Digital Image Watermarking Resilient to Local Desynchronization Attacks

Mahesh R. Shimpi[1] Prof. S. V. Gumaste[2]
[1]ME Student [2]Professor and Head of Department
[2]Department of Computer Engineering
[1,2]SPCOE, Otur (Pune)

Abstract— New opportunities have been explored in social, business, entertainment and scientific fields due to the development of high speed computer networks and that of, internet in particular. Absurdly, the cause for the development is apprehensive because of the use of digital formatted data. Digital media has several advantages over analog media such as easy editing high fidelity copying and high quality. Software products which hide information within digital audio, images and video files have been introduced to address these growing concerns. Digital watermarking is one of the data hiding techniques. The watermarking is the process of embedding a signal in to other signal robustly and invisibly at the same time, the embedded signal is called watermark and the other signal is called cover or host signal. In this paper we are presents a brief overview of digital image watermarking techniques in time and transform domain, advantages of transform (frequency) domain over time domain techniques and proposed a watermarking algorithm in transform domain by using the discrete wavelet transform.

Key words: Digital Image Watermarking, Steganography, Discrete Wavelet Transform, Haar Wavelet Transform, Single Valued Decomposition, Discrete Cosine transform, Binary Image

I. INTRODUCTION

The prisoner's problem which is the classic model for invisible communication was first proposed by Simmons [1]. It suggests that Bob and Alice are arrested for some crime and are sent in two different cells. A warden Wendy has intervened all communications between them which acts as a barrier to their escape plan. If any suspicious communication is found by the warden she will forbid the transfer of all messages and place them in solitary jail. So they must use subliminal channel for communication. For instance, a meaningful message may be hided in some harmless message. Unfortunately their escape may be obstructed by other problems like Wendy could change the information sent by Bob to Alice or could forge the messages and sent it to other prisoners through subliminal channel.

Technique in which message signal is hided in the host signal without any perceptual distortion is referred to as data hiding. It is a form of communication which relies on channel used to transfer host content. Classification of data hiding in based on relative importance of cover and message signals, nature of cover content, need for a cover signal for extraction of message signal, type of subliminal communication (synchronous or asynchronous) and type of attacks for removal of hidden messages (active and passive wardens).

Steganography and digital watermarking are two types of data hiding techniques [3]. Steganography refers to hiding of a secret message inside another message in order to avoid others to detect or decode it.

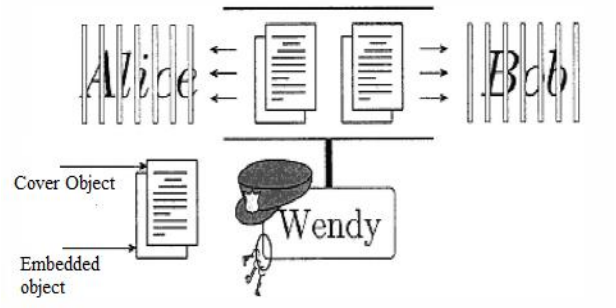

Fig. 1: The prisoner's problem

Steganography is used for spying in corporate and intelligence industries like for copyright purposes in entertainment industry [4]. In Digital Watermarking a watermark signal is embedded into a host signal (image, audio, video or a text document) robustly and invisibly at the same time [5].

Steganography and Watermarking are different from each other as:

(1) The Watermarking system always hides the information of a digital object whereas steganographic systems hide any information.
(2) Criteria of robustness differ in both since detection of hidden message is basically the main concern of steganography whereas removal of hidden message by pirate is potential concern of watermarking.
(3) Communication in watermarking systems is usually one to many while that in steganography is usually between.

II. BASIC WATERMARKING MODEL

A common model [5] for a digital watermarking system is shown in Figure 2. The inputs of the system are a vector $x = [x_1, x_2, \dots, x_M]$, representing either the original host signal samples/pixels or, more generally, a set of features of the host signal computed by a suitable transform (common examples are the Discrete Fourier Transform (DFT) and the Discrete Cosine Transform (DCT)), and some application dependent to be hidden information, here represented as a binary vector $b = [b_1, b_2, \dots b_L]$with b_i taking values in 0; 1. The embedder inserts the watermark code b into the host signal to produce a watermarked signal x_w, usually making use of a secret key s_k to control some parameters of the embedding process and allow the watermark recovery only to authorized users. The general form of the embedding function can thus be written as

$$x_w = E(x; b; s_k) \quad \dots (1)$$

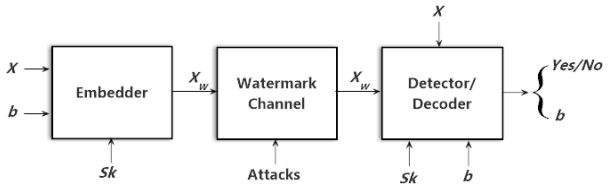

Fig. 2: A digital watermarking model

It is often useful to describe the embedding function by introducing a watermarking signal$w$, so that the watermarked signal can be expressed as

$$x_w = x + w \quad \ldots(2)$$

When the watermarking signal w depends only on b and s_k, the scheme is usually referred to as blind embedding. More advanced watermarking techniques, however, take into account also the host signal x according to the principle of digital communications with side information at the encoder, which permits the achievement of higher embedding capacities. Such schemes are referred to as informed embedding. All manipulations (both intentional and nonintentional) the watermarked content may undergo during Figure 2.

A digital watermarking system distribution and use are modeled by the watermark channel, which modifies $w_w$into the received version $\widehat{x_w}$. Based on $\widehat{x_w}$, the hidden information can be retrieved either by a watermark detector, which verifies the presence, or the absence of a specific message given to it as input, i.e.

$$D(\widehat{x_w}, b, sk) = yes/no \quad \ldots(3)$$

or by a watermark decoder, which reads the binary information conveyed by the watermarked signal, i.e.

$$D(\widehat{x_w}, b, sk) = b \quad \ldots(4)$$

When detectors and decoders do not depend from the original content$x$, as in the examples above, they are referred to as blind or oblivious detector/decoder. In some cases, however, detectors and decoders may also use the original content x to retrieve the hidden information, in which case they are referred to as nonblind detector/decoder.

III. WORKING DOMAIN

Currently, there are two most popular digital watermarking technologies including the Methods in Time Domain and Methods in Transformation Domain. Methods in the former one can be implemented more simply, but the robustness is poorer, while methods in the latter one are more popular with their stronger anti-attack functions. The typical Transformation-Domain Methods are mostly based on the domain of Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), etc. Recently, some researchers began to make use of Singular Value Decomposition (SVD) to embed a watermark [1]. SVD is a compression technique that can be used in a wide range of applications where data may be organized in a matrix representation. This paper focuses on the Haar Wavelet transform. The proposed method of watermarking is enhancement over the existing systems.

IV. WATERMARK CHARACTERISTICS

- *Fidelity*- The watermark should not lessen the quality of the content nor should it is visible to human visual system.
- *Robustness*- The watermark must survive the distortions and transformations if any. Two issues are catered by robustness. Firstly, whether or not the watermark is present after distortion in the data and secondly whether it can be detected by the watermark detector.
- *Fragility*- Sometimes opposite of robustness is required by the user of application e.g. bank notes containing physical watermarks. Any kind of copying is not survived by these watermarks and hence can be used to indicate authenticity of the bills.
- *Key Restrictions*- Restriction placed on the ability to read the watermark is an important distinguishing characteristic. Algorithms differ in their suitability to the usage of unrestricted and restricted key.
- *False Positive Rate*- Data that doesn't contain watermark and the one that contains watermark must be distinguished in most of the applications. Probability that an un-watermarked piece of data is identified as containing a watermark is known as the false positive rate
- *Modification and Multiple Watermarks*- It may be desirable to alter the watermark after its insertion. Changing the watermark can be accomplished by two ways. Either by removal of first watermark and then adding a new one or by inserting a second watermark such that both are readable, but one overrides the other. Coexistence of multiple watermarks is preferred over the first alternative.
- *Computational Cost*- The computational costs of inserting and detecting watermarks are important.

V. APPLICATIONS OF WATERMARKING

Digital watermarking can be used for a wide range of applications, such as:

- *Source Tracking*- Different watermarked content is sent to different recipients.
- *Broadcast Monitoring*- Digital watermarks are inserted into broadcast video and audio which can be detected through specialized use of software or hardware. Thus accurate content of tracking is enabled when it is distributed or broadcasted.
- *Copy Control Authentication.*- Prevention of making unofficial copies of copyrighted content.
- *Owner identification*- Ownership of the content is established.
- *Fingerprinting*- Illegal duplication and distribution of content is traced back.

VI. WHY DISCRETE WAVELET TRANSFORM

Based on the type of document the watermarking techniques are divided into the following four categories [8]: Text Watermarking, Image Watermarking, Audio Watermarking and Video Watermarking. The Image Watermarking techniques are further distinguished on the bases of two domain methods [9]: spatial domain method and transform domain method. In Spatial domain methods [10, 11] (LSB substitution, spread spectrum image steganography and patchwork) the data is embedded directly by manipulating

the pixel values, bit stream or code values of the host signal. This is much computationally simple and straightforward. Spatial domain methods are less complex as no transform is used, but are not robust against attacks whereas on the other hand transform domain watermarking techniques are more robust. This is because in transform domain watermarking when the image is inverse wavelet transformed the watermarks are irregularly distributed over the whole image which makes it difficult for the attacker to read or decode it. In this method the data is embedded by modulating the coefficients in transform domain like Discrete Fourier transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet transform (DWT). Wavelet domain watermarking has the ability to provide both spatial and frequency resolutions [12-14]. In this method a key dependent wavelet transform can be selected in order to improve the security. The wavelet transform also allows localized watermarking of image. The main advantages of wavelet transform domain for watermarking applications are:

- Space Frequency Localization: It provides good space frequency localization for the analysis of edges and textured areas.
- Multi-Resolution Representation: it provides good multi resolution representation of image, also provides hierarchical processing.
- Adaptivity: it is flexible and easily adapts to a given set of images or application.
- Linear Complexity: wavelet transform has a linear computational complexity of $0(n)$.

Digital watermarking is not secure despite its robustness [18, 19], which is a major issue in many applications. Spread spectrum scheme is the solution to the watermark security problems [20-22]. Spread spectrum is a military communication scheme which was designed to combat interference due to jamming, hiding a signal in order to transmit it at low power and to achieve secrecy [23]. In this paper we present a new approach for image hiding based on a frequency domain technique. The proposed method having good PSNR (Peak Signal to Noise Ratio) value that has been tested on four different images (Baboon, Satellite, Lena and Medical). Where the PSNR is calculated between the original and watermarked image. Larger the PSNR value, more similar is watermarked image to the original image.

$$PSNR = \frac{MN \min(m,\ n)\, I_{m,n}^2}{\sum_{m,n}(I_{m,n} - I'_{m,n})^2} \qquad \ldots (5)$$

Where $I_{m,n}$ represent a pixel, coordinate $(m;\ n)$ in the original image, $I'_{m,n}$ represent a pixel, coordinate (m, n) in the watermark image and MN-represent number of rows and columns respectively.

VII. THE PROPOSED ALGORITHM

This section presents the methods for embedding and extraction of hidden data. In the embedding process, the Haar Wavelet transform is performed on cover image Co and decomposed the cover image in to n-level (where n=4) wavelet transform. The watermarks are then embedded in the blocks located at the even columns of the HL (high-low frequency) sub band and the blocks located at the odd columns of the LH (low-high frequency) sub-band. A watermark bit is embedded in a block by modifying the four coefficients in the block according to an embedding rule. The watermark used as binary image form in the proposed algorithm. Finally, the inverse Haar wavelet transform is performed to form a watermarked image.

A. Watermark Embedding Algorithm:

1) Step 1: Read the Cover image Co (M, N) of size M x N.
2) Step 2: Read the watermark image and convert it into binary sequences B.
3) Step 3: Determine the size of watermarked image.
4) Step 4: Apply DWT to the cover image of size M x N to get four sub-bands [coff LL4, coff HL4, coff LH4, coff HH4] of size $\frac{M}{N} x \frac{M}{N}$ at n level (n = 4) decomposition. Middle frequency sub-bands HL1 and LH1 are selected for better imperceptibility and robustness.
5) Step 5: If k is the gain factor then, add PN sequences to LH1 and HL1 components.
   coff AAAH1 = coff cAAAH1 + k * pn sequence h;
   coff AAAV1 = coff cAAAV1 + k * pn sequence v;
   Here we assumed that
   coff LL4 — coff AAAA1,
   coff HL4 — coff AAAH1,
   coff LH4 — coff AAAV1, and
   coff HH4 — coff AAAD1
6) Step 6: To extract the watermark, apply the inverse DHWT on the including the modified coefficient sets, to produce the watermarked image.

B. Watermark Extraction Algorithm:

The extraction algorithm is reverse to the insertion algorithm.

- Step 1: Read the stego-image and determine size of original watermark.
- Step 2: Transform the stego image using Haar Wavelet transform to find the coefficients.

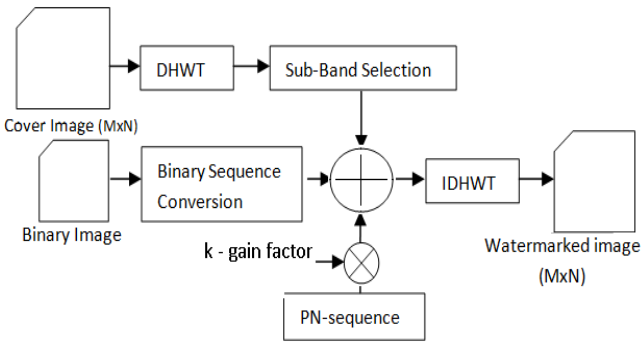

Fig. 4: Watermark Insertion Scheme

- Step 3: Add PN sequences of size $\frac{M}{N}$ x $\frac{M}{N}$ to H1 and V1 components.
  for (kk=1:Length(message vector))
  pn sequence h=round(2*(rand(Mw/16,Nw/16)-0.5));
  pn sequence v=round(2*(rand(MwI16,Nw/16)-0.5));
  corr h(kk)=corr2(cAAAH1,pn sequence h);
  corr v(kk)=corr2(cAAAV1,pn sequence v);
  corr(kk)=(corr h(kk)+corr v(kk))/2

– Step 4: The watermark image is reconstructed by converting watermark vector into watermark image (binary image) display recovered watermark image.

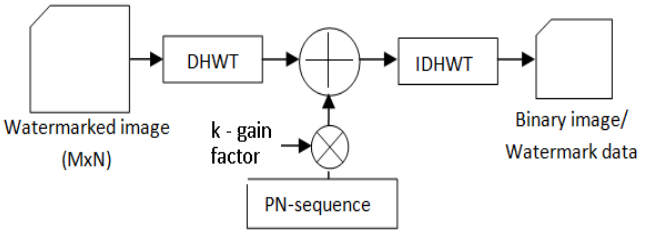

Fig. 5: Watermark Extraction Scheme

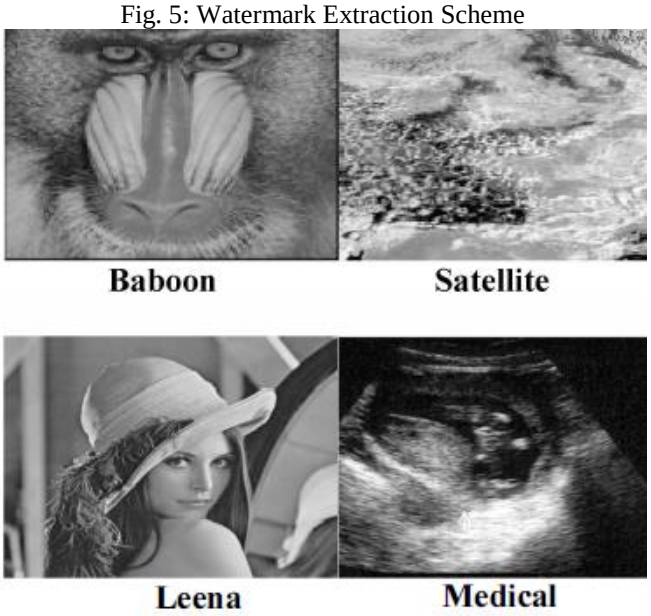

Fig. 6: Images used for Experiment

VIII. EXPERIMENTAL RESULTS

Performance of the proposed method was tested on four images (Baboon, Satellite, Leena and medical). The watermarks are in binary image formats which add robustness by allowing extraction of the watermarks even at low correlation between original and extracted watermarks as Perceptual quality of the watermarked image is measured by calculating PSNR between host and watermarked image, At the receiver side, watermark is extracted from the watermarked image. Recovered watermark is evaluated by measuring its correlation with the original watermark. The PSNR value is calculated at different gain factor, when the gain factor value is to be high the PSNR value of the image decreases (Table I, II and III).

Sr.	Image	PSNR k = 2	PSNR k = 3	PSNR k = 4
1	Baboon	38.45	33.90	30.61
2	Satellite	36.12	31.14	26.79
3	Lena	37.77	32.12	27.35
4	Medical	32.14	28.33	24.33
	Average	**36.12**	**31.34**	**27.27**

Table I: PSNR at various Gain factor

A. Robustness Analysis

Experiments of global attacks, common image-processing attacks, non-invertible attacks and local attacks have been performed to check the robustness and effectiveness of the proposed watermarking scheme. The bit error rate (BER) is used to evaluate the robustness of the watermarking scheme against various attacks. The decoding bit error rate (BER)B, defined as the ratio between the number of incorrectly decoded bits and the total number of embedded bits, is$(N_w - \varepsilon)/N_w$.

Attacks	Baboon	Satellite	Lena	Medical
Median Filter 2x2	1.2	2.1	1.1	3.5
Median Filter 3x3	4.1	6.3	3.3	9.4
Median Filter 4x4	6.7	18.9	9.9	17.3
Mean Filter 2x2	9.4	12.5	16.5	18.8
Gaussian Filter 2x2	18.1	19.8	23.2	18.8
Gaussian Filter 3x3	19.8	22.4	22.4	21.4
Gaussian Filter 4x4	20.3	25.6	25.6	25.6
Salt&Pepper Noise σ = 0.01	1.3	2.4	3.0	2.4
Salt&Pepper Noise σ = 0.02	4.8	5.9	6.1	5.9
Salt&Pepper Noise σ = 0.03	9.4	10.2	9.4	10.2
Gaussian Noise σ = 0.01	0	0	0	0
Gaussian Noise σ = 0.02	10.6	18.6	17.6	18.6
Gaussian Noise σ = 0.03	16.3	28.8	31.7	28.8
JPEG Compression 90	0	0	0	6.4
JPEG Compression 80	0	3.1	3.1	10.4
JPEG Compression 70	3.1	9.4	9.4	11.1
JPEG Compression 60	9.4	15.6	15.6	14.8
JPEG Compression 50	10.6	25.6	28.6	28.2
JPEG Compression 40	18.8	34.4	37.7	31.1
JPEG2000 40%	0	0	0	0
JPEG2000 30%	0	4.2	3.3	4.8
JPEG2000 20%	1.8	7.5	8.5	12
Rotation 0.10^0	2.1	1.2	1.8	3.1
Rotation 0.15^0	8.6	9.8	11.8	12.6
Rotation 0.20^0	12.5	22.9	23.1	28.4

Table II: Robustness against Various Some Global Attacks and Common Image-Processing Attacks with (%)

IX. CONCLUSION & FUTURE WORKS

The factors like, robustness, imperceptibility, and capacity need to be kept in the watermarking methods. These requirements are blocking each other. So according to application requirements, there is some tradeoff between these requirements. For the practical point of view, the computational cost is also an important factor. The watermarking in transform domain exploits the spatial and frequency information of the transformed data in multiple resolutions to gain robustness. The performance of watermarking methods in frequency transform domain

highly depends on the insertion and extraction techniques; one of the main advantages of watermarking in wavelet transform domain is its compatibility with the upcoming image coding standards, JPEG2000. In analyzing the drawback of the spatial domain watermarking scheme, in this paper, we have proposed an effective resynchronization method against both global attacks and local attacks. The major contributions are the following: 1) it presents a new enhanced haar wavelet based watermarking scheme, and 2) it introduces the very secure and robust watermarking of images using binary images (watermarks). The watermark is spread over the whole image so it becomes very hard to detect watermarks bits without proper gain and pn_sequences. Moreover, the scheme overcomes the drawbacks of the feature-based watermarking scheme. Our approach can be further improved by developing a more robust embedding method than DWT.

ACKNOWLEDGMENT

The author would like to thank Dr. S. V. Gumaste for providing his valuable support for result and performance comparisons and Prof. S. A. Kahate for the very helpful discussions and suggestions while working on this paper.

REFERENCES

[1] Simmons G. J., ”The Prisoners’ Problem and the Subliminal Channel” in Advances in Cryptology, Proceedings of CRYPTO Plenum Press, pp. 51-67, 1984.
[2] T. Armstrong and K. Yetsko, ”Steganography” CS-6293 Research Paper, Instructor: Dr. Andy Ju An Wang, 2004.
[3] A. Sequeira,”Enhanced Watermark Detection” M. Sc., thesis, University of Toronto, Canada, 2003.
[4] G. C. Langlaar, I. Satyawan and R. L. Lagendijk, ”Watermarking Digital Image and Video Data. A State-of-the-Ar Overview”, IEEE Signal Processing Magazine, Vol. 17, No. 5, pp. 20-46, September 2000.
[5] M. Kutter, and F. A. P. Petitcolas, ”Watermarking Digital Image and Video Data. A State-of-the-Art Overview”, IEEE Signal Processing Magazine, Vol. 19, No. 8, pp. 44-60, September 2002.
[6] S. P. Mohanty, ”Watermarking of Digital Images”, M.S. Thesis, IISc. Bangalore, India, 1999.
[7] C. M. Wolak, ”Digital Watermarking”, Preliminary Proposal, Nova Southeastern University, United States, 2000.
[8] N. Nikolaidis and L. Pitas, ”Digital Image Watermarking: An Overview”, IEEE ICMCS, Florence, Vol. I, June 7-11, pp. 1-6, 1999.
[9] I.0020J. Cox and M. L. Miller,”The First 50-Years of Electronic Watermarking”, EURASIP Journal on Applied Signal Processing, No. 2, pp. 126-132, 2002.
[10] P. Meerwald and A. Uhl, ”A Survey of Wavelet Domain Watermarking Algorithms”, Proceedings of the SPIE Security and Watermarking of Multimedia Contents, San Jose, Vol. 4314, pp. 505-516, 2001.
[11] S. Hajjara, M. Abdallah and A. Hudaib, ”Digital Image Watermarking Using Localized Biorthogonal Wavelets”, European Journal of Scientific Research, Vol. 26, No. 4, pp. 594-608, 2009.
[12] A. H. Paquet and R. K. Ward, ”Wavelet-Based Digital Watermarking for Authentication”, Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering, Winnipeg, Vol. 2, pp. 879-884, 2002.
[13] J. Feng, I. Chang Lin, C. S. Tsai and Y. P. Chu, ”Reversible Watermarking: Current and Key Issues”, International Journal of Network Security, Vol. 2, No. 3, pp. 161-170, May 2006.
[14] S. Lee, C. D. Chang and T. Kalker, ”Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform”, IEEE Transaction on Information Forensics and Security, Vol. 2, No. 3, September 2007, pp. 321-330.
[15] M. Terry, ”Medical Identity Theft and Telemedicine Security”, Telemedicine and e-Health, Vol. 15, No. 10, pp. 1-5, December 2009.
[16] C. Fontaine, F. Cayre, and T. Furon, ”Watermarking Security: Theory and Practice”, IEEE Transactions on Signal Processing, Vol. 53, No. 10, pp. 3976- 3987, October 2005.
[17] L. P. Freire, J. R. T. Pastoriza, P. Comesana, and F. P. Gonzalez, ”Watermarking Security: A Survey”, LNCS Transactions on Data Hiding and Multimedia Security, pp. 41-72, 2006.
[18] L. L. Cox, L. Kilian, F. T. Leighton and T. Shamoon, ”Secure Spread Spectrum Watermarking for Multimedia”, IEEE Transactions on Image Processing, Vol. 6, No. 12, pp. 1673-1687, 1997.
[19] H. Malvar and D. Florencio, ”Improved Spread Spectrum: A New Modilation Technique for Robust Watermarking”, IEEE Transactions on Signal Processing, Vol. 51, No. 4, 2003.
[20] L. Perez-Freire and F. Perez-Gonzalez, ”Spread-Spectrum Watermarking Security”, IEEE Transactions on Information Forensics and Security, Vol. 4, No. 1, 2009.
[21] D. Kahn, ”Cryptology and the Origins of Spread Spectrum”, IEEE Spectrum, Vol. 21, pp. 70-80, September 1984.
[22] M. Kansal, G. Singh and B. V. Kranthi,”DWT, DCT and SVD based Digital Image Watermarking”, International Conference on Computing Sciences, pp. 77-81, November 2012.
[23] B. Lei, I. Y. Soon, and Ee-Leng Tan, ”Robust SVD-Based Audio Watermarking Scheme With Differential Evolution Optimization”, IEEE Transactions on Audio, Speech, and Language Processing, Vol. 21, No. 11, November 2013.

