Lossless Remodel Records Hiding In Encrypted Images Using Wavelet Transforms

Balaji.M[1] ,T.Bathinababu[2]
Department of ECE
[1, 2]Seshachala Institute Of Technology,Puttur

Abstract-*Steganography gained importance in the past few years due to the increasing need for providing secrecy in an open environment like the internet. With almost anyone can observe the communicated data all around, steganography attempts to hide the very existence of the message and make message undetectable. Many techniques are used to secure information such as cryptography that aims to scramble the information sent and make it unreadable while steganography is used to conceal the information so that no one can sense its existence. In most algorithms used to secure information both steganography and cryptography are used together to secure a part of information.*

Steganography has many technical challenges such as high hiding capacity and imperceptibility. In this thesis, we try to optimize these two main requirements by proposing a novel technique for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of different wavelet transforms likeHaar, Daubechies2, Biorthogonal3.5, coiflet2, symlets4 and the cover image with the optimum pixel adjustment (OPA) algorithm.

The coefficients used are selected according to a pseudorandom function generator to increase the security of the hidden data. The OPA algorithm is applied after embedding secret message to minimize the embedding error. The proposed system showed high hiding rates with reasonable imperceptibility compared to other steganographic systems.

Keywords*-*Stegnography, DCT, DWT, Data hiding of Digital Images.

I. INTRODUCTION

1.1 Steganography

Steganography is the art and science of hiding secret data in plain sight without being noticed within an innocent cover data so that it can be securely transmitted over a network. The word steganography is originally composed of two Greek words steganos and graphia, which means "covered writing". The use of steganography dates back to ancient times where it was used by Romans and ancient Egyptians. The interest in modem digital Steganography started by Simmons in 1983 when he presented the problem of two prisoners wishing to escape and being watched by the warden that blocks any suspicious data communicated between them and passes only normal looking one. Any digital file such as image, video, audio, text or IP packets can be used to hide secret message. Generally the file used to hide data is referred to as cover object and the term stego-object is used for the file containing secret message.

Among all digital file formats available nowadays image files are the most popular cover objects because they are easy to find and have higher degree of distortion tolerance over other types of files with high hiding capacity due to the redundancy of digital information representation of an image data.

There are a number of steganographic schemes that hide secret message in an image file; these schemes can be classified according to the format of the cover image or the method of hiding. We have two popular types of hiding methods; spatial domain embedding and transform domain embedding. The Least Significant Bit (LSB) substitution is an example of spatial domain techniques. The basic idea in LSB is the direct replacement of LSBs of noisy or unused bits of the cover image with the secret message bits. Till now LSB is the most preferred technique used for data hiding because it is simple to implement offers high hiding capacity, and provides a very easy way to control stego-image quality but it has low robustness to modifications made to the stego-image such as low pass filtering and compression and also low imperceptibility. Algorithms using LSB in grayscale images can be found.

The other type of hiding method is the transform domain techniques which appeared to overcome the robustness and imperceptibility problems found in the LSB substitution techniques. There are many transforms that can be used in data hiding, the most widely used transforms are; the discrete cosine transform (DCT) which is used in the common image compression format JPEG and MPEG, the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT). Examples to data hiding using DCT can be found.

Most recent researches are directed to the use of DWT since it is used in the new image compression format JPEG2000and MPEG4, examples of using DWT can be found. In the secret message is embedded into the high frequency coefficients of the wavelet transform while leaving the low frequency coefficients sub band unaltered. While in an adaptive (varying) hiding capacity function is employed to determine how many bits of the secret message is to be embedded in each of the wavelet coefficients. The advantages of transform domain techniques over spatial domain techniques are their high ability to tolerate noises and some signal processing operations but on the other hand they are computationally complex and hence slower . In all proposed techniques for steganography whether spatial or transform the key problem is how to increase the size of the secret message without causing noticeable distortions in the cover object. Some of these techniques try to achieve the high hiding capacity low distortion result by using adaptive techniques that calculate the hiding capacity of the cover according to its local characteristics.

.

The steganographic transform-based techniques have the following disadvantages; low hiding capacity and complex computations. Thus, to get over these disadvantages, the present paper proposes an adaptive data hiding technique joined with the use of optimum pixel adjustment algorithm to hide data into the integer wavelet coefficients of the cover image in order to maximize the hiding capacity as much as possible. We also used a pseudorandom generator function to select the embedding locations of the integer wavelet coefficients to increase the system security.

II. PROPOSED SYSTEM

The proposed novel method for RDH in encrypted image is encryption after allocating some space. In the proposed method, we first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then embed the image with some data, so the positions of the bits in the encrypted image can be used to embed data. Real data hiding with data concealment is realized, that is, data extraction and image recovery are free of any error. For given embedding rates, the PSNR so encrypted image containing the embedded data can be improved and for the satisfactory error occurrences, the range of embedding rate is greatly enlarged.

The method in segments the encrypted image into a number of non-overlapping blocks sized by each block is used to carry one additional bit. To do this, pixels in each block are gathered and divided into two sets and according to a data hiding key. For data extraction and image recovery, the receiver alters the pixels in to a new decrypted block. One of them will be decrypted to the original block. Due to spatial correlation in natural images, original block is presumed to Be a lot smoother than interfered block and embedded bit can be extracted correspondingly. Moreover, there's a trouble in bit extraction and picture recovery whilst divided block is quite small or has plenty specific textures.

The new framework "Reserving room before encryption" Since losslessly vacating room from the encrypted pix is noticeably tough and on occasion inefficient, If we opposite the order of encryption and vacating room, i.E., reserving room prior to photograph encryption at content material proprietor facet, the RDH duties in encrypted photos could be more natural and a lot less difficult which leads us to the novel framework,"booking room earlier than encryption (RRBE)" [1]. In order to successfully realise digital photograph encryption and decryption, two one-dimensional discrete Chebyshev chaotic sequences are used for row and column scrambling of the pixels of authentic and encrypted digital pictures. Experiment results indicates that the encrypting set of rules in all fairness viable and effective, and can make certain encrypted images enough security in their garage and transmitting tactics.

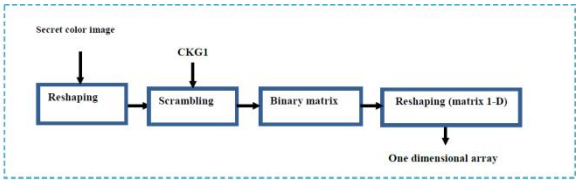


Figure (1) Block diagram for preprocessing stage

2.1 Lifting wavelet transform

The lifting scheme of DWT is an algorithm to implement wavelet transforms in an efficient way. It is also a wonderful method to create so-called second-generation wavelets. The lifting wavelet transform is a multi-resolution representation that means the signal divided to two parts the first called approximation sub-band and second part named detail sub-band these parts are obtained by applying corresponding wavelet filters (high-pass filter, low-pass filter). Generally lifting scheme consists of three steps, Splitting, production, and update [4, 5]:

2.2 Splitting (Lazy wavelet transform)

This stage splits entire set of signal to two frames. One frame consists of even index samples such as ($\lambda 0,0$,$\lambda 0,2$, $\lambda 0,4$,…… $\lambda 0,2\ k$) we will call this frame as smoother resolution signal or approximation other frame consists of odd

samples or call as detail such as ($\lambda 0,1$, $\lambda 0,3$, $\lambda 0,5$……. $\lambda 0,2k+1$).

New sequence can be given as: $\lambda -1, = \lambda 0,2k$ where $k \in Z$.

The sequence $\gamma -1$, can be given as: $\gamma -1 , k = \lambda 0,2k+1$, Where $k \in Z$.

Minus sign indicates that new data set is smaller compare to the original data set.

2.3 Prediction (Dual lifting)

Predict the odd samples by using linear interpolation predict the odd coefficient based on a linear combination of even samples and odd samples (replace (**λ0**,+**1**) with $\gamma -1 , k$) as follow:

$\gamma -1 , = \lambda 0,2k+1 - P \quad \lambda -1,k \quad \cdots\cdots\cdots (1)$

Odd value Predicted value

$P \quad \lambda -1, \quad = 12 (\lambda -1, + \lambda -1.k+1) \ldots\ldots (2)$

Substitute's equation (2) in (1) getting equation (3):

$\gamma -1 , = \lambda 0 , 2k+1 - 12 (\lambda -1,k + \lambda -1.k+1 \ldots.. (3)$

2.4 Update (Primal lifting)

Update the even samples based on a linear combination of difference samples obtained from the predict step [4, 5]. We require constructing update operator U for this lifting process.

$U(\gamma -1)=14 \quad \gamma -1,k-1+\gamma -1,k \quad \cdots\cdots\ldots (5)$

$\lambda -1, = \lambda 0,2k+14 \quad \gamma -1,k-1+\gamma -1,k \quad \cdots.(6)$

Figure (1) represents forward transform scheme of three stages for multi levels of LWT.

To finding level 2 equation (3) and equation (7) become as follows:

$\gamma -2 , = \lambda -1 , 2k+1 - 12 (\lambda -2,k + \lambda -2.k+1 \ldots.(11)$

$\lambda -2, = \lambda -1,2k+14 \quad \gamma -2,k-1+\gamma -2,k \quad \ldots.(12)$

III. INVERSE WAVELET TRANSFORM

Inverse wavelet transform is exactly reverse process of forward wavelet transform in lifting scheme it is very easy to find out inverse wavelet transform because it can be obtained by just changing sign. Inverse lifting wavelet transform consists of following steps [6]:

- Undo Update (Inverse Primal Lifting): Original even samples are recovered by simply subtracting the update information. The Equation (8) represents undo update, which is obtained by changing sign in Equation (7).

$\lambda -1, = \lambda 0,2k-14 \quad \gamma -1,k-1+\gamma -1,k \quad \cdots(8)$

- Undo Predict (Inverse Dual Lifting): Odd samples can be recovered by adding prediction data to loss of data that can be given by Equation (9) by changing sign in equation (3)

$\gamma -1 , = \lambda 0 , 2k+1+ 12 (\lambda -1,k + \lambda -1.k+1 \ldots.(9)$

- Merge: After recovering odd and even samples, final job is to merge them together to get original signal.

$\lambda 0,k = Merge \quad \lambda -1 , \gamma -1 \quad \cdots.(10)$

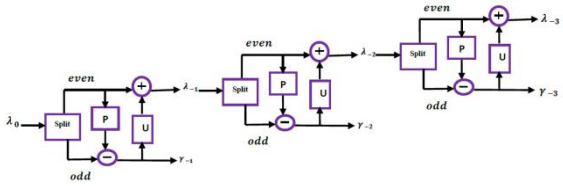
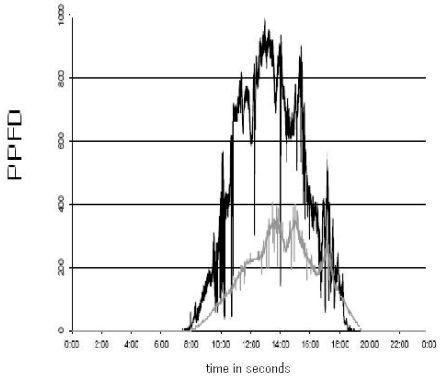


Figure 2 multilevel wavelet transform with lifting scheme

IV. EXPECTED RESULTS

A lot of analysis is made on the present method and a number of the computation have been applied on the large number of the data set in a well oriented fashion and also the takes place in the different types of the environment in a well effective fashion respective. A comparative analysis is made between the present method to that of the several previous methods in a well oriented fashion and the implementation of the system is shown in the below figure in the form of the graphical representation and is explained in the elaborative fashion respectively. Here the present method completely overcome the drawback of the several previous methods in a well oriented fashion respectively.



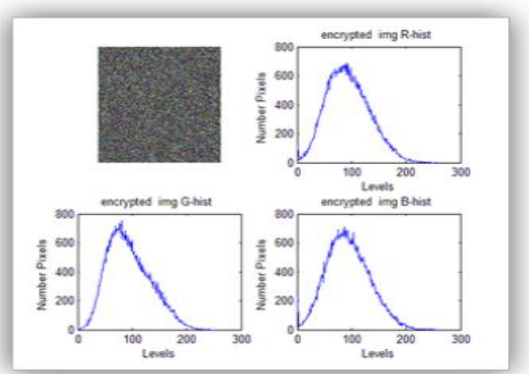


Fig 3: shows the graphical representation of the present method respectively

V. CONCLUSION

In this paper we proposed a novel data hiding scheme that hides data into the different integer wavelet coefficients of different wavelet transforms like Haar, Daubechies2, Biorthogonal3.5, coiflet2, symlets4 of an image. The system combines an adaptive data hiding technique and the optimum pixel adjustment algorithm to increase the hiding capacity of the system compared to other systems. The proposed system embeds secret data in a random order using secret key only known to both sender and receiver. It is an adaptive system which embeds different number of bits in each wavelet coefficient according to a hiding capacity function in order to maximize the hiding capacity without sacrificing the visual quality of resulting stego image.

The proposed system also minimizes the difference between original coefficients values and modified values by using the optimum pixel adjustment algorithm. The proposed scheme was classified into three cases of hiding capacity according to different applications required by the user. Each case has different visual quality of the stego-image. Any data type can be used as the secret message. There was no error in there covered message (perfect recovery) at any hiding rate. From the experiments and the obtained results the proposed system proved to achieve high hiding capacity up to 48% of the cover image size with reasonable image quality and high security because of using random insertion of the secret message.

The proposed system can be further developed to increase its robustness by using some sort of error correction code which increases the probability of retrieving the message after attacks, also investigating methods to increase visual quality of the stego-image (PSNR) with the obtained hiding capacity.

REFERENCES

[1] G. J. Simmons, "The prisoners' problern and the subliminal channel," in Proceedings of Crypto' 83, pp. 51-67, 1984.

[2] N. Wu and M. Hwang. "Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan. 2007.

[3] W. Chen, "A Comparative Study of Information Hiding Schernes Using Amplitude, Frequency and Phase Embedding," PhD Thesis, National Cheng Kung University, Tainan, Taiwan, May 2003.

[4] C. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469-474, Mar. 2004.

[5] Changa, C. Changa, P. S. Huangb, and T. Tua, "A Novel bnage Steganographic Method Using Tri-way Pixel-Value Differencing," Journal of Multimedia, Vol. 3, No.2, June 2008.

[6] H. H. Zayed, "A High-Hiding Capacity Technique for Hiding Data in images Based on K-Bit LSB Substitution," The 30th International Conference on Artificial Intelligence Applications (ICAIA - 2005) Cairo, Feb. 2005.

[7] A. Westfeld, "F5a steganographic algorithm: High capacity despite better steganalysis," 4th International Workshop on Information Hiding, pp.289-302, April 25-27, 2001.

[8] H. W. Tseng and C. C. Chnag, "High capacity data hiding in jpeg compressed images," Informatica, vol. 15, no. I, pp. 127-142,2004.