SECURING INFORMATION USING STEGANOGRAPHY

S. Sai Pavan[1], Md. Zaheeruddin[2], B. Naveen Kumar[3],
G. Ravindranath Kumar[4]

[1, 2, 3] B.Tech (ECE), [4] Working as Professor & HoD, Department of (ECE)
Visvesvaraya College of Engineering and Technology, M.P Patelguda,
Ibrahimpatnam (M), Ranga Reddy (D), Affiliated to JNTUH, (India)

ABSTRACT

This abstract explains mainly that the security of data can be obtained through a special technique. Communicating the information using Steganography is defined ascovering and hiding of the data.This system is implemented by security-using Steganography. In this method, the user identifies associate degree image it goes to know because the carriers of information. The data file is protected from other users. This message is hidden inside the image. The image is hacked and interpreted from an external party user open up however not displaying the data. This project data have been invisible and therefore be secure during transmission. To produce low noise the image is converted to DWT which is well known as Discrete Wavelet Transform. After apply of the DWT we will get an unnecessary pixels to hide the data. Finally we get the hidden secured data for the transformation

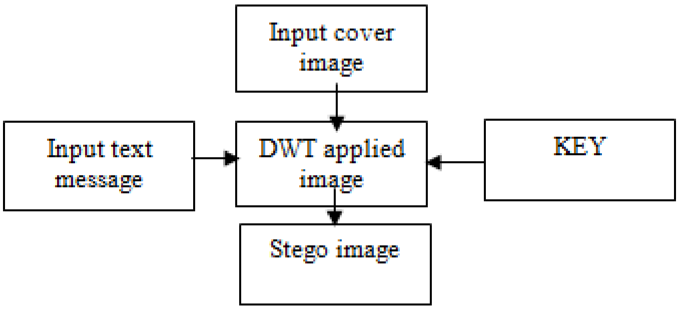
Key Words**: **Hiding Technique, MATLAB, Steganography

I. INTRODUCTION

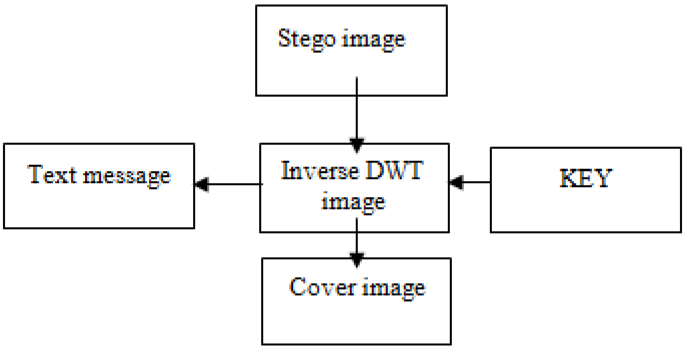
The users transmits the data in a secure purpose in the digital communication at some particular time using present technology. The internet communication have become very common source for the data transfer. The user may send high important data to the receiver through internet. But due to improper security the data encryption and the data decryption are not implemented in proper way.In the previous days data were secured by the cryptography technique. The user encrypted data may be obtained by applying cryptanalysis technique on it, then the intruder can achieve the original message through hacking.The data here is in the form of image is to be hided for the security purpose.One of the explanations that intruders are often successful is that almost all information they acquire from a system is in a form that they will scan and compare. The data is reveal to the intruders or others, may be modify to implement a singular or multiple data. A solution of this drawback is, use of steganography. The Steganography is one of thetechnical methodin digital media. In contrast to petrography, it is not to make others from knowing the hiddendata however it is to stay away to others from thinking the data even exists.Steganography is an art and science for writing the hidden messages so that none of others, except the rightrecipientonly knows the exact key of the original message. The word “steganography” is originated from Greek which means “hiding” and“writing”. The word is described as “secret” and “writing”. In trendy digital steganography, information is first encrypted by the same old means that so inserted, employing special formula, into redundant information that's a part of a selected file format like a JPEG or BITMAP image. Consider all the bits that represent an equivalent colour pixels continual in an exceedinglyrow. By implementing the encrypted information to the current redundant information in some random or non-conspicuous approach, the result are going to be data that seems to possess the "noise" patterns of standard, no encrypted information.

II. PROPOSED TECHNIQUE

2.1 Embedding Section



2.2 Extraction Section



2.3 Discrete Wavelet Transform

Here for each pair n, k of integers in Z, the Haar function $\psi_{n,k}$ ok is defined at the actual line R by using the system

$$\psi_{n,k}(t) = 2^{n/2}\psi(2^n t - k), \qquad t\epsilon R$$

This equation is suitable for right-open interval $I_{n,\ k}$ = (k 2^{-n}, (k+1) 2^{-n}), i.e., it vanishes outside interval.

$$\int_R \psi_{n,k}(t)dt = 0, \qquad \|\psi_{n,k}\|^2_{L^2(R)} = \int_R \psi_{n,k}(t)^2 dt = 1$$

These functions are pair wise orthogonal

$$\int_R \psi_{n1,k1}(t)\psi_{n2,k2}(t)dt = \delta_{n1,n2}\delta_{k1,k2}$$

2.4 Least Significant Bit Insertion

Least significant bit (LSB) insertion of the bit is a technical approach for embedding information.In LSB insertion, information will be inserted at a particularpixels.

Example for least significant bit insertion technique.

The alphabet letter 'C' is an ASCII code of 67 in decimal, where in binary is1000011.So it needs 3 consecutive pixels for storing a 72-bit image 'C':

The pixels before the LSB insertion are:

10000000	10100100	10110101
10110101	11110011	10110111
11100111	10110011	00110011

Then the originalvalues will change after the insertion of a 'C' will be:

10000001	10110100	10100100
10110100	10110110	11110010
11100111	00110011	10110011

Due to the insertion of the data into the image there is some disturbances there are some differences in original and executed image. For the calculations the disturbances we do the comparing of the data of original image, output image, using the Peak Signal to Noise Ratio and Mean Square Error of an output image to the noise of the image. Before reading the data of an image as cover image if the image is colored image then the image is converted into the grey color image since DWT is only applicable on 2-D systems instead of 3-D color images. So only a grey color image processed by the fixed size.

2.5 Block Diagram

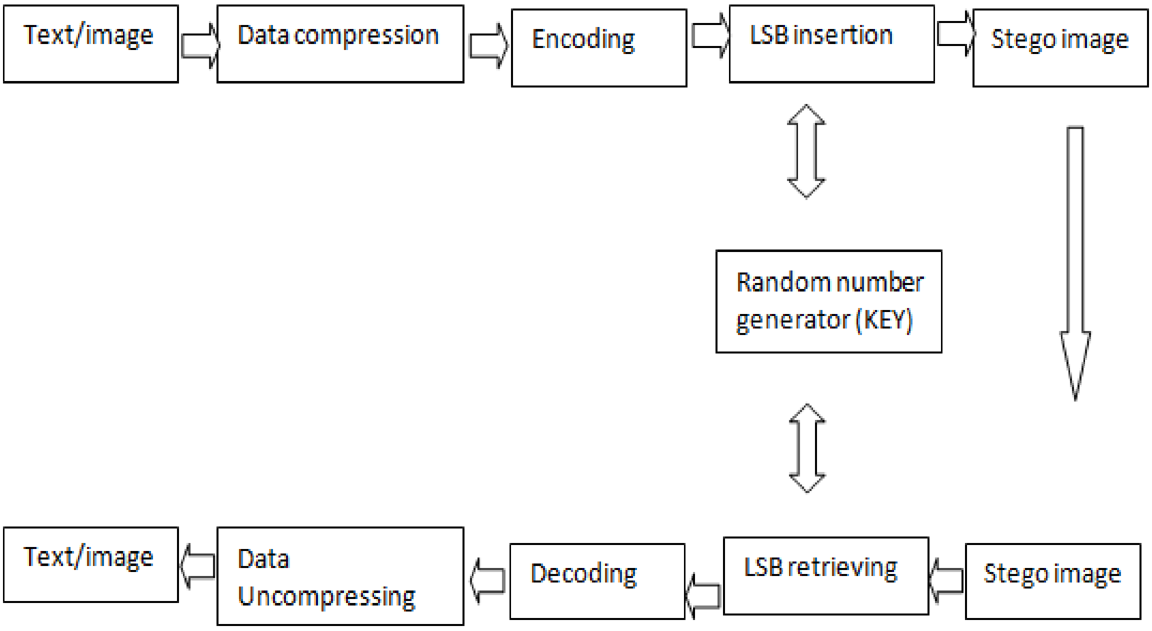


Figure: 1.0 proposed technique flow chart

2.6 Random Number Generators

By random number generator. The formula has shown below,

$$Xi+1=(X)^2 \mathrm{mod}\ n$$

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

The pseudo random bit generator is used for generation ofrandom numbers in cryptography.Two large primenumbers, and the range is the inputs for the pseudo random bitgenerators. The mathematical formulae has shown below,

$Xi+1= (PXi+Q) \bmod n$

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

Steganography is that the art of concealing and sending information through carriers in an attempt to hide the existed information. Generally the steganography and cryptography square measure closely connected. Wherever cryptography scramble messages so that they can't be simply understood by an unauthorized person, steganography on the opposite hand can hide the message thus there's no data of the existence of the message within the initial place. If anyone or persons who views the item that information or data is hidden inside he or she's going to don't have any knowledge that there's any hidden information, so the persons won't plan to decode the data.

III. RESULTS

The results of the project are obtained below

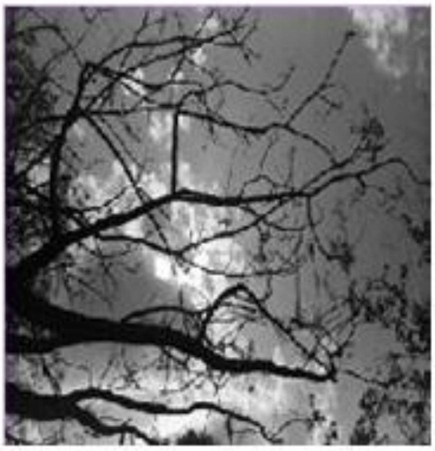


Fig: a

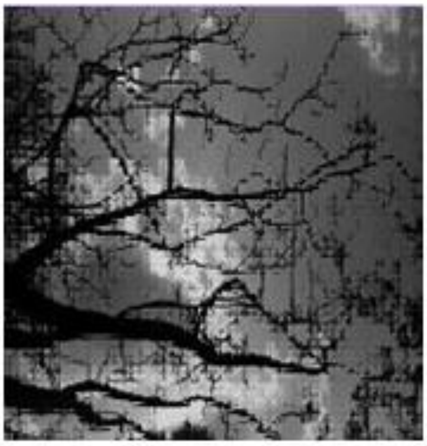
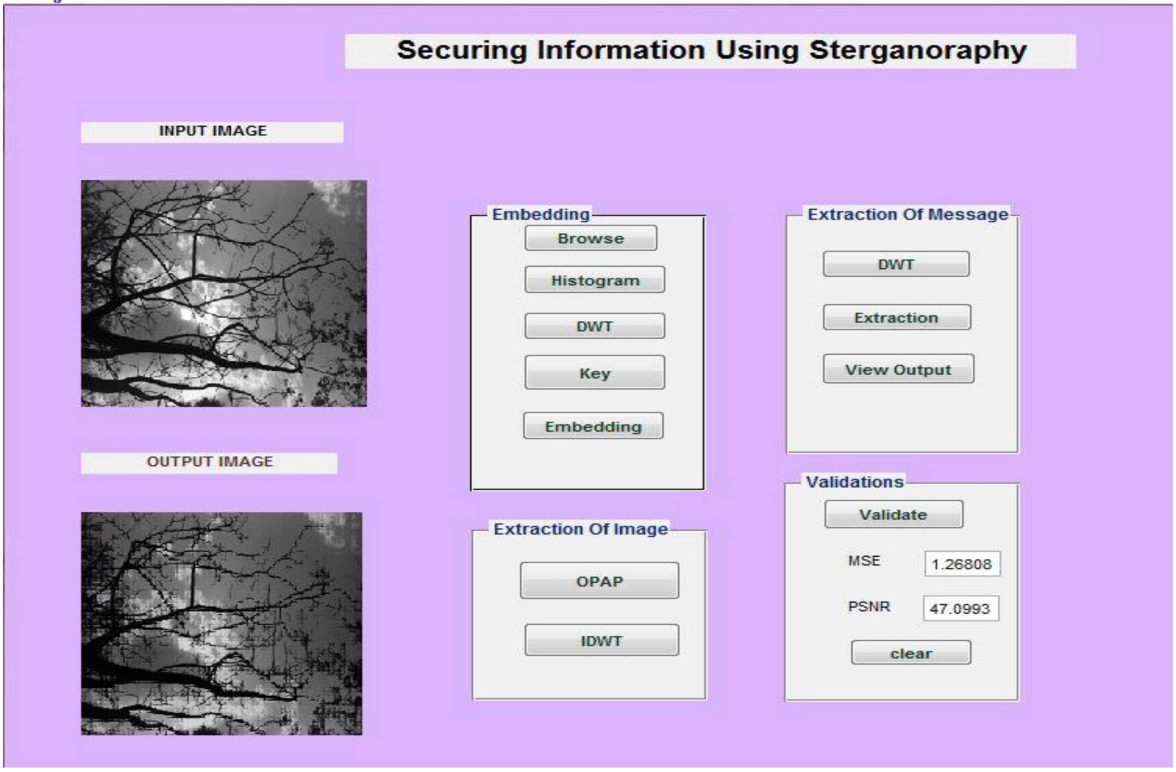


Fig: b

The image fig: a is the input image before applying histogram and the image is embedded and encrypted with a key then the fig: b shows the output of the result with noise and text is inserted in it.The proposed results ensures that high embedding rates and also maintaining high levels of security. The experimental work has been done using MATLAB and in the experiment we observed that the messages were successfully embedded into the cover images.



MSE 1.26808

PSNR 47.0993

Fig : c

In the first we need to extract the frames of the image and apply 2-DWTwhich results in high noise ratio when compared to the two-dimensional image. Here it should be note that the original image as well as the cover image are exactly same having same extensions of .jpg. The above image fig c shows the resultant images. The resulting imagewill have the double extension of image. The above image shows the embedding and extraction of image in two colours. Without the secret key we are unable to spot the secret pixels where we inserted the message. Inverse logics are applied at the time of the message extraction when the secret pixels are detected.

IV. CONCLUSION

We explore the bounds of steganography theory and practices. We point to out the strengthening of the imagestenographic system by using LSB technique to this is away of secure. Astego key is inserted to the system during embedded of themessage into the cover-image. In our approach, the message bits are sledded randomly into the cover layer of image pixels instead of consecutive. Finally, we have shown that steganography which uses a key has good security performance than non-key steganography. This is so as a result if the valid key not available, it is difficult to a third party or malicious folks to recover the embedded message. However there is a unit still some problems want to be tackled to implement LSB on a digital image as a cover-object using random pixels.

Steganography can still increase in quality over cryptography because it gets additional advanced steganalysis tools for detective work it. At the previous time the most of the tools will observe the files hidden in any image. There is additionally appears a little number ofworking tools for hiding the videos. There are some tools for audio, however this can be still lags behind image steganography. The long run might even see audio files and video streams that might probably be decoded on the fly to create their correct messages.

REFERENCES

[1] N. Provos and P. Honeyman, "Hide and seek: An introduction to Steganography", *IEEE Conference on Security and Privacy*, pp. 32-44, 2003.

[2] C. Cachin, “An Information-Theoretic Model for Steganography”, *Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science*, May 1998

[3] “Peak Signal to Noise Ratio (PSNR)” from Wikipedia http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.

[4] Jessica Fridrich and Jan Kodovsky, “Rich Models for Steganalysis of Digital Images”, IEEE *Transactions on Information Forensics and Security*, Vol. 7, No. 3, pp. 868-882, June 2012.

[5] C.C. Chang, P. Tsai, and M.H. Lin, “An Adaptive Steganography for Index- based images using Codeword Grouping”, *Advances in Multimedia Information Processing-PCM, Springer*, Vol. 3333, pp. 731–738, 2004.

[6] "Cryptography" from Wikipedia, http://en.wikipedia.org/wiki/Encryption

[7] MohZan and Nyein Aye," A Modified High Capacity Image Steganography using Discrete Wavelet Transform", *International Journal of Engineering Research & Technology* (IJERT), Vol. 2,No. 8, pp. 2712-2715, August - 2013.

[8] Ali Al-Ataby and Fawzi Al-Naima, “A Modified High Capacity Image Steganography Technique Based on Wavelet Transform” *The International Arab Journal of Information Technology*, Vol. 7, No. 4, October 2010.

[9] NedaRaftari and Amir MasoudEftekhariMoghadam, “Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT”, *Fourth International Conference on Computational Intelligence, Communication Systems and Networks*, 2012.

[10] Andrew Westfeld, “F5-a steganographic algorithm: high capacity despite better steganalysis”, *Proc.of the 4th Information Hiding Work-shop*, vol. 2137, pp. 289-302, Springer, 2001

[11] T. Narasimmalou, Allen Joseph .R, “Optimized Discrete Wavelet Transform based Steganography”, *IEEE International Conference on Advanced Communication Control and Computing Technologies* (ICACCCT), 2012.

[12] Rajbirkaur, Surbhi Gupta, and Parvinder S. Sandhu, “Randomized Steganography using Ycbcr Color Model Characteristics”, *International Conference on Computer and Communication Technologies* (ICCCT' 2012) May 2012, Phuket.

AUTHOR DETAILS

S.SAI PAVAN

B.Tech (ECE) from Visvesvaraya College of Engineering and Technology, M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy (D), Affiliated to JNTUH, India.

MD. ZAHEERUDDIN

B.Tech (ECE) from Visvesvaraya College of Engineering and Technology, M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy (D), Affiliated to JNTUH, India.

B.NAVEEN KUMAR

B.Tech (ECE) from Visvesvaraya College of Engineering and Technology, M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy (D), Affiliated to JNTUH, India.

G.RAVINDRANATH KUMAR (HOD)

Working as Professor & HOD (ECE) from Visvesvaraya College Of Engineering And Technology, Patelguda, Ibrahimpatnam, RangaReddy dist., Telangana, INDIA.