RESEARCH ARTICLE OPEN ACCESS

A Secure & Optimized Data Hiding Technique Using DWT With PSNR Value

Farheen Fatima[1], Dr.Deepak Arora[2]
[1]*Amity University, Lucknow, India*
[2]*Amity University, Lucknow, India*

ABSTRACT
Multimedia applications are becoming increasingly significant in modern world. The mushroom growth of multimedia data of these applications, particularly over the web has increased the demand for protection of copyright. Digital watermarking is much more acceptable as a solution to the problem of copyright protection and authentication of multimedia data while working in a networked environment. In this paper, a DWT based watermarking scheme is proposed. We have used Genetic Algorithm (GA) in order to make an optimum tradeoff between imperceptibility and robustness by choosing an optimum watermarking level for each coefficient of the cover image. In addition to the suitable watermarking strength, the selection of best block size is also necessary for superior perceptual shaping functions. To achieve this goal we have trained and used GA to pick the best block size to tailor the watermark in one of the coefficients of the DWT. The fitness function criterion for the genetic algorithm decision making is based on PSNR values.

Keywords: Steganography,Watermarking,Discrete Wavelet Transform,Genetic Algorithm, Peak Signal to noise Ratio, Data Hiding.

I. INTRODUCTION

Data Hiding or Steganography offers an essential alternative to image integrity and authenticity problem. It is a kind of data hiding technique that provides another way of security protection for digital image data. Unlike utilizing a particular cipher algorithm to protect secret data from illicit access, the purpose of steganography is to embed secret data in preselected meaningful images, called cover images, without creating visually perceptible changes to keep an invader unaware of the existence of the secret. Digital data hiding is a multidisciplinary research area involving theory of communications, signal processing, multimedia coding, information theory, cryptography and computer science etc. Soft computing is one sub branch of computer science which may be used to achieve tractable, robust, low cost, optimal and adaptive solutions in data hiding problems. Fuzzy Logic (FL), Rough Sets (RS), Artificial Neural Networks (ANN), Genetic Algorithms (GA) and Support Vector Machine (SVM) etc. are the various components of soft computing and each one offers specific attributes. In data hiding problem, Genetic Algorithm(GA) may be used for optimizing the fundamentally conflicting requirements of imperceptibility, security and robustness. Neural network may be used to design robust watermarking for images to take advantages of relatively easy algorithmic specification,pattern mapping and classification. The feasibility of Support Vector Machine (SVM) may be explored to determine automatically where the significant blocks are and to what extent the intensities of the block pixels can be modified.

The proposed work is focused at achieving watermarking of digital gray scale images using Discrete Wavelet Transform (DWT), where the hidden message image is to be embedded in one of the coefficients out of the available four sub bands of a 2D-DWT transform of the cover image. The genetic algorithm based technique has been used to embed the hidden image to the original image. The rest of the paper gives a detailed description of the method and result and analysis on various images.

II. BACKGROUND

The word "Steganography" is a Greek word which literally means "covered or hidden writing". In other words Steganography is an art and science of hiding secret information behind the cover medium. It is the art of concealed communication. Cover medium can be any multimedia content like digital images, audio files or video files. K.B. Raja et al have mentioned that the main motive of steganography is to hide the existence of communication [1]. Steganography, watermarking and cryptography are the three fields which are closely interrelated to each other and belong to same family i.e. Security. Steganography and watermarking process is very difficult to differentiate especially for those which are from different disciplines. Figure 1 demonstrates the taxonomy of security system.

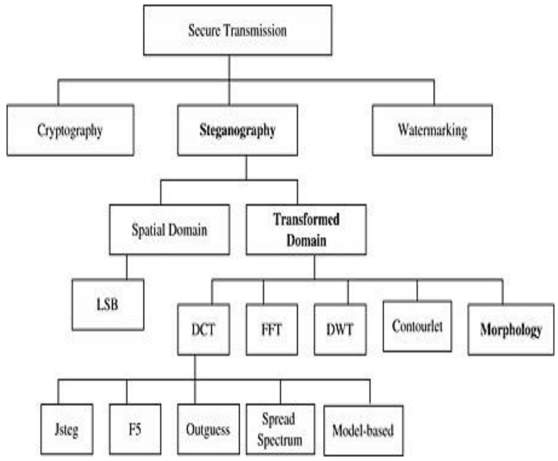

Fig 1: Taxonomy of Security Systems

GA are adaptive heuristic search algorithm based relying on the evolutionary thoughts of usual collection and inheritance. In [10]Gopesh Joshi's work stand for a bright development of a random investigation used to explain optimization problems. The basic technique of the Gas are planned to stimulate process in usual system essential for progress ,particularly those go after the standard laid down.GA are based on an similarity with the genetic structure and performance of chromosomes within a population of those. In the genetic algorithm crossover and mutation operators are used for to generate the optimized production in the crossover which represents the mate among those. And mutation which represent random modification, selection operator provide liking to better individuals, allow them to pass on their genes to the next generation. The honesty of all individual depends leading its fitness. In crossover operator main famous factor of GA from extra optimization techniques.

Let us suppose we have the chromosome:

$C = x+y*y-x/y$ (1)

And the appliance of mutation operator affect the genes.

Then a new obtained chromosome can be:

$C = x+x*y+x/y$ (2)

The value of the gene corresponding to the third position has been changed from y to x and the value of the gene corresponding to the sixth position ("-") to ("+").

Types of Steganography Technique

1) Spatial Domain Steganography

In spatial domain steganographic techniques secret information is directly embedded in pixel values i.e. pixels are directly altered to store secret messages. Basically these techniques are very simple but have greater impact then other techniques.

a) Least Significant Bit Substitution Algorithm: LSB substitution algorithm is simplest form of algorithm in which LSBs of the cover image is modified according to the secret message. It is simple yet effective technique of embedding secret data into images. Each pixel is of 8 bits in case of Gray scale images. Color RGB images use 24 bits to store color information each 8 bits for Red, Green and Blue components. The Advantages of this algorithm is simplicity and high perceptual efficiency. It can also achieve high embedding capacity but this algorithm is sensitive to image manipulations such as cropping, scaling and rotations, Lossy compression and addition of noise. There are number of variations of this algorithm including Edge and texture masking of cover image to determine the number k bits of LSBs for data embedding [3], Adaptive LSB algorithm based on brightness, optimized LSB algorithm using cat swarm and genetic algorithm [4,5], image steganography based on histogram modifications [6,7] etc. This research work mainly focuses on LSB steganography algorithm, so the rest of all the algorithms available in the literature will not be discussed in detail.

b) Pixel Value Differencing: This technique sub divides the cover image into non overlapping blocks consisting of two connecting pixels. This technique hides the data by altering the difference between two connected pixels. High difference in the cover image pixel value allows the higher alterations. Area of the pixel decides the hiding capacity of this technique for example if edge area is chosen then the difference is high in between the connecting pixels, whereas in smooth areas, difference is low.So ideal choice is to select edge areas to embed the secret message that is having more embedding capacity.As inferred by the results of D.Wu et al. [8], stego image produced by this technique has more quality and has better imperceptibility results .

c) Grey Level Modification: In this technique data is mapped by applying some modifications to the gray values of the image pixels. This technique will not hide or embed data, instead it map the data by using some mathematical functions. Set of pixels are selected for mapping using this mathematical function. It uses the concept of odd and even numbers for mapping the data in cover image. V.M.Potdar et al.[9] have given a technique in which high hiding capacity and low computational are some advantages of this technique.

2) Prediction based Steganography

In this technique pixel values are predicted with the help of predicator. This technique removes the loopholes of other techniques which directly embed the secret data into pixel values. In order to improve hiding capacity and visual quality it uses prediction error values (EV). EVs are altered to hide the secret data. It consists of two steps, namely prediction step and entropy coding. In prediction step predicators are used to determine the pixel values of a cover image and in the second step entropy coding of prediction error values is done.

3) Transform or Frequency Domain Steganography

Transform domain steganography techniques are the most complex way to embed the secret data in the cover image. Any image in digital form is made up of high and low frequency components. Digital image can have smooth and edge (sharp) areas. Smooth areas represent low frequency whereas high frequency is represented by edge or sharp areas of the cover image. Changes done in low frequency areas can easily be visible to human eyes. So it is not possible to embed equal amount of secret information in all the regions. It has number advantages over the spatial domain methods of steganography such as it is more robust against compression, image processing and cropping and these methods are less prone to attacks. These techniques are not dependent upon image file format. Transform domain steganography techniques are broadly classified into following types:

a) Discrete Wavelet Transformation Technique: Discrete wavelet transformation techniques divides the cover image into four sub bands where higher band represent finer details and lower band has more important information. Entropy coders locate the transform coefficients and encode them. DWT technique has extra edge over DCT that it offers efficient energy compaction than DCT without any blocking artifacts after the process of coding. DWT has multi-resolution nature that make it best fit for scalable image coding. There are several other types of transforms that can applied with DWT such as integer transform, curvelet transform, contourlet transform, dual tree DWT etc.

b) Discrete Cosine Transformation Technique: Discrete cosine transformation is very famous steganography techniques which is best suited for JPEG images. JPEG images are widely used over the internet and have lossy nature of compression. DCT is extensively used for image and video compression. Every block of DCT is quantized with the help of quantization table of JPEG. Quantized coefficients are used to embed the secret message. Afterward coding methods are applied such as Huffman coding. In this technique high frequency regions are better for information hiding as they often become zero after the process of quantization. Hence it is not necessary to modify the coefficient value if the embedded data is zero. JSteg/ JPHide, F5, YASS (Yet another steganographic scheme) and outguess are some of the DCT steganography tools.

III. EXPERIMENTAL SETUP

The proposed work uses Genetic Algorithm to locate the optimal positions for embedding the watermark. The below diagram shows a flowchart for the embedding and extraction process.

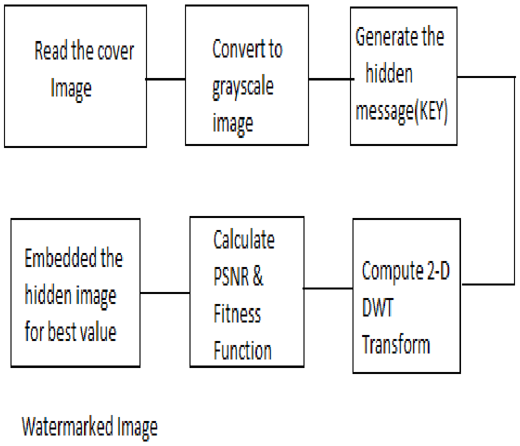
Read the cover Image
Convert to grayscale image
Generate the hidden message(KEY)
Compute 2-D DWT Transform
Calculate PSNR & Fitness Function
Embedded the hidden image for best value
Watermarked Image

Fig. 2: Embedding Procedure

The image which is to be secured also known as original image, is read into the engine, as shown in the above diagram. It is converted to grayscale type. The hidden message is then generated. The hidden message which is to be watermarked or embedded inside the original image can be any text, image or audio message. For our, engine we have taken a bit mapped image, with text 'BEST' written in it as shown in Fig 5. The 2-d Wavelet Transform is then computed to get the detailed coefficients of the image. The Daubechies filter 'db1' is used as wavelet filter. The PSNR values are then calculated for all coeffcients and based on it, the fitness function is generated. The fitness function is given as a vectorized PSNR obtained from each co-efficients.

Fitness Funtion:

$$F=PSNR(1)+PSNR(2)+PSNR(3)+PSNR(4) \quad (1)$$

where PSNR is Peak Signal to Noise Ratio and 1,2,3,4 are the indexes of four quadrants of DWT.

The genetic algorithm is then applied with the given fitness function and the image is watermarked into the co-efficient for which best value is obtained. This summarizes the complete embedding procedure.

The block diagram for extraction is as shown below:

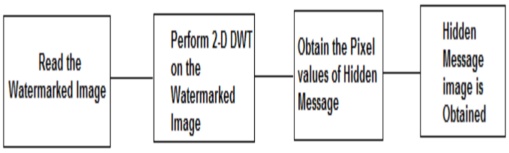
Read the Watermarked Image
Perform 2-D DWT on the Watermarked Image
Obtain the Pixel values of Hidden Message
Hidden Message image is Obtained

Fig 3: Extraction procedure

The extraction method is comparatively simple; the image which is supposed to be watermark is read into the system. 2-D watermark using the same filters is applied to it. The equation (2), given below is applied to it, to obtain the pixel value information of the hidden message. If the image is watermarked one, then the hidden message i.e the image 'BEST' is obtained either partially or fully. The partial appearance is attributed to the noise or distortion, which can be added at various stages of data transmission

$$cc=abs(cv1./N) \qquad (2)$$

where cc is hidden message, cv1 is the coefficients of DWT and N is watermark size.

IV. RESULTS AND DISCUSSION

The simulation is performed using MATLAB software platform on standard gray scale images of size 256x256 like mandrill, boat, peppers and Lena. MATLAB contains an extensive platform for programming, calculation and graphics which makes it a tool of choice for academic research and study. The below figures show the various results taking a peppers image.

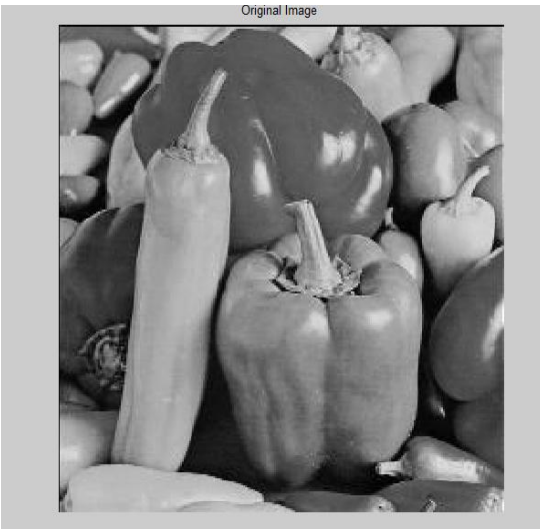

Fig 4: Original Image (Peppers)

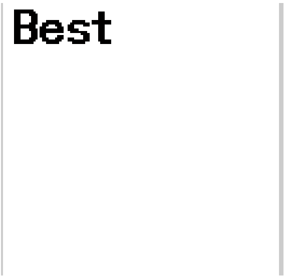

Fig 5: Hidden Message

Fig 5.shows the hidden message which is a bit mapped(.bmp) image, which is being used as the authentication key.

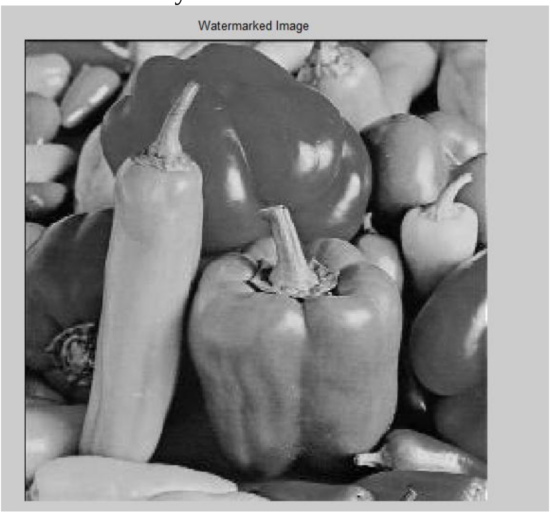

Fig 6: Watermarked Image

As can be seen from Fig 6, the method gives a high level of image perceptibility which is necessary for invisible watermarking applications. The watermarked image appears exactly similar to the original image and it is fairly impossible to differentiate it with the original image.

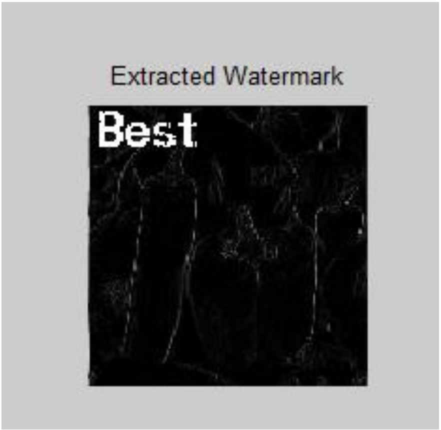

Fig. 7: Extracted Watermark

The Fig. 7, contains the watermarked or hidden message as extracted from the watermarked image, thus the method performs good on the security ground as well.

Now let us consider a situation, where this system is being used as a security and authentication measure. The images are transmitted from one end. Before transmitting every image is embedded with a particular hidden security keyword as in the above case is 'BEST'.

At the receiver end, we will have the extraction procedure. After going through the extraction procedure, if the hidden message is retrieved, either partially (due to noise addition during transmission) or completely (as shown in Fig. 6), then we can be assured that the image received at the receiver end is the original image.

Now let us suppose, an intruder hacks our data transfer system and fraudulently replaces the image with some other fake image. Then, on passing through the extraction procedure, the image will not yield the key. Thus, proving that the image received is not at all, the original one sent at the transmitter end.

Thus, the security of a particular communication system or data transfer involving images can be ensured by using the proposed method, where both the transmitter and receiver are aware of the 'Key Image', which is hidden inside the cover or original image. In a way it is a public key sharing based cryptography method.

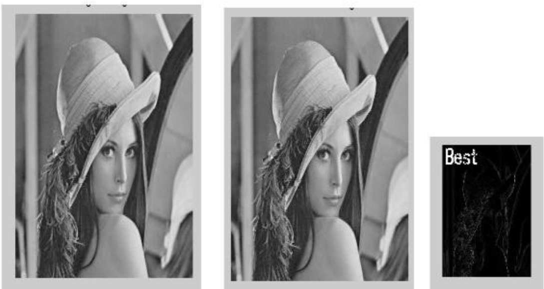

Figure 8: Results on Lena Image

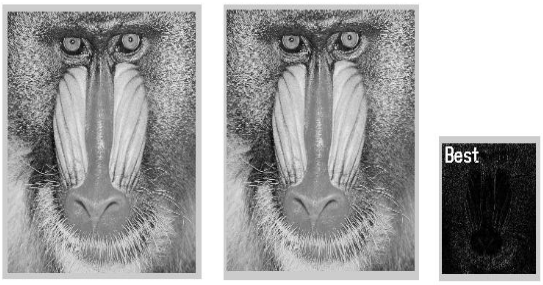

Figure 9: Results on Mandrill Image

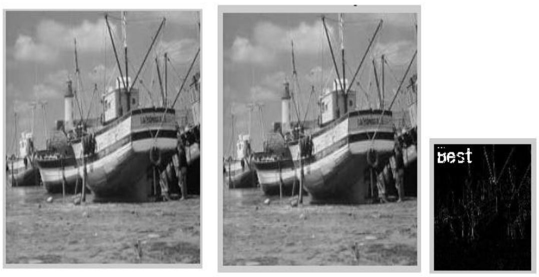

Figure 10: Results on Boat Image

Table 1: Comparison Results with Other Papers

Host Image	**PSNR Values [1]**	**PSNR Values [2]**	**Proposed Work**
Peppers	44.8291	30.65	56.70
Boat	44.860226	29.75	53.45
Lena	44.783592	30.34	48.65
Mandrill	44.9216	26.46	52.62

V. CONCLUDING REMARKS

The area of data security is always a key concern when designing any communication system. In this research, security of image data has been studied at length in terms of Image Watermarking and Steganography. The various paradigms of image security have been discussed. The research then moves on to suggesting a Genetic Algorithm based watermarking technique, which is based out of basic 2-D DWT. The Genetic Algorithm optimization technique is used to find out the best region for the hidden message to be embedded in. The PSNR values of the various sub bands of DWT are used to form the fitness function used in this research. The technique is then tested on some standard test images and shows a considerable improvement in PSNR values and at the same time maintaining a high level of perceptibility of the Watermarked Image.

REFERENCES

[1]. 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", Proceeding of 3rd IEEE International conference on Intelligent Sensing and Information Processing (ICISIP), (2005) December 14-17, Bangalore, India.

[2]. A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: survey and analysis of current methods", Signal Processing, vol. 90, no. 3, (2010).

[3]. H. Yang, X. Sun, and G. Sun, "A High-Capacity Image Data Hiding Scheme using Adaptive LSB Substitution" , Radio Engineering, vol. 18, no. 4, (2009).

[4]. Z. H. Wang, C. C. Chang, and M. C. Li, "Optimizing Least Significant Bit

Substitution using Cat Swarm Optimization Strategy", Information Sciences, vol. 192, no. 1, (2012).

[5]. S. Wang, B. Yang, and X. Niu, "A secure steganography method based on genetic algorithm", Journal of Information Hiding and Multimedia Signal Processing", vol. 1, no. 1 (2010).

[6]. Z. Zhao, H. Luo, Z. M. Lu, and J. S. Pan, "Reversible Data Hiding Based on Multilevel Histogram Modification and Sequential Recovery", International Journal of Electronics and Communication, vol. 65, no. 10, (2011).

[7]. C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel Reversible Data Hiding Based on Histogram Modification of Difference Images", Pattern Recognition, vol. 41, no. 12, (2008).

[8]. D. Wu, and W.H. Tsai, "A Steganographic Method for Images by Pixel Value Differencing", Pattern Recognition, vol. 24, no. 9-10, (2003).

[9]. V. M. Potdar, and E. Chang,"Gray Level Modification Steganography for Secret Communication", Proceeding of 2nd IEEE International Conference on Industrial Informatics (INDIN), (2004) June 26-26, Berlin, Germany.

[10]. Gopesh Joshi, "Review of Genetic Algorithm: An Optimization Technique", InternationalInternational Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4,April2014

[11]. Tsai, P., Hu, Y.-C., & Chang, C.-C."A color image watermarking scheme based on color quantization. Signal Processing", 84(1), 95-106. doi: 10.1016/j.sigpro.2003.07.012.

[12]. Su, J. K., Hartung, F., & Girod, B. " Digital watermarking of text, image, and video documents" Computers &amp; Graphics, 22(6), 687-695. doi: 10.1016/s0097-8493(98)00089-2,1998

[13]. Popa, R. An analysis of steganographic techniques. The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering,1998

[14]. Yu, Y.-H., Chang, C.-C., & Lin, I.-C. "A new steganographic method for color and grayscale image hiding. Computer Vision and Image Understanding", 107(3), 183-194. doi: 10.1016/j.cviu.2006.11.002, 2007

[15]. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing, 90*(3), 727-752,2007