International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.1, No.7, November 2012 DOI:10.15693/ijaist/2012.v1i7.39-43

Data Embedding in Gray Scale Image Using Wavelet Transform for Secure Communication

S. Uma Maheswari
M.Tech(Communication Systems)
PRIST UNIVERSITY.

K.R.Vinothini
Assistant Professor(Sl.Gr)/ECE
A.V.C College of Engineering.

K.Nivitha
Assistant Professor(Sr.Gr)/ECE
A.V.C College of Engineering.

***Abstract*- In this world now a day, secure our information plays a vital role because, the unauthorized person may misuse the information (or) data during the transmission across the wireless link. In order to avoid this type of situation, our project introduced the method called secure data transmission. In this method, wavelet based steganography is used. A wavelet based steganography is a new idea in the wavelet application. There are two process involved in this method. They are embedding process and extraction process. The concept of this paper is, a message is embedded in to the cover image C through an embedding algorithm using secret key. So, that the cover image (C) is changed to stego image (S).The stego image is then transmitted through the Stegosystem(Channel) and it can be extracted using the same secret key through an extraction algorithm. During the transmission, the unauthorized person may have the chance to monitor the image but he/she can monitor only the image without discovering the existence hidden message. The pixels in the cover image(C) is selected for embedding the information using pixel mapping method. So, there will be no degrading in the stego image(S) compared to the cover image(C).**

Key Word: Steganography, Wavelet transform, Pixel mapping method (PMM).

I INTRODUCTION

Data hiding is the art of hiding a message signal in a host signal without any perceptual distortion of the host signal. The composite signal is usually referred to as the stego signal. Data hiding is a form of subliminal communication. Any form of communication relies on a channel or medium. Data hiding, or Steganographic, communications rely on the channel used to transmit the host content. As the stego content moves around the globe, perhaps over the Internet, or by any other means usually deployed for communicating the host signals, so does the embedded, covert message signal. The Block diagram of this technique is also given.

II BLOCK DIAGRAM

A Block diagram of embedding process is shown in the Fig.1

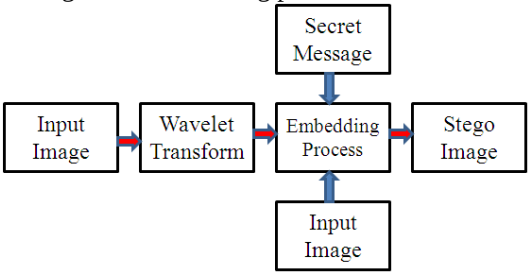

Fig.1 Embedding Process

A Block diagram of extraction process is shown in the Fig.2

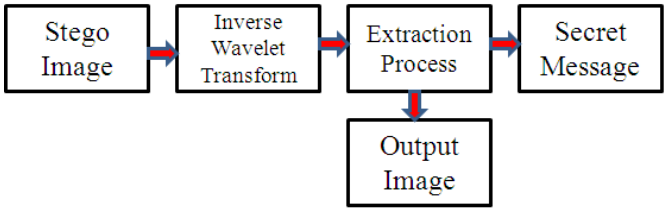

Fig.2 Extraction Process

III STEGANOGRAPHY SYSTEM

A Block diagram of image steganography system is shown in the Fig 3

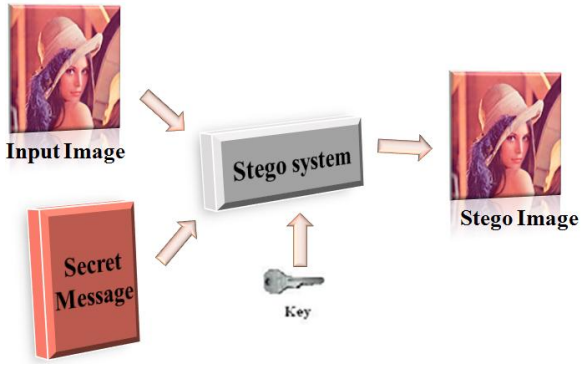

Fig 3: A Generic form of Steganographic system

A message is embedded in a digital image (cover image) through an embedding algorithm, with the help of a secret key. The resulting stego image is transmitted over a channel to the receiver where it is processed by the extraction algorithm using the same key. During transmission the stego image, it can be monitored by unauthenticated viewers who will only notice the transmission of an image without discovering the existence of the hidden message.

A. Image Steganographic Techniques

The various image Steganographic techniques are: (i) Substitution technique in Spatial Domain: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even

simple attacks such as compression, transforms, etc. (ii)Transform domain technique: The various transform domains techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) are used to hide information in transform coefficients of the cover images that makes much more robust to attacks such as compression, filtering, etc. (iii) Spread spectrum technique: The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information. The SNR in every frequency band is small. Hence without destroying the cover image it is very difficult to remove message completely. (iv)Statistical technique: The cover is divided into blocks and the message bits are hidden in each block. The information is encoded by changing various numerical properties of cover image. The cover blocks remain unchanged if message block is zero. (v) Distortion technique: Information is stored by signal distortion. The encoder adds sequence of changes to the cover and the decoder checks for the various differences between the original cover and the distorted cover to recover the secret message.
Among all these five techniques we have chosen a technique called Transform domain techniques. Let us see this technique briefly.

B. Transform Domain Technique

The widely used transformation functions include Discrete Cosine Transformation (DCT), Fast Fourier Transform (DFT), and Wavelet Transformation. The basic approach to hiding information with DCT, FFT or Wavelet is to transform the cover image, tweak the coefficients, and then invert the transformation. If the choice of coefficients is good and the size of the changes manageable, then the result is pretty close to the original. Let us briefly discuss about the two methods of transform domain techniques.

(i)DCT Based Data Hiding

DCT is a mechanism used in the JPEG compression algorithm to transform successive 88-pixel blocks of the image from spatial domain to 64 DCT coefficients each in frequency domain. Some DCT based steganographic work has been given in [2], [3] and [4].

In our project we have chosen a DWT based data hiding.

(ii)DWT Based Data Hiding

Wavelet-based steganography [1], [5], [6], [7] and [8], [9] is a new idea in the application of wavelets. However, the standard technique of storing in the least significant bits (LSB) of a pixel still applies. The only difference is that the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels. The idea is that storing in the least important coefficients of each 4 x 4 Haar transformed block will not perceptually degrade the image. While this thought process is inherent in most steganographic techniques, the difference here is that by storing information in the wavelet coefficients, the change in the intensities in images will be imperceptible.

IV PIXEL MAPPING METHOD

Pixel Mapping Method is a method for information hiding within the spatial domain of any gray scale image. Embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the seed pixel and its 8 neighbors are selected in counter clockwise direction. Before embedding a checking has been done to find out whether the selected embedding pixels or its neighbors lies at the boundary of the image or not. Data embedding are done by mapping each two or four bits of the secret message in each of the neighbor pixel based on some features of that pixel.Fig.4 shows the mapping information for embedding two bits or four bits respectively. Extraction process starts again by selecting the same pixels required during embedding. At the receiver side other different reverse operations has been carried out to get back the original information.

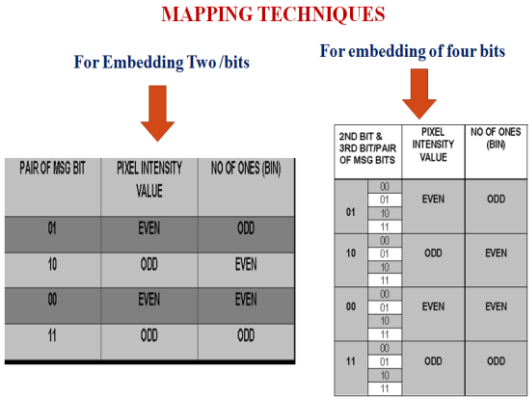

Fig 4: For Embedding two and four bits

A. Pixel Selection Method

Random Pixel Generation for embedding message bits is dependent on the intensity value of the previous pixel selected. It includes a decision factor (dp) which is dependent on intensity with a fixed way of calculating the next pixel. The algorithm for selection of pixel for embedding is described below:

- Input: C , previous pixel position (x,y),pixel intensity value (v).
- Consider dp (Decision Factor)=1 if (intensity ≤80),dp=2 if (intensity ≥ 80 & ≤ 160) ,dp=3 if(intensity > 160 & ≤ 255).
- t = x+2+dp.
- if (t ≥ N)m = 2, n = y +2+dp.
- else m = x+2+dp, n = y.
- Return m and n.
- End.

122	45	69	132	256	145	56	79	112
156	125	169	123	79	78	12	186	123
224	212	145	125	147	86	45	110	236
119	248	46	112	48	23	79	45	90
119	79	116	189	53	63	130	90	141
56	71	26	83	43	75	93	67	116
90	112	179	212	201	38	99	119	157
83	53	89	115	63	78	90	76	255
131	141	176	159	126	146	255	73	86

Fig 5.Snapshot of selected pixels for embedding.

V PROPOSED SYSTEMS

In the proposed systems the input messages can be in any digital form, and are often treated as a bit stream. The proposed approach works by converting the gray level image in transform domain using discrete integer wavelet technique through lifting scheme[10], [11] and [12].This approach performs a 2-D lifting wavelet decomposition through Haar lifted wavelet of the cover image and computes the approximation coefficients matrix CA and detail coefficients matrices CH, CV, and CD. Next step is to apply the PMM [13] technique for 2 bit embedding in those coefficients for embedding the secret message and apply the inverse transformation on those wavelet coefficients to form the stego image. Embedded wavelet coefficients are selected based on some mathematical function which depends on the intensity value of the seed coefficient and its 8 neighbors are selected in counter clockwise direction. Extraction process starts again by selecting the same wavelet coefficients required during embedding. At the receiver side other different reverse operation has been carried out to get back the original information.

VI WAVELET TRANSFORM

Wavelet domain techniques are becoming very popular because of the developments in the wavelet stream in the recent years.Wavelet transform is used to convert a spatial domain into frequency domain. The use of wavelet in image stenographic model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis.

The wavelet lifting scheme is a method for decomposing wavelet transform into a set of stages. An advantage of lifting scheme is that they do not require temporary storage in the calculation steps and have required less no of computation steps. The lifting procedure consists of three phases, namely, (i) split phase, (ii) predict phase and (iii) update phase.

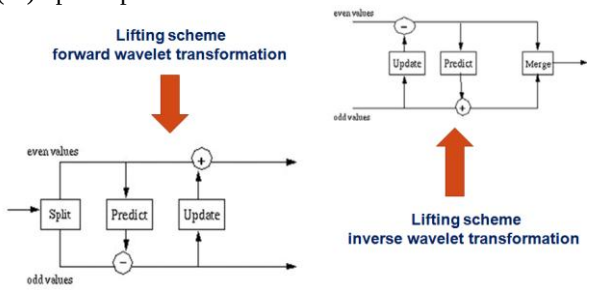

Fig 6: Lifting Scheme forward wavelet and inverse wavelet transformations.

Splitting: Split the signal x into even samples and odd samples: xeven : si ← x2i, xodd : di ← x2i+1
Prediction: Predict the odd samples using linear interpolation: di ← di − (si+si+1) 2
Update: Update the even samples to preserve the mean value of the samples:si ← si + (di−1+di) 4
The output from the s channel provides a low pass filtered version of the input where as the output from the d channel provides the high pass filtered version of the input. The inverse transformed is obtained by reversing the order and the sign of the operations performed in the forward transform.

VII EXPERIMENTAL RESULTS

A. Embedding Process

Step 1: Browse the cover image from the file that to be transmitted through the channel.
Step 2: Preprocess the cover image if required.
Step 3: Apply the wavelet transform to convert the cover image C in to stego image S.
Step 4: Generate the 4 bit secret key for secure transmission.
Step 5: Finally, embed the cover image and secret message "**I am an Indian and I proud to be an Indian**"

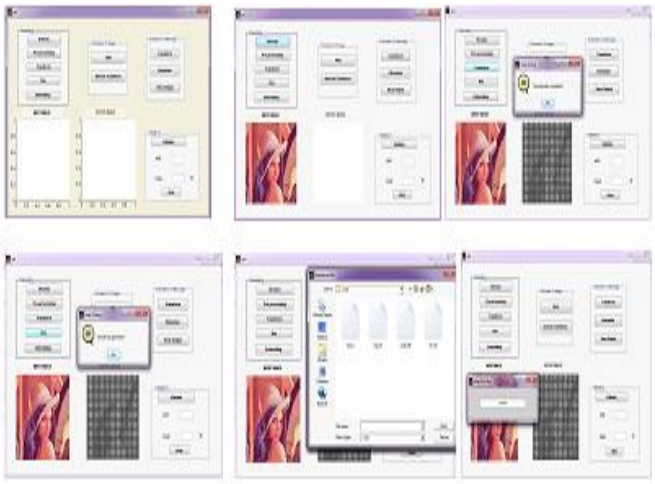

Fig 7: Embedded Steps involved in proposed system.

B. Extraction Process

(i)Extraction of image

Step 1: Apply the inverse wavelet transform to regenerate the cover image C.

Thus, we get an original image cover image C without any degradation.

(ii)Extraction of Secret message

Step 2: Enter the same 4 bit secret key to extract the secret message.
Step 3: Finally view the secret message as "**I am an Indian and I proud to be an Indian"**

Fig 8: Extraction Steps involved in proposed systems.

VIII CONCLUSION

The work dealt with the techniques for steganography in wavelet domain as related to gray scale image. A new and efficient Steganographic method for embedding secret messages into images without producing any major changes has been proposed. Although in this method it has been shown that each two bit of the secret message has been mapped in the pixels of the cover image, but this method can be extended to map n no of bits also by considering more no of features of the embedding pixels. This method is also capable of extracting the secret message without the cover image. This approach may be modified to work on color images also.

REFERENCES

[1] *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, 7:358–364, 2010.*
[2] *R K Chhotaray K B Shiva Kumar, K B Raja and Sabyasachi Pattanaik. Bit length replacement steganography based on dct coefficients. International Journal of Engineering Science and Technology, 2:3561–3570, 2010.*
[3] *Ajit Danti and Preethi Acharya. Randomized embedding scheme based on dct coefficients for image steganography. IJCA Special Issue on Recent Trends in Image Processing and Pattern Recognition, 2010.*
[4] *Chia-Chen Lin. High capacity data hiding scheme for dct-based images.Journal of Information Hiding and Multimedia Signal Processing, 1,2010.*
[5] *Bo Yang and Beixing Deng. Steganography in gray images using wavelet. In Proceedings of ISCCSP 2006.*
[6] *Po-Yueh Chen and Hung-Ju Lin. A dwt based approach for image steganography. International Journal of Applied Science and Engineering, 4:275–290, 2006.*
[7] *Dr.S.T.Gandhe K.T.Talele and Dr.A.G.Keskar. Steganography security for copyright protection of digital images using dwt. (IJCNS) International Journal of Computer and Network Security, 2:21–26, 2010.*
[8] *H S Manjunatha Reddy and K B Raja. High capacity and security steganography using discrete wavelet transform. International Journal of Computer Science and Security (IJCSS), 3:462–472.*
[9] *V. Kumar and D. Kumar. Performance evaluation of dwt based image steganography. In Proceedings of Advance Computing Conference (IACC), 2010 IEEE 2nd International, pages 223–228, 2010.*
[10] *W. Sweldens R. Calderbank, I. Daubechies and B.L. Yeo. Wavelet transforms that map integers to integers. Appl. Comput. Harmon. Anal., 5:332–369, 1998.*
[11] *W. Sweldens. The lifting scheme. A construction of second generation wavelets. SIAM J. Math. Anal., 29:511–546, 1997.*
[12] *Geert Uytterhoeven Dirk Roose Adhemar Bultheel. Integer wavelet transforms using the lifting scheme. In CSCC Proceedings, 1999.*
[13] *Souvik Bhattacharyya. and Gautam Sanyal. Hiding data in images using pixel mapping method (pmm). In Proceedings of 9th annual Conference on Security and Management (SAM) under The 2010 World Congress in Computer Science,Computer Engineering, and Applied Computing(WorldComp 2010), LasVegas,USA, July 12-15,2010.*
[14] *N. Jacobsen, K. Solanki, U. Madhow, B. S. Manjunath, and S. Chandrasekaran,"Image-adaptive high-volume data hiding based on scalar quantization," in Proc. IEEE Military Commun. Conf., Anaheim, CA, Oct. 2002.*
[15] *R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," in Proc. ICIP, Oct. 2001.*
[16] *J. Eggers, R. Buml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," IEEE Trans. Signal Processing, vol. 51, pp. 1003–1019, Apr. 2003.*
[17] *J. Fridrich, R. Du, and M. Long, "Steganalysis of LSB encoding in color images," in Proc. ICME, New York, July 31–Aug. 2, 2000.*
[18] *N. F. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software," in Information Hiding, D. Aucsmith, Ed. New York: Springer-Verlag, 1998, pp. 32–47.*
[19] *A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems,"in Information Hiding, A. Pfitzmann, Ed. New York: Springer-Verlag,1999, pp. 61–76.*

[20] *A. Westfeld, "Detecting low embedding rates," in Proc. Inf. Hiding Workshop, Springer LNCS, vol. 2578, 2002, pp. 324–339.*

Authors Profile

S.Uma Maheswari received the **B.E.** degree in Electronics and Communication Engineering from the A.V.C College of Engineering, Mayiladuthurai, India, in 2011. Currently doing **M.Tech** degree in Communication Systems from PRIST University, Tanjore, India. Her research interest includes Steganography, Embedded Systems and Digital image processing.

K.R.Vinothini received the **B.E.** degree in Electronics and Communication Engineering from the A.V.C College of Engineering, Mayiladuthurai, India, in 2002.**M.E** degree in Power Elctronics drives Jerusalem college of Engineering, Pallikaranai, Chennai, India in 2006. Her research interest includes Microwave Engineering, cryptography and network security and Digital image processing.

K.Nivitha received the **B.E.** degree in Electronics and Communication Engineering from the Periyar Maniammai College of technology for women, Tanjore, India, in 2009. **M.E** degree in VLSI Design from Easwari engineering college, Chennai, India, in 2012. Her research interest includes VLSI, Testing of VLSI circuits, cryptography and Digital image processing.