Comprehensive Information Hiding in an Image Using Wavelet Transform

Snehal Ghormade, Bhagwat Kakde

Abstract— This research paper is concerned with the steganography in a digital image. Steganography is always preferred upon encrypting the secret information because hiding arouses less suspicion as it conceals its very existence. The techniques developed in the past mainly comprises of hiding only a text or an image within an image. The scheme presented here is an attempt to achieve an efficient wavelet based technique for hiding different forms of multimedia information within an image. This system will certainly provide additional intelligence as audio, text and image are embedded in a single image concurrently. Experimental results show that the proposed algorithm can be successfully implemented with very high quality and imperceptibility. Further, the approach used here provides an additional security which prevents the intruder from retrieving the secret information even if the existence of secret information is noticed.

Index Terms—Discrete wavelet transform, Image Processing, Information Hiding, Steganography, Secured Digital Communication.

I. INTRODUCTION

Secure data transmission has been a significant problem throughout human history. It is often thought that communication may be secured by encrypting the traffic, but this has rarely been adequate in practice. From ancient times, the art of hiding is always preferred upon enciphering the secret information because hiding arouses less suspicion as it conceals its very existence. This preference persists in many operational contexts to this day. For example, Military and intelligence agencies require inconspicuous communications. Even if the content is encrypted, the detection of a signal on a modern battle field may lead rapidly to an attack on the signaler. For this reason, military communications use techniques such as spread spectrum modulation or meteor scatter transmission to make signals hard for the enemy to detect or jam.

Secure data transmission can be carried out by hiding a message in cover data; the concept which is termed as Steganography. Steganographic techniques allow communication between two authorized parties without an observer being aware that the communication is actually taking place. These techniques have many Army applications in the defensive information warfare arena, such as hidden communication, in-band captioning, and tamper-proofing. A useful steganographic system must provide a method to embed data in an imperceptible manner, allow the data to be readily extracted, promote a high information rate or payload capacity, and incorporate a certain amount of robustness to removal [1].

Many interesting steganographic techniques have been created and its continuing evolution is guaranteed by a growing need for information security. A large number of steganographic tools employing different data hiding schemes are available as commercial software or freeware. These schemes are simple but, significant overhead, insufficient visual quality and merely single media embedding capability are serious problems and limitations.

In this paper, an efficient wavelet based technique for hiding different forms of data within an image is presented. The proposed approach has several advantages such as exceptionally high intelligence, very high imperceptibility and smartness incorporated in embedding.

The paper is organized as follows: Section II reviews the existing state of the data hiding research. Here, the main categories of information hiding algorithms covered till date are discussed. Although, the survey is not exhaustive and some of the algorithms may have been missed out. Section III presents some necessary background on wavelet transforms and decomposition. Section IV presents the projected information hiding system followed with Section V which evaluates the results to demonstrate the performance. Conclusion and further implications are covered in section VI.

II. RELATED WORK

Steganography and watermarking techniques though have different implications but are based on the same methodology of embedding. Before putting forward the proposed system, some necessary background is presented in this section.

Several information hiding systems have been proposed with different contributions. Roughly speaking, these contributions can be categorized according to their processing domain and signal type of secret data. The two processing domain categories, the spatial domain and the frequency domain information hiding have been extensively used in past. Spatial domain steganographic techniques, also known as substitution techniques, are a group of relatively simple techniques that create a covert channel in the parts of the cover image in which changes are likely to be a negligible when compared to the human visual system (HVS). The earlier watermarking schemes are almost spatial-domain approaches. The simplest approach for embedding watermark by inserting it in the least significant bits (LSBs) of image pixels was proposed by Van *et. al.*; however, they lack the basic robustness [2]. These were able to survive simple operations such as cropping, any additive noise, however, it was not possible to process the composite image under operations such as intensity enhancement, resampling, requantization, image enhancement, etc.

Manuscript published on 28 February 2014.
* Correspondence Author (s)

Snehal Ghormade*, Department of Electronics & Communication Engineering, RGPV, Bhopal, India.
Bhagwat Kakde, Department of Electronics & Communication Engineering, RGPV, Bhopal, India.

Another spatial domain technique based on the statistical method called patchwork was proposed by Bender *et.al.* [3] which was having high resistance to most non-geometric image modifications. However, low bit-rate and difficulty in decoding the image under severe affine transformations were the limitations. Predictive coding scheme in which the correlations between adjacent pixels were exploited can also be found in literature [4]. This technique when compared to LSB substitution coding shows much more robustness.

In contrast to the spatial-domain techniques, frequency domain techniques can embed more bits of secret data and are more robust to attack; thus, they are more attractive than the spatial-domain-based methods. These techniques take the advantage of the human visual system's low sensitivity to high and middle frequency information. A DCT based system was proposed which was highly resistant to the JPEG compression and significant amount of noise [5]. The main advantage of DCT which makes it attractive for information hiding is its energy compaction property. This property divides the image into distinct frequency bands which makes it easy to embed the information in the desired area of the image. Cox *et.al.* used the spread spectrum communication for multimedia watermarking. They embedded a set of independent and identical distributed sequences drawn from a Gaussian distribution into the perceptually most significant frequency components of an image [6]. This method resists JPEG compression with a quality factor down to 5%, scaling, dithering, cropping and collusion attacks. On the other hand, several methods used wavelet transform to hide data to the frequency domain to provide extra robustness. This transformation which is very similar to the theoretical model of Human Visual System (HVS).

The wavelet based information hiding systems are more preferred choice because of the advantages listed out by several authors in their respective research over the years. Xia *et. al.* added a Gaussian random noise to the large coefficients in the DWT domain [7] which proved to be robust to several kinds of distortion such as additive noise, resolution reduction and compression. In another system, a pseudo-random sequence was adaptively added to the DWT coefficients of three largest detail sub-bands while the detection was achieved by measuring the correlation between the watermarked coefficients and the watermarking code [8]. Kundur *et. al.* proposed a multi-resolution fusion based watermarking method for embedding gray scale logos into wavelet transformed images. Simulation results showed that the proposed technique was highly robust to compression and additive noise. A watermarking algorithm using a combination of DWT and singular value decomposition (SVD) was developed which verify robustness under the image operations such as filtering, addition of noise, JPEG compression, cropping, resizing, rotation and pixilation [9]. Ramani *et. al.* proposed an algorithm based on Integer to Integer Wavelet Transform (IWT) with Bit Plane Complexity segmentation (BPCS). This system provided evidence of very high data hiding capacity [10]. Another method with very easy embedding and extracting processes was presented which embeds the invisible watermarks into the salient features of the original image [11]. However, the size constraints of the watermark were a drawback. A technique based on combination of joint DWT-DCT transformation by scrambling the binary watermark logo using Arnold cat map can be found in literature [12]. This technique was more robust and imperceptible as the visual artifact drawback of the block based DCT method is reduced giving comparatively higher PSNR value. Most of the papers in literature propose new algorithms. Some of these algorithms, although very intellectual, cannot be used to hide the different forms of media simultaneously.

III. BACKGROUND ON WAVELETS AND FILTER BANKS

Before we introduce the algorithm, some necessary background on wavelets and filter banks is reviewed. The study of the wavelet transform has thrived in the past two decades. Now, the wavelet transform is considered to be a fairly simple mathematical tool, and it has many applications in various fields. The continuous and discrete wavelet transforms are given in (1) and (2), respectively

$$W(a,b)_{cwt} = \int_{-\infty}^{\infty} f(t)\frac{1}{\sqrt{a}}\psi^*\left(\frac{t-b}{a}\right)dt \qquad \text{------ (1)}$$

$$W(a,b)_{dwt} = \left\{\sum_j x[j]h(\text{n}-\text{j}); \sum_j x[j]\text{g}(\text{n}-\text{j})\right\} \text{------ (2)}$$

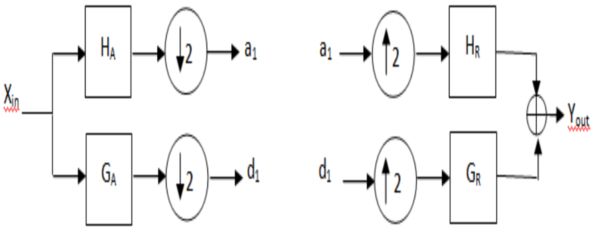
Where, $f(\text{t})$: square integrable function,

$\psi(\text{t})$: mother wavelet function,

$h[n]$: low-pass analysis filters

$g[n]$: high-pass analysis filters

The wavelet function also finds its way into the field of signal analysis. Compared with the traditional transforms, the Fourier transform for instance, the wavelet transform has an advantage of achieving both spatial and frequency localization. In digital signal and image processing, the discrete wavelet is closely related to filter banks. A typical two channel analysis and reconstruction structure is given in Fig 3.1.



(i) (ii)

Fig. 3.1 Two-channel filter banks for (i) analysis and (ii) reconstruction

It is known that the filter banks will provide perfect reconstruction (i.e. $Y_{out} = X_{in}$) if they satisfy Eq. (3) and (4).

$$H_A(\text{z})H_R(\text{z}) + G_A(\text{z})G_R(\text{z}) = 2 \qquad \text{--------- (3)}$$

$$H_A(-\text{z})H_R(\text{z}) + G_A(-\text{z})G_R(\text{z}) = 0 \qquad \text{--------- (4)}$$

To extend the above analysis to images, we can consider digital images as two-dimensional signals and apply the one dimensional wavelet transform to the horizontal and vertical directions separately.

The structure is given in Fig. 3.2.To do multiresolution analysis, structures in Fig 3.1 (i and ii) can be cascaded depending on the dimensions of the signal.

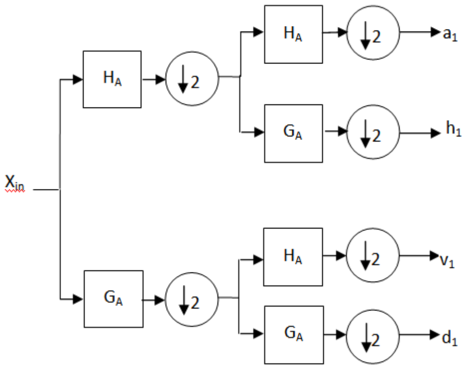
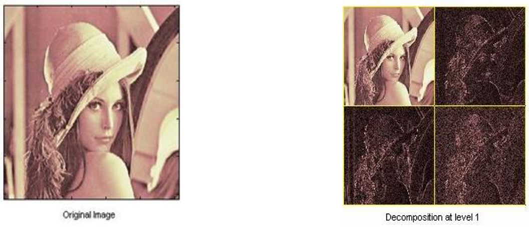


Fig. 3.2 One level DWT filter structure for an image

A. *Wavelet Transform of an Image*

The basic idea of the DWT for a two-dimensional image is described as follows. An image is first decomposed into four parts of high, middle, and low frequencies (i.e., a1, h1, v1, d1 subbands) by critically subsampling horizontal and vertical channels using subband filters. The subbands labeled h1, v1 and d1 represent the finest scale wavelet coefficients. To obtain the next coarser scaled wavelet coefficients, the subband a1 is further decomposed and critically subsampled. This process is repeated several times, which is determined by the application at hand. An original 512 × 512 Lena image and its DWT decomposition are shown in Fig. 3.3. As can be seen, the approximation subband contains most of the energy of the input image while the other sub-bands don't convey much information.



(i) *(ii)*

Fig. 3.3 Two level 2D DWT decomposition of an image using 'Haar' wavelet

B. *Wavelet Transform of an Audio*

An audio being a one dimensional signal is decomposed into two pieces of low frequency (a_1) and high frequency (d_1) subbands by performing sub-sampling using sub-band filters. A one level decomposition of an audio signal is shown in Fig. 3.4. Here also, most of the information lies in the low frequency approximation sub-band (a_1).

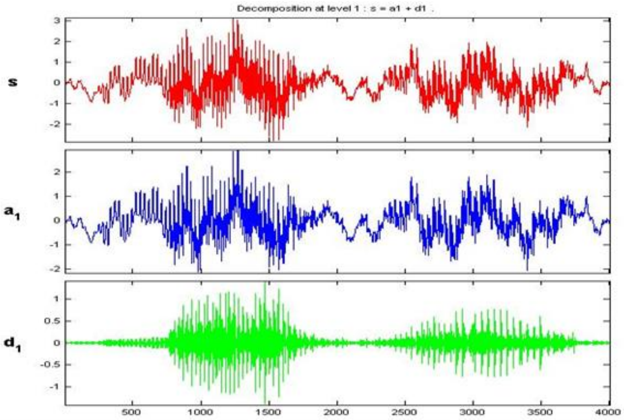


Fig. 3.4 One level 1D DWT of an audio input using 'Haar' wavelet

From the wavelet decomposition of a image and an audio, it can be said that the most significant information of a media lies in the approximation subband.

IV. PROPOSED SYSTEM

In this section, the system for hiding information in the digital images is presented. It is already known that the human visual system has different sensitivities for different frequencies. It was pointed out by the author that the low frequency noise is usually more noticeable [13]. Thus in this system, the secret information is inserted in the mid and high frequency range to achieve the desired imperceptibility from the intruder.

The embedding framework is shown in Fig. 4.1. In this approach, the gray scale cover image is decomposed using DWT into four sub-bands: low frequency approximation, middle frequency horizontal, middle frequency vertical and high frequency diagonal (a, h, v and d). In the same manner, the secret image is decomposed in a_1, h_1, v_1 and d_1. In the subsequent step, the audio is decomposed using one dimensional DWT to give the approximation (a_3) and the diagonal (d_3) sub-bands. Here, the inserted text is first converted into an identical image and then the same DWT decomposition is performed to obtain a_2, h_2, v_2 and d_2. The two scaling constants: k and q are selected such that the difference between two is as much as possible. Assuming that the secret image, secret text and secret audio are to be embedded in h, v and d sub-bands respectively, the embedding can be accomplished as follows:

i) For embedding secret image, $h = k*h+q*a_1$

ii) For embedding secret text, $v = k*v+q*a_2$

iii) For embedding secret audio, $d = k*d+q*a_3$

Finally, the inverse DWT is performed to obtain the stego-image.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

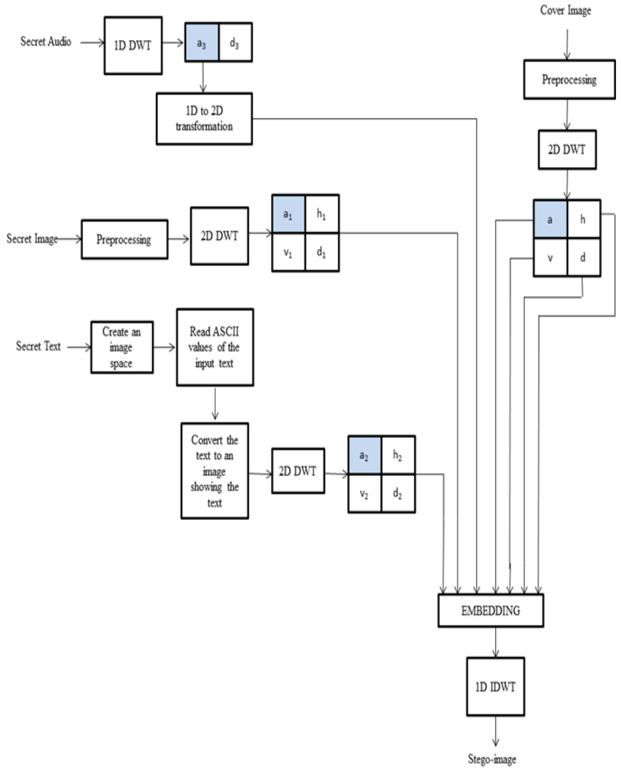


Fig. 4.1 The Embedding Framework

In the extraction phase, the steps employed in the embedding phase are applied in the reverse order. The recovered image is decomposed using the same wavelet family as that used during embedding phase and is related with the decomposed cover image. The approximation coefficients of all the hidden data are calculated using the following manipulations;

i) For Secret Image, $a_1 = (h_R - k*h)/q$

ii) For Secret Text, $a_2 = (v_R - k*v)/\mathrm{q}$

iii) For Secret Audio, $a_3 = (d_R - k*d)/\mathrm{q}$

After applying the IDWT (1D for audio and 2D for image) by assigning the coefficients of all the sub-bands as zero except for the approximation coefficients obtained from above manipulations i.e. a_1, a_2, a_3, the hidden data can be easily retrieved.

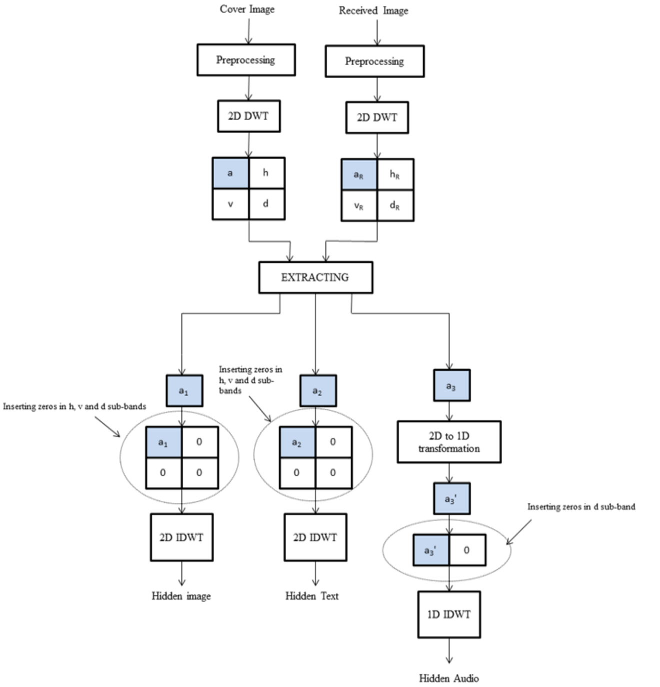


Fig. 4.2 The Extracting Framework

V. RESULTS AND DISCUSSIONS

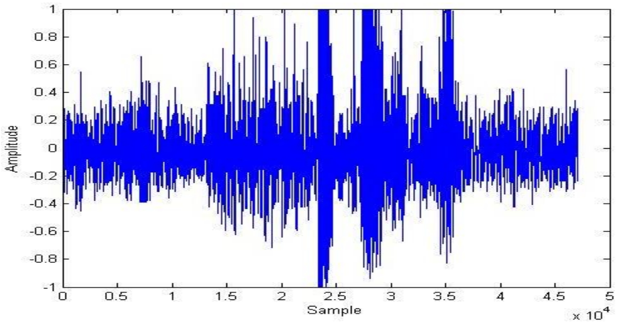
In this section, the performance of the proposed system is demonstrated. The test images of size 512 x 512 are used. The text input is also converted into an equivalent image of size 512 × 512 while the audio input is selected such that the number of samples must be less than 65536 x 2 in order to incorporate it within the cover image. The similarity metrics such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Maximum Difference (MD), Average Difference (AD), Normalized Cross Correlation (NCC), Structural Content (SC) and Normalized Absolute Error (NAE) are calculated to check the effectiveness of the system.

A. Embedding Process Assessment

The cover image and the secret information in the form of secret image, secret text and secret audio are shown in Fig.5.1.

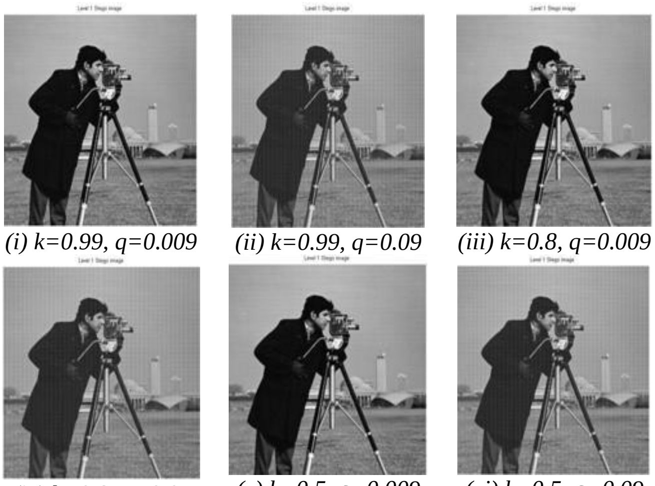
The resultant stego-image obtained after the embedding phase with different values of scaling constants is shown in Fig. 5.2. The performance evaluation is done by computing the values of the similarity metrics which are tabulated in Table 5.1.

(i) *(ii)* *(iii)*



(iv)

***Fig. 5.1** The Different Form of media for Embedding (i) Cover Image, (ii) Secret Image, (iii) Secret Text and (iv) Secret Audio.*



(i) k=0.99, q=0.009 *(ii) k=0.99, q=0.09* *(iii) k=0.8, q=0.009*

(iv) k=0.8, q=0.09 *(v) k=0.5, q=0.009* *(vi) k=0.5, q=0.09*

Fig. 5.2: The Resulted Stego-Images with Different Embedding Constants

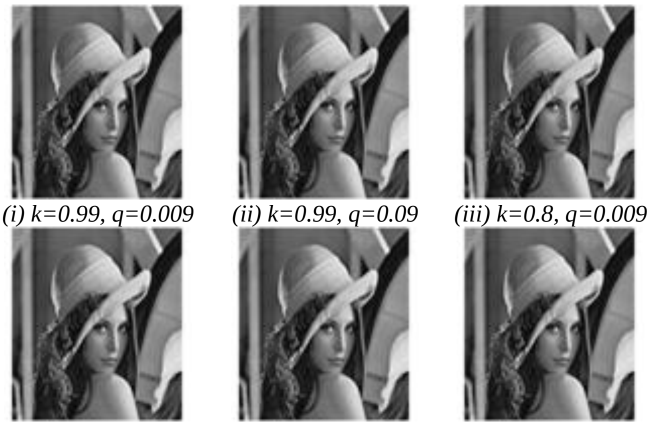
Table 5.1 Calculated Values of Similarity Metrics between the Cover Image and Stego Image

Metrics	k=0.990 q=0.009	k=0.990 q=0.09	k=0.8 q=0.009	k=0.8 q=0.09	k=0.5 q=0.009	k=0.5 q=0.09
MSE	40.1328	20.1271	38.2350	20.1266	33.4562	20.0299
PSNR	0.0196	0.1969	0.0689	0.2032	0.1539	0.2770
MD	-1.3E-16	-1.3E-16	-1.3E-16	-1.3E-16	-1.3E-16	-1.3E-16
AD	1.0000	1.0005	0.9990	0.9995	0.9974	0.9979
NCC	0.9996	0.9648	1.0015	0.9667	1.0037	0.9690
SC	0.0194	0.1942	0.0215	0.1934	0.0344	0.1927
NAE	9.70E-05	0.0097	1.50E-04	0.0097	4.51E-04	0.0099

B. Extraction Process Assessment

The main criterion for the successful retrieval of the secret data is to be able to extract the information intended for being transmitted secretly while maintaining the imperceptibility of the stego-image. The recovered secret data are shown in the Fig. 5.3, 5.4 and 5.5. The images are compared based on the similarity metrics which are tabulated in the Table 5.2, 5.3, 5.4. For estimating the quality of the retrieved audio signal, peak signal to noise ratio is calculated between the original audio and the retrieved audio signal. Here, it can be observed that the quality of the extracted secret data is independent of the user inserted constant k and q.

a) Retrieved Secret Images:



(i) k=0.99, q=0.009 *(ii) k=0.99, q=0.09* *(iii) k=0.8, q=0.009*

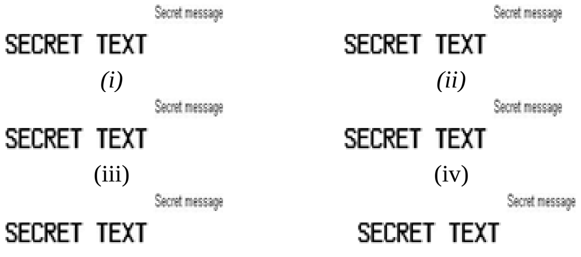
(iv) k=0.8, q=0.09 *(v) k=0.5, q=0.009* *(vi) k=0.5, q=0.09*

Fig. 5.3 Retrieved Secret Images for Different Embedding Constants

Table 5.2 Image Similarity Metrics between the Embedded Secret Image and the Retrieved Secret Image

Metrics	k=0.990 q=0.009	k=0.990 q=0.09	k=0.8 q=0.009	k=0.8 q=0.09	k=0.5 q=0.009	k=0.5 q=0.09
MSE	09.63E-4	09.63E-4	09.63E-4	09.63E-4	09.63E-4	09.63E-4
PSNR	30.15	30.15	30.15	30.15	30.15	30.15
MD	00.37	00.37	00.37	00.37	00.37	00.37
AD	01.7E-16	-02.1E-16	-01.8E-16	-02.1E-16	-02.0E-16	-02.2E-16
NCC	00.99	00.99	00.99	00.99	00.99	00.99
SC	01.00	01.00	01.00	01.00	01.00	01.00
NAE	00.04	00.04	00.04	00.04	00.04	00.04

Retrieved Secret Text Images


Secret message
SECRET TEXT
Secret message
SECRET TEXT
Secret message
SECRET TEXT
Secret message
SECRET TEXT
Secret message
SECRET TEXT
Secret message
SECRET TEXT

(i) *(ii)*

(iii) (iv)

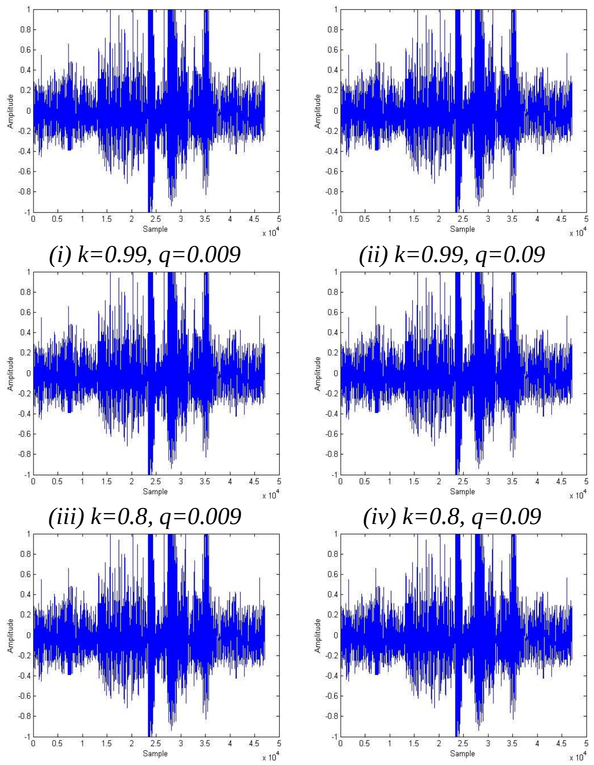
(v) *(vi)*

Fig. 5.4 Retrieved Secret Texts for Different User Inserted Constants

Table 5.3 Image Similarity Metrics between the Embedded Secret Text Image and the Retrieved Secret Text Image

Metrics	k=0.990 q=0.009	k=0.990 q=0.09	k=0.8 q=0.009	k=0.8 q=0.09	k=0.5 q=0.009	k=0.5 q=0.09
MSE	1.0E-029	3.9E-31	1.0E-029	3.8E-31	8.1E-30	3.8E-31
PSNR	289.82	304.00	289.89	304.11	290.86	304.10
MD	1.2E-14	8.4E-16	1.1E-14	8.6E-16	1.1E-14	7.7E-16
AD	-6.7E-16	-5.2E-16	-6.9E-16	-5.1E-16	-7.3E-16	-5.0E-16
NCC	01.00	01.00	01.00	01.00	01.00	01.00
SC	01.00	01.00	01.00	01.00	01.00	01.00
NAE	2.4E-15	5.4E-16	2.4E-15	5.3E-16	2.1E-15	5.2E-16

a) Retrieved Secret Audio



(i) k=0.99, q=0.009 *(ii) k=0.99, q=0.09*

(iii) k=0.8, q=0.009 *(iv) k=0.8, q=0.09*

(v) k=0.5, q=0.009 *(vi) k=0.5, q=0.09*

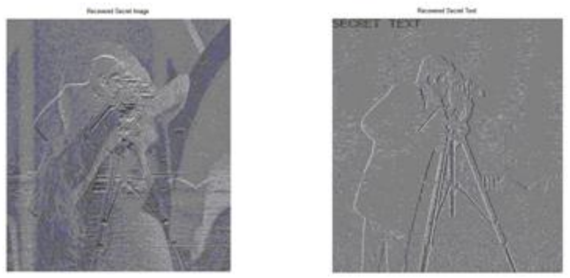
Fig. 5.5 Retrieved Secret Audio plots for Different Embedding Constants

Table 5.4 PSNR of the Retrieved Audio Signal for Different Values of User Inserted Constants

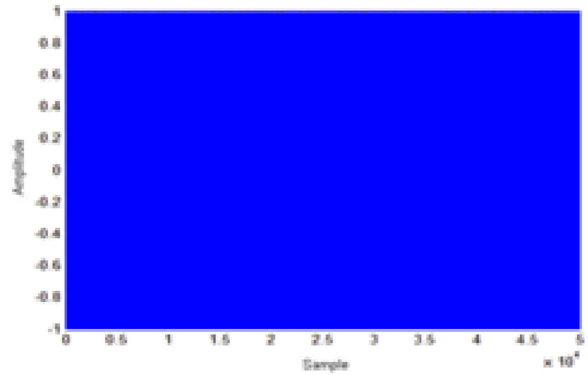
Values of user inserted constants		**PSNR (dB)**
k	**q**	
0.99	0.0090	31.5892
0.99	0.0900	31.5892
0.8	0.0090	31.5892
0.8	0.0900	31.5892
0.5	0.0090	31.5892
0.5	0.0900	31.5892

C) *Performance under Attacking Conditions*

The most common and important attack in steganography is the identification of the secret data in the cover image. As stated, the imperceptibility of the proposed system is very high, although if by some means an intruder knows the embedding/extracting algorithm, it will be still very difficult to retrieve the hidden message as the probability of entering the same values of the constants by the intruder is very less because it can be any decimal point number. Fig. 5.6 shows the retrieved secret messages when the embedding constants were assigned values as k = 0.99 and q = 0.009 during embedding, while for retrieving the intruder assigns the values as k = 0.90 and 1 = 0.001.



(i) Retrieved Secret Image *(ii)* Retrieved Secret Text



(iii) Retrieved Secret Audio

Fig. 5.6 The Retrieved Secret Information When Intruder Enters Erroneous Values of The Constants

VI. CONCLUSION

In this paper, an intelligent steganography system is designed in which the DWT is used because of its efficiency in robustness, payload capacity and imperceptibility for hiding information in a digital media to hide diverse forms of digital media in an image. The experimental results show that the imperceptibility of the stego-image is very high *i.e.* the possibility of suspicion for containing secret information in an image is negligible. It can also be pointed out that the imperceptibility of the system totally depends on the difference between the two constants (k and q) such that higher the difference between them, higher will be the imperceptibility and vice-versa. Also, the retrieved secret information is of very good quality and it is independent of the values of constants used in embedding process. The system shows robustness under the intruder attack as the intruder cannot retrieve the information until and unless he knows the exact values of embedding constants. Thus this system inherits properties such as embedding effectiveness, perceptual similarity, robustness, security and ability to carry different pay loads.

For increasing its level of security, multi-level DWT can also be incorporated with the provision for using any of the available wavelet families. This will make a very complex task for the intruder to extract the secret information from the stego-object and will also modify its pay-load capacity. The proposed model can be utilized in a wide range of applications such as in military communication, hiding important credentials in an image, law enforcement and counter intelligence, banking services, *etc*. Thus, there are ample of fields where this proposed model can be established and that too with a good level of security.

REFERENCES

[1] Gunjal and R. Manthalkar, “ An Overview of Transform Domain Robust Digital Image Watermarking Algorithms,” J. Emerging Trends in Computing and Inform. Sci. vol. 2, no. 1, 2011, pp.37-42.

[2] R. van Schyndel, A. Tirkel, and C. Osborne, “A digital watermark,” Proc. IEEE Int. Conf. Image Processing, vol. 2, pp. 86–90, 1994.

[3] W. Bender, D. Gruhl, N. Morimoto, A. Lu, “Techniques for data hiding,” IBM Systems Journal, vol. 35, nos. 3,4, pp.313-336,1996.

[4] F. Hartung and M.Kutter, “Multimedia watermarking techniques,” Proc. IEEE, vol. 87, pp. 1079–1107, July 1999.

[5] B. Kaur, A. Kaur, J. Singh, "Steganographic Approach For Hiding Image In Dct Domain," Intl. Journal Of Advances In Engineering & Technology, Vol. 1,Issue 3,pp.72-78, July 2011.

[6] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking For Multimedia," IEEE Trans. Image Processing, vol. 6, pp. 1673–1687, Dec. 1997.

[7] X. Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark For Digital Images," in Proc. IEEE Int. Conf. Image Processing, vol. 1, pp. 548–551, Oct. 1997.

[8] M. Barni, F. Bartolini, and A. Piva, "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking," IEEE Trans. Image processing, vol. 10, no. 5, 2002, pp.783-791.

[9] G. Bhatnagar and B. Raman, "A New Robust Reference Watermarking Scheme Based on DWT-SVD," Computer Standards and Interfaces, vol.31, no.5, pp. 1002-1013, 2009.

[10] K. Ramani, E. V. Prasad, Dr. S. Varadarajan, "Steganography Using BPCS To The Integer Wavelet Transformed Image," Intl. Journal of Computer Science and Network Security, vol.7 no.7, pp. 293-302,July 2007.

[11] A. Singh and A. Mishra, "Wavelet Based Watermarking On Digital Image," Indian Journal of Computer Science and Engineering,Vol 1 No 2, pp. 86-91,2011.

[12] L. Feng, L. Zheng and P. Cao, "A DWT-DCT Based Blind Watermarking Algorithm for Copyright Protection," Proc. IEEE Int. Conf. Computer Science and Information Tech., vol.7, pp.455-458, July 2010.

[13] N. Jayant, J. Johnston, and R. Safranek, "Signal compression based on models of human perception," *Proc. IEEE*, vol. 81, pp. 1385–1422, Oct. 1993.

Snehal Ghormade is presently student of M.E. in Digital Communication from RKDF IST Bhopal. She received her B.E. in Electronics and Telecommunication from Sant Gadge Baba Amravati University in 2010. Her area of research includes Image Processing, Wavelet Analysis and Digital Watermarking.

Bhagwat Kakde is Assistant Professor in Department of Electronics and Communication Engineering in RKDF IST Bhopal. He is having a teaching experience of more than 5 years. His research areas includes Signal Processing and Digital Communication.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)