower as well as the higher payload. Here also describes about the process of Steganography which is based on the components like DSIS approach for creating the group of unequal divisions. Also these divisions may got applied randomly for wrapping the image unless this may wrap hide it ina sequence. By applying DWT process for getting high loss-less-compression-ratio to increase the amount of the image that are consider as secret for sending.Also implement the advanced-encryption-standard for making the secret image to be un-readable for the attackers.

Within this paper [15] suggested the secure LSB approach for the image-Steganography which is implementing the approach of the chaos which is a non-linear system having dynamic nature. And this chaotic method is very sensitive in regards of the values or the parameter that are supplied to the system. Also it is suggested an approach in this paper which may provides security for the basic type of Steganography process. Within this paper also deployed a unique chaotic sequence to the encryption process of every portion of the image which is considered as secret for providing the protection. Therefore the suggested concept has got applied to the host based image files for wrapping the private data by not following any proper format. In this paper a performance analysis have been performed over this suggested technique and compare it along with the 3-3-2 process of LSB which is much better. And this suggested approach is implemented to the JPEG files though it may be operate along with some other types of formats also.

Here in this paper [16] suggested an algorithm which is used for the data which needs to be encrypted by the use of Extended-Substitution-Algorithm also within this algorithm the cipher text is hidden at the two or three LSB positions of sending image. In this approach described mostly all kind of symbols and the alphabets. And the encrypted text is hidden in different ways within the LSBs. Hence, this is one of the powerful algorithms. In this approach the visible features of the sending image before hiding of message and after hiding should be remained nearly similar. And this algorithm is applied by the use of Matlab tool.

Within this paper [17] suggested the combination of cryptography and the Steganography approaches in order to generate an effective algorithm for hiding the data against the unauthorized types of users that were presented in the network. And for this an audio channel has been used for Steganography process along with the Least-Significant-Bit algorithm have also been implemented in order to encode the message within the audio or sound file. And the suggested algorithm may never damage the actual size of file after doing encoding also and this is applicable for all type of file format that are used for audio. This type of encryption process and the decryption process are applied within this approach in order make it more secure. And hence this system is suggested to be used by various Internet users in order develop a secured network for communication.

V. PROPOSED WORK

This section deals with the proposed work. This proposed work is divided into two parts.

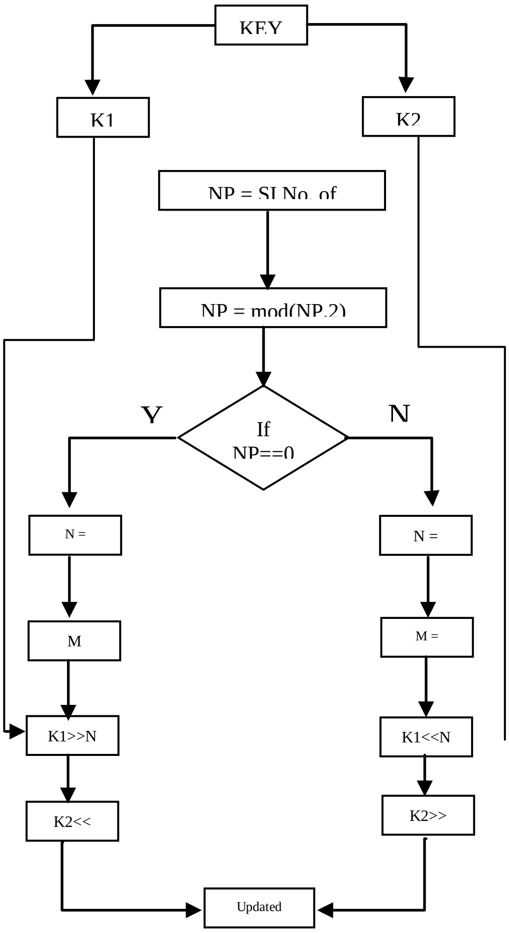


Figure 1: Key Generation

First part deals with key generation. This portion is responsible for generating the key. This key generation is based on the size of the secret key. If this size is even then key generation is of one type where if size is of odd then key generation is of other type. Key generation is shown in figure 1whereas; Figure 2 shows the concept and working of proposed Steganography work.Here, we have used various concepts in our concepts in work.

Proposed Steganography work uses S-Box and Expansion. S-box is a method which is used for substitution of contents when expansion is used for converting the small bit string into large bit string.

VI. RESULT ANALYSIS

This section deals with evaluated results through Existing as well as proposed technique by using selected performance parameters analysis. Analysis is done on following parameters:

1. Peek Signal to Noise Ratio (PSNR) analysis,
2. Entropy analysis,
3. Correlation analysis

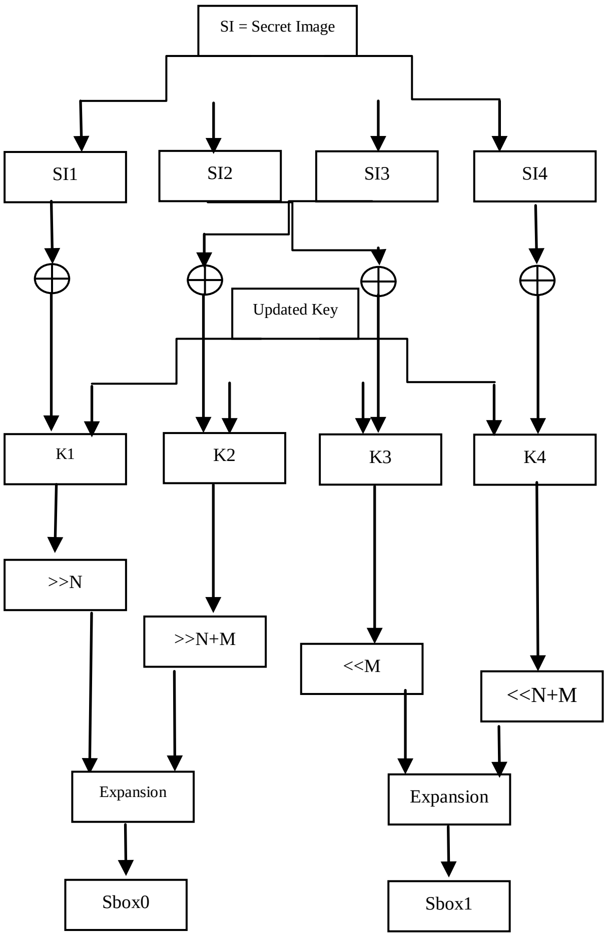


Figure 2: Proposed Stagnography

Proposed system is design in MATLAB programming language. There is image which has selected for Performance of the proposed system. During evaluation proposed system has run on number of several size of image information and captured overall performance on selected parameters. Here results is based on selected secret images which is follow in figure 3 and cover images which are shown in figure 4.

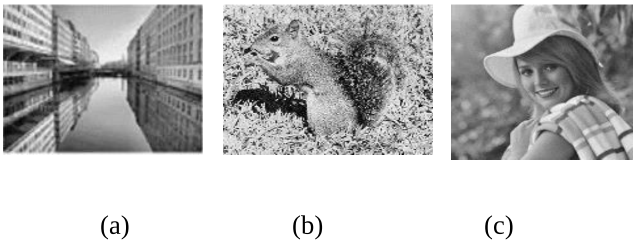


Figure 3: Secret Images

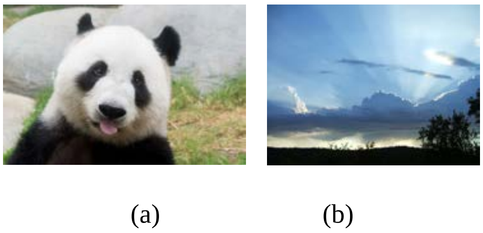


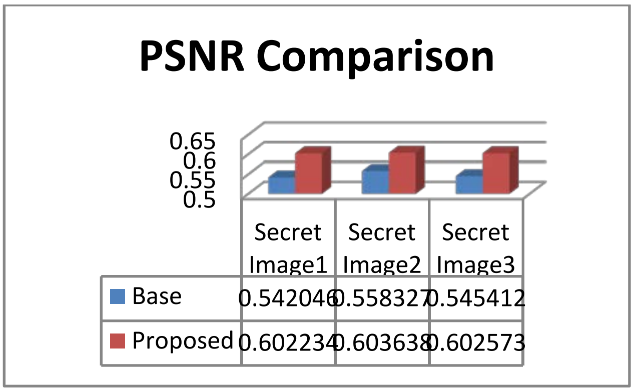
Figure 4: Cover Images

Peek Signal to Noise Ratio (PSNR) Analysis: PSNR is defined as assume that N is the total number of pixels in the input or output image, MSE (Mean Squared Error) is evaluated.

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

Table I: PSNR performance of Proposed Concept over Cover Image figure 4(a).

	Base	Proposed
Secret Image1	48.9662	52.133
Secret Image2	50.6421	52.1086
Secret Image3	50.5444	52.0932

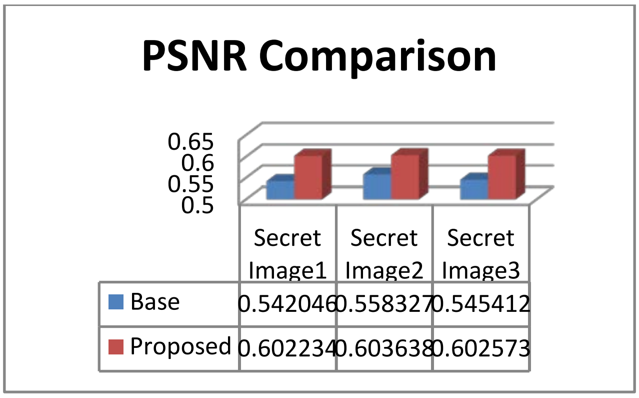


	Secret Image1	Secret Image2	Secret Image3
🟦 Base	0.542046	0.558327	0.545412
🟥 Proposed	0.602234	0.603638	0.602573

Graph1: PSNR performance of Proposed Concept over Cover Image figure 4(a).

Table II: PSNR performance of Proposed Concept over Cover Image figure 4(b).

	Base	Proposed
Secret Image1	44.8386	45.7266
Secret Image2	45.261	45.7204
Secret Image3	45.2247	45.7132



Graph 2: PSNR performance of Proposed Concept over Cover Image figure 4(b)

Entropy Analysis: Entropy defined as follows.

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

Where:*He*: entropy.

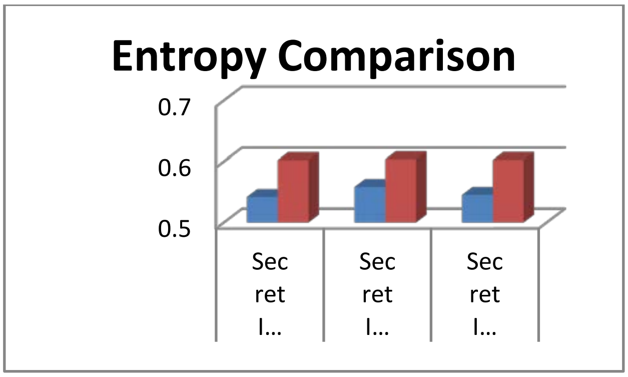
G: gray value of input image (0... 255).

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

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

Table III: Entropy Performance between Existing and Proposed Concept over Cover Image Figure 4(a)

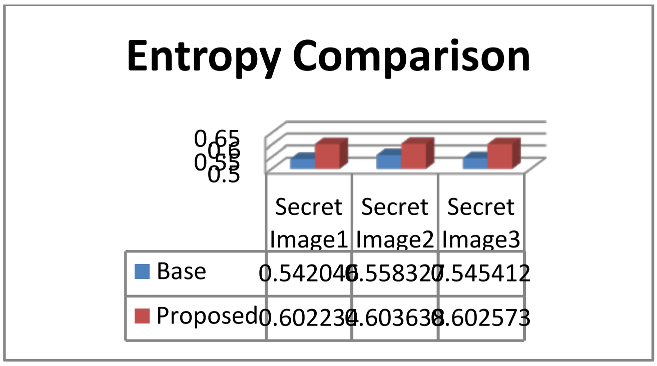
	Base	Proposed
Secret Image1	7.63475	7.67019
Secret Image2	7.64285	7.67003
Secret Image3	7.64285	7.66969



Graph 3: Entropy Performance between Existing and Proposed Concept over Cover Image Figure 4(a)

Table IV: Entropy Performance between Existing and Proposed Concept over Cover Image Figure 4(b)

	Base	Proposed
Secret Image1	7.76946	7.77451
Secret Image2	7.7734	7.77515
Secret Image3	7.77393	7.77529



Graph 4: Entropy Performance between Existing and Proposed Concept over Cover Image Figure 4(b)

Correlation Analysis: In addition to the histogram analysis, we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image/cipher image respectively. Firstly, we randomly select 2000 pairs of two adjacent pixels from an image. Then, we calculate their correlation coefficient using the following two formulas [30]:

$$cov(x,y) = E(x - E(x))(y - E(y)),$$

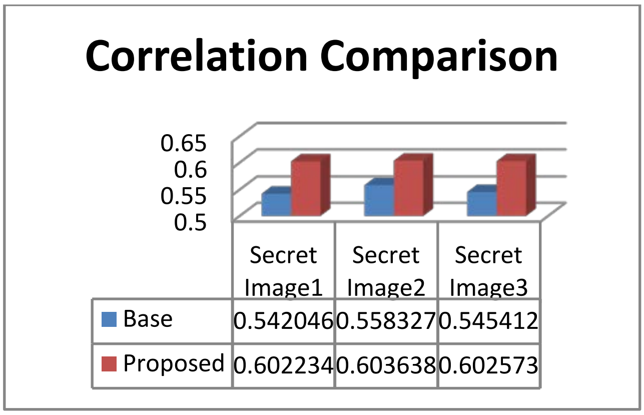
$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

Where

X and y are the values of two adjacent pixels in the image.

Table V: Correlation Performance of Proposed Concept over Cover Image Figure 4(a)

	Base	Proposed
Secret Image1	0.617211	0.637825
Secret Image2	0.627417	0.636784
Secret Image3	0.627868	0.639774



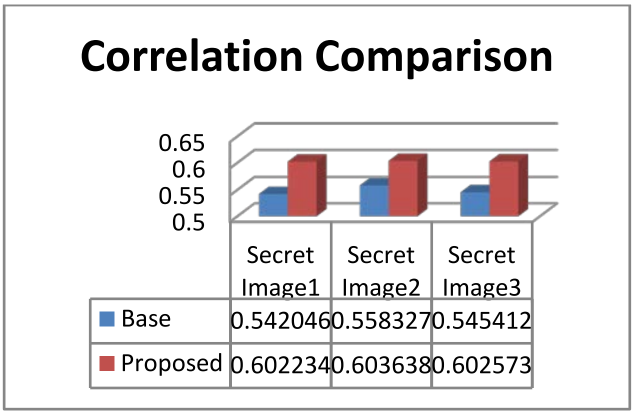
Graph 5: Correlation Performance of Proposed Concept over Cover Image Figure 4(a)

Table VI: Correlation Performance of Proposed Concept over Cover Image Figure 4(b)

	Base	**Proposed**
Secret Image1	0.542046	0.602234
Secret Image2	0.558327	0.603638
Secret Image3	0.545412	0.602573

VII. CONCLUSION

In this paper it is concluded that here represented a brief analysis on the various types of steganographicapproaches along with their types Within this suggested paper, described the detailed analysis on the traditionally algorithms and tools that are used within the security ofdata which is transmitted on the networks. Also in this paper describes the comparison within the Steganography approach and the cryptography approach both which are used for ensuring the security but some shortcomings are also there in both approaches' capabilities in regards of the providing security rules efficiently. Last section shown that the efficiency of the proposed work is much higher than the existing work



GRAPH 6: CORRELATION PERFORMANCE OF PROPOSED CONCEPT OVER COVER IMAGE FIGURE 4(B)

REFERENCES

[1] GunjanChugh, "Image Steganography Techniques: A Review Article", Bulletin of Engineering, Faculty ofEngineering, Hunedoara, Romania, July-September 2013.

[2] Manisha Rana andRohitTanwar, "Genetic Algorithm in Audio Steganography", International Journal ofEngineering Trends and Technology (IJETT) – Volume 13 Number 1 – Jul 2014.

[3] Adeel Jawed andAtanuDas."Security Enhancement in Audio Steganography by RSA Algorithm", InternationalJournal of Electronics & Communication Technology (IJECT) Vol. 6, Issue 1, Spl-1 Jan - March 2015.

[4] Andriotis, P., Oikonomou, G., Tryfonas, T. (2013). JPEG steganography detection with Benford'sLaw. Digital Investigation, 9(3), 246-257.

[5] Nitin, K., kirit, R., Avalik, R., Vijaysinh, J. and Ashish, N.2014. "A Novel Technique for Image SteganographyTechniques Based on LSB and DCT Coefficients,"International Journal for Scientific Research and Development (IJSRD), Vol. 1 (11). PP 2479-2482.

[6] Arun A.S. and George M. Joseph, (2013) "High Security Cryptographic Technique usingSteganographjy and Chaotic Image Encryption", in Proc. of Journal of Computer Engineering (IOSRJCE), vol 2, pp 49-54.

[7] Usha B.A ,Srinath N.K "Data Embedding Technique in Image Steganography using neural network ,IJARCCE - Vol. 2,Issue 5, 2013.

[8] Hilal Almara'beh, "Steganography Techniques - Data Security Using Audio and Video", Volume 6, Issue 2, February 2016 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[9] Tahir Ali Amit Doegar, "A Novel Approach of LSB Based Steganography Using Parity Checker", Volume 5, Issue 1, January 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[10] Hamdan Lateef Jaheel and Zou Beiji, "A NOVEL APPROACH OF COMBINING STEGANOGRAPHY ALGORITHMS", INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS VOL. 8, NO. 1, MARCH 2015.

[11] Kamal1, Lovnish Bansal2 , "Enhancement Key Of Cryptography And Steganography Using RSA And Neural Network", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 5, May 2014.

[12] Abdelmgeid A. A., Tarek A. A., Al-Hussien Seddik Saad, Shaimaa M. H., "New Image Steganography Method using Zero Order Hold Zooming.", International Journal of Computer Applications (0975 – 8887) Volume 133 – No.9, January 2016.

[13] Reyadh Naoum1, Ahmed Shihab2, Sadeq AlHamouz, "Enhanced Image Steganography System based on Discrete Wavelet Transformation and Resilient Back-Propagation", IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.1, January 2015.

[14] Odai M. Al-Shatanawi1 and Nameer N. El. Emam, "A NEW IMAGE STEGANOGRAPHY ALGORITHM BASED ON MLSB METHOD WITH RANDOM PIXELS

SELECTION.", International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.2, March 2015.

[15] Debiprasad Bandyopadhyay1, Kousik Dasgupta2, J. K. Mandal3, Paramartha Dutta, "A NOVEL SECURE IMAGE STEGANOGRAPHY METHOD BASED ON CHAOS THEORY IN SPATIAL DOMAIN.", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 3, No 1, February 2014.

[16] R.S. Gutte1, Y.D. Chincholkar2 and P.U. Lahane3, "STEGANOGRAPHY FOR TWO AND THREE LSBs USING EXTENDED SUBSTITUTION ALGORITHM.", ICTACT JOURNAL ON COMMUNICATION TECHNOLOGY, MARCH 2013, VOLUME: 04, ISSUE: 01.

[17] Abikoye Oluwakemi C., Adewole Kayode S., Oladipupo Ayotunde J., "Efficient Data Hiding System using Cryptography and Steganography", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4– No.11, December 2012.