2012 International Conference on Advanced Computer Science Applications and Technologies

Digital Image Watermarking, Analysis of Current Methods

Ghassan N. Mohammed
School of computing
University Utara Malaysia
Kedah, Malaysia
ghanm1971@yahoo.com

Azman Yasin
School of computing
University Utara Malaysia
Kedah, Malaysia
yazman@uum.edu.my

Akram M.Zeki
Department of Information System
International Islamic University Malaysia
Kuala Lumpur, Malaysia
akramzeki@iium.edu.my

Abstract— **The rapid evolution in data transmission by the wide use of the internet, as provided an urgent need to prevent penetration and maintain the confidentiality of this data through the applying of some techniques to hide data within the carrier for example, text, image, audio and Video. A variety of image watermarking techniques have been published in the last few years which attempts to develop techniques and methods which are used to obtain better results through the fact that the changes that took place after the concealment is visible to the human eye. Digital image watermarking is one of the general information hiding problem. This study is to highlight some of these studies and analysis for use in future research and development to get to the best results.**

Keywords- Lsb; Isb; Watermarking; Spatial Domain; Frequency Domain.

I. INTRODUCTION

Digital watermarking is a technique used in identifying the ownership of various types of multimedia. It achieves the copyright protection purpose by embedding a signal that contains useful certifiable information for the original owner media, such as company logo, producer's name into the host media. Generally, any watermarking system is required not to obviously degrade the quality of the image, while the embedded watermark should be reliable retrieved. In addition, the embedded watermark should be robust against various kinds of noise and common image processing attack, such as image blurring, image sharpening, image compression, and image cropping [1]. In relation with the types of documents to be watermarked, the watermarking host media can be one of the following: image watermarking, video watermarking, audio watermarking, and text watermark.

Generally, any watermarking systems for digital media can be divided into two important stages: (1) watermark embedding (2) watermark extracting [5], the embedded data should keep the quality of the host media and the watermarked image should be similar to the original image.
The embedding process is illustrated in Figure 1, in which the watermark is embedded into a host image through a key file, either for visible or invisible watermarking. Thus, the watermarked image can be obtained. While the extraction stage as illustrated in figure 2 conversely requires reading the watermarked image and the key file to extract the watermark. The watermark will be extracted using the same key used in the embedding stage.
So as to reach the copyright protection, any system should convene these three important requirements:
i) Quality (imperceptibility): The watermark should not affect the quality of the original image.
ii) Robustness: The watermarked data should be robust against attacks such as filtering, compression, filtering with compression.
iii) Capacity: the number of bits that can be embedded at one time of the host image [2].

These requirements are often opposing with each other and need to make a trade-off among them. The relationship between these requirements is that when the robustness of the watermarking method improves, the imperceptibility decreases, and the capacity increases.
In the digital world, a watermark is a pattern of bits inserted into a digital medium that can be identified by the creator or authorized users. The digital watermark, which is not like the printed visible stamp watermark, is designed to be invisible to the audience. The bits embedded into an image are scattered all around to avoid identification or modification. Therefore, a digital watermark must be robust enough to survive in the detection, compression, and operations that are applied on it. Figure1 depict a common digital watermarking system.

The figure1 explains that the watermarking begins with a watermark messaging being embedded into a media message, which is defined as the host image. The resulting image is the watermarked image. In the embedding process, a secret key, such as, a random number generator is sometimes involved to generate a more secured watermark. The watermarked image is then transmitted along a communication channel. The watermark can be detected or extracted later by the receiver. On the other hand, there are two types of watermarking techniques depending on human perception: visible watermark, and invisible watermark. Visible watermark is a translucent overlaid into an image and is visible to the viewer. It is used to indicate ownership and for copyright protection. An invisible watermark is embedded into the data in such a way that the changes made to the pixel values are perceptually not noticed.

In term of the watermarking extraction process, techniques can be divided into three types: non-blind, semi-blind, and blind.

978-0-7695-4959-0/13 $25.00 © 2013 IEEE
DOI 10.1109/ACSAT.2012.90

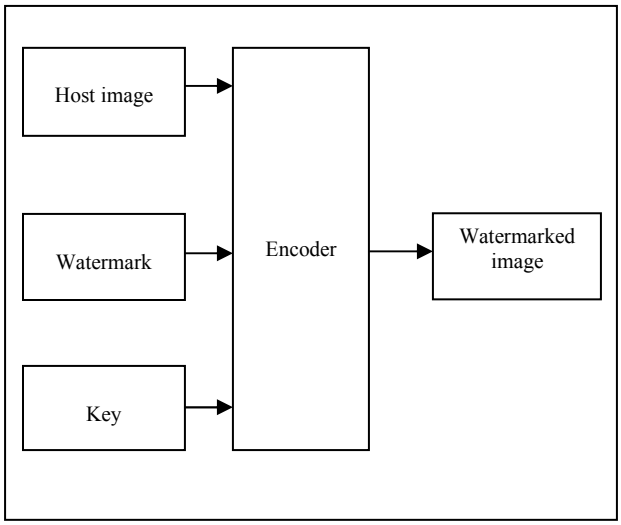

Figure 1. Embedding Watermark

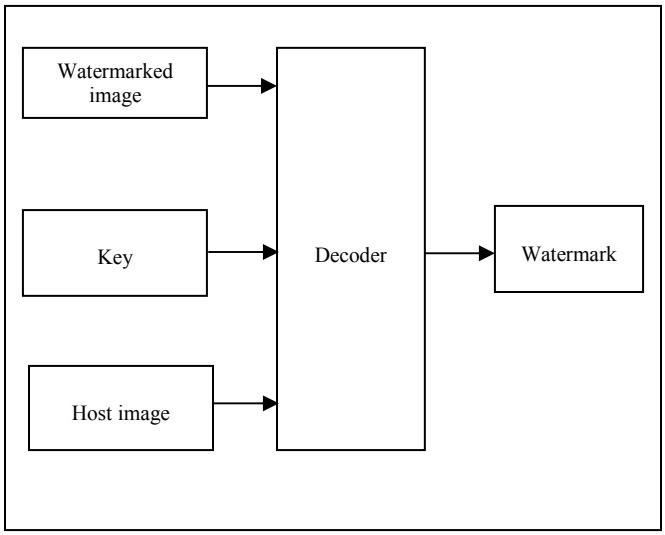

Figure 2. Watermark Extraction

The non-blind watermarking scheme requires an original image and a secret key for watermark detection whereas the semi-blind scheme requires a secret key and a watermark bit sequence for extraction. Meanwhile, the blind scheme needs only a secret key for extraction.

The watermarks added to digital content serve a variety of purposes like, data authentication, medical applications, fingerprinting, data hiding, military applications and copyright protection [3].

II. WATERMARKING TECHNIQUES

Many research works on image watermarking have been constantly carried out in the past. They can be classified according to the domain into frequency domain based, spatial domain based, or both [4, 5]. Figure 3 shows this classification. This study will focus on the applied frequency like, Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) domain or Discrete Wavelet Transform (DWT), and the applied spatial such as, Least Significant Bit (LSB), or Intermediate Significant Bits (ISB).

A. Spatial Domain

In the spatial domain, the watermark could be simply inserted into the host image by changing the gray levels of some pixels in the host image. It has the advantages of low complexity and easy implementation, but the inserted information may be easily detected using computer analysis or could be easily attacked [6]. It is a domain in which an image is represented through the intensities at the known points in space. This is the most commonly-used illustration for image data. In the spatial domain technique inserts direct watermarks into a host image by changing the pixel values. The embedding capacity of the spatial domain is perhaps great, but the hidden information could be easily detected by some type of attacks [7, 8, and 9].

In addition, in the spatial domain, pixels in randomly selected regions of the image are modified according to the signature or logo desired by the author of the product.

The spatial techniques insert a watermark in the underused Least Significant Bit (LSB) of the image, which allows the watermark to be inserted in an image without affecting the value of the image. The advantages of using this technique include it is very easy, fast, efficient, and the watermarked image quality might be simply controlled [6]. On top of that, the technique might simply be applied to any image, [10]. Also this method makes possible for a small object to be embedded several times so that even if most of the images are lost because of the attacks, a single surviving watermark would be considered a success.

1.The Least Significant Bit

Many techniques which were based on the LSB method have been developed; most of them use only one bit-plane (the 8th bit-planes) for embedding, while others use three bit-planes (6-8th bit-planes). Even the 4 bit-planes have been used for embedding (5-8th bit-plane) with a claimed acceptable image quality [11]. A bit-plane of digital images is a set of bits having the same position in the respective pixels of the digital images [12].

The LSB coding is the simple and fast calculated method for hiding watermarking [13], and represents an example of a spatial domain watermarking technique whereby data is inserted into digital signals in the noise-free environment. There are many variants of this technique. It essentially involves embedding the watermark by replacing the least significant bit of the image data with a bit of the watermark data [14].

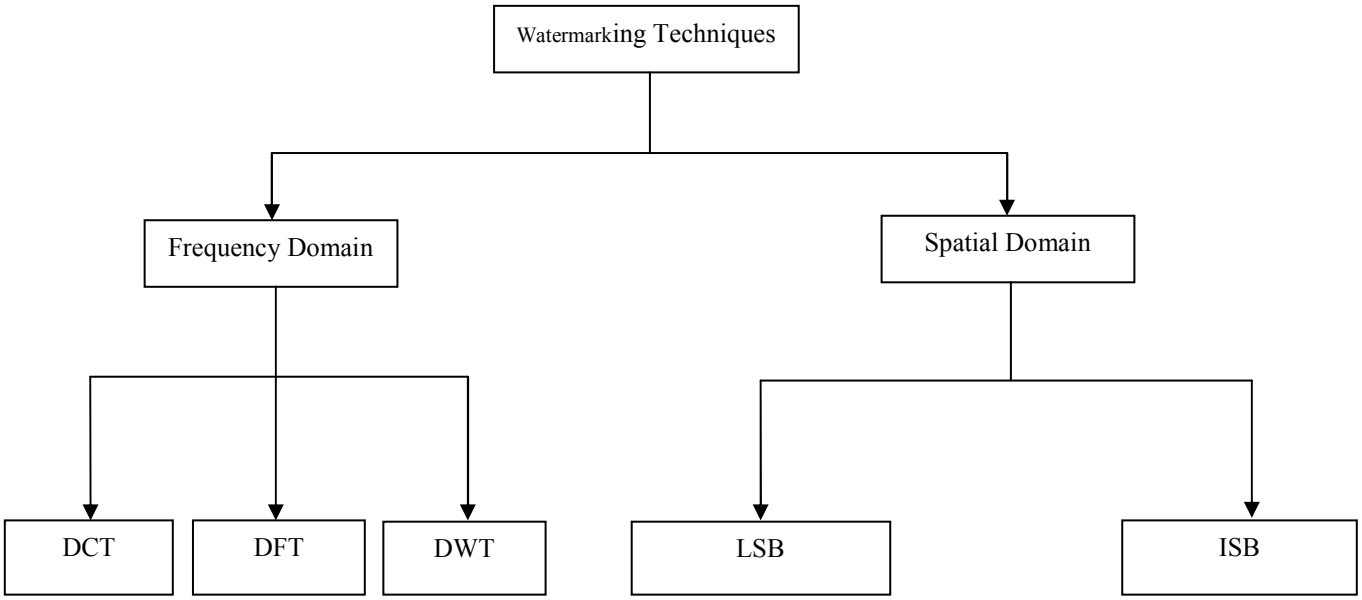

Figure 3. The watermarking techniques classification according to domain

One of methods presented an improvement on LSB method by using the third and the fourth least significant bits (LSB), this method done by embedding two bits in the third and fourth LSB bits, there is no different between the watermarked image and the original image [15].

Another proposed algorithm investigated the trade-off between the quality and the robustness of the LSB watermarking. In this algorithm, the significant bit-planes of the watermarked image are put instead of the lower bit-planes of the asset picture. Meanwhile, the effects of image compression over the watermark investigated, also the evaluation of the robustness and the imperceptibility by measuring the distortion due to watermarking quality metrics [16].

2. Intermediate Significant Bit

Another digital watermarking Technique which was proposed by [13], takes a bit-plane of digital images as a set of bits having the same position in the respective binary numbers. In the grey scale image representation, there are 8 bit-planes: in which the first bit-plane contains the set of the Most Significant Bits (MSB) and the 8th bit-plane contains the LSB. The set in between i.e. from 2nd to 7th bit-planes are Intermediate Significant Bits (ISB).

The method uses one bit-plane to embed the watermarked object into a selected bit-plane. After selecting one bit-plane for embedding, it finds the ranges of the chosen bit-plane. The length of the range (L is the maximum value of each range – the minimum value of the range + 1) and the number of ranges in each bit-plane is 256 / L, which means, the bit changes between 0 and 1 in each range. Meanwhile, the number of ranges for the first bit-plane are two only, either [0:127] or [128:255]. In other words, the bit in the first range is 0, whereas the bit in the second range is 1 and the length of each range of the first bit-plane is 128. In contrast, for the second bit-plane there are 4 ranges as follows: [0:63] [64:127] [128:191] [192:255] and the length of the ranges is 64, and so on as shown in Table 1. The method try to find best pixel value in between the middle and the edge of the range that can protect the watermark object from different types of attacks and at the same time keeping minimum distortion of watermarked image. This was done by positioning the watermarked pixel away from the edge of the range. ISB technique improves the robustness and maintains the quality of watermarked images.

The method tested the location of the watermark pixel according to the range of each bit-plane, so if the watermarked pixel is in the middle of the range then any effect on the pixel by attacks will be difficult to move the selected bit to another range. Whereas if the pixel value is located in the edges of ranges, any small change by attacks will move the pixel from a range to another, and the watermark cannot be extracted. Also, the study was trying to find the best pixel value in between the middle and the edge of the range that can keep the watermarked object from different types of attacks and at the same time keeping minimum distortion of the watermarked image. This was done by positioning the watermarked pixel away from the edge of the range. They found that the best extracted logo from the undistorted watermarked image was in the 4th bit-plane, in which the distance from the edge of the range to the position of the watermarked pixel was 6. In short, the study contributes to the body of knowledge by replacing the classic LSB technique with a new technique called Intermediate Significant Bits (ISB) which improves the robustness and maintains the quality of the watermarked images. The threshold values for the best embedding status are found based on the ISB.

Recently, many studies used this techniques to improve the watermarking system, one of these studies suggested an algorithm is based on changing the ISB of the low frequency approximation subband (LL) of the DWT domain to embed watermark into host image [17]. Another study by [18], try

to find a Threshold value, based on Intermediate Bit Values (TIBV) of image by selecting the image pixel for inserting the watermark. In addition [19] developed a system based on multiple watermarks in which two different watermarks embed concurrently into the ISB of the host image pixels. Also, [20] suggested ISB model based block of pixels, which can improve the robustness against different types of attacks and at the same time maintain the quality of the image.

In addition, [21] developed another ISB model by repeating the watermark data certain number of times (3, 5, 7, and 9 times) in order to improve the robustness of the watermarking technique, correspondingly, a majority criterion is used in the watermark detecting procedure, which makes the algorithm more robust, especially to the geometric transform attacks. Through the above methods used in spatial domain, it is noticed that when used, the LSB coding is the simple and fast calculated method for hiding watermarking by embedding one , two or three bits to increase the capacity, however the main problem in this method it is not robust enough against attacks, this problem solved by the other method ISB by replacing the watermarked image pixels by new pixels which can protect the watermark data against attacks and at the same time, keeping the new pixels very close to the original pixels. The technique was based on testing the value of the watermark pixel according to the range of each bit-plane and positioning the watermarked pixel away from any of the edges of the range. The best pixel value in between the middle and the edge of the range (threshold value) was found in order to protect the watermarked object from the different types of attacks and keep the minimum distortion of the watermarked image.

B. frequency domain

The watermark is embedded by modifying the frequency domain coefficients. The applied frequency may be DCT, DFT, or DWT.

A Discrete Cosine Transform (DCT) domain has been used extensively for embedding a watermark for a number of reasons. Using the DCT, an image is divided into frequency bands, and the watermark can be conveniently embedded in the visually important low to middle frequency bands. Sensitivities of the human visual system to changes in those bands have been extensively studied in the context of JPEG compression, and the results of those studies can be used to minimize the visual impact of the watermark embedding distortion [22].

Another watermarking in the DCT domain was first introduced by [23]. The image is divided into square blocks of size 8 x 8 for which the DCT is computed. From a pseudo randomly selected block, a pair of mid frequency coefficients is selected from 12 predetermined pairs. To embed a bit, the coefficients are then modified such that the difference between them is either positive or negative, depending on the bit value. In order to accommodate lossy JPEG compression, the quantization matrix is taken into account when altering the DCT coefficients. This method shows good robustness to JPEG compression.

A DWT based watermarking scheme by [24], makes use of both blind and non-blind algorithms. The highlight of the algorithm is that besides protecting the copyright of the host image, it also protects the watermark from any misuse. Since the embedding process uses data from the source image, the extraction of the watermark by an unauthorized person is not possible. It thus serves the twin purposes of providing copyright protection to the watermark and increasing the security of the whole process. The proposed method has been developed mathematically and used at various stages in the algorithm. The watermarked image was tested under various attacks and the results show that the proposed technique is better than other techniques

On the other hand, [25] presented a semi-blind reference watermarking scheme based on DWT and Singular Value Decomposition SVD for copyright protection and authenticity. They used a gray scale logo image as the watermark instead of the randomly generated Gaussian noise type watermark. In embedding the watermark, the original image is transformed into a wavelet domain and a reference sub-image is formed using directive contrast and wavelet coefficients. To embed the watermark into reference image by modifying the singular value of reference image, the singular value of the watermark is used. The reliable watermark extraction scheme is developed for the extraction of the watermark from distorted images.

A semi-blind watermarking system for embedding watermark in color images by using the Discrete Fourier Transform (DFT) domain [26], the proposed watermarking system using several cover images. The robustness of the proposed watermarking system was tested using a range of attacks; a given watermark is embedded in three frequency bands: Low, middle, and high. The watermarks extracted from the lower frequencies have the best visual quality for low pass filtering, adding Gaussian noise, JPEG compression, resizing, rotation, and scaling, and the watermarks extracted from the higher frequencies have the best visual quality for cropping, intensity adjustment, histogram equalization, and gamma correction. Extractions from the fragmented and translated image are identical to extractions from the un-attacked watermarked image. The collusion and re-watermarking attacks do not provide the hacker with useful tools.

Although the frequency domain is usually more robust than the spatial domain techniques, it still loses some embedded data after performing the lossy compression process to the watermarked image [27 and 28].
Thus, users are unable to hide the media information in it [29]. Besides, [22] explain that the process of compression and hiding is highly complex than the spatial domain.

Another disadvantage of the transform domain technique is that it cannot restrict visual degradation of the cover image as it is global in nature (global within the block in the block-based approach).

In the spatial domain scheme, degradation in the quality of image, due to watermarking, could be controlled locally by leaving the region of interest unaffected [24].

The DCT of an image is generally complex valued, and this leads to a magnitude and phase representation for the image.

TABLE I. RANGES OF EACH BIT-PLANE WITH THE LENGTH

Bit -Plane	Length of the ranges	Number of ranges	Ranges
1	128	2	[0:127] [128:255]
2	64	4	[0:63] [64:127] [128:191] [192:255]
3	32	8	[0:31] [32:63] … [192:223] [224:255]
4	16	16	[0:15] [16:31] … [224:239] [240:255]
5	8	32	[0:7] [8:15] … [240:247] [248:255]
6	4	64	[0:3] [4:7] … [248:251] [252:255]
7	2	128	[0:1] [2:3] … [252:253] [254:255]
8	1	256	[0] [1] … [254] [255]

CONCLUSION

Digital watermarking is one of the general information on hiding problem. It is apparent that digital watermarking can be achieved by using either transform techniques or embedding the watermark data into the frequency domain representation of the host image or by directly embedding the watermark into the spatial domain data of the image.

Digital watermarking has many applications, in other word different applications have different requirements. There are no general requirements for all watermarking problems. The review also shows there are several requirements that the embedding method has yet to satisfy.

- Creating robust watermarking methods is still a challenging research problem. These algorithms are robust against some attacks but not against most of them. As an example, they cannot withstand geometric attacks such as rotation or cropping.
- Also, some of the current methods are designed to suit only specific application, which limits their widespread use.
- In the spatial domain, the watermark could be simply inserted into the host image by changing the gray levels of some pixels in the host image. It has the advantages of low complexity and easy implementation, but the inserted information may be easily detected using computer analysis or could be easily attacked.
- While the frequency domain is usually more robust than the spatial domain techniques, it still loses some embedded data after performing the lossy compression process to the watermarked image.
- For each of the two techniques, different methods in embedding the image watermark, LSB and ISB are the most important methods for spatial techniques, while DCT, DFT and DWT are the most famous methods for transforming techniques.

All these studies and researches open the way for new ideas to apply more and more methods in the future by reaching the trade-off between the three important requirements quality, robustness and capacity.

REFERENCES

[1] A. Peungpanich and T. Amornraksa, "An Improving Method for Image Watermarking Using Image Averaging and Tuned Pixels Prediction," IEEE, ISCIT, pp. 755-760, 2010.

[2] V. Singh, "Digital Watermarking: A Tutorial," Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected. Tirkel and C. F. Osborne, "A digital watermark", International Conference on Image Processing, Los Alamitos, CA, November 1994, Vol. 2, pp. 86–90.

[3] S. Juergen, "Digital Watermarking for Digital Media," University of Cooperative Education Heidenheim, Germany. ISBN: 159140519X. , 2005.

[4] R. G. van Schyndel, A. Z Amornraksa, "An Improving Method for Image Watermarking Using Image Averaging and Tuned Pixels Prediction," IEEE, ISCIT, pp. 755-760, 2010.

[5] M. D. Swanson, M. Kobayashi and A. H. Tewfik, "Multimedia data embedding and watermarking technologies", Proceedings of the IEEE, Vol. 86, No. 6, 1998, pp. 1064–1087.

[6] N. I. Wu and M. S. Hwang, "Data Hiding: Current Status and Key Issues," International Journal of Network Security. January 2007, vol. 4(1), pp. 1–9.

[7] M. Celik, G. Sharma, E. Saber, and A. Tekalp. Hierarchical watermarking for secure image authentication with localization. IEEE Trans. Image Process, 11(6):585–595, June 2002.

[8] D. Mukherjee, S. Maitra, and S. Acton. Spatial domain digital watermarking of multimedia objects for buyer authentication. IEEE Trans. Multimedia, 6(1):1–15, February 2004.

[9] N. Nikolaidis and I. Pitas. Robust image watermarking in the spatial domain. Signal Process, 66(3):385–403, 1998.

[10] C. F. Wu, "The Research of Improving the Image Quality of Digital Watermarking Technique and Its Applications," National Sun Yat-sen University, Kaohsiung, 80424, Taiwan. Etd-0612101-142904, 2001.

[11] A. Habes, "Information Hiding in BMP image Implementation, Analysis and Evaluation," Information Transmissions in Computer Networks, vol. 6, 1, pp. 1-10, 2006.

[12] A. M. Zeki and A. A. Manaf, "A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit," World Academy of Science, Engineering and Technology vol. 50, pp. 989-996, 2009.

[13] A. M. Zeki and A. A. Manaf, "Robust Digital Watermarking Method Based on Bit Planes'Ranges," Studies in Informatics and Control Journal. September, vol. 16 No.3, pp. 245-254, 2007.

[14] A. Z. Tirkel, C. F. Osborne, and R. G. Schyndel, "Image Watermarking - A Spread Spectrum Application," IEEE 4th International Symposium on Spread Spectrum Techniques and Applications Proceedings, pp. 785-789, 1996.

[15] A. Bamatraf, I. Rosziati, & M. N. M. Salleh, "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit," Journal of Computing Press, NY, USA, ISSN 2151-9617, vol. 3,4, pp. 1-8, 2011.

[16] S. Fazli, & Khodaverdi, G. "Trade-off between Imperceptibility and Robustness of LSB Watermarking using SSIM Quality Metrics," ICMV '09. Second International Conference on Issue Date: 28-30 Dec. 2009 101-104. , 2010.

[17] Y.Dejun, Y. Rijing, Y. Yuhai, and X. Huijie, "Blind Digital Image Watermarking Technique Based On Intermediate Significant Bit and Discrete Wavelet Transform," IEEE 2009.

[18] S. M. Perumal and V. V. Kumar, "A Wavelet based Digital Watermarking Method using Thresholds on Intermediate Bit Values," International Journal of Computer Applications (0975 – 8887), February, vol. 15– No.3, pp. 29-36, 2011.

[19] M. S. Emami, G. B. Sulong, and S. B. Seliman, "A Novel Multiple Semi-Blind Enhanced ISB Watermarking Algorithm Using Watermark Bit-Pattern Histogram For Copyright Protection," International Journal of Innovative Computing, Information and Control ICIC International, ISSN 1349-4198 , March, vol. Volume 8, No 3(A), pp. 1665-1687, 2012.

[20] A. M. Zeki A. A. Manaf, and S.S. Mahmod, "Analysis of ISB watermarking model: block based methods vs. embedding repetition methods," 9th International Conference on Advances in Mobile Computing and Multimedia, pp. 198-201, 2011.

[21] A. M. Zeki and A. A. Manaf, "Improving the robustness of ISB watermarking techniques by repetition of the embedding," In: Communications in Computer and Information Science. Springer-Verlag Berlin Heidelberg, pp. 592-599, 2011.

[22] E. Muharemagic and B. Furht, "Survey Of Watermarking Techniques And Applications," 2004.

[23] C. Busch, W. Funk, and S. Wolthusen, "Digital watermarking: From concepts to real-time video applications," IEEE Comput. Graphics Applicat., pp. 25–35, Jan. 1999.

[24] S. Tripathi, N. Ramesh, and B. K. Neeraj, "A DWT based Dual Image Watermarking Technique for Authenticity and Watermark Protection," An International Journal (SIPIJ) vol. Vol.1, No.2 pp. 33-45, 2010.

[25] G. Bhatnaga and B. Raman, "A new robust reference watermarking scheme based on DWT-SVD," Computer Standards & Domain Digital Image Watermarking with DCT Based Watermarking," International Journal of Computer Theory and Engineering, August 2010, vol. 2, No. 4, pp. 647-653.

[26] J. Kusyk and A. M. Eskicioglu, "A Semi-Blind Logo Watermarking Scheme for Color Images by Comparison and Modification of DFT Coefficients," 2005.

[27] K. L. Chung, et al., "A Novel SVD- and VQ-based Image Hiding Scheme," Pattern Recognition Letters. 22, pp. 1051-1058, 2001.

[28] M. D. Swanson, B. Xu, and A.H.Tewfik, "Robust Data Hiding for Images," 7th Digital Signal Processing Workshop (DSP96). Loen, Norway, pp. 37-40, 1996.

[29] S. P. Maity and M. K. Kundu, "Robust and Blind Spatial Watermarking In Digital Image," Proceedings of 3rd Indian Conf. on Computer Vision, Graphics and Image Processing (ICVGIP '2002). 16-18th December. Ahmedabad, India, pp. 388-393, 2002.

.