A ROBUST STEGANOGRAPHY MODEL USING WAVELET-BASED BLOCK-PARTITION MODIFICATION

Sherin Youssef[1], Ahmed Abu Elfarag[2], Reta Raouf[3]

[1]Department of Computer Engineering, Arab Academy for Science & Tech, Alx., Egypt.
sherin@aast.edu

[2]Department of Computer Engineering, Arab Academy for Science & Tech, Alx., Egypt. Abouelfarag@aast.edu

[3] Department of Computer Engineering, Arab Academy for Science & Tech, Alx., Egypt. rita.raouf@gmail.com

ABSTRACT

An efficient steganographic method is proposed for embedding secret messages into gray scale and RGB colored images. In this paper, a wavelet domain steganography is adopted for hiding a large amount of data with high security, good invisibility and no loss of secret message. The information is embedded in those areas of the host image that contains high texture to reduce visibility of the embedded information in the host image. The qualified significant wavelet coefficients and their texture and sensitivity to gray value variations across different coarse scales (level 1, level 2 and level 3 wavelet decompositions) are utilized to determine the positions and the magnitudes to adaptively embed the secrete message. We consider the highly textured areas near the edges in high frequency subbands in the wavelet domain. The transformed cover image is divided into number of joint non-overlapping 4 × 4 blocks in each layer (R, G, and B layers). A difference value is calculated from the values of the adjacent pixels in each block, producing the partitioned difference image (PDI). The wavelet subbands are selected to calculate the changes. The selection of the range intervals is based on the characteristics of human vision's sensitivity to gray value variations from smoothness to contrast. The number of bits which can be embedded in each block varies and is decided by the width of the range to which the difference value of the two pixels and block histogram peak (Pk) belongs to. The embedded secret message can be extracted from the resulting stego-image and the original cover image is reversed. The proposed model will produce a high-capacity image steganography technique with acceptable level 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. Experimental results show the feasibility of the proposed methods. Various statistics attacks were also conducted to collect related data to show the security of the method. The experimental results show that the algorithm has a high embedding capacity and a good invisibility. Moreover PSNR of cover image with stego-image shows better results compared with other existing steganography approaches.

KEYWORDS

Message hiding, difference image, embedding, wavelet transform.

1. INTRODUCTION

Data hiding refers to the process of embedding information into a cover object [1]. Steganography is the art and science of concealing information in unremarkable cover media so as not to arouse an eavesdropper's suspicion. It is an application under information security field [2, 3, 4]. Digital steganography exploits the use of a host data to hide a piece of information in such a way that it is imperceptible to a human observer. Being classified under information security, steganography will be characterized by having set of measures that rely on strengths and counter measures (attacks) that are driven by weaknesses and vulnerabilities. Today, computer and network technologies provide easy-to-use communication channels for steganography. The existing image hiding methods usually adopt the frequency domain method [3, 4]. The major advantages of the frequency domain method are as follows, the energy of the hiding information can be distributed into the whole pixels in spatial image domain, and the HVS characteristics can be utilized conveniently for improving the invisibility and capability of the cover image. Moreover, the frequency domain approaches are more robust to signal processing operation such as filtering operation and the compression of JPEG. However, the information hiding algorithms in DCT domain [14, 16, 20] have to depend on a premise that the AC coefficients of a cover-image after embedding information must be completely equal to the AC coefficients of the corresponding stego-image. Otherwise a very little error can result in great distortion errors in the restored secret image. However, the rounding off errors in the computation of the stego-image pixel value is inevitable and this grave problem has not been solved by the current information hiding algorithm in DCT domain. Focusing on the above-mentioned problem, we present a new embedding scheme for color image hiding in DCT domain which can effectively reduce the distortion errors introduced in the secret image. The aim of this paper is to propose a modified high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security. Inevitably, hiding some data will change the cover image even though the distortion caused by hiding is imperceptible to the human visual system [2]. However, for some sensitive images, such as military images, medical images or artwork preservation, even the slightest alteration in pixel values is intolerable. To make sure a sensitive image can be completely recovered after embedded messages are completely extracted, reversible data hiding, or so-called lossless data embedding, has been proposed. Hiding a secret message/image in the special domain can easily be extracted by unauthorized user. In this paper, a reversible data hiding scheme is proposed. In this paper, we proposed a frequency domain steganography technique for hiding a large amount of data with high security, a good invisibility and no loss of secret message. The basic idea to hide information in the frequency domain is to alter the magnitude of all of the DCT coefficients of cover image.

The paper is organized as follows. Section 2 gives a survey of some related work. Section 3 introduces the proposed model with illustration of each phase. Experimental results are illustrated in section 4, while conclusions are carried out in section 5.

2. RELATED WORK

Steganography differs from cryptography in the sense that where Cryptography focuses on concealing the contents of a message, steganography focuses on concealing the existence of a message [5]. Two other technologies that are closely related to steganography are watermarking and fingerprinting [6].Watermarking is a protecting technique which protects (claims) the owner's property right for digital media (i.e. images, music, video and software) by some hidden watermarks. Therefore, the goal of steganography is the secret messages while the goal of watermarking is the cover object itself. Steganography is the art and science of hiding information in a cover document such as digital images in a way that conceals the existence of hidden data. The word steganography in Greek means "covered writing" (Greek words "stegos" meaning "cover" and "grafia" meaning "writing") [7]. The main objective of steganography is to communicate securely in such a way that the true message is not visible to the observer. That is

unwanted parties should not be able to distinguish in any sense between cover-image (image not containing any secret message) and stego-image (modified cover-image that containing secret message). Thus the stego-image should not deviate much from original cover-image. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

A simple way of steganography is based on modifying the least significant bit layer of images, known as the LSB technique [9]. The LSB technique directly embed the secret data within the pixels of the cover image. In some cases (Fridrich et al. [10]) LSB of pixels visited in random or in certain areas of image and sometimes increment or decrement the pixel value. Some of the recent research studied the nature of the stego and suggested new methodologies for increasing the capacity. Habes in [11] proposed a new method (4 least Significant) for hiding secret image inside carrier image. In this method each of individual pixels in an image is made up of a string of bits. He took the 4-least significant bit of 8-bit true color image to hold 4-bit of the secret message /image by simply overwriting the data that was already there. The schemes of the second kind embed the secret data within the cover image that has been transformed such as DCT (discrete cosine transformation). The DCT transforms a cover image from an image representation into a frequency representation, by grouping the pixels into non-overlapping blocks of 8 × 8 pixels and transforming the pixel blocks into 64 DCT coefficients each [12,13,14]. A modification of a single DCT coefficient will affect all 64 image pixels in that block. The DCT coefficients of the transformed cover image will be quantized, and then modified according to the secret data. Tseng and Chang in [14] proposed a novel steganography method based on JPEG. The DCT for each block of 8×8 pixels was applied in order to improve the capacity and control the compression ratio. Capacity, security and robustness [16], are the three main aspects affecting steganography and its usefulness. Capacity refers to the amount of data bits that can be hidden in the cover medium. Security relates to the ability of an eavesdropper to figure the hidden information easily. Robustness is concerned about the resist possibility of modifying or destroying the unseen data.

3. THE PROPOSED MODEL

Hiding the secret message/image in the spatial domain can easily be extracted by unauthorized user. In this paper, a wavelet domain steganography is adopted for hiding a large amount of data with high security, good invisibility and no loss of secret message. We embed the information in those areas of the host image that contains high texture to reduce visibility of the embedded information in the host image. The qualified significant wavelet coefficients and their texture and sensitivity to gray value variations across different coarse scales (level 1, level 2 and level 3 wavelet decompositions) are utilized to determine the positions and the magnitudes to adaptively embed the secrete message. In this paper, a 2-D wavelet decomposition of each layer of the gray scale (or coloured) cover image is applied. The transformed RGB cover image is then divided into number of joint non-overlapping blocks in each layer (R, G, and B layers). A difference value is calculated from the values of the two adjacent pixels in each block, producing the partitioned difference image (PDI). We consider the highly textured areas in the areas near the edges in LHi, HLi, and HHi subbands. All possible difference values are classified into a number of ranges.

In an arbitrary wavelet sub-band HL_i, we determine the entropy of each coefficient in HL_i based on current coefficient and its surrounding coefficients. If a coefficient has higher entropy denotes the violent variation of spatial domain in the host image, to embed message in the center coefficient of the context could improve the transparency of the stego image and robustness to extracted message. A block Image histogram is analyzed for each block in the decomposed sub-bands in the partitioned difference image (PDI) and the peak value (Pk) is identified. Each block is categorized according to the difference of the gray values. The difference value in each block is then replaced by a new value to embed the value of a sub-stream of the secret message if this difference value is greater than the peak Pk.

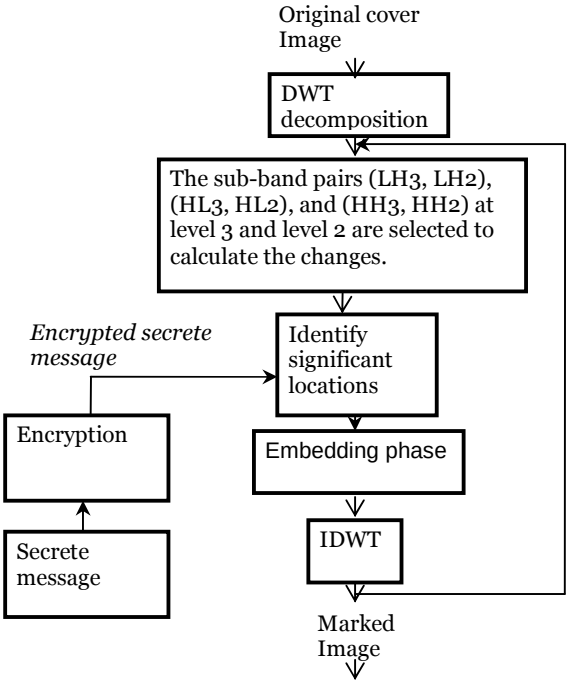


Figure 1(a): A Block diagram of the proposed secrete hiding model.

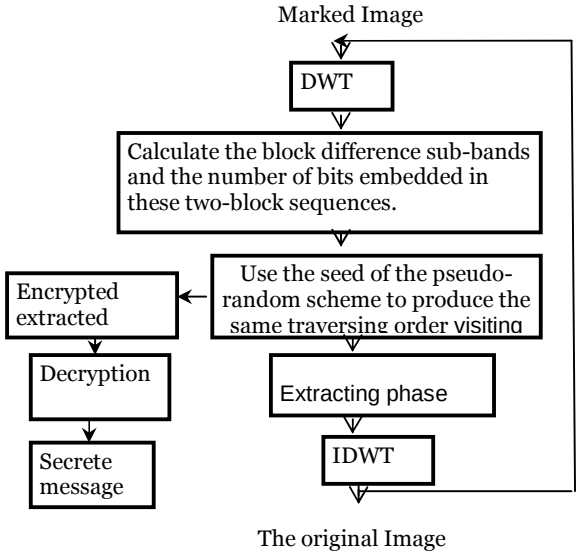


Figure 1(b): A Block diagram of the proposed extraction model.

Changes of the gray values of pixels in smooth areas in images are more easily noticed by human eyes. The pixels in edged areas may, tolerate larger changes of pixel values than those in the smooth areas. So, in the proposed method we embed more data in edged areas than in the smooth areas. And it is in this way that we keep the changes in the resulting stego-image unnoticeable. The number of bits which can be embedded in a pixel pair is decided by the width of the range

that the difference value belongs to. The number of bits which can be embedded in each block varies and is decided by the width of the range to which the difference value of the two pixels and block histogram peak (Pk) belongs to. The embedded secret message can be extracted from the resulting stego-image and the original cover image is reversed. The schematic/ block diagram of the whole process is given in figure 1(a) and figure 1(b).

Creating histogram phase

To create a large free space for data hiding, a difference image of an image must be generated before the hiding phase. For a grayscale image H(i, j), P×Q pixels in size, a difference image D(i, j), P×(Q−1) pixels in size can be generated from the original image H by using following formula:

$$D(i,j) = |H(i,j) - H(i,j+1)|, \quad 0 \leqslant i \leqslant P-1, \quad 0 \leqslant j \leqslant Q-2, \qquad (1)$$

Here | · | is the absolute value operation.

By using the property of the difference image histogram, we can hide a larger number of messages in comparison with the original image.

Discrete Wavelet Transform

The Wavelet Transform (WT) is a technique for analyzing signals. It was developed as an alternative to the short time Fourier Transform (STFT) to overcome problems related to its frequency and time resolution properties. More specifically, unlike the STFT that provides uniform time resolution for all frequencies the DWT provides high time resolution and low frequency resolution for high frequencies and high frequency resolution and low time resolution for low frequencies. The Discrete Wavelet Transform (DWT) is a special case of the WT that provides a compact representation of a signal in time and frequency that can be computed efficiently. The DWT is defined by the following equation:

$$W(j,k) = \sum_{j}\sum_{k} x(k) 2^{-j/2} \psi(2^{-j} n - k) \qquad (1)$$

Where ψ (t) is a time function with finite energy and fast decay called the mother wavelet. The DWT analysis can be performed using a fast, pyramidal algorithm related to multi-rate filter banks.

As a multi rate filterbank the DWT can be viewed as a constant Q filterbank with octave spacing between the centers of the filters. Each subband contains half the samples of the neighboring higher frequency subband. In the pyramidal algorithm the signal is analyzed at different frequency bands with different resolution by decomposing the signal into a coarse approximation and detail information. The coarse approximation is then further decomposed using the same wavelet decomposition step. This is achieved by successive highpass and low pass filtering of the time domain signal and is defined by the following equations:

$$y_{high}[k] = \sum_{n} x[n] g[2k - n] \qquad (2)$$

$$y_{low}[k] = \sum_{n} x[n] h[2k - n] \qquad (3)$$

Where y [k], y [k] high low are the outputs of the highpass (g) and lowpass (h) filters, respectively after subsampling by 2. Because of the downsampling the number of resulting wavelet coefficients is exactly the same as the number of input points. A variety of different

wavelet families have been proposed in the literature. In our implementation, the 4 coefficient wavelet family (DAUB4) proposed by Daubechies is used.

Quantization

A difference value d is computed from every non-overlapping block of two consecutive pixels, say p_i and p_{i+1}, of a given cover image in the wavelet domain the way of partitioning the cover image into two- pixel blocks runs through all the rows of each image. Assume that the gray values of p_i and p_{i+1} are g_i and g_{i+1}, respectively, then d is computed as $g_i - g_{i+1}$. Only the positive values of d are considered and classified into a number of contiguous ranges, say R_i where i= 1, 2, …., n. These ranges are assigned indices 1 through n. The lower and upper bound values of R_i are denoted by l_i and U_i, respectively, where l_1 is 0. The width of R_i is u_i-l_i+1. In the proposed method, the width of each range is taken to be a power of 2. A difference value which falls in a range width index k is said to have index k. All the values in a certain range (i.e. all the values with identical index) are considered as close enough. That is, if a difference value in a range is replaced by another in the same range, the change presumably cannot be easily noticed by human eyes.

Steps of the proposed model

Step 1:

If case of the secret message is in text form, the 1D bit stream is obtained by simply converting the ASCII code of each character into an 8-bit binary representation, and then concatenating them as a sequence. In case e that the secrete message is a gray scale image, we can form the bit stream by simply converting each pixel value into an 8-bit gray-level representation, and then concatenating them as a sequence.

The information bits are then encrypted using ACHTERBAHN-128 stream cipher before embedding them in the elements of the host. Pseudorandom permutation of secrete message is used for increasing security of embedded message. The idea behind the permutation is that the permutation generator uses the stego key and produces as output different sequences of the set {1, 2, 3,…, length (message)}. Nobody can guess the generated random sequence without knowing the secret key. This ensures that only recipients who know the corresponding secret key will be able to extract the message from a stego-object.

Step 2:

Converting the coloured image in transformed domain using 2D discrete integer wavelet transform. This approach performs a 2-D wavelet decomposition of the cover image and computes the approximation coefficients and detail coefficients matrices. Decompose the original image into different levels (for example: four levels - thirteen sub-bands) as shown in Fig. 2.

Step 3:

Find the associated three 2×2 and 4×4 sub-block pairs at the horizontal, vertical, and diagonal directions of level 3 and level 2 as illustrated in Fig. 2 and Fig. 3(a).

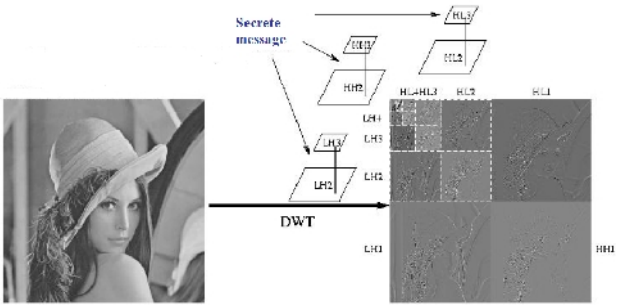


Figure 2. Block diagram of the hiding sub-bands.

For each sub-block pair:

If the sub-block pair contains the qualified significant wavelet coefficients (i.e., each value in the sub-block is greater than the median value of the corresponding sub-band) Calculate the changes to the sub-block pair

Divide the transformed image sub-bands into blocks A×B in size. Generate a difference image $D_b(I,j)$ of size A×(B−1) for each block by using following formula:

$$D_b(i,j) = |H_b(i,j) - H_b(i,j+1)|, \quad 0 \leqslant i \leqslant A-1,$$
$$0 \leqslant j \leqslant B-2, \quad 0 \leqslant b \leqslant \frac{M \times N}{A \times B} - 1.$$

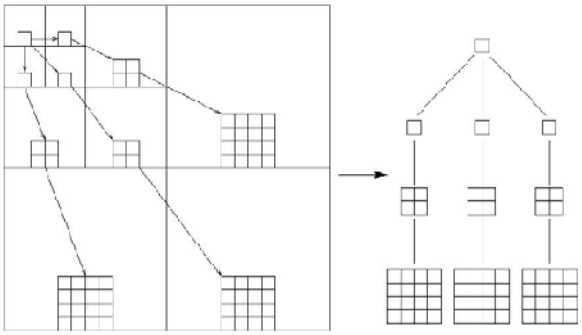


Figure 3(a). Parent-child dependencies of 2D 3-level wavelet decomposition

Generate the histogram of the difference image D_b and record the peak point P_b for each block.

Step 4:

Using a seed of a pseudo-random generator to produce a traversing order for visiting the two-pixel blocks for the embedding process. Consider the highly textured areas including the areas near the edges in LH_i, HL_i and HH_i subbands. If the pixel value $D_b(i, j)$ of the block difference image (b) is larger than the peak point P_b of block b, change the pixel value $D_b(i, j)$ of block b to $D_b(i, j)+1$. Otherwise, the pixel value $D_b(i, j)$ remains unchanged. The modification is defined as:

$$D'_b(i,j) = \begin{cases} D_b(i,j)+1 & \text{if } D_b(i,j) > P_b, \\ D_b(i,j) & \text{otherwise,} \end{cases}$$

$$\text{for } 0 \leqslant i \leqslant A-1, \quad 0 \leqslant j \leqslant B-2, \text{ and } 0 \leqslant b \leqslant \frac{M \times N}{A \times B} - 1,$$

Where P_b is the peak point of block b.

Setp 5: Embedding of Secret Message:

The encrypted stream of secrete message is handled to be embedded in the LH_3, HL_3, HH_3, LH_2, HL_2, and HH_2 sub-bands using the proposed embedding block partitioned scheme.

We consider the secret message as a long bit stream. We want to embed every bit in the bit stream into the two-pixel blocks of the transformed cover image. The number of bits which can

be embedded in each block varies and is decided by width of the range to which the difference value of the two pixels in the block belongs. Given a two-pixel block B with index k and gray values difference d, the number of bits, say n, which can embedding this block, is calculated by $n=\log_2(u_k-l_k+1)$ is an integer where u_k is the upper limit and l_k is the lower bound. A Sub-stream *S* with *n* bits is selected next from the secret message for embedding in *B*.

Decompose a host image into three levels with ten sub-bands of a wavelet pyramid structure. Choose a subband HL_i, for example HL_3, to embed the secret message. In an arbitrary wavelet sub-band HL_i, where we determine entropy of each coefficient in HL_i is based on current coefficient and its surrounding coefficients. Template made of nine coefficients form the context is shown in Figure 3(b). We use the current coefficient and its surrounding coefficients to calculate the entropy of each coefficient in selected sub-band, and choose the larger entropy to embed message. If a coefficient has higher entropy denotes the violent variation of spatial domain in the host image, to embed message in the center coefficient of the context could improve the transparency of the stego image and robustness to extracted message. Let $x0$ be the current target coefficient to estimate its entropy, xi, $1< i <8$, is a $x0$'s surrounding coefficients as shown in Figure 3(b).

Calculate the weighted entropy E_n of coefficients in sub-band HL_i.

x_1	x_2	x_3
x_4	x_0	x_5
x_6	x_7	x_8

Figure 3(b).Template made of nine coefficients form the sub-band block.

The embedding is done by changing a difference value in one range into any of the difference values in the same range. In other words, in the proposed data embedding process, we adjust the gray values in each two- pixel pair by two new ones whose difference value cause changes unnoticeable to an observer of the stego-image.

Compute a new difference d':

$$d' = \begin{cases} l_k + b & for \quad d \geq 0 \\ -(l_k + b) & for \quad d < 0 \end{cases} \tag{4}$$

Where *b* is the value of the sub-stream *S*.

Because the value *b* is in the range from 0 to $u_k - l_k$, the value of *d'* is in the range from uk to l_k. If we replace *d* with *d'*, the resulting changes are presumably unnoticeable to the observer. We then embed *b* by performing an inverse calculation from *d'* described next to yield the new gray values (g'$_i$, g'$_{i+1}$) for the pixels in the corresponding two pixel block (p'$_i$, p'$_{i+1}$) of the stegno-image.

The embedding of the message bit into sub-band HL_i is done by the following embedding strategy:

$$\begin{aligned} &g_{j'} = g_j - v_i \cdot \lceil (d'-d)/2 \rceil, \; g_{j+1'} = g_{j+1} + v_i \cdot \lfloor (d'-d)/2 \rfloor, && \text{if } d \text{ is an odd number} \\ &g_{j'} = g_j - v_i \cdot \lfloor (d'-d)/2 \rfloor, \; g_{j+1'} = g_{j+1} + v_i \cdot \lceil (d'-d)/2 \rceil, && \text{if } d \text{ is an even number}. \end{aligned} \tag{5}$$

where g_j is a *sub-band coefficient*, $v_i = En_i \cdot (T_0+T_1+T_2)/3 = En_i \cdot T_1$. (6)

$T_0 = Avg(|B_i|)$, $T_1 = T_0 + 1/16 \cdot Std(|B_i|)$, $T_2 = T_0 + 1/8 \cdot Std(|B_i|)$, *Avg*, *Std* denote the average, stand Deviation of block B_i, respectively. The above equation satisfies the requirement that the difference between g'_i and g'_{i+1} is proportional to d'. The value of scaling factor v_i is the maximum variances to modify the embedded coefficients for robustness while embedding message bits to the target coefficients and M_{index} is a secret message. A coefficient with larger weighed entropy could embed a secrete message with larger scaling factor for robustness without obviously degrading the host image.

The embedding process is finished when all the bits of the secret message are embedded. We may repeat this for more than one level.

Setp 6:

Apply the IDWT (Inverse Discrete Wavelet Transform) using the newly updated sub-band values at the level 3 and level 2 to obtain the marked image.

Message retrieval phase

The process of extracting the embedded message proceeds by using the seed of the pseudo-random scheme to produce the same traversing order for visiting the two-pixel blocks as the embedding process. Assume that the block in the transformed stego-image that the gray value (g^*_i, g^*_{i+1}), and that the difference d^* of the two gray values is with index K.

Calculate the wavelet transform of the marked cover image

Calculating the difference of the two pixels and the number of bits embedding in these two pixels:

$$d^* = g^*_{i+1}, - g^*_i \tag{7}$$

From d^* we can calculate the number of bits *n* as before.

Replace *d* with a new value *d'* which is based on bits values to be extracted and the lower bound value of range *k* according to width of range *K*. The value of b, which is embedded in this two-pixels block is then extracted out using the equation

$$b = \begin{cases} d^* - l_k & for \quad d^* \geq 0 \\ -d^* - l_k & for \quad d^* < 0 \end{cases} \tag{8}$$

Then, we can calculate the original pixels value in the transformed domain by the following equation:

$g_{j'} = g_j^* + v_i \cdot \lceil (d'-d^*)/2 \rceil$, $g_{j+1'} = g_{j+1}^* - v_i \cdot \lfloor (d'-d^*)/2 \rfloor$, *if d is an odd number*

$g_{j'} = g_j^* + v_i \cdot \lfloor (d'-d^*)/2 \rfloor$, $g_{j+1'} = g_{j+1}^* - v_i \cdot \lceil (d'-d^*)/2 \rceil$, *if d is an even number* (9)

where $d^* = g^*_{i+1}, - g^*_i$,

$$d' = \begin{cases} l_k + n & for \quad d^* \geq 0 \\ -(l_k + n) & for \quad d^* < 0 \end{cases} \tag{10}$$

Reconstruct the original cover by apply the inverse wavelet transform (IDWT).

4. EXPERIENTAL RESULTS

In this section, experiments are carried out to prove the efficiency of the proposed scheme. The proposed method has been simulated using the MATLAB 7 program on Windows XP platform. A set of images of size 512 × 512 are used for experimental test as original cover (carrier) images (as illustrated in Figure 4).

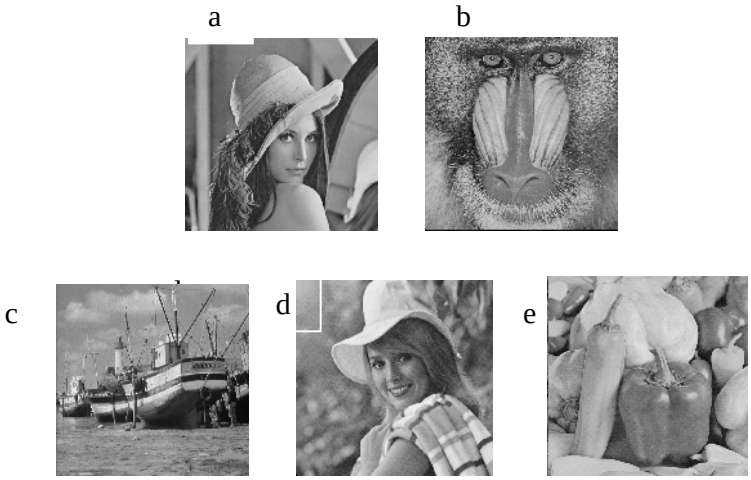


Figure 4: Example of some tested cover images (512 X 512) (a)"Lena", (b) "Baboon", (c) "boat", (d) "elaine", and (e) " peppers"

Figure 5 illustrates the PSNR versus different message sizes applied for Lena image. The figure shows that the PSNR remains considerably high even for large message sizes. Figure 6 demonstrates the hiding capacity versus different hiding levels for five test images. Figure 7 shows the change in PSNR, at different hiding levels, for embedded secrete messages of different lengths. These experiments prove that a high hiding capacity (payload) is adopted with a slight decay in the PSNR.

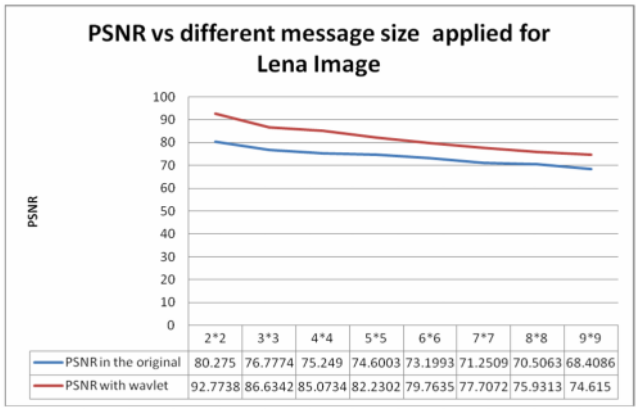


Figure 5: PSNR vs. different message size applied for Lena image

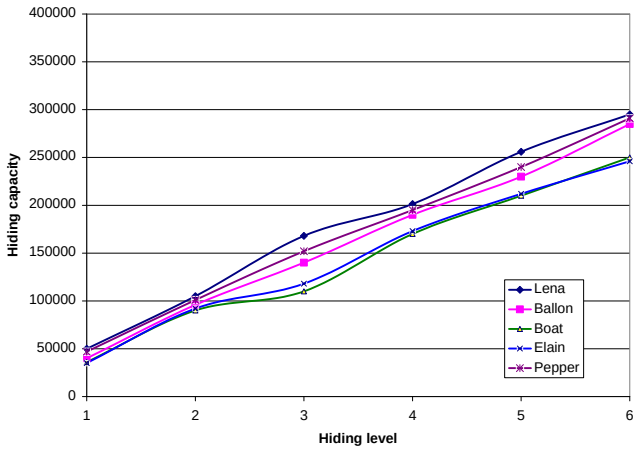


Figure 6: Hiding capacity versus hiding levels for five test images

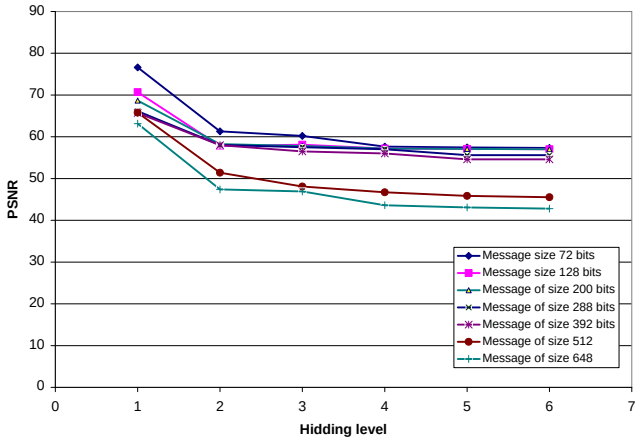
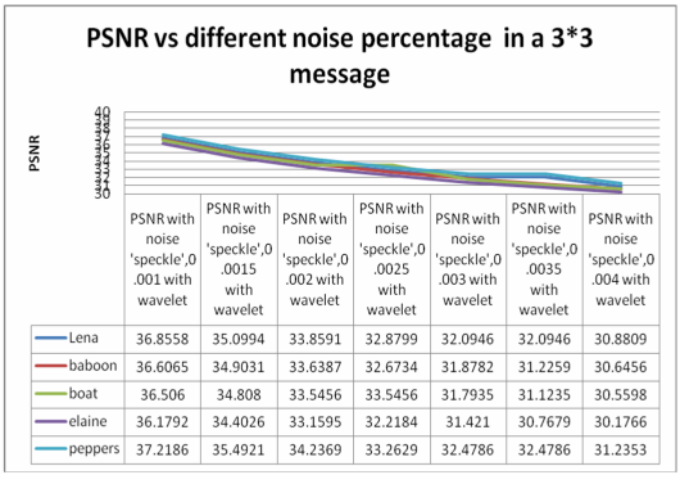


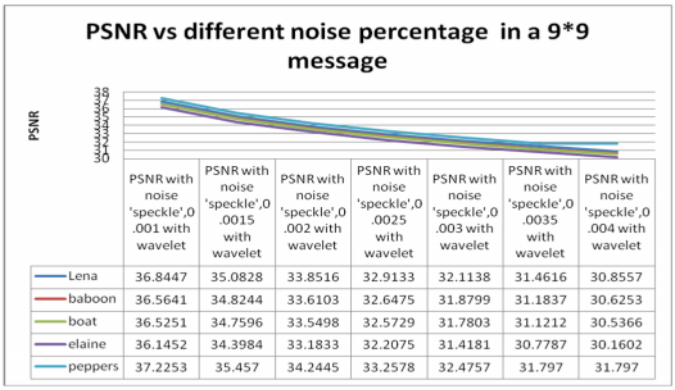
Figure 7: PSNR versus different levels with different message sizes, applied on Lena image.

To illustrate the robustness of the proposed model versus different types of noise, experiments have been carried out on the experimental test best with different percentages of noise. Figure 8 illustrates the PSNR vs. different noise percentage applied on various test images (Lena, balllon, boat, Elaine and peppers), for embedding a secrete message of size a 3*3 bytes, while figure 9 shows the PSNR vs. different noise percentage for a payload of size a 3*3 bytes.



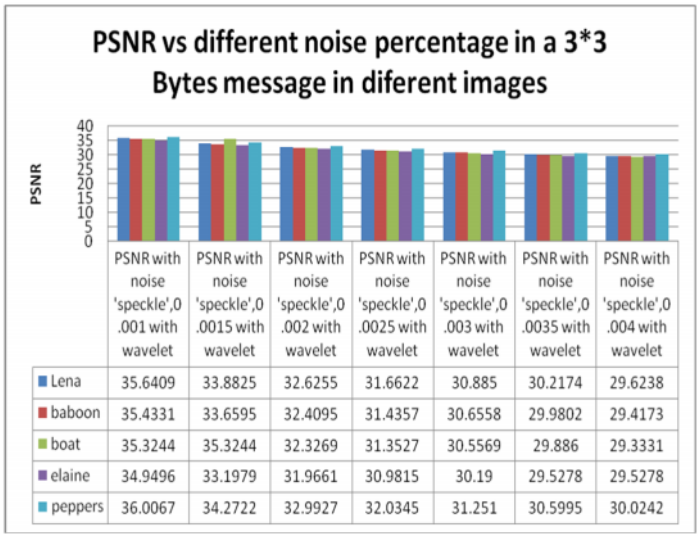
	PSNR with noise 'speckle',0.001 with wavelet	PSNR with noise 'speckle',0.0015 with wavelet	PSNR with noise 'speckle',0.002 with wavelet	PSNR with noise 'speckle',0.0025 with wavelet	PSNR with noise 'speckle',0.003 with wavelet	PSNR with noise 'speckle',0.0035 with wavelet	PSNR with noise 'speckle',0.004 with wavelet
Lena	36.8558	35.0994	33.8591	32.8799	32.0946	32.0946	30.8809
baboon	36.6065	34.9031	33.6387	32.6734	31.8782	31.2259	30.6456
boat	36.506	34.808	33.5456	33.5456	31.7935	31.1235	30.5598
elaine	36.1792	34.4026	33.1595	32.2184	31.421	30.7679	30.1766
peppers	37.2186	35.4921	34.2369	33.2629	32.4786	32.4786	31.2353

Figure 8: PSNR vs. different noise percentage in a 3*3 message



	PSNR with noise 'speckle',0.001 with wavelet	PSNR with noise 'speckle',0.0015 with wavelet	PSNR with noise 'speckle',0.002 with wavelet	PSNR with noise 'speckle',0.0025 with wavelet	PSNR with noise 'speckle',0.003 with wavelet	PSNR with noise 'speckle',0.0035 with wavelet	PSNR with noise 'speckle',0.004 with wavelet
Lena	36.8447	35.0828	33.8516	32.9133	32.1138	31.4616	30.8557
baboon	36.5641	34.8244	33.6103	32.6475	31.8799	31.1837	30.6253
boat	36.5251	34.7596	33.5498	32.5729	31.7803	31.1212	30.5366
elaine	36.1452	34.3984	33.1833	32.2075	31.4181	30.7787	30.1602
peppers	37.2253	35.457	34.2445	33.2578	32.4757	31.797	31.797

Figure 9: PSNR vs. different noise percentage in a 9*9 message



	PSNR with noise 'speckle',0.001 with wavelet	PSNR with noise 'speckle',0.0015 with wavelet	PSNR with noise 'speckle',0.002 with wavelet	PSNR with noise 'speckle',0.0025 with wavelet	PSNR with noise 'speckle',0.003 with wavelet	PSNR with noise 'speckle',0.0035 with wavelet	PSNR with noise 'speckle',0.004 with wavelet
Lena	35.6409	33.8825	32.6255	31.6622	30.885	30.2174	29.6238
baboon	35.4331	33.6595	32.4095	31.4357	30.6558	29.9802	29.4173
boat	35.3244	35.3244	32.3269	31.3527	30.5569	29.886	29.3331
elaine	34.9496	33.1979	31.9661	30.9815	30.19	29.5278	29.5278
peppers	36.0067	34.2722	32.9927	32.0345	31.251	30.5995	30.0242

Figure 10: PSNR vs. different noise percentage in a 3*3 Bytes message in different images

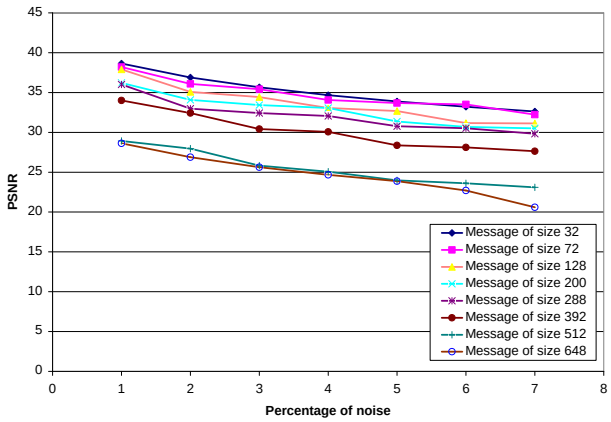


Figure 11: PSNR vs. message sizes with different noise(attack) percentage applied for Lena image

Figure 11 illustrates the change in PSNR versus different percentages of noises, for various sizes of embedded secrete messages.

Table 1 compares the performance of our proposed model with Chen et al.; 2009 and A. Nag et al. (2010). As observed from the table, the hiding capacity and PSNR of our proposed model is better than the modified slide match algorithm [19] and A. Nag et al. (2010) [16].

TABLE I. PSNR COMPARISON WITH THE MODIFIED SIDE MATCH SCHEME [19] AND A. NAG ET AL. (2010) SCHEME [16]

Cover Images	Modified Side Match			A. Nag		Proposed Method	
	Size (Kb)	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)
Lenna	256	168,289	48.64	299520	50.5	343726	75.2
Baboon	256	306,209	39.31	299520	50.3	386951	60.3
Boat	256	207,497	44.33	299520	50.4	380897	70.5

As observed from the table above, there is an average improvement of 20% in the PSNR of the proposed model compared with that of A. Nag model and 22% improvement compared with the modified sliding match algorithm. Moreover, a considerable increase in the embedding capacity is achieved.

5. CONCLUSION

A new efficient computer-based steganographic method has been proposed for embedding secret messages into images without producing noticeable changes. The proposed model explores the possible of providing higher hiding capacity with lower distortion in the wavelet domain. The method utilizes the characteristic of the human vision's sensitivity to gray value variations. Experimental results showed the high invisibility of the proposed model as well as the large hiding capacity it provides. It provides an easy way to produce a more imperceptible result than those yielded by simple least-significant-bit replacement methods. The method not only provides a better way for embedding large amounts of data into cover images with imperception, but also offers an easy way to accomplish secrecy.

REFERENCES

[1] Johnson, N. F. and Katzenbeisser, S. (2000) A survey of steganographic techniques, in S. Katzenbeisser and F. Peticolas (Eds.): *Information Hiding*, Artech House, Norwood, MA, pp.43-78.

[2] Chung Kuo, W., Hung Kuo, S. , Chyau Wuu, L. (2010) High Embedding Reversible Data Hiding Scheme for JPEG, *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Darmstadt, Germany, pp.74-77.

[3] Verkhovsky, B. S. (2011) Scheme for Secure Communication via Information Hiding Based on Key Exchange and Decomposition Protocols, *Int'l J. of Communications, Network and System Sciences*, Vol.4 No.2., PP.77-81

[4] Katzenbeisser, S., Sadeghi, A. Information Hiding, 11th International Workshop (2009) Darmstadt, Germany, June 8-10, 2009, *Lecture Notes in Computer Science 5806*, Springer.

[5] Wang, H and Wang, S, (2004) Cyber warfare: Steganography vs. Steganalysis, *Communications of the ACM*, 47:10, October 2004

[6] Jamil, T., (1999) Steganography: The art of hiding information is plain sight, *IEEE Potentials*, 18:01, 1999.

[7] Moerland, T. (2009) Steganography and Steganalysis, Leiden Institute of Advanced Computing Science,

[8] Bandyopadhyay, S. K., Maitra, I. K. (2010) An Application of Palette Based Steganography, *International Journal of Computer Applications, Volume 6– No.4*, pp. 24-27.

[9] Li, Zhi., Sui, Ai, Fen., and Yang, Yi, Xian. (2003) A LSB steganography detection algorithm, *IEEE Proceedings on Personal Indoor and Mobile Radio Communications*: 2780-2783.

[10] Fridrich, J. and Goljan, M. (2003) Digital image steganography using stochastic modulation, SPIE Symposium on Electronic Imaging, San Jose, CA.

[11] Habes, A. (2005) 4 least Significant Bits Information Hiding Implementation and Analysis , *ICGST Int. Conf. on Graphics, Vision and Image Processing (GVIP-05)*, Cairo, Egypt.

[12] Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf

[13] Chang, C.-C., Chen, T.-S., and Chung, L.-Z. (2002) A steganographic method based upon JPEG and quantization table modification, *Information Sciences*, vol. 141, 2002, pp. 123-138.

[14] Chu, R., You, X., Kong, X. and Ba, X. (2004) A DCT-based image steganographic method resisting statistical attacks", InProceedings of (ICASSP '04), *IEEE International Conferenceon Acoustics, Speech, and Signal Processing*, 17-21 May.vol.5, pp V-953-6.

[15] Tseng, H.-W. and Chang, C.-C. (2004) Steganography using JPEG-compressed images, *The Fourth InternationalConference on Computer and Information Technology*, CIT'04, pp. 12-17.

[16] Chen, B. and G.W. Wornell, (2001) Quantization index modulation: A class of provably good methods for digital watermarking and information embedding.*IEEE Trans. Inform. Theor.*, 47: 1423-1443.

[17] Nag, A., Biswas, S., Sarkar, D., Sarkar, P.P. (2010) A novel technique for image steganography based on Block-DCT and Huffman Encoding, *International Journal of Computer Science and Information Technology*, Volume 2, Number 3, pp.103-112.

[18] Fridrich, J. and Goljan, M. (2003) Digital image steganography using stochastic modulation, SPIE Symposium on Electronic Imaging, San Jose, CA.

[19] Lewis, A. S. and Knowles, G. (1992) Image compression using the 2D wavelet transform *IEEE Trans. Image Processing*, Vol. 1, pp. 244-250.

[20] Chen, P.Y. and Wu, W.E. (2009) A Modified Side Match Scheme for Image Steganography, *International Journal of Applied Science and Engineering*, 7, 1: 53 – 60.

[21] Qing-zhong, L., Chen, Y., Dong-sheng, C. (2006) Robust color image hiding method in DCT domain, *OPTOELECTRONICS LETTERS*, Vol.2 No. 3, pp. 218-220.