

# A Steganography Approach to Protect Secret Information in Computer Network

Prajakta B. Diwan<sup>1</sup>, V. B. Bhagat<sup>2</sup>

<sup>1</sup>SGBAU University, Department Computer Science and Engineering, Amravati, Maharashtra, India

<sup>2</sup>Professor, SGBAU University, Department Computer Science and Engineering, Amravati, Maharashtra, India

**Abstract:** *Everyone use computer networks to share resource and to exchange information. Protection of data is a demanding issue in today's era. The prevalent part of the data or information pass throughout the internet and it becomes difficult to make data secure. There arises a need of data hiding. Steganography is different as the study of hidden communication. Steganography is the skill and science of hiding a pinnacle secret communication in a cover media such as image, text, signals or sound in such a approach that nobody, with the exception of the intentional beneficiary knows the existence of the data. This paper express the thought to protect secret information in computer network by means of exploring initially what is the steganography, cryptography and DWT and the necessities associated to steganography. In this paper, we implemented the security and data hiding technique that are used to implement a steganography.*

**Keywords:** steganography, computer security, Information hiding, image processing, communication

## 1. Introduction

Steganography[11] is by no means a modern practice. Literally meaning "covered writing" it is the practice of hiding messages within other messages in order to conceal the existence of the original. Steganography is derived from Greek words Steganos meaning "covered" and graphy meaning "writing". So it is known as "covered writing". Steganography is a rough Greek translation of the term Steganography is secret writing technique which is used to hide the message and prevent the detection of hidden message and has been used in various forms for 2500 years. It has found use in variously in military, diplomatic, personal and intellectual property applications. Briefly stated, steganography is the expression applied to any number of processes that will hide a message within an objective where the secret message will not be visible to an viewer.

Examples of its use can be found throughout history, dating as far back as ancient Greece. However, with the digital media formats in use for data exchange and communication today providing abundant hosts for steganographic communication, interest in this practice has increased. Couple this fact with the multitude of freely available, easy to use steganography software tools on the internet, the ability to exchange secret information without detection is available to virtually anyone who desires to do so, and provides unique challenges and opportunities for the security professional. For the security professional, this means that data you are paid to protect could be leaving your control without your knowledge.

Conversely, one of the emerging uses for steganographic techniques is digital watermarking, which provides an organization with a way to ensure the integrity of data they wish to disseminate by embedding copyright or other information in a digital file. Regardless of whether it is used for good or ill, an understanding of current methods of data hiding should be part of every security professional's

knowledge base. Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. Even though both methods provide security, a study is made to combine both cryptography and Steganography methods into one system for better confidentiality and security. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not.

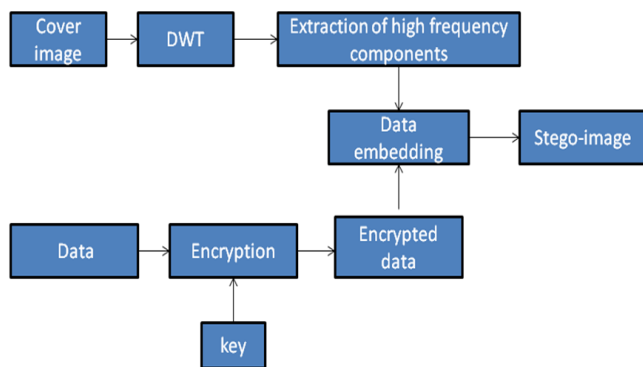
## 2. Related Work

Image steganography takes the advantage of limited power of human visual system (HVS). Here, unlike watermarks which embed added information in every part of an image, only the complex parts of the image holds added information. Straight message insertion will simply encode every bit of information in the image. More complex encoding can be done to embed the message only in "noisy" areas of the image that will attract less attention [3]. The least significant bit (LSB) insertion method [4] is probably the most well known image steganography technique. The main advantage of this method is that human eye is not able to notice the change; however unfortunately, it is extremely vulnerable to attacks, such as image manipulation. The usual steganographic methods fetch few bits from the secret data to be embedded. But R. Amirtharajan[5], describes Hiding Streams of 1s and 0s method it fetches the 1s or 0s present consecutively for hiding. This is an innovative steganographic method where

the data to be hidden is converted to binary. The number of 1s and 0s are counted and stored in the pixels of the cover image in this method. The number of 1s is stored in the odd columns of the pixel and the number of 0s is stored in the even columns. Jessica Fridrich and Miroslav Goljan[6], describes Digital image steganography by using stochastic modulation. Vinay Kumar\*and S. K. Muttoo[7], describes the concept of finding natural relationship between a digital cover and a message which can be used to hide the information in cover without actually replacing or distorting any useful bits of the cover. It introduces a concept called sustainable embedding of message in a cover using natural relationship and representing it using graph theoretic approach. Ankita agrawal[8], presents a new generalized model for combining cryptographic and steganographic technique by using simplified data encryption standard(S-DES) algorithm. Samir Kumar Bandyopadhyay[9], proposed technique converts 4 bit image into 4 shaded Gray Scale image. This image will be act as reference image to hide the text. Using this grey scale reference image any text can be hidden. Graeme Bell and Yeuan-Kuen Lee[10], describes fast and accurate detection of steganography is demonstrated experimentally here across arrange of media types and a variety of steganography approaches.

### 3. Proposed Work

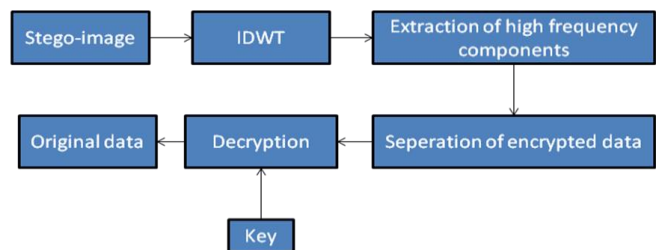
The process of hiding information inside another media is called steganography. The media with secret information is called stego media and without hidden information is called cover media. Steganalysis is a process of extracting information from the stego media. Steganalysis is just opposite to steganography.



**Figure 1:** Block diagram of sender side

The proposed technique is shown in fig.1 the proposed method embeds secret message into DWT coefficients in frequency components and restores the original image coefficients after the secret messages have been extracted. Wavelet transform is used to converts an image from time or spatial domain to frequency domain. Decomposition of digital image will be pair of waveform with high frequency corresponds to detailed parts of an image & low frequency corresponds to smooth parts of image. The secret message will be embedding low frequency components & the image will be reconstructed to get cover image with secret message hidden. Embedded image decomposed into inverse discrete wavelet transform. Inverse wavelet transform is used to convert

frequency domain to spatial domain. Hence it is frequency-time representation. Embedded image will be extracted in to sub-band frequencies using dwt method. The data will be taken from the sub-band frequency components & the extracte data will be compared with original message. This system includes the procedures of embedding & extraction.



**Figure 2:** Block diagram of receiver side

The Wavelet transform decomposes the image into three spatial directions: horizontal, vertical and diagonal. The multi-resolution of wavelet allows representing an image at more than one resolution level. The magnitude of DWT coefficients is larger in the lowest bands (LL) and is smaller in other bands HH, LH and HL, at each level of decomposition. High resolution sub bands help to easily locate edge and texture patterns in an image. Wavelet transform can accurately model Human Visual System (HVS). This allows embedding higher energy in regions, where HVS is less sensitive. Embedding secret data in these regions allow us to increase robustness without damaging image fidelity. DWT provides multi-resolution of an image, so that the image can be sequentially processed from low resolution to high resolution. The advantage of this approach is that the features of an image that might not be detected at one resolution can easily be detected at another resolution. It reduces the detectable distortion in a joint photographic experts group (JPEG) file during data hiding process. According to the human vision system point of view, the changes in the plain region can be easily identified but not in the variation regions.

### 4. Result Analysis

The images with 512\*512 pixels and the various keys used for testing. The proposed method is tested using MATLAB. The imperceptibility and the robustness of the image are tested with PSNR, MSE and NC. For performance evaluation, the visual quality of image is measured using the Peak Signal to Noise Ratio, which is defined in Equation (1).

$$PSNR = 10 \log_{10}(R^2/MSE) \quad (1)$$

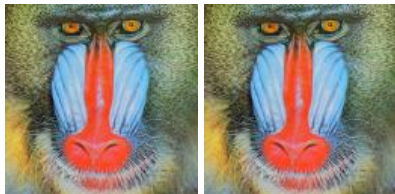
R is the maximum fluctuation in the input image data type.

To compute the PSNR, the block first calculates the meansquared error using the following equation:

$$MSE = \sum_{M,N} \frac{[I_1(m,n) - I_2(m,n)]^2}{M \cdot N} \quad (2)$$


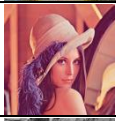


M and N are the number of rows and columns in the input images, respectively. Then the block computes the PSNR.

The performance evaluation of the method is done by measuring imperceptibility and robustness. The normalized correlation coefficient (NC) is used to measure the similarity between the cover image and the stego image. Peak Signal-to-Noise Ratio (PSNR) is used to measure the imperceptibility of the stego image. The robustness of the stego image is tested by attacks such as median filtering and average filtering. The cover image of size 512x512 and the secret message of 16 bytes is embedded in cover image which gives stego image are shown in figure (3). The stego images without any attack are shown in table (1).

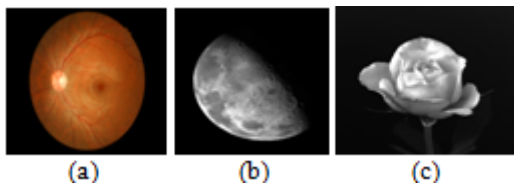


**Figure 3:** (a) cover image (b) stego image

**Table1:** PSNR (db), MSE and Nc of stego images

Image	message	PSNR	MSE	NC
	Password is 2145	78.3022	0.000961304	1
	Meet me tomorrow	77.8446	0.00106812	1
	Mission X cancel	62.9997	0.0325918	1
	Password is 4569	78.6613	0.00088501	1

According to invisibility benchmark PSNR 30dB is acceptable. In our proposed method the average PSNR value of stego image is 74.45195 & MSE is 0.008876555, which indicates that there is very little deterioration in the quality of the image and which is greater than method of type Substitution-based steganography[1].



**Figure 4:**(a)retina, (b)moon & (c)rose of stego image

**Table2:** PSNR (db),MSE and Nc of stego images under different attacks

Stego images	attacks	Average filter	Median filter	none
retina	PSNR	39.003	43.6181	71.6418
	MSE	8.1809	2.82661	0.00445557
	NC	0.99939	0.999788	1

moon	PSNR	34.8808	37.886	65.9263
	MSE	21.1351	10.57988	0.016613
	NC	0.997464	0.9987	0.9999
rose	PSNR	33.7276	38.5072	62.8714
	MSE	27.7226	9.16977	0.0335693
	NC	0.9968	0.998945	1

The robustness of the proposed scheme is evaluated against several attacks including median filter, average filter. After adding such attacks our system gives original message without making any changes, this shows robustness of system. Table 2 shows PSNR & MSE of distorted stego images under above distortions.

## 5. Conclusion

Cryptography and steganography are two major branches of data security. In this system cryptographic and steganographic security is combined to give two tier security to secret data. We proposed a new robust scheme, which provides lossless data embedding using a DWT to improve data hiding capacity & retain good stego image quality. Cover image within (text) message Embedded into Horizontal (H1) & vertical (V1) sub bands using DWT & finally we get the stego image and the hidden message is invisible. Hence the security, capacity and DD will get improve.. Lastly we can conclude that the proposed technique is effective for secret data communication. Also, In this project we have presented a new system for the combination of cryptography and Steganography which could be proven a highly secured method for data communication in near future. Steganography, especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The proposed method provides acceptable image quality with very little distortion in the image. The main advantage of this Crypto/Stegno System is that the method used for encryption, AES, is very secure and with the DWT transformation steganography techniques are very hard to detect.

## References

- [1] V. Saravanan and A. Neeraja, "Security Issues in Computer Networks and Steganography," in Proc. seventh International Conference on Intelligent Systems and Control, pp. 363-366, 2012.
- [2] F.A.P.Petitcolas,R.J.Anderson,M.G.Kuhn:"Information Hiding- A Survey," Proc of IEEE, 87(7), 062-1078, July1999.
- [3] C. Stanley, Pairs of Values and the Chi-squared Attack, Master's thesis, Department of Mathematics, Iowa State University, 2005.
- [4] M. A. F. Al-Husainy, "Message Segmentation to Enhance the Security of LSB Image Steganography", International Journal of Advanced Computer Science and Applications, 3(3),57-62,2012.

- [5] R. Amirtharajan, R. Akila, P. Deepikachowdavarapu, "A Comparative Analysis of Image Steganography", International Journal of Computer Applications, 2(3),41-47,2010.
- [6] Jessica Fridrich and Miroslav Goljan, Digital image steganography using stochastic modulation, Department of Electrical and Computer Engineering, SUNY Binghamton, Binghamton, NY 13902-6000, USA.
- [7] Vinay Kumar and S. K. Muttoo, "Principle of Graph Theoretic Approach to Digital Steganography", Proc of the 3rd National Conference,26 – 27, February2009.
- [8] Ankita agrawal, "Security Enhancement Scheme for Image Steganography using S-DES Technique", International Journal of Advanced Research in Computer Science and Software Engineering, 2(4), 164-169, April 2012,.
- [9] Samir Kumar Bandyopadhyay, "An Alternative Approach of Steganography using Reference Image", International Journal of Advancements in Technology,1(1) ,June 2010,95-102.
- [10] Graeme Bell and Yeuan-Kuen Lee, "A Method for Automatic Identification of Signatures of Steganography Software", IEEE Transactions on information forensics and security ,354-358,June 2010.
- [11] N.F. Johnson, S. Jajodia, "Exploring steganography: seeing the unseen," In Proceedings of the IEEE Congress on Evolutionary Computation (CEC) 31 (2), 26–34,1998.

### Author Profile



**Miss. Prajakta B. Diwan** Completed B.E. in Information Technology from P.R.Patil College of Engineering, SGBAU University in 2012. Pursuing M.E. CSE from SGBAU University. Submitted research paper in other national & international journals for publication.



**Prof. V. B. Bhagat** Completed B.E. and M.E. from Amravati, Maharashtra. Currently working as Profeseor in P.R.Patil College of Engineering in CSE Department, SGBAU University, Amravati. Submitted research paper in other national & international journals for publication.