ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue X, October 2016

Secure Data Hiding Using Multilevel Steganography

SUJA G.P[1], Mrs.M.NARMATHA[2],
M.Phil Scholar[1], Assistant Professor[2]
Department Of Computer Science
Sri Jayendra Saraswathy Maha Vidyalaya College Of Arts And Science,
Coimbatore, India

***Abstract*— The advancement in internet has paved way for the ease of communication. The data communication over computer network has increased. The security of information transmitted over network is a concerned issue. Methodologies such as cryptography and steganography provide ways for security. Cryptography obscures the content of the secret message while Steganography conceals the message as well as its existence. In steganography the secret information is embedded in a carrier file which could be text, image, audio or video file. The schemes of steganography include spatial domain embedding and transfer domain embedding. The data hiding process efficiency is based on capacity, security and robustness. Multilevel steganography is proposed which exploits both the spatial and transfer domain process and involves two cover and stego images. The DWT is applied to the inner cover image and then the secret information is embedded in the resultant wavelet bands which forms the inner stego image. The outer cover image is preprocessed which leads to image enhancement. The inner stego image is then embedded in the enhanced outer cover image by LSB substitution. The use of multilevel steganography ensures security. Security is further enhanced by the use of encryption key and selective pixel embedding. Thus the proposed system has high embedded capacity and enhanced security.**

***Index Terms*—Steganography; LSB Technique; DWT; cover image; stego image; PSNR; MSE**

I. Introduction

The rapid development of technology has made communication easier. The secure transmission of data is challenging. Cryptography encodes secure information into unreadable format and steganography hides secure information within a medium to establish an invisible communication.

The term Steganography is derived from two Greek words “stegos” which means “cover” and “grafia” which means “writing”. Steganography is “Concealed writing”. Steganography is art of passing secret information through any medium such that the existence of secret message is unknown. This way, it not only hides the secret message, but also hides the fact that a message is being transferred. Steganography is one of the most powerful techniques used to conceal the existence of a hidden secret data inside a cover object. Cover objects can be image, audio, video or text file. But images are the most popular cover objects, and thus the importance of Image steganography.

Image Steganography involves three main objects:

i. Cover image: It is any image that can carry a hidden message.

ii. Secret message: It is the information which we hide in the cover image. [E.g. Small image or Text]

iii. Stego-image: It is the image that carries the secret message.

Cover image + Secret message = Stego-image

The stenography techniques based on the cover modifications applied in the embedding process is of two types namely spatial domain techniques and rework domain techniques. Special domain techniques plant secret data within the intensity of the pixels directly, whereas in rework domain, the message is embedded within the image when its transformation. Special domain involves cryptography at the extent of the LSB. rework domain techniques 1st transforms the duvet pictures victimization separate circular function transformation or separate wave transformation so hides the information within them. Transform domain techniques hide data in mathematical functions.

II. Literature Review

A. Steganography Vs Cryptography

Both steganography and cryptography are used for secure transmission of data. In cryptography a secret key is used to encrypt the data whereas in steganography there is no secret key. In steganography the secret data is hidden in any common cover object. The major difference between cryptography and steganography is that cryptography is used to protect the secret data whereas steganography is used to protect the existence of secret data [1]. Thus steganography provides more secure way for communication of sensitive data.

B. Spatial Domain Method

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue X, October 2016

In spatial domain scheme, the secret messages is directly embedded in the carrier. Least significant bit(LSB) insertion method is the most common and simplest steganography method. In the LSB technique, the least significant bits of the pixels are replaced by the message bits. Most steganography methods hide information by replacing only the least LSB of an image with bits from the file that is to be hidden which is called LSB encoding. These modifications could be interpreted as random noise, which should have any perceptible effect on the image[2].The algorithms of LSB will modify the pixels in a random walk in a random walk or simply increment or decrement the pixel value [3]. Advantages of spatial domain approach are high embedding capacity, ease of implementation and imperceptibility of hidden data. The disadvantage is that it cannot withstand simple statistical analysis method.

C. Transfer Domain Method

In the transfer domain scheme, the transformation of image to frequency domain happens and then the messages are embedded in the transformed image. If we have a tendency to implant info in abstraction domain, it's going to be subjected to the losses if the image undergoes any image process technique like compression, cropping etc. to beat this drawback we have a tendency to implant {the info|the knowledge|the data} in frequency domain specified the key information is embedded on the numerous frequency values whereas higher frequency half is omitted. Transformation is 1st applied to the image so the info is hidden by dynamic the values of the transformation coefficients consequently. The transformations applied could also be quick Fourier remodel, distinct trigonometric function remodel and distinct rippling remodel. quick Fourier remodel (FFT) strategies introduce spherical off errors and therefore it's not appropriate for hidden communication [4].

III. PROPOSED SYSTEM

The proposed system combines the advantages of both spatial and transfer domain process. The proposed system is separated into the following module's.

A. Transfer Domain

The DWT is applied to the cover image. Wavelet transform decomposes a signal into a set of functions called wavelets. The wavelet coefficients separate the high and low frequency information on a pixel to pixel basis. Haar DWT wavelet transform approach is used in which time domain is passed through low-pass and high-pass filters and the high and low frequency wavelet coefficients are generated by taking the difference and average of the two pixel values respectively. The operation of Haar DWT on the cover image results in the formation of 4 sub-bands, namely the approximate band (LL), horizontal band (HL), vertical band (LH) and the diagonal band (HH) as shown in Fig.1. The approximate band contains the most significant information of the spatial domain image and other bands contain the high frequency information such as edge details. Thus, the DWT technique describes the decomposition of the image in four non overlapping sub-bands with multi-resolution. Any modifications done to the LL band will result is observable distortion in the image. Thus the secret message to be hidden is replaced in the LH, HL and HH bands.

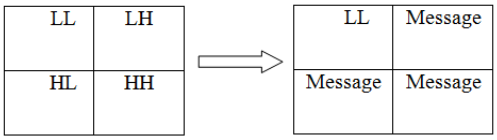

Fig.1. Basic DWT image

To further increase the embedding capacity a second level DWT is applied to the carrier image. This leads to the decomposition of LL band into LL, LH, HL and HH sub-bands as shown in Fig.2.

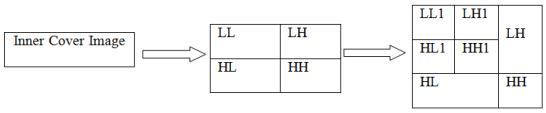

Fig.2. 2D DWT

The secret message to be embedded is then hidden in the LH, HL, HH bands on 1D DWT and LH,HL,HH sub bands of 2D DWT and results in the inner stego image.

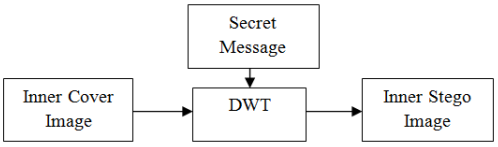

Fig.3. Stego image of transfer domain

Inverse DWT is then applied to the modified carried image to result in stego image. At the receiver side DWT is applied to the stego image. The message pixels are extracted from the corresponding bands and the original message is reconstructed.

B. Preprocessing – Image Enhancement

The cover image of spatial domain is subjected to preprocessing step which leads to image enhancement. The preprocessing imposes more variation in pixel intensities of cover image compared to the original one. The hiding of secret data in cover image which has more pixel value variation [5] are less detectable by the statistical steganalysis methods[6].The cover image is contrast enhanced which

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue X, October 2016

increases the payload of the image without compromising the visual quality.

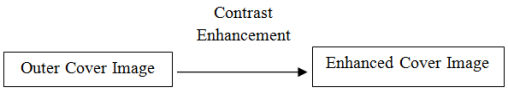

Fig.4. Cover image enhancement

C. Spatial Domain

The resultant stego image from the first layer of security is then hidden in another cover image using LSB replacement. Adaptive steganography is followed in which the embedded bit depends on the second least significant bit and the information bit. There are four rules based upon which value of least significant bit is calculate and then replaced. This would lead to increase in robustness.

TABLE I. ENHANCED XOR ALGORITHM

Second LSB of Image	Bit of Information to be Hidden	Resultant LSB bit to be Replaced
0	0	1
0	1	0
1	0	0
1	1	1

Replacing in consecutive LSB bits cannot stand against most steganalysis attack. Thus instead of substituting LSB of consecutive bytes, the LSB of bytes to be replaced is selected using a random number generator. Random encoding will make the message bits more difficult to find and hopefully reduce the realization of patterns in the image.

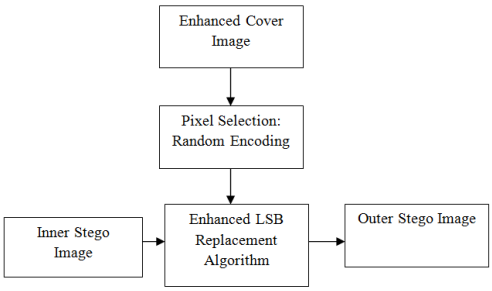

Fig.5. Stego image of spatial domain

D. Cryptography

Cryptography is embedded together with steganography to enhance security. An encryption key is used. Only if the correct key is entered at the decrypting side the secret message is extracted.

IV. IMPLEMENTATION

MATLAB is used to implement the stego image generation and extraction module.

A. Stego Image Generation Module

Input: Inner Cover Image, Outer Cover Image, Encryption Key, Secret Message
Output: Outer Stego Image
Step 1: DWT is applied to the inner cover image and the secret message is embedded in the LH, HL, HH region. This results in the inner stego image.
Step 2: The outer cover image is enhanced by a contrast enhancement algorithm.
Step 3: The pixels in which the secret message is to be embedded is selected using the random number generator.

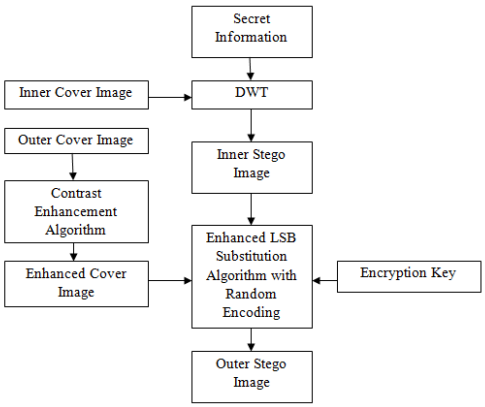

Fig.6. Stego image generation module

Step 4: The inner stego image is then embedded in the enhanced cover image. The bits of the secret message are embedded in the cover image by using the enhanced LSB algorithm. The 2nd LSB of the cover image is XORed with the secret bit to be embedded and the resultant bit is embedded in LSB of cover image. This results in the outer stego image.
Step 5: The stego image is then encrypted with the key.
The resultant encrypted stego image is ready for transmission.

B. Stego Image Extraction Module

Input: Outer Stego Image, Decryption Key
Output: Secret Message
Step 1: The decryption key entered is checked with the encryption key. If both match the successive steps are executed else an error message is prompted.
Step 2: The pixels of the stego image is selected. In the selected pixels , the 7th and 8th bit are XORed and the result obtained is used to construct the inner stego image.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue X, October 2016

Step 3: Two level DWT is applied to the inner stego image and the secret message is extracted from the LH, HL,HH bands and LH1,HL1 and HH1 sub-bands.

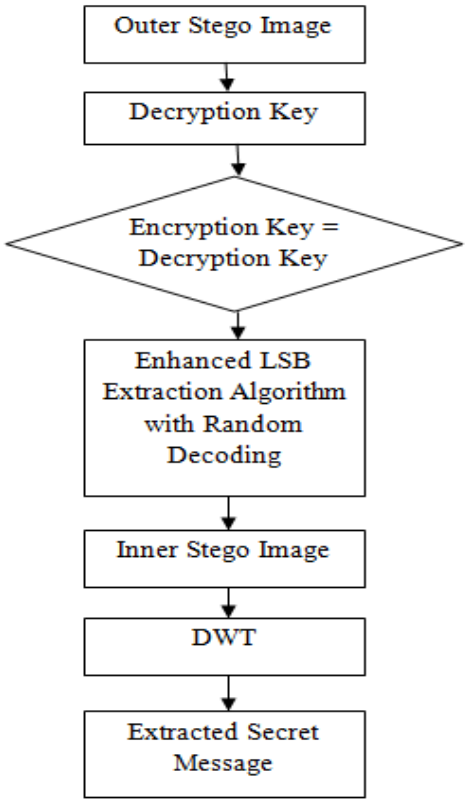

Fig.7. Stego image extraction module

Following are results of the system that uses LSB algorithm for hiding text in an image and again uses another image for hiding image that contains hidden message. In this example Figure 8 shows input image as follows.

Figure 8 Input Image

The text image with sequential encoding technique or random encoding with key encryption between the range 0-255 is encrypted with the above figure 8 and text file with "hi" message as shown in figure 9.

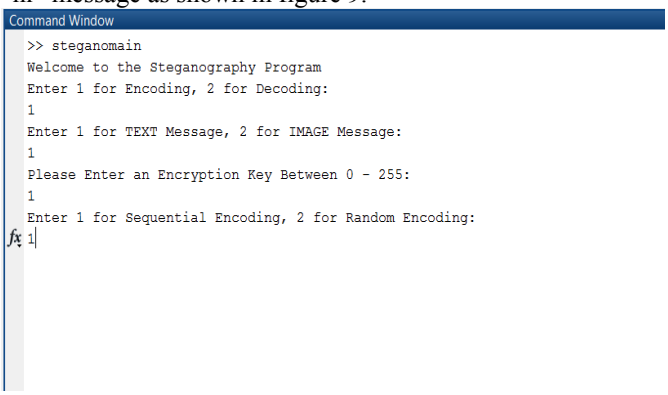

Figure 9 Encoding process

The decryption of image with the text file output is shown in figure 10 as follows.

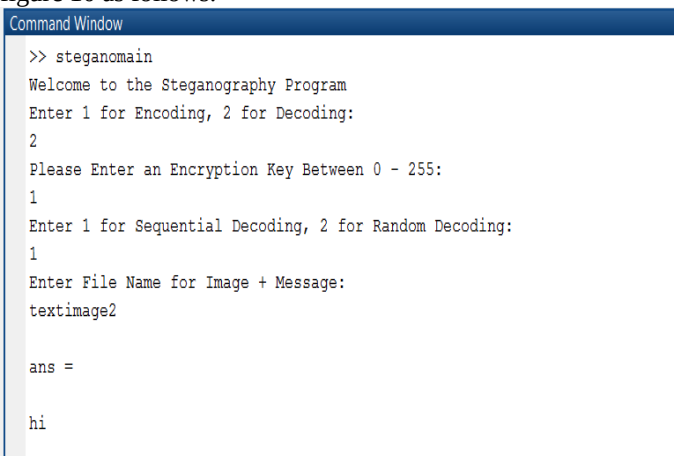

Figure 10 Decoding Process

The image steganography with another image using sequential encoding or random encoding is made. The encoding image are shown in figure 11 with the figure 8 as follows.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue X, October 2016

Figure 11 Input image

The decoding of image file with sequential/ random decoding process obtains an output as shown in figure 12.

Figure 12 Decoded Image

VI. Conclusion And Future Work

1) The usage of both transfer domain and spatial domain technique leads to high level of security.

2) The inclusion of cryptography feature of usage of secret key at encryption and decryption side further adds to the security.

3) The enhanced LSB algorithm serves to increase the image quality.

4) Random Encoding helps to withstand steganalysis attack.

5) The usage of image enhancement technique leads to increased embedding capacity.

The future work will be focused extending the algorithm to audio and video messages. Algorithms which further lead to more embedding capacity and robustness to be implemented.

References

[1] T. Morkel, J. Eloff, and M. Olivier, "An Overview of Image Steganography," The Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, July 2005.

[2] R. Chandramouli and N. Memon, “Analysis of LSB based image steganography techniques,” International Conference On Image Processing, 2001,p.1019-1022.

[3] Vishal, Wilson and Bryon, “Linear, color separable human visual system model for vector diffusioning system”, Journal of Electronic Imaging, Vol.1,pp.277-292, 1992.

[4] K..B. Raja, C.R. Chowdary, K.R. Venugopal and L.M. Patnaik, “A secure image steganography using LSB, DCT and compression techniques on raw images,” Proceedings of IEEE 3rd International Conference on Intelligent Sensing and Information Processing, ICISIP’05, Bangalore, India, 14-17 Dec. 2005, pp.170-176.

[5] H. Sajedi, and M. Jamzad.,”BSS: Boosted steganography scheme with cover image preprocessing,” Expert Systems Appl. 2010, 37, 7703–7710.

[6] B.E. Carvajal–Gamez, F.J. Gallegos–Funes and A.J. Rosales Silva, ”Color local complexity estimation based steganographic (CLCES) method,” Expert Systems Appl.2013, 40, 1132–1142.

BIBLIOGRAPHY

Mrs.M.Narmatha working as Assistant Professor in the Department of Computer Science, Sri Jayendra Saraswathy Maha Vidyalaya College of Arts and Science, Singanallur,

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue X, October 2016

Coimbatore. She has 7.5 years of teaching experience. Her area of interest Networking.

Suja G.P Received the Bachelor of science Degree in Department Of Computer Science , Bishop Ambrose College Of Arts And Science ,Coimbatore. She Completed her Master of Science Degree in Department Of Computer Science , Sri Jayendra Saraswathy Maha Vidyalaya College Of Arts And Science, Coimbatore . She is Currently Pursuing her Master Of Philosophy in Computer Science , Sri Jayendra Saraswathy Maha Vidyalaya College Of Arts And Science .Her Area Of Interest is Software Engineering and Software Project Managament.