World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:4, No:8, 2010

Data Hiding in Images in Discrete Wavelet Domain Using PMM

Souvik Bhattacharyya and Gautam Sanyal

Open Science Index, Computer and Information Engineering Vol:4, No:8, 2010 publications.waset.org/9450/pdf

Abstract—Over last two decades, due to hostilities of environment over the internet the concerns about confidentiality of information have increased at phenomenal rate. Therefore to safeguard the information from attacks, number of data/information hiding methods have evolved mostly in spatial and transformation domain.In spatial domain data hiding techniques,the information is embedded directly on the image plane itself. In transform domain data hiding techniques the image is first changed from spatial domain to some other domain and then the secret information is embedded so that the secret information remains more secure from any attack. Information hiding algorithms in time domain or spatial domain have high capacity and relatively lower robustness. In contrast, the algorithms in transform domain, such as DCT, DWT have certain robustness against some multimedia processing.In this work the authors propose a novel steganographic method for hiding information in the transform domain of the gray scale image.The proposed approach works by converting the gray level image in transform domain using discrete integer wavelet technique through lifting scheme.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 technique in those coefficients to form the stego image. The aim of this paper is to propose a high-capacity image steganography technique that uses pixel mapping method in integer wavelet domain with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security. This solution is independent of the nature of the data to be hidden and produces a stego image with minimum degradation.

Keywords—Cover Image, Pixel Mapping Method (PMM), Stego Image,Integer Wavelet Tranform.

I. Introduction

INFORMATION hiding is a general term encompassing many sub disciplines. One of the most important sub disciplines is steganography as shown in Figure 1. Steganography, is derived from a work by Johannes Trithemus (1462-1516) entitled ”Steganographia” and comes from the Greek defined as ”covered writing”. It is an ancient art of hiding information in ways a message is hidden in an innocent-looking cover media so that will not arouse an eavesdropper's suspicion[19].A famous illustration of modern day steganography is **Simmons' Prisoners' Problem** [34].Compared with cryptography attempting to conceal the content of the secret message, steganography conceals the very existence of that [3]. Another form of information hiding is digital watermarking [36], which is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video or text only. A covert channel could be defined as a communications channel that transfers some kind of information using a method originally not intended to transfer this kind of information. Observers are unaware that a covert message is being communicated. Only the sender and recipient of the message notice it. In steganography two aspects are usually addressed. First, the cover-media and stego media should appear identical under all possible statistical attacks. Second, the embedding process should not degrade the media fidelity, that is, the difference between the stego media and the cover-media should be imperceptible to human perceptual system. Steganography works have been carried out on different transmission media like images, video , text, or audio [28].Among them image steganography is the most popular of the lot. In this method the secret message is embedded into an image as noise to it, which is nearly impossible to differentiate by human eyes [24], [31], [21].In video steganography, same method may be used to embed a message [38], [13], [14]. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range [16]. One major category, perhaps the most difficult kind of steganography is text steganography or linguistic steganography because due to the lack of redundant information in a text compared to an image or audio [17], [29]. The text steganography is a method of using written natural language to conceal a secret message as defined by Chapman et al. [28].For a more thorough knowledge of steganography methodology the reader may see [29], [37].Some Steganographic model with high security features has been presented in [4], [5], [6] and [35].

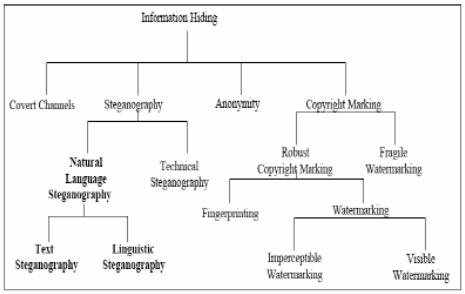


Fig. 1. Types of Information Hiding

S. Bhattacharyya is with the Department of Computer Science and Engineering, University Institute of Technology, The University of Burdwan, West Bengal, India e-mail: (souvik.bha@gmail.com).

G. Sanyal is with with the Department of Computer Science and Engineering, National Institute of Technologyy West Bengal, India e-mail: (nitgsanyal@gmail.com).

Open Science Index, Computer and Information Engineering Vol:4, No:8, 2010 publications.waset.org/9450/pdf

II. Image Steganography System

A block diagram of a generic image steganographic system is given in Fig. 2.

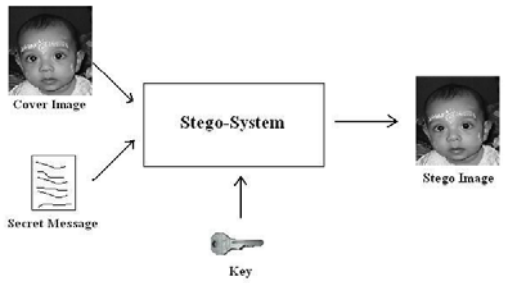


Fig. 2. Generic form of Image Steganography

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.

B. Steganalysis

Steganalysis is the science of detecting hidden information. The main objective of Steganalysis is to break steganography and the detection of stego image is the goal of steganalysis. Almost all steganalysis algorithms rely on the Steganographic algorithms introducing statistical differences between cover and stego image. Steganalysis deals with three important categories: (a) Visual attacks: In these types of attacks with a assistance of a computer or through inspection with a naked eye it reveal the presence of hidden information, which helps to separate the image into bit planes for further more analysis. (b) Statistical attacks: These types of attacks are more powerful and successful, because they reveal the smallest alterations in an images statistical behavior. Statistical attacks can be further divided into (i) Passive attack and (ii) Active attack. Passive attacks involves with identifying presence or absence of a covert message or embedding algorithm used etc. Mean while active attacks is used to investigate embedded message length or hidden message location or secret key used in embedding. (c) Structural attacks: The format of the data files changes as the data to be hidden is embedded; identifying this characteristic structure changes can help us to find the presence of image.

In this work a specific image based steganographic method for hiding information in the transform domain of the gray level image has proposed.The proposed approach works by converting the gray level image in transform domain using discrete integer wavelet technique through lifting scheme.In this method instead of directly embedding the secret message into the wavelet coefficients of cover image a mapping technique has been incorporated to generate the stego image. This method is capable of extracting the secret message without the presence of the cover image.

This paper has been organized as following sections: Section II describes some related works, Section III deals with proposed method. Algorithms are discussed in Section IV and Experimental results are shown in Section V. Section VI contains the analysis of the results and Section VII draws the conclusion.

III. Related Works

In this section various steganographic data hiding methods both in spatial domain and transform domain has been discussed.

A. Spatial Domain Steganographic Method

1) Data Hiding by LSB : Various techniques about data hiding have been proposed in literatures. One of the common techniques is based on manipulating the least-significant-bit (LSB) [9], [10] and [25], [33]planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity but unfortunately LSB insertion is vulnerable to slight image manipulation such as cropping and compression.

2) Data Hiding by PVD : The pixel-value differencing (PVD) method proposed by Wu and Tsai [39] can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. The pixel-value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A

Open Science Index, Computer and Information Engineering Vol:4, No:8, 2010 publications.waset.org/9450/pdf

larger difference in the original pixel values allows a greater modification. In the extraction phase, the original range table is necessary. It is used to partition the stego-image by the same method as used to the cover image. Based on PVD method, various approaches have also been proposed. Among them Chang et al. [20]. proposes a new method using tri-way pixel-value differencing which is better than original PVD method with respect to the embedding capacity and PSNR.

3) Data Hiding by GLM : In 2004, Potdar et al.[15] proposes GLM (Gray level modification) technique which is used to map data by modifying the gray level of the image pixels. Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. GLM technique uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

4) Data Hiding by the method proposed by Ahmad T et al.: In this work [2] a novel Steganographic method for hiding information within the spatial domain of the grayscale image has been proposed. The proposed approach works by dividing the cover into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel.

B. Transform Domain Steganographic Method

Transform Domain methods hides messages in significant areas of cover image which makes them robust against various image processing operations like compression,enhancement etc.Many transform domain methods exist.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.

1) 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. The least significant bits of the quantized DCT coefficients are used as redundant bits into which the hidden message is embedded. The modification of a single DCT coefficient affects all 64 image pixels. Because this modification happens in the frequency domain and not the spatial domain, there are no noticeable visual differences.The advantage DCT has over other transforms is the ability to minimize the block-like appearance resulting when the boundaries between the 8x8 sub-images become visible (known as blocking artifact). The statistical properties of the JPEG files are also preserved.The disadvantage is that this method only works on JPEG files since it assumes a certain statistical distribution of the cover data that is commonly found in JPEF files.Some DCT based steganographic work has been given in [18], [12]and [27].

2) DWT based Data Hiding: Wavelet-based steganography [1], [40] , [11], [22] and [32], [23]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(PMM)

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.3 and Fig.4 shows the mapping information for embedding two bits or four bits respectively.

PAIR OF MSG BIT	PIXEL INTENSITY VALUE	NO OF ONES (BIN)
01	EVEN	ODD
10	ODD	EVEN
00	EVEN	EVEN
11	ODD	ODD

Fig. 3. Mapping Technique for embedding of two bits

2ND BIT & 3RD BIT/PAIR OF MSG BITS		PIXEL INTENSITY VALUE	NO OF ONES (BIN)
01	00	EVEN	ODD
	01		
	10		
	11		
10	00	ODD	EVEN
	01		
	10		
	11		
00	00	EVEN	EVEN
	01		
	10		
	11		
11	00	ODD	ODD
	01		
	10		
	11		

Fig. 4. Mapping Technique for embedding of four bits

Extraction process starts again by selecting the same pixels required during embedding. At the receiver side other different

Open Science Index, Computer and Information Engineering Vol:4, No:8, 2010 publications.waset.org/9450/pdf

reverse operations has been carried out to get back the original information.

One important point needs to be kept in mind that a specific order for selecting the neighbors of the seed pixel has to be maintained for embedding / mapping process and also for the process of extraction other wise it would not be possible to retrieve the data in proper sequence. This sequence has been shown in Figure 5.

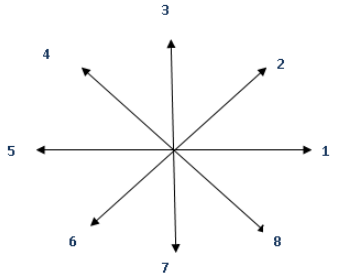


Fig. 5. Sequence of data embedding

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 ($intensity \leq 80$),dp=2 if ($intensity \geq 80$ & ≤ 160) ,dp=3 if ($intensity > 160$ & ≤ 255).
- $t = x + 2 + dp$
- if $(t \geq N) m = 2, n = y + 2 + dp$
- 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. 6. Snapshot of Selected Pixel for embedding.

B. Algorithms for Data Embedding Method

Let C be the original 8 bit gray scale image of size N x N i.e. C = $(P_{ij} \mid 0 \leq i < N, 0 \leq j < N, P_{ij} \in 0, 1, \ldots, 255)$. Let MSG be the n bit secret message represented as MSG =$(m_k \mid 0 \leq k < n, m_k \in 0, 1)$.A seed pixel P_{rc} can be selected with row (r) and column (c). Next step is to find the 8 neighbors $P_{r'c'}$ of the pixel P_{rc} such that $r' = r + l$, $c' = c + l$,$-1 \leq l \leq 1$. The embedding process will be finished when all the bits of every bytes of secret message are mapped or embedded. Algorithm of the embedding method are described as :

- Input : Cover Image(C), Message (MSG).
- Find the first seed pixel P_{rc}.
- $count = 1$.
- while ($count \leq n$)
- begin (for embedding message in message surrounding a seed pixel).
- cnt=Count number of ones of one of the $P_{r'c'}$ of intensity (V).
- m_k=Get next msg bit.
- $count = count + 1$.
- m_{k+1}=Get next msg bit.
- $count = count + 1$.
- Bincvr= Binary of V.
- If($m_k = 0$ & $m_{k+1} = 1$)
- $Bincvr(zerothbit) = 0$
- If($cnt \bmod 2 = 0$)
- $Bincvr(firstbit) = \neg Bincvr(firstbit)$
- If($m_k = 0$ & $m_{k+1} = 0$)
- $Bincvr(zerothbit) = 1$
- If($cnt \div 2 \neq 0$)
- $Bincvr(firstbit) = \neg Bincvr(firstbit)$
- If($m_k = 0$ & $m_{k+1} = 0$)
- $Bincvr(zerothbit) = 0$
- If($cnt \bmod 2 \neq 0$)
- $Bincvr(firstbit) = \neg Bincvr(firstbit)$
- If($m_k = 0$ & $m_{k+1} = 1$)
- $Bincvr(zerothbit) = 1$
- If($cnt \bmod 2 = 0$)
- $Bincvr(firstbit) = \neg Bincvr(firstbit)$
- End
- Get the next neighbor pixel $P_{r'c'}$ for embedding based on previous $P_{r'c'}$ and repeat.
- End
- Return the stego image (S).

C. Algorithms for Data Extraction Method

The process of extraction proceeds by selecting those same pixel with their neighbors. The extracting process will be finished when all the bits of every bytes of secret message are extracted. Algorithm of the extraction method are described as :

- Input : Stego image (S) , count.
- $count = count \div 2$.
- BinMsg= " ".
- Find the first seed pixel P_{rc}.
- I=0.
- While ($count \leq N$)
- begin (for extract message in message around a seed pixel).
- Get the (First/Next) neighbor pixel $P_{r'c'}$.
- cnt=Count number of ones of one of the $P_{r'c'}$ of intensity (V).
- Bincvr=Binary of V.
- Binmsg(i)=ZerothBit of Bincvr.
- $count = count + 1$.

Open Science Index, Computer and Information Engineering Vol:4, No:8, 2010 publications.waset.org/9450/pdf

- $i = i + 1$.
- Binmsg(i)=Enters according to One of ones in the intensity(1 for odd :0 for even).
- $i = i + 1$.
- End.
- Get the next neighbor pixel $P_{r'c'}$ for embedding based on previous $P_{r'c'}$ and repeat.
- End loop.
- Binmsg is converted back to Original message.
- Return Original Message.
- End.

V. Proposed Method

In this section the authors propose a new method for information hiding in discrete integer wavelet domain of gray scale image.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[30], [26] and [8].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 [7] technique for 2 bit embedding in those coefficients for embedding the secret message and the apply 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. Before embedding a checking has been done to find out whether the randomly selected wavelet coefficients or its neighbor lies at the boundary of the image or not.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.

A. Algorithms for Embedding Procedure

- Start from the Haar wavelet and get the corresponding lifting scheme.
- Perform a integer 2D-LWT at level 1 of the cover image C.
- Extract approximation coefficients matrix CCA and detail coefficients matrices CCH, CCV, and CCD of level 1 of the cover image C.
- Embed the secret messages in each of CCA, CCH, CCV, and CCD using the embedding method of PMM.
- Apply the inverse 2D-LWT to CCA,CCH,CCV and CCD to form the stego image S.

B. Algorithms for Extraction Procedure

- Start from the Haar wavelet and get the previous lifting scheme.
- Perform a integer 2D-LWT at level 1 of the stego image S.
- Extract approximation coefficients matrix SCA and detail coefficients matrices SCH, SCV, and SCD of level 1.
- Extract the secret messages from the SCA, SCH, SCV, and SCD using the extraction method of PMM.

VI. Wavelet Applications

In mathematics, a wavelet series is a representation of a square-integrable real number or complex number or complex valued function by a certain orthonormal series generated by a wavelet.

A function $\psi \in L^2(\mathbb{R})$ is called an orthonormal wavelet if it can be used to define a Hilbert basis,that is a complete space or complete orthonormal system, for the Hilbert space $L^2(\mathbb{R})$ of square integrable functions.

The Hilbert basis is constructed as the family of functions $\psi_{jk} : j, k \in Z$ by means of Dyadic transformation or dyadic translations and dilations of ψ is $\psi_{jk}(x) = 2^{j/2}\psi(2^j x - k)$ for integers $j, k \in \mathbb{Z}$. This family is an orthonormal system if it is orthonormal under the inner product $\langle \psi_{jk}, \psi_{lm} \rangle = \delta_{jl}\delta_{km}$ where δ_{jl} is the Kronecker delta and $\langle f, g \rangle$ is the standard inner product $\langle f, g \rangle = \int_{-\infty}^{\infty} \overline{f(x)} g(x) dx$ on $L^2(\mathbb{R})$ The requirement of completeness is that every function $f \in L^2(\mathbb{R})$ may be expanded in the basis as $f(x) = \sum_{j,k=-\infty}^{\infty} c_{jk}\psi_{jk}(x)$

The integral wavelet transform is defined as

$$[W_\psi f](a, b) = \frac{1}{\sqrt{|a|}} \int_{-\infty}^{\infty} \overline{\psi\left(\frac{x-b}{a}\right)} f(x) dx \qquad (1)$$

The wavelet coefficients c_{jk} are then given by

$$c_{jk} = [W_\psi f](2^{-j}, k2^{-j}) \qquad (2)$$

Here, $a = 2^{-j}$ is called the binary dilation or dyadic dilation and $b = k2^{-j}$ is the binary or dyadic position.

A. 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.

A continuous wavelet transform (CWT) is used to divide a continuous-time function into wavelets. More formally it is written as:

$$\gamma(s, tau) = \int f(t)\psi^*_{s,tau} t dt. \qquad (3)$$

where * denotes complex conjugation. This equation shows how a function f(t) is decomposed into a set of basis functions $\psi^t_{s,tau}$ called the wavelets.The variables s and τ, scale and translation, are the new dimensions after the wavelet transform.The wavelets are generated from a single basic wavelet ψ_t the so-called mother wavelet, by scaling and translation

$$\psi_{s,tau}(t) = \frac{1}{\sqrt{s}}\psi(\frac{t - tau}{s}) \qquad (4)$$

As CWT maps a one-dimensional signal to a two-dimensional time-scale joint representation that is highly redundant. The time-bandwidth product of the CWT is the square of that of the signal and for most applications, which

Open Science Index, Computer and Information Engineering Vol:4, No:8, 2010 publications.waset.org/9450/pdf

seek a signal description with as few components as possible, this is not efficient. To overcome this problem discrete wavelets have been introduced. Discrete wavelets are not continuously scalable and translatable but can only be scaled and translated in discrete steps. This is achieved by modifying the wavelet representation in eqn (4)

$$\psi_{j,k}(t) = \frac{1}{\sqrt{s_0^j}}\psi(\frac{t - k\tau_0 s_0^j}{s_0^j}) \quad (5)$$

Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer corresponding resolution needed. A one dimensional DWT is a repeated filter bank algorithm, and the input is convolved with high pass filter and a low pass filter. The result of latter convolution is smoothed version of the input, while the high frequency part is captured by the first convolution. The reconstruction involves a convolution with the synthesis filter and the results of this convolution are added. In two dimensional transform, first apply one step of the one dimensional transform to all rows and then repeat to all columns. This decomposition results into four classes or band coefficients.The Haar Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are approximate band (LL), Vertical Band (LH), Horizontal band (HL), and diagonal detail band (HH). The approximation band consists of low frequency wavelet coefficients, which contain significant part of the spatial domain image. The other bands also called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image.This DWT decomposition of the signal continues until the desired scale is achieved .Two-dimensional signals, such as images, are transformed using the two-dimensional DWT. The two-dimensional DWT operates in a similar manner, with only slight variations from the one-dimensional transform. Given a two-dimensional array of samples, the rows of the array are processed first with only one level of decomposition. This essentially divides the array into two vertical halves, with the first half storing the average coefficients, while the second vertical half stores the detail coefficients. This process is repeated again with the columns, resulting in four sub bands within the array defined by filter output. Fig 7. shows a one level decomposition using the two-dimensional DWT . Since the discrete wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them, hence it is expected to make the process of imperceptible embedding more effective.

B. Integer Wavelet Transform through lifting scheme

The lifting scheme is a technique for both designing wavelets and performing the discrete wavelet transform. Actually it is worthwhile to merge these steps and design the wavelet filters while performing the wavelet transform.The technique was introduced by Wim Sweldens [26].The lifting scheme is an algorithm to calculate wavelet transforms in an

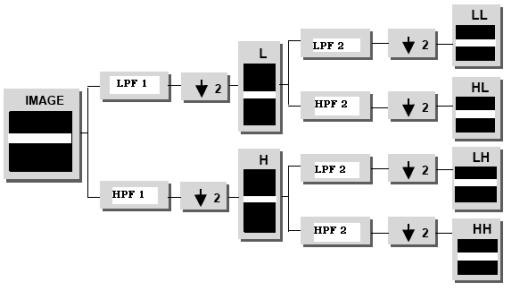


Fig. 7. One-level decomposition using the two-dimensional DWT, where LPF1 Represents low-pass filtering of the image rows, HPF1 represents high-pass filtering of Image rows, LPF2 represents low-pass filtering of image columns, and HPF2 represents high-pass filtering of image columns.

efficient way. It is also a generic method to create so-called second-generation wavelets. They are much more flexible and can be used to define wavelet basis on an interval or on an irregular grid, or even on a sphere..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.

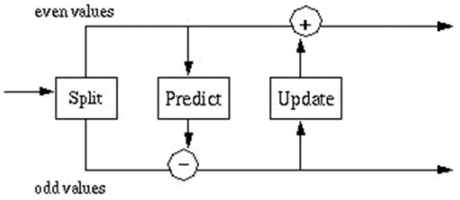


Fig. 8. Lifting scheme forward wavelet transformation

Splitting: Split the signal x into even samples and odd samples: $x_{even} : s_i \leftarrow x_{2i}$, $x_{odd} : d_i \leftarrow x_{2i+1}$

Prediction: Predict the odd samples using linear interpolation:$d_i \leftarrow d_i - \frac{(s_i + s_{i+1})}{2}$

Update: Update the even samples to preserve the mean value of the samples:$s_i \leftarrow s_i + \frac{(d_{i-1} + d_i)}{4}$

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.

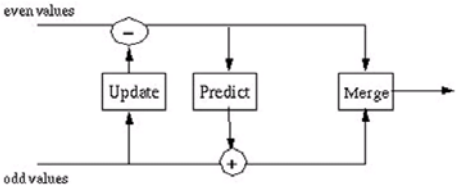


Fig. 9. Lifting scheme inverse wavelet transformation

Open Science Index, Computer and Information Engineering Vol:4, No:8, 2010 publications.waset.org/9450/pdf

C. Lifting Scheme Haar Transform

In the lifting scheme version of the Haar transform, the prediction step predicts that the odd element will be equal to the even element. The difference between the predicted value (the even element) and the actual value of the odd element replaces the odd element. For the forward transform iteration j and element i, the new odd element, j+1,i would be: $odd_{j+1,i} = odd_{j,i} - even_{j,i}$. In the lifting scheme version of the Haar transform the update step replaces an even element with the average of the even / odd pair (e.g. the even element s_i and its odd successor s_{i+1}) is $even_{j+1,i} = \frac{(even_{j,i}+odd_{j,i})}{2}$. The original value of the $odd_{j,i}$ element has been replaced by the difference between this element and its even predecessor. The original value is :$odd_{j,i} = even_{j,i} + odd_{j+1,i}$.Substituting this into the average, we get $even_{j+1,i} = \frac{(even_{j,i}+even_{j,i}+odd_{j+1,i})}{2}$

VII. Experimental Results

In this section the authors present the experimental results of the proposed method based on two benchmarks techniques to evaluate the hiding performance. First one is the capacity of hiding data and another one is the imperceptibility of the stego image, also called the quality of stego image. The quality of stego-image should be acceptable by human eyes. In this section experimental results of the proposed method are shown based on two well known images: Lena and Pepper.Embedding capacity of PMM in integer wavelet domain has been illustrated in figure 10.

IMAGE	SIZE	EMBEDDING CAPACITY
LENA	128X128	2240
	256X256	9536
	512X512	40048
PEPPER	128X128	2832
	256X256	11440
	512X512	46776

Fig. 10. Embedding capacity of the proposed method



Fig. 11. A) Cover Image B) Stego Image of Lena after embedding "I am an Indian and I feel proud to be an Indian."

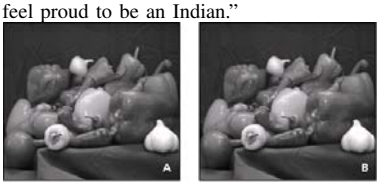


Fig. 12. A) Cover Image B) Stego Image of Pepper after embedding "I am an Indian and I feel proud to be an Indian."

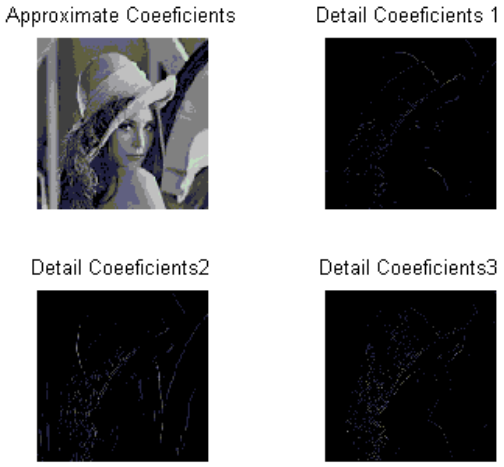


Fig. 13. Level 1 Wavelet Decomposition of Lena

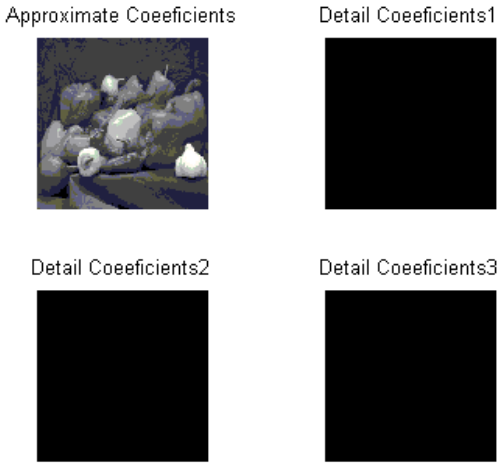


Fig. 14. Level 1 Wavelet Decomposition of Pepper

A. Peak Signal to Noise Ratio (PSNR)

PSNR measures the quality of the image by comparing the original image or cover image with the stego-image, i.e. it measures the percentage of the stego data to the image percentage. The PSNR is used to evaluate the quality of the stego-image after embedding the secret message in the cover. Assume a cover image C(i,j) that contains N by N pixels and a stego image S(i,j) where S is generated by embedding / mapping the message bit stream. Mean squared error (MSE) of the stego image as follows:

$$MSE = \frac{1}{[N \times N]^2} \sum_{i=1}^{N} \sum_{j=1}^{N} [C(ij) - S(ij)]^2$$

The PSNR is computed using the following formulae:

$$PSNR = 10 \log_{10} 255^2 / \ MSE \ db.$$

Open Science Index, Computer and Information Engineering Vol:4, No:8, 2010 publications.waset.org/9450/pdf

PSNR value of the stego image has been shown after embedding in various wavelet coefficients of the cover image.

EMBEDDING IN CA COEFFICIENTS			
Image Size	Message Size (in char)	PSNR (STEGO IMAGE)	PSNR OF RESPECTIVE COEEFICIENTS
128x128	100	32.2765	53.2957
	200	32.2455	50.6693
	400	32.1966	47.8935
	500	32.1673	47.0272
256x256	100	36.1441	59.7751
	200	36.1380	56.7339
	400	36.0994	53.6892
	800	36.0305	50.7738
	1600	35.8733	47.6721
	2000	35.8111	46.7785

Fig. 15. PSNR after embedding in Approximate Coefficients (CA)of Lena Image

EMBEDDING IN CH COEFFICIENTS			
Image Size	Message Size (in char)	PSNR (STEGO IMAGE)	PSNR OF RESPECTIVE COEEFICIENTS
128x128	100	30.0156	54.9145
	200	29.9981	52.3483
	400	29.9593	49.3380
	500	29.9403	48.3650
256x256	100	33.5571	62.3581
	200	33.5512	58.7430
	400	33.5380	55.4320
	800	33.5070	52.6250
	1600	33.4335	49.4883
	2000	33.4035	48.5574

Fig. 16. PSNR after embedding in Detail Coefficients (CH)of Lena Image

EMBEDDING IN CV COEFFICIENTS			
Image Size	Message Size (in char)	PSNR (STEGO IMAGE)	PSNR OF RESPECTIVE COEEFICIENTS
128x128	100	27.8995	54.6592
	200	27.8856	51.9448
	400	27.8559	48.9704
	500	27.8449	48.0260
256x256	100	31.1573	62.3371
	200	31.1464	58.7460
	400	31.1367	55.5489
	800	31.1105	52.3079
	1600	31.0631	49.1563
	2000	31.0470	51.0951

Fig. 17. PSNR after embedding in Detail Coefficients (CV)of Lena Image

B. Similarity Measure

For comparing the similarity between cover image and the stego image, the normalized cross correlation coefficient (r) has been computed.

$$r = \frac{\sum_{(C(i,j)-m_1)(S(i,j)-m_2)}}{\sqrt{(\sum_{C(i,j)-m_1})^2}\sqrt{(\sum_{S(i,j)-m_2})^2}}$$

Here C is the cover image, S is the stego image,m_1 is the mean pixel value of the cover image and m_2 is the mean pixel value of stego image. It has been seen that the correlation coefficient computed here for all the images is almost one which indicates the both the cover image and stego image are of highly correlated i.e. both of these two images are same.

EMBEDDING IN CD COEFFICIENTS			
Image Size	Message Size (in char)	PSNR (STEGO IMAGE)	PSNR OF RESPECTIVE COEEFICIENTS
128x128	100	35.1962	58.8355
	200	35.1917	56.9044
	400	35.1831	54.4863
	500	27.8449	48.0260
256x256	100	35.1962	58.8355
	200	35.1917	56.9044
	400	35.1831	54.4863
	800	35.1673	51.8371
	1600	35.1317	49.0398
	2000	35.1174	48.1247

Fig. 18. PSNR after embedding in Detail Coefficients (CD)of Lena Image

Image	Correlation
Lena(128x128)	0.9997
Lena(256x 256)	0.9998
Lena(512x512)	0.9994
Pepper(128x128)	0.9996
Pepper(256x256)	0.9996
Pepper(512x512)	0.9996

Fig. 19. Similarity Measure between Cover and Stego

VIII. Analysis of the Results

In this article the authors proposed an efficient image based steganography approach for hiding information in wavelet domain of a gray scale image.Embedding capacity of the proposed method has been computed which is better than in most cases compared to the existing methods.The PSNR value is also better than the existing methods after embedding of the secret message in various coefficients of the cover image.The similarity measures proves that the proposed method is better than the existing methods which ensures that cover image and the stego image is almost identical.Also as the message bits are not directly embedded at the pixels of the cover image, steganalysis may be able to find out the embedded bits but can not be able to extract the original message bits.

IX. 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 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] Ahmad T. Al-Taani. and Abdullah M. AL-Issa. A novel steganographic method for gray-level images. *International Journal of Computer, Information, and Systems Science, and Engineering*, 3, 2009.

[3] Ross J. Anderson. and Fabien A.P.Petitcolas. On the limits of steganography. *IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright and Privacy Protection*, 16:474–481, 1998.

Open Science Index, Computer and Information Engineering Vol:4, No:8, 2010 publications.waset.org/9450/pdf

[4] Souvik Bhattacharyya. and Gautam Sanyal. Study of secure steganography model. In *Proceedings of International Conference on AdvancedComputing and Communication Technologies (ICACCT-2008)*, Panipath,India, 2008.
[5] Souvik Bhattacharyya. and Gautam Sanyal. An image based steganography model for promoting global cyber security. In *Proceedings of International Conference on Systemics, Cybernetics and Informatics*, Hyderabad,India, 2009.
[6] Souvik Bhattacharyya. and Gautam Sanyal. Implementation and design of an image based steganographic model. In *Proceedings of IEEE International Advance Computing Conference*, Patiala ,India, 2009.
[7] 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.
[8] Geert Uytterhoeven Dirk Roose Adhemar Bultheel. Integer wavelet transforms using the lifting scheme. In *CSCC Proceedings*, 1999.
[9] J.Y. Hsiao. C.C. Chang. and C.-S. Chan. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, 36:1583–1595, 2003.
[10] C.K. Chan. and L. M.Cheng. Hiding data in images by simple lsb substitution. *Pattern Recognition*, 37:469–474, 2004.
[11] 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.
[12] 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.
[13] G. Doerr and J.L. Dugelay. A guide tour of video watermarking. *Signal Processing: Image Communication*, 18:263–282, 2003.
[14] G. Doerr and J.L. Dugelay. Security pitfalls of frameby-frame approaches to video watermarking. *IEEE Transactions on Signal Processing, Supplement on Secure Media*, 52:2955–2964, 2004.
[15] Potdar V.and Chang E. Gray level modification steganography for secret communication. In *IEEE International Conference on Industria lInformatics.*, pages 355–368, Berlin, Germany, 2004.
[16] K. Gopalan. Audio steganography using bit modification. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03)*, volume 2, pages 421–424, 6-10 April 2003.
[17] N.F. Maxemchuk J.T. Brassil, S. Low and L. O.Gorman. Electronic marking and identification techniques to discourage document copying. *IEEE Journal on Selected Areas in Communications*, 13:1495–1504, 1995.
[18] 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.
[19] D. Kahn. *The Codebreakers - the comprehensive history of secret communication from ancient times to the Internet*. Scribner, 1996.
[20] P Huang. K.C. Chang., C.P Chang. and T.M Tu. A novel image steganography method using tri-way pixel value differencing. *Journal of Multimedia*, 3, 2008.
[21] Kran Bailey Kevin Curran. An evaluation of image based steganography methods. *International Journal of Digital Evidence,Fall 2003*, 2003.
[22] 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.
[23] 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.
[24] Jr. L. M. Marvel, C. G. Boncelet and C. T. Retter. Spread spectrum image steganography. *IEEE Trans. on Image Processing*, 8:1075–1083, 1999.
[25] Y. K. Lee. and L. H.Chen. High capacity image steganographic model. *IEE Proc.-Vision, Image and Signal Processing*, 147:288–294, 2000.
[26] W. Sweldens. The lifting scheme. A construction of second generation wavelets. *SIAM J. Math. Anal.*, 29:511–546, 1997.
[27] Chia-Chen Lin. High capacity data hiding scheme for dct-based images. *Journal of Information Hiding and Multimedia Signal Processing*, 1, 2010.
[28] G. Davida M. Chapman and M. Rennhard. A practical and effective approach to large-scale automated linguistic steganography. In *Proceedings of the Information Security Conference*, pages 156–165, October 2001.
[29] N.F.Johnson. and S. Jajodia. Steganography: seeing the unseen. *IEEE Computer*, 16:26–34, 1998.
[30] 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.
[31] Nasir Memon R. Chandramouli. Analysis of lsb based image steganography techniques. In *Proceedings of IEEE ICIP*, 2001.
[32] 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.
[33] C.F. Lin. R.Z. Wang. and J.C. Lin. Image hiding by optimal lsb substitution and genetic algorithm. *Pattern Recognition*, 34:671–683, 2001.
[34] Gustavus J. Simmons. The prisoners' problem and the subliminal channel. *Proceedings of CRYPTO.*, 83:51–67, 1984.
[35] Avinash Prasad Kshitij. Souvik Bhattacharyya. and Gautam Sanyal. A novel approach to develop a secure image based steganographic model using integer wavelet transform. In *Proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing (Indexed by IEEE Computer Society)*, Cochin ,India, 2010.
[36] S.P.Mohanty. *Digital Watermarking: A Tutorial*. 1999.
[37] JHP Eloff. T Mrkel. and MS Olivier. An overview of image steganography. In *Proceedings of the fifth annual Information Security South Africa Conference.*, 2005.
[38] N. Morimoto W. Bender, D. Gruhl and A. Lu. Techniques for data hiding. *IBM Systems Journal*, 35:313–316, 1996.
[39] D.C. Wu. and W.H. Tsai. A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 24:1613–1626, 2003.
[40] Bo Yang and Beixing Deng. Steganography in gray images using wavelet. In *Proceedings of ISCCSP 2006*.



Souvik Bhattacharyya received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India, presently known as Bengal Engineering and Science University (BESU) and M.Tech degree in Computer Science and Engineering from National Institute of Technology, Durgapur, India. Currently he is working as a Senior Lecturer in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. He has a good no of research publication in his credit. His areas of interest are Natural Language Processing, Network Security and Image Processing.



Gautam Sanyal has received his B.E and M.Tech degree National Institute of Technology (NIT), Durgapur, India. He has received Ph.D (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Vision. He possesses an experience of more than 25 years in the field of teaching and research. He has published nearly 50 papers in International and National Journals / Conferences. Two Ph.Ds (Engg) have already been awarded under his guidance. At present he is guiding six Ph.Ds scholars in the field of Steganography, Cellular Network, High Performance Computing and Computer Vision. He has guided over 10 PG and 100 UG thesis. His research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering and also holding the post of Dean (Students' Welfare) at National Institute of Technology, Durgapur, India.