International Journal of Engineering and Technology Vol. 1, No.3, August, 2009
ISSN: 1793-8236

A Robust Blind Image Watermarking Scheme in Spatial Domain for Copyright Protection

Dr.M.A.Dorairangaswamy

***Abstract*—In recent times, the rapid growth of the Internet has led to the critical issue of copyright protection of digital contents. The two significant tasks of the Digital Rights Management (DRM) system are: Protection of the high-value digital assets and Control over the distribution and usage of those digital assets. One of the most promising means to safe guard the copyright of digital images is watermarking. Digital watermarking hides the secret or private information in digital images in order to facilitate copyright protection. Here, we propose a robust and blind watermarking scheme for copyright protection against digital image piracy. The proposed watermarking scheme invisibly embeds a binary watermark image into the host image for protecting its copyrights. In watermark embedding, an individual watermark pixel is embedded into every 2x2 block of the host image. The watermark extraction process necessitates only the watermarked image and not the original image or any of its characteristics, as the proposed watermarking scheme is blind. The experimental results recorded with the aid of attack analysis illustrate the efficiency and robustness of the proposed watermarking scheme.**

***Index Terms*—Attacks, Blind Scheme, Copyright Protection, Digital Rights Management (DRM), Digital images, Digital image watermarking, Robustness.**

I. Introduction

Digital content distribution is swiftly emerging as one of the flourishing fields owing because of the recent improvements in digital technologies, together with more and more interrelated high-speed networks and the diminution in costs of high-performance digital devices. These developments in digital content distribution have brought about immense prospects for business content suppliers and with that also claim to be a major threat because of the simplicity of illegal copying and distribution of the digital data. Hence, in order to safeguard digital content from illegitimate utilization, business content suppliers bearing the legislation demand technologies [1]. Digital Rights Management (DRM) is one amongst the potential solutions for the aforementioned issue. DRM is a method of honoring copyright provisions established by the proprietors of the intellectual assets, such as license terms and usage agreements. The DRM includes a set of technologies to prevent exploitation of the digital content by establishing privileges, specifically by means of content protection [2].

The primary motives of Digital Rights Management systems are 1) securing the valuable digital properties and 2) restricting the circulation and utilization of digital data. The DRM system is expected to provide unrelenting content security in contrast to barely restraining the users with appropriate consent to access to the digital content. The access rights for diverse classes of digital content (for instance: music files, video streams, digital books, images) across diverse platforms (for example PCs, laptops, PDAs1, mobile phones) should be organized effectively by DRM in a supple manner [3]. DRM includes a collection of technologies such as encryption, copy control, digital watermarking, fingerprinting, traitor tracing, authentication, integrity checking, access control, tamper-resistant hardware and software, key management, revocation and risk management architectures.

In general, a DRM policy is composed of copyright permissions, rights expression languages and other forms of metadata and making it machine-readable is achieved by the utilization of other technologies [4]. Copyright protection is a crucial task performed in digital rights management. The spotlight of the resolution methods of copyright protection is to avoid disagreements emerging from proprietorship assertions during the trade of digital documents. Therefore, to authenticate the document proprietorship prior to its sales and equally to demonstrate valid consumers, the problem necessitates a fool-proof mechanism [5]. The probable reason stated for the vulnerability of illegitimate replication, alterations and distribution of digital images is owing to the emergence of image processing tools. The digital image protection is a chief concern due to the omnipresent internet. The digital media piracy is a fret for the media content owners causing possible loss of revenue, thus increasing the apprehension about copyright protection of digital contents [6].

Digital rights management systems are likely to affect the copyright balance between copyright owners and users while identifying the legitimate expectation of copyright owners, including the content industry, to safeguard their copyrights in the face of technological progression. In order to avoid replication or to confine utilization of a digital file, several techniques are included in Digital Rights Management (DRM). There is a disagreement in such technology as the regular use which is conventionally authorized is limited as well. Rather than thwarting replication, the supposed forensic techniques facilitate the copyright owner to track the pirates and prosecute when unauthorized copies appear. The disagreement in DRM is higher than forensic techniques as the latter intervenes only when an offense is apparent [7]. The scope for innovative research in copyright protection is abundant as the numerous technological methods available to

Manuscript received June 19, 2009.

Dr. M. A. Dorairangaswamy, Arcot Road, Virugambakkam, Chennai, India. Pincode: 600 092. Ph: 09840162750.

encounter copyright piracy could not propose an ideal or commonly established accessible solution. There is a rapid escalation in the attention paid towards digital watermarking, recommended as a method for copyright protection or ownership identification of digital images.

The digital watermarking technique protects the digital images from illegitimate replication and usage. Watermarking is a process of embedding data into a multimedia element such as image, audio or video [8]. The embedded data could be later removed or recognized in the multimedia element for achieving a variety of functions such as copyright protection, access control and broadcast monitoring. Digital watermarking, based on its application can be categorized into image watermarking, video watermarking and audio watermarking. Image and video copyright protection has been the primary goal of the existing digital watermarking methods [9]. In general, an image is embedded with a code, a digital watermark offering the image an impression of proprietorship or legitimacy thus performing a task of a digital signature. The prime advantage of watermarking is its ability to remain inseparable from the original content. Several significant characteristics namely: recognition difficulty, common distortion tolerance, malicious attack resistance, ability to carry numerous bits of information, coexistence with other watermarks and little computation for insertion or detection, are demonstrated by a watermark [10].

On splitting the existing watermarks and watermarking techniques in different manners, a variety of new watermarks and watermarking techniques with diverse characteristics can be attained. Watermarking, based on there requirements of watermark extraction or detection can be is classified into Non-blind, Semi-Blind and Blind schemes [11], [12]. Non-blind watermarking techniques make use of the original image and secret keys to detect the watermark whereas the semi-blind techniques necessitate the secret key(s) and the watermark bit sequence for extraction. Nonetheless, the blind techniques employ only the secret key(s) for extraction. Another classification of watermarks can be made as, visible and invisible embedded data (watermark); in visible watermark, a secondary image is embedded in a primary image such that it is deliberately perceptible by a human observer; nevertheless, in invisible watermark, the embedded data is imperceptible, although can be extracted by a computer program [13]. Watermark based on its credibility can be also categorized into robust watermark, which is secure against un-malevolent or malevolent attacks for instance: scaling, cropping, lossy compression, etc. and fragile watermark, which just recognizes the infinitesimal vacillation to the novel digital content. The principal focus of the robust watermarking is copyright protection [14]. There exist many probable restrictions to a visible watermark such as attack vulnerability in direct image processing and its capability to assess image reliability. Several researches on copyright protection of digital images through watermarking schemes have been presented [15 – 20].

In our earlier work [24], we have presented a novel invisible and blind watermarking scheme for protecting copyrights of digital images. In this paper, we have analyzed the robustness of the presented scheme with the aid of attacks on the watermarked images. In the proposed watermarking scheme, the watermark data chosen for embedding is a binary image. A binary watermark image pixel is embedded into every 2x2 non-overlapping blocks of the host image with the aid of embedding strength and signum function using the approach discussed. The proposed scheme is blind and hence it doesn't necessitate the original image or any of its characteristics for the extraction of watermark. The watermark image size and the embedding strength are utilized for extracting the binary watermark from the watermarked image. The proposed watermarking scheme is proved for its robustness with the support of experimental results obtained from various attacks on watermarked images.

The rest of the paper is organized as follows. Section II gives a concise review of some of the recent works that employs digital watermarking for copyright protection of digital images. The proposed robust and blind watermarking scheme is presented in Section III. The experimental results are illustrated in Section IV and conclusions are summed up in Section V.

II. Review of Existing Researches

A number of earlier works available in the literature that employs digital image watermarking for copyright protection of digital images have motivated us to do this research. Here, some of those recent motivating researches are briefly described.

Jung-Chun Liu *et al.* [15] have proposed a multi-scale Full-Band Image Watermarking scheme by merging both of the DDWT-based and the SVD-based techniques for meeting the security obligations for copyright protection. They take advantage of the characteristics of both the DDWT method e.g. robustness against cropping attacks, and that of the SVD method e.g. robustness against geometric attacks like rotation and scaling and non-geometric attacks like Gaussian noise, sharpening, and contrast adjustment. Results demonstrated that the DWT-SVD method was not robust enough as the multi-scale Full-Band Image Watermarking scheme.

Yen-Chung Chiu and Wen-Hsiang Tsai [16] have presented a watermark embedding technique for color images by coding and synchronization of coefficient-value peak locations in the DFT domain. Based on the characteristics of the image coefficients in the DFT domain, they embedded the watermark through creation of peaks circularly and symmetrically in the middle frequencies. Moreover, they utilized a combinatorial operation to code the peak locations and a supplementary synchronization peak was used for the synchronization of the peak locations. In watermark extraction, to obtain a watermark the positions of the coefficient-value peaks are identified and mapped into a combinatorial operation. The embedded watermark was proved its robustness and capability of surviving print-and-scan operations. Their method successfully accomplished the objective of protecting the image copyright ownership.

Ming-Chiang Hu *et al.* [17] have proposed a two-phase watermarking scheme that extracts both the binary and grayscale watermark from the protected images to achieve

copyright protection. The grayscale and binary watermarks can be extracted sequentially by only those who have the original grayscale watermark and the corresponding secret keys, thereby improving the security and robustness of the proposed watermarking system. The results demonstrated that the proposed system satisfied the general requirements of image watermarking and the system performed well in transparency and robustness when compared with the related works. Thus, because of its flexible characteristics the proposed method was more feasible and practical for copyright protection.

Ming-Shi Wang and Wei-Che Chen [18] have provided a scheme for digital image copyright protection on the basis of visual cryptography (VC) and singular value decomposition (SVD) techniques. Initially, their scheme applied SVD to a host image to construct a master share and the two-out-of-two VC scheme was used for ownership share construction by the joint utilization of master share with a secret image. The secret image can be disclosed for ownership identification by stacking the master share and the ownership share. In their proposed scheme, the secret image was embedded without any modification to the host image and the original host image and the assistance of computers are not necessitated for hidden secret image extraction. The scheme achieved stronger robustness against several common attacks in contrast to the existing schemes and the same is proved by the experimental results.

Shih-Hao Wang and Yuan-Pei Lin [19] have proposed a wavelet-based watermarking technique by quantizing the super trees for protecting the copyrights. The experimental results verified the robustness to frequency based attacks, for example the high-pass band removal in low-pass processing, and the high-pass details removal in JPEG compression. Moreover, an illustration of the robustness to time domain attacks such as pixel shifting and rotation were provided. Data hiding or image authentication was also supported by the proposed watermarking scheme along with copyright protection.

Chin-Chen Chang and Pei-Yu Lin [20] have proposed an adaptive scheme for copyright protection without the application of discrete cosine transformation (DCT) and discrete wavelet transformation (DWT). The proposed approach improved the watermark's robustness because it allows image owners to adjust the strength of watermarks based on a threshold. In addition, diverse signal processing operations (such as blurring, JPEG compression, and noising) and geometric transformations (such as cropping, rotation, and scaling) were handled by their scheme. They illustrated that their scheme was superior and was more appropriate for medical and artistic images as it maintained the data lossless requirement.

A digital watermarking algorithm that works based on the concept of embed digital watermark and modifying frequency coefficients in discrete wavelet transform (DWT) domain for copyright protection was proposed by Abou Ella Hassanien [21]. The proposed algorithm embedded the watermark into the original image's detail wavelet coefficients with the assistance of a key. A random key produced was employed to choose the precise locations in the wavelet domain for embedding the watermark. The proposed watermarking algorithm's performance was robust to a wide range of signal distortions like JPEG, image cropping, geometric transformations and noises.

Shang-Lin Hsieh *et al.* [22] have proposed a watermarking scheme for copyright protection of color images. The requirements of a reasonable watermarking scheme namely, imperceptibility and robustness were satisfied by their scheme. Their proposed algorithm had number of advantages over the other related works: Resistant against many attacks for instance cropping, scaling, JPEG compression and more, Ability extract unique features from diverse images, a vital prerequisite for feature extraction, and Ability to compute the scaling factor for different images whilst preserving the robustness and imperceptibility requirement.

III. Robust and Blind Watermarking Scheme

This section details the proposed robust and blind watermarking scheme for copyright protection of digital images. The proposed digital watermarking scheme is designed based on the blind watermarking scheme and hence it doesn't necessitate the original image or any of its characteristics for watermark extraction. The watermark data utilized in our scheme is a binary image and its pixels are invisibly embedded into the host image for safeguarding the host image's copyrights. The following subsections describe the steps involved in the watermark embedding and extraction processes.

A. Watermark Embedding

This sub-section presents the embedding process of the binary watermark image into the host image. The host image chosen ought to be dyadic (2^nx2^n) and a binary image is made use of as watermark. Primarily, the non-overlapping blocks sized 2x2 are extracted from the host image. Each pixel of binary watermark image is embedded into a single block of the host image. The watermark embedding process utilizes the following set of operations: mean calculation, embedding strength (g) and signum function. To begin with, each non-overlapping block is represented by means of a vector, and vector's mean value is computed. Subsequently, the embedding strength (g) is used to divide the mean value to be used for embedding. As the watermark chosen is a binary image, we obtain to two possible cases of watermark embedding: embedding '1' valued pixel and embedding '0' valued pixel. Based on the embedding pixel value '0' and '1', two distinct mathematical operations are performed. Fig. 1 depicts the block diagram of the watermark embedding process.

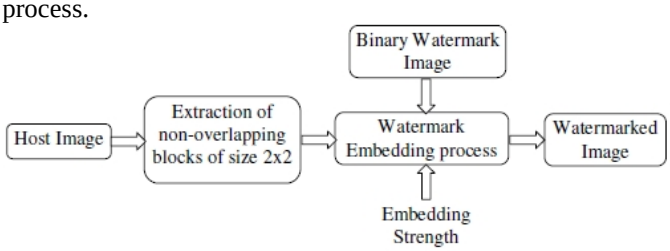

Fig. 1 Watermark Embedding Process

Watermark Embedding Steps:

Input: Host Image (I), Binary Watermark Image (W), Embedding strength (g)

Output: Watermarked Image (I_W)

1. Extraction of non-overlapping blocks sized 2x2 from the host image. The binary watermark image (W) sized (n x n) will consist of $n^2/4$ number of 2x2 non-overlapping blocks. The extracted $n^2/4$ non-overlapping blocks are stored in a vector B.
$$B = [b_1, b_2, b_3, ..., b_N]; \ \ where\ 0 < N \le |W|$$
2. Conversion of each individual matrix in the vector B into a vector V_B.
$$V_B = [x_1, x_2, x_3, x_4]$$
3. Calculation of the mean value for all the individual translated vectors V_B.
$$\overline{V_B} = \frac{\sum_{i=1}^{k} V_{B_k}}{k}; \ \ where\ 0 < k \le 4$$
4. Performing division operation on the individual mean value $\overline{V_B}$ of all the vectors by the embedding strength g. The resultant value is stored in as Q.
$$Q = \frac{\overline{V_B}}{g}; \ \ where\ g = 2$$
5. Embedding the binary watermark image pixels into the blocks in vector B. The actual embedding process makes use of the predetermined Q and embedding strength g. The embedding process involves the following steps namely,
   (i) Calculation of the signum function for each individual block in vector B. The computed signum function is stored in a vector X. The signum function is the real valued function defined for real x as follows [23]:
$$\text{sgn}(x) = \begin{cases} +1, & if\ \ x > 0, \\ 0, & if\ \ x = 0, \\ -1, & if\ \ x < 0. \end{cases}$$
   For all real x we have $\text{sgn}(-x) = -\text{sgn}(x)$ .Similarly, $|x| = \text{sgn}(x)x$. If $x \neq 0$ then also $\frac{d}{dx}|x| = \text{sgn}(x)$. The second property implies that for real non-zero x we have $\text{sgn}(x) = x/|x|$.
   (ii) For pixel value '0', below mathematical operation is performed,
$$t = ((round(Q * 0.5) * 2) * g)$$
   (iii) Similarly, for pixel value '1' the following mathematical operation applied,
$$Q_t = (Q - 1)$$
$$t = ((round(Q_t * 0.5) * 3) * g))$$
   (iv) Multiplication of the calculated value t on each block in vector X based on the watermark pixel value. The resultant values are placed in a vector B.
$$B << (X_{(i)} .* t) \ ; \ where\ 0 < \text{i} \le \text{k}$$
6. Mapping of the modified blocks in the vector B back to its original position in host image I . On completion of the above process for each individual block, we obtain the watermarked image I_W .

B. Watermark Extraction

This sub-section explains the process employed in our proposed scheme for the extraction of binary watermark image from the watermarked image. The scheme proposed is blind and hence the extraction necessitates: watermarked image, size of watermark image and embedding strength. Initially, non overlapping blocks sized 2x2 are extracted from the watermarked image and the number of blocks to be extracted is based on the size of the watermark image. The blocks thus extracted are stored in a vector. Subsequently, all the individual extracted blocks are converted into separate vectors and the mean value of each vector is calculated. Consequently, the mean values of all the blocks are divided by the embedding strength. The extraction of watermark is performed based on the resultant value. Finally, the extracted pixel values are placed in a newly initialized matrix of size of watermark image. The resultant matrix represents the watermark image. Fig. 2 depicts the block diagram of the watermark extraction process.

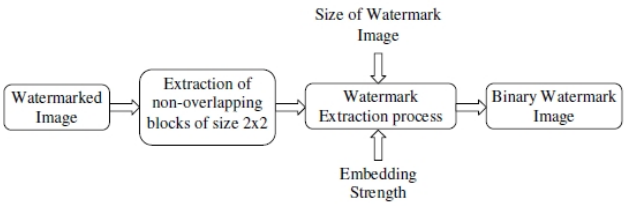

Fig. 2 Watermark Extraction Process

Watermark Extraction Steps:

Input: Watermarked Image (I_W), Size of watermark image ($|W|$), Embedding strength (g)

Output: Watermark Image (W)

1. Extraction of non-overlapping blocks of size 2x2 from the watermarked image (I_W). The number of blocks extracted is equivalent to the size of watermark image. The extracted blocks are stored in a vector BV .
$$BV = [b_1, b_2, b_3, ..., b_N]; \ \ where\ 0 < N \le |W|$$
2. Translation of each individual block in the vector BV , into a vector V_B .
$$V_B = [x_1, x_2, x_3, x_4]$$
3. Calculation of the mean value of all the translated vectors V_B .

$$\overline{V_B} = \frac{\sum_{i=1}^{k} V_{B_k}}{k}; \quad where\, 0 < k \le 4$$

4. Division operation is applied on the calculated mean value $\overline{V_B}$ of all the individual vectors by the embedding strength g. The resultant value thus is represented as Y.

$$Y = (\overline{V_B} / g); \quad where\, g = 2$$

5. The below mathematical operation is performed to obtain the individual pixel values W_p of the watermark.

$$W_p << (Y[i] \bmod 2); \quad 0 \le i \le |W|$$

6. A matrix of watermark image's size is initialized and the extracted pixel values (W_p) are placed in it to attain the watermark image (W).

IV. Experimental Results

This section depicts the experimental results of the proposed watermarking scheme. The presented watermarking scheme is programmed in Matlab (Matlab7.4) and is tested with images of different sizes. In general, the binary watermark images are embedded effectively into the host images and on the other hand, the embedded watermarks are extracted efficiently from the watermarked images. The watermarked images obtained have good Peak Signal to Noise Ratio (PSNR) and good visual quality. The watermark and watermarked images of four different host images are shown in Fig. 3, 4, 5 and 6 along with their corresponding PSNR values. To prove the robustness of the proposed watermarking scheme, we have carried out a variety of attacks on watermarked images. Fig. 7 portrays the results of different image attacks for instance Gaussian blur, Gaussian noise, Intensity value adjustment, Cropping, Sharpening and wiener filtering along with their extracted watermark images and corresponding correlation coefficients computed between the original watermark and the extracted watermark from the attacked watermarked images. The experimental results have illustrated that the correlation coefficient's value is above 0.3. Thereby, the robustness of the proposed scheme is evident from the results obtained.

V. Conclusion

The modern society has addressed an incredible development of electronic commerce applications and online services; yet, the fear of illegal duplication and distribution of copyrighted material has crept into the service providers minds. The extensive availability of internet has caused serious concern over the security of images. We have presented a blind and robust digital watermarking scheme for protecting the copyrights of images along with attack analysis for its robustness. A binary image has been used as the digital watermark and every pixel of the binary watermark image is embedded into 2x2 non-overlapping blocks of the host image. Afterwards, the watermark image is extracted from the watermarked image using the approach discussed. The watermarked images are in good visual quality and have good PSNR values. The experimental results have demonstrated the effectiveness and robustness of the proposed scheme with the aid of attack analysis.

References

[1] Claudine Conrado, Milan Petkovic, Michiel van der Veen and Wytse van der Velde "Controlled Sharing of Personal Content Using Digital Rights Management", Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006.

[2] L. C. Anderson, J. B. Lotspiech, "Rights Management and Security in the Electronic Library," Bulletin of the American Society for Information Science, Vol. 22, No.1, October-November 1995, pp.21-3.

[3] Qiong Liu, Reihaneh Safavi-Naini and Nicholas Paul Sheppard, "Digital Rights Management for Content Distribution", Proceedings of the Australasian information security workshop conference on ACSW frontiers, Adelaide, Australia, Vol. 21, 2003, pp. 49 – 58.

[4] Ian Kerr, "Hacking@privacy: Why We Need Protection from the Technologies That Protect Copyright", In proc. of Conference on privacy and identity, 2007.

[5] A. Piva, F. Bartolini, and M. Barni, "Managing copyright in open networks," IEEE Trans. Internet Computing, vol. 6, no. 3, May–Jun. 2002, pp. 18–26.

[6] Shang-Lin Hsieh, Lung-Yao Hsu, and I-Ju Tsai, "A Copyright Protection Scheme for Color Images using Secret Sharing and Wavelet Transform", proceedings of World Academy of Science, Engineering And Technology, Vol. 10, December 2005.

[7] Hans Georg Schaathun, "On watermarking/fingerprinting for copyright protection", First International Conference on Innovative Computing, Information and Control, ICICIC '06, Beijing, Vol. 3, August 2006, pp. 50-53,

[8] Authors Emir Ganic, Ahmet M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies", International Multimedia Conference, Magdeburg, Germany, 2004, pp. 166 - 174.

[9] Xiang-Yang Wang and Hong Zhao, "A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT", IEEE Transactions On Signal Processing, Vol. 54, No. 12, December 2006.

[10] Miller, M.; Cox, I.J.; Linnartz, J.P.M.G.; Kalker, T., "A review of watermarking principles and practices," In Digital Signal Processing in Multime11]dia Systems, Edit. K. K. Parhi and T. Nishitani, Marcell Dekker Inc., 1999, pp. 461-485.

[11] [P. Tao and A. M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the DWT Domain," Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference, Philadelphia, PA, October 25-28, 2004, pp. 133-144.

[12] Ersin Elbasi and Ahmet M. Eskicioglu, "A Semi-Blind Watermarking Scheme for Color Images Using a Tree Structure," in proc. of IEEE Sarnoff Symposium, March, 2006.

[13] Yeung, M. & Minzter, F., "An Invisible Watermarking technique for image verification," Proceeding on the IEEE International Conference on Image Processing, pp: 680-683, 1997.

[14] Shaowei Weng, Yao Zhao and Jeng-Shyang Pan, "A Novel Reversible Data Hiding Scheme," International Journal of Innovative Computing, Information and Control, Vol. 4, No. 2, 2008, pp. 351-358.

[15] Jung-Chun Liu, Chu-Hsing Lin, Li-Ching Kuo and Jen-Chieh Chang, "Robust Multi-scale Full-Band Image Watermarking for Copyright Protection", Lecture Notes in Computer Science, Springer Berlin, Heidelberg, Vol. 4570, 2007, pp. 176-184.

[16] Yen-Chung Chiu and Wen-Hsiang Tsai, "Copyright Protection against Print-and-Scan Operations by Watermarking for Color Images Using Coding and Synchronization of Peak Locations in Frequency Domain", Journal Of Information Science And Engineering, Vol. 22, 2006, pp. 483-496.

[17] Ming-Chiang Hu, Der-Chyuan Lou and Ming-Chang Chang, "Dual-wrapped digital watermarking scheme for image copyright protection," Computers & Security, Vol. 26, No. 4, 2007, pp. 319-330.

[18] Ming-Shi Wang and Wei-Che Chen, "Digital image copyright protection scheme based on visual cryptography and singular value decomposition", Optical Engineering, Vol. 46, No. 6, 2007.

[19] Shih-Hao Wang and Yuan-Pei Lin, "Wavelet Tree Quantization for Copyright Protection Watermarking", IEEE Transactions On Image Processing, Vol. 13, No. 2, February 2004.

[20] Chin-Chen Chang, Pei-Yu Lin, "Adaptive watermark mechanism for rightful ownership protection," Journal of Systems and Software, Vol. 81, No. 7, 2008, pp. 1118-1129.

[21] Abou Ella Hassanien, "A Copyright Protection using Watermarking Algorithm", Informatica, Vol. 17, No. 2, April 2006, pp. 187-198.
[22] Shang-Lin Hsieh, I-Ju Tsai, Bin-Yuan Huang and Jh-Jie Jian, "Protecting Copyrights of Color Images using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform", Journal Of Multimedia, vol. 3, no. 4, October 2008.
[23] Stefean Porubsky, "Signum Function", Retrieved 2009/4/30 from Interactive Information Portal for Algorithmic Mathematics, Institute of Computer Science of the Czech Academy of Science, Prague, Czech Republic, Web-page http://www.cs.cas.cz/portal/AlgoMath/MathematicalAnalysis/SpecialFunctions/SignumFunction.htm
[24] M.A.Dorairangaswamy, A Novel Invisible and Blind Watermarking Scheme For Copyright Protection of Digital Images, International Journal Of Computer Science And Network Security, Vol. 9, No. 4, 2009, pp. 71-78.

Dr.M.A.Dorairangaswamy is a Professor in Computer Science and Engineering. Basically an Electronics and Communication Engineer with masters in Systems Information and Computer Science. He has received PhD from University of Honollulu, USA in 2003 and from Magadh Universiy, India in 2007 in Computer Science and Engineering. Prof Dorai rangaswamy has a rich experience of 18 years in teaching for various universities/colleges in India like SRM Easwari Engineering College, Chennai, QIS College of Engg Tech, Ongole,, Manipal University, Chennai, SRM University, Chennai;; Bharath University, Chennai, Sathyabama University, Chennai, SRM Valliammai Polytechnic College, Chennai for graduate, postgraduate students and mentoring research scholars. He is a member of IETE,ISTE, IACSIT. His research interests include processors architecture, image processing, multimedia, data and video mining. He is also a professional counselor and psychotherapist. Email id – drdorairs@yahoo.co.in; Contact number :09840162750.

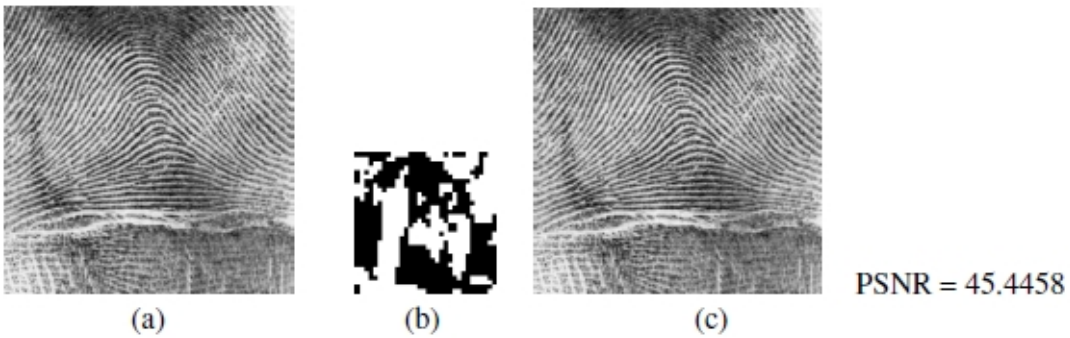

Fig. 3 (a) Host Image (b) Watermark Image (c) Watermarked Image with PSNR value

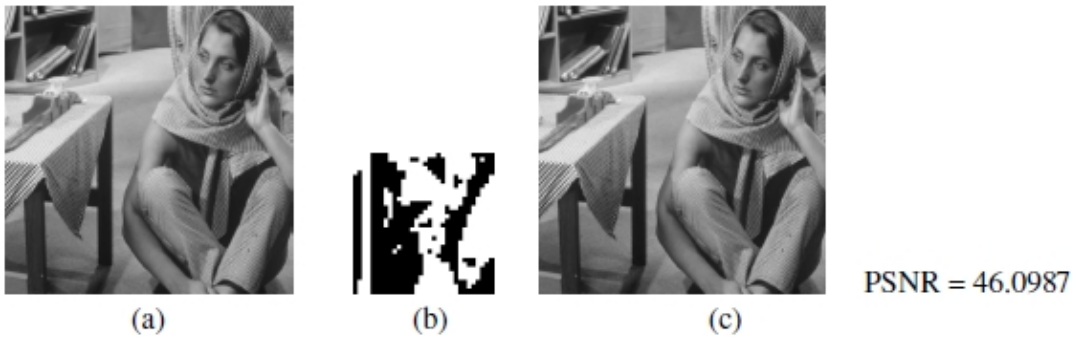

Fig.4 (a) Host Image (b) Watermark Image (c) Watermarked Image with PSNR value

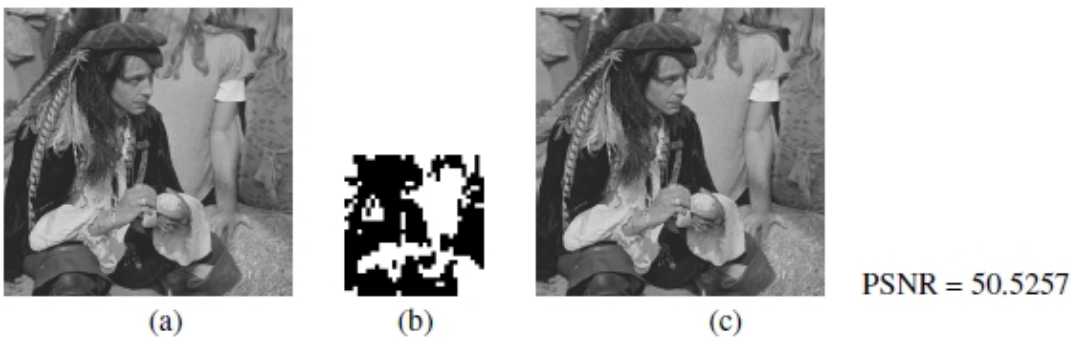

Fig. 5 (a) Host Image (b) Watermark Image (c) Watermarked Image with PSNR value

Fig. 6 (a) Host Image (b) Watermark Image (c) Watermarked Image and the PSNR value

Attack	Gaussian Noise (σ = 25)	Gaussian Noise (σ = 50)	Gaussian Noise (σ = 75)
Attacked Images			
Extracted Watermark			
Correlation Coefficient	0.9058	0.8115	0.7290

(a)

Attack	Gaussian Blur (l=2,θ =10)	Gaussian Blur (l=6,θ =10)	Gaussian Blur (l=10,θ =10)
Attacked Images			
Extracted Watermark			
Correlation Coefficient	0.9296	0.7801	0.6922

(b)

Attack	Intensity Adjustment (Low – 0.2, High - 0.4)	Intensity Adjustment (Low - 0.4 , High – 0.6)	Intensity Adjustment (Low - 0.6, High – 0.8)
Attacked Images			
Extracted Watermark			
Correlation Coefficient	0.9196	0.8607	0.8371

(c)

Attack	Cropping (Left Upper 100x100)	Cropping (Middle 100x100)	Cropping (Right Upper 100x112)
Attacked Images			
Extracted Watermark			
Correlation Coefficient	0.8123	1	0.7609

(d)

Attack	Sharpening (α = 0.2)	Sharpening (α = 0.6)	Sharpening (α = 0.9)
Attacked Images			
Extracted Watermark			
Correlation Coefficient	0.9058	0.7488	0.6622

(e)

Attack	Weiner Filtering (2x2)	Weiner Filtering (4x4)	Weiner Filtering (4x8)
Attacked Images			
Extracted Watermark			
Correlation Coefficient	0.9137	0.8395	0.6865

(f)

Fig 7. Attacked watermarked Images, Extracted watermark image and correlation coefficient of (a) Gaussian Noise (b) Gaussian Blur (c) Intensity Adjustment (d) Cropping (e) Sharpening (f) Wiener Filtering Attacks