Multiple Watermarking Scheme for Image Authentication and Copyright Protection using Wavelet based Texture Properties and Visual Cryptography

S. Radharani
Lecturer,
Dept of Computer Science,
Sree Narayana Guru College,
Coimbatore.

Dr. M.L. Valarmathi
Assistant Professor,
Dept. of Computer Science and Engineering
Government College of Technology,
Coimbatore.

ABSTRACT
Advancement in communication medium is producing large volume of digital information which needs to be protected. Watermarking is a technique that is used to hide secret signal into digital signal in a manner that does not reduce overall quality of the original signal. In relation to digital image watermarking, another area that is drawing attention is the multiple watermarking, where more than one watermark is embedded into single multimedia object. Multiple watermarks are normally proposed as a method to provide extra security to an image by embedding two or more secret messages into the cover image. In the present research work, the concept of multiple watermarking is used to hide both copyright and authentication information into a color image. For this purpose a wavelet transformation based on texture properties and secret sharing using visual cryptography is used. Experimental results indicate that the proposed watermarking scheme is highly robust and does not degrade the original signal.

General Terms
Steganography, Cryptography, Watermarking.

Keywords
Discrete Wavelet Transformation, Visual Cryptography, Fingerprint, Human Visual System, Adaptive Order Dithering Algorithm.

1. INTRODUCTION
Technological advancements in both hardware and software are making communication easy and cost effective, which in turn, is producing large volume of digital information being transmitted through the Internet and communication networks. This advancement, in recent years, has created awareness on the risk of piracy and on the importance of protection of content being shared. Several researches have been focused on providing solutions to copyright protection and authentication. These techniques mainly fall into three categories, namely, Steganography, Cryptography and Watermarking. Out of these, watermarking techniques have gained more popularity for proving integrity and authenticity of the owner [1, 2, and 3].

Digital watermarking is defined as an algorithm that can be used to hide secret signal into digital audio, video, image or documents in a manner that does reduce the overall quality of the original signal. The secret signal, identified as the watermark, can be copyright notices or authentication information or secret text. The original signal is called as 'cover signal' or 'host signal'. The process of inserting the secret signal is called embedding and the image after embedding is called 'watermarked image'. Extraction or detection is a process retrieves the stored watermark. Thus the two main components of digital watermarking systems are (i) Embedding and (ii) Extraction.

Digital watermark is used in many applications including copyright protection, fingerprinting, copy protection, broadcast monitoring and data authentication. The watermarking techniques are grouped as text-based watermarking [4], image watermarking [5], video watermarking [6], audio watermarking [7] and 3D watermarking [8]. As almost 90% of the content being transmitted in image and video [9, 10], more number of techniques have been developed for these two groups. Regardless of the application, all these techniques have the common goal of protecting digital signal.

In relation to digital image watermarking, another area that is drawing attention is the multiple watermarking, where multiple watermarks are embedded into single multimedia object [11]. Multiple watermarks are normally proposed as a method to provide extra security to an image by embedding two or more secret messages into the cover image. The goals of such schemes are to propose robust watermarking technique that has the properties of confidentiality (only the entitled users have access to the information), availability (ability of an information system to be used in the normal scheduled conditions of access) and reliability. Reliability can be achieved based on Integrity (the information has not been modified by unauthorized people) and authenticity (act as a proof that the information belongs to the correct person). Moreover, the scheme should satisfy two conflicting requirements. The first is that it must not introduce any distortion in the host signal and secondly, the watermark must be immune against intentional or unintentional attacks or removals. Finally, the proposed scheme must be efficient in terms of tranparency (the watermark is not visible in the image under typical viewing conditions), capacity (ability to detect watermarks with a low probability of error as the number of

watermarked versions of the image increases) and robustness (the watermark can still be detected after the image has undergone some linear or non linear operations). In order to achieve the above said goals, this paper proposes the use of multiple watermarking which acts as an authentication mechanism and which can protect the copyright information.

Recently, [12], proposed a watermarking scheme that used wavelets that analyzed the texture properties of a color image and visual cryptography to embed copyright information. Texture properties represent the details of a color image surface and consist of contrast, coarseness and density. Texture properties from an image can be obtained by using statistical model-based method or transform-based method. This paper uses a wavelet transform based method. This method had the advantage of being robust and reliable, while also satisfying the goals of less distortion and able to resist all common attacks. In the present paper, this paper is enhanced to include authentication that can satisfy the goal of capacity. The paper is modified to use a novel method that can embed a biometric digital image that can be used to authenticate the correct owner. A biometric is defined as a "life measure" and the biometric recognition technology uses images of human body parts, captured through cameras and scanning images. Watermarking techniques are increasingly used in biometric security systems for authentication requirements and they use biometric characteristics such as face, voiceprint, fingerprint, etc. Out of these, fingerprint image is most frequently used because of easy availability and non-intrusive method required to capture them. More the human fingerprints have the advantage of being unique.

This paper is organized as follows. Section 2 provides a crisp review of the previous works proposed in the field of multiple watermarking. Section 3 describes the proposed methodology, while Section 4 presents the results obtained. Section 5 concludes the present work with future research directions.

2. PREVIOUS STUDIES

Digital image watermarking algorithms have been used for the past few years, which increase robustness of the watermark against different kinds of attacks and embed a single watermark for this purpose. Recently, the usage of multiple watermarks has attracted several proposals [13, 14]. While in most of the cases, multiple watermarking is used in multimedia applications, it has also been used in other applications like protection in wireless sensor networks [15]. A review of the various methods used for multiple watermarking is given by [16].

The initial contribution to the field of multiple watermarking was proposed by [17], where methods to recover multiple watermarks from the same image was first shown. This work was followed several contributions. According to [18], the insertion of multiple watermarks can be exploited to convey multiple sets of information. Most of the works focus on extending single watermarking algorithms to use multiple watermarks [19, 20]. Proposed the use of virtual border, where extra line of pixels was added around the image as borders and watermarks were embedded within these borders. [22] Used the concept of multiple watermarking to protect relational database using images. [23] Employed pair-coupled maps to improve the security of watermarked image, and to encrypt the embedding position of the host image. [24] used Discrete Cosine Transformation for multiple-watermarking still images.

While many techniques have been probed, wavelets have been the most explored technique in both single and multiple watermarking domains. [25] Proposed a wavelet-based watermarking scheme to embed multiple watermarks in medical images. [26] And [27] used watermarking techniques for secure data hiding in wavelet compressed fingerprint images.

Visual Cryptography is another field which is used for content protection. Visual cryptographic has been applied to many applications, including but not restricted to information hiding, general access structures [28], visual authentication and identification [29]. The solutions normally operate on binary or binarized inputs. After its initial introduction, many researchers have found different variations of VC [30]. The improvement varies from binary image to halftone images, gray scale and color images. Luo, H., Lu, Z.M. and Pan, J.S. [31] has used this concept for multiple watermarking. More detailed information about visual cryptography can be found in [32]. All these techniques focus on improving the technique in terms of various aspects like confidentiality, integrity and robustness. Notwithstanding the application potential of such methodologies, multiple-image watermarking is still an open problem, where improvements are still being investigated. One such attempt is made in this paper, where an existing single watermarking technique is enhanced to a multiple watermarking scheme using wavelets and visual cryptography.

3. TECHNIQUES USED

The proposed model is based on three techniques, namely, wavelets, visual cryptography and feature extraction from the human fingerprint image. These techniques are described in this section.

3.1. Discrete Wavelet Transformation and Texture Properties

Discrete Wavelet Transformation (DWT) of image produces the multi-resolution representation of image. A multi-resolution representation provides a simple hierarchical framework for interpreting the image information. At different resolutions, the details of an image generally characterize different physical structures of the image. At a low level resolution, these details correspond to the larger structures which provide the image content.

Wavelet transformation consist of two main steps namely DWT and IDWT (Inverse DWT). DWT segments a digital signal into high frequency quadrant and low frequency quadrants. The low frequency quadrant is split again into two more parts of high and low frequencies and this process is repeated till the signal has been entirely decomposed. In watermarking, generally 1-5 level of decompositions is used. The reconstruct of the original signal from the decomposed image is performed by IDWT.

Several types of wavelets exist for decomposition. Some examples include Haar, Daubeschies, Coiflets, Symlets, Morlets, Mexican Hat Meyer and Biorthogonal wavelets. More generally, application of DWT divides an image into four subbands (Figure 1a), which arise from separable applications of vertical and horizontal coefficients. The LH, HL and HH subbands represents detailed features of the images, while LL subband represents the approximation of the image. To obtain the next coarse level, the LL subband is further be decomposed (Figure 1b), thus resulting in the 2-level wavelet decomposition. The

level of decomposition performed is application dependent. The present work considers decomposition up to two levels.

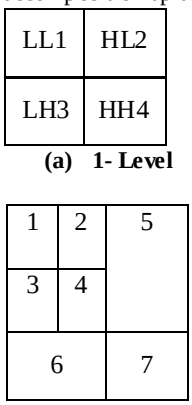

Figure 1: Wavelet Decompositions

- **Texture Properties**

The 2-D wavelet transformation thus segments images into different frequency layer. At each resolution level, three new features, namely, scale depth, horizontal, vertical and diagonal components can be obtained. As the micro textures or macro textures varied by non-uniform pixel values, they are statically characterized by the features in approximation and detailed images. Thus the values in the sub-band images or derived features from these subbands uniquely characterize the texture properties [33], which can be used to decide the subband for embedding watermark. The representative texture feature vectors are used for analyzing the image for watermarking. The various co-occurrence features such as energy, homogeneity and contrast at the output of each channel are calculated using Equations (1), (2) and (3) and are used as feature vectors at each level of the decomposed image.

$$\text{Energy}_L = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} I_L^2(i,j) \quad (1)$$

$$\text{Homogeneity}_L = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{1}{1+(i-j)^2} I_L(i,j) \quad (2)$$

$$\text{Contrast}_L = \sum_{i=1}^{M} \sum_{j=1}^{N} (i-j)_2 I_L(i,j) \quad (3)$$

Where $I_L(i, j)$ refers an image obtained in L^{th} subband and $L \in \{LL, LH, HL, HH\}$, with resolution of $M \times N$ having been determined by wavelet analysis.

3.2. Visual Cryptography

Visual Cryptography (VC), a paradigm introduced by [34] is a Visual Secret Sharing Scheme (VSSS) which uses the Human Visual System (HVS) to decrypt a secret message without expensive and complicated decoding process [35]. The basic VC system starts with the encoding phase, where a secret image is divided into a collection of 'm' black and 'n' white pixels. Each collection of m x n pixels is referred to as a share, which will resemble a noisy image when separated. During decoding phase, these shares or subset of shares are stacked together which will allow the visual recovery of the secret message. It has been applied to many applications, including but not restricted to E-voting system [36], financial documents [37], information hiding [38], general access structures [28], visual authentication and identification [39]. More detailed information about visual cryptography can be found in [32].

Out of the many VC schemes proposed, the (2, 2) VSS scheme is more frequently used. In this algorithm, each pixel of the copyright image is expanded into 2 * 2 pixels (Figure 2). To share a white pixel of the secret image, one row from the first 6 rows of table1 is chosen randomly. Similarly, the two shares of a black pixel are determined by a random selection from the 6 last rows of Figure 2. As a result, an M*N pixels secret image is expanded into two 2M*2N pixels share-images. Considering security of the method, presence of only one share image reveals nothing about the corresponding secret image, i.e., each 2*2 pixels block of one share-image may correspond to either a white pixel or a black pixel of the secret image. As Figure 2 shows, stacking the shares of a black secret pixel results in 4 black sub pixels, whereas only 2 black sub pixels is gained by stacking shares of a white secret pixel [40]. So, secret image is revealed to human eyes by stacking the shares without performing any cryptographical computations. Using (2, 2) VSS Scheme causes loss in contrast and therefore, a XOR based V CS scheme is generally used. In this scheme, the shared images are superimposed using XOR operation, results in perfect reconstruction of both black and white pixels as shown in Figure 2. An example of VC scheme is shown in Figure 3.

The above scheme works well for binary images. While considering gray scale images, the procedure used consist of two steps. The first step converts the gray scale image into a binary image and the second step creates the shares from the result of step using the conventional (2, 2) VSS scheme. The conversion algorithm used is the Space-Filling Curve Ordered Dither (SFCOD) technique [45]. Usage of SFCOD lowers the quality of the image after decryption and hence in this paper, Adaptive Order Dithering (AOD) algorithm [41] as suggested by [12], is used. Adaptive order Dither technique does the halftones of gray-level image by using a space-filling curve to perform an adaptive variation of the cluster size and inherits the advantages of the *SFCOD* and the stochastic screening dithering method

[42]. The scheme used has the advantages of (i) Simple to implement (ii) Encryption process with heavy computations (iii) No separate decryption algorithm (uses only Human Visual System) and Provides secure method.

Pixel		Share 1	Share 2	Result
	P = ½			
	P = ½			
	P = ½			
	P = ½			

$C0=\left\{\begin{bmatrix}0&1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\1&0\end{bmatrix}\right\}$ $C1=\left\{\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}1&0\\0&1\end{bmatrix}\right\}$

Figure 2: (2, 2) VSS Scheme (2 Subpixels)

Original Image | Share 1 | Share 2 | OR (2, 2) VSS | XOR (2, 2) VSS

Figure 3: Example of VC Scheme

3.3. Fingerprint Feature Extraction

The human fingerprint image is first decomposed using 4-level Haar 2-DWT. This result with four types of coefficients: (a) coefficients that result from a convolution in both directions (HH) representing diagonal features of the image. (b) Coefficients that result from a convolution on the columns after a convolution with h on the rows (HL) corresponding to horizontal structures. (c) Coefficients from high pass filtering on the rows and low pass filtering on the columns (LH) providing vertical information (d) The coefficients from low pass filtering in both directions are again processed in the next step. Thus, the original image is decomposed into 16 quadrants. The average standard deviation for each of the high frequency subbands is calculated and is used to generate a feature vector. The feature extraction algorithm was developed using MATLAB and the standard deviation is represented as single value which uses 4 bytes for storage. Thus there are 12 quadrants, whose average produce 4 values and thus represent a fingerprint image occupying only 128 bits. Irrespective of the image size, the feature extraction module will always produce a vector occupying only 128 bits. Thus, this process increases the capacity.

4. PROPOSED WATERMARKING SCHEMES

The highest energy subband of Luminance channel of the color image is used for embedding the watermark. Before embedding the watermark, the watermark is split into two shares by applying Visual cryptography Scheme (*VCS*) using Adaptive Order Dither Technique. One of these binary share is embedded into cover image where as the other share is kept secret. The algorithm for embedding and extraction of the watermark are shown below.

Embedding algorithm

Stage 1:

1. Read the grayscale human fingerprint image and convert them into feature vectors.

Stage 2:

2. Read the copyright image and use the AOD based (2, 2) visual cryptographic algorithm to create two shares S1 and S2. S2 is embedded as watermark, while S1 is used as master share and is kept secret.

Stage 3:

1. Read the cover image and convert the color space from RGB to YUV.

2. Apply DWT to Luminance (Y) Channel to get subband coefficients (*LL*1, *LH*1, *HL*1 and *HH*1).

3. Extract texture property energy for each subband coefficients

4. Select subband with high energy and apply DWT again to get second level decomposition

5. Extract texture property energy for each subband coefficients at second level

6. Select subband with high energy and embed the fingerprint features first, followed by S1 using the following equation

$$Y' = \sum_{i,j=1}^{M} (|Y(i,j)| + \alpha)B$$

Where Y' represents the modified frequency coefficient after embedding the watermark, Y is the original frequency coefficient, α represent the watermark scaling factor and B is either the bits from fingerprint feature vector or S1 pixel value.

7. After replacing modified coefficients, apply IDWT twice to get the watermarked luminance channel.

8. Combine Y, U and V channels to get the watermarked image.

Extraction algorithm

Stage 4:

1. Read the watermarked image and perform color space conversion to convert RGB to YUV.

2. Apply DWT to Luminance (Y) Channel to get subband coefficients (*LL*1, *LH*1, *HL*1 and *HH*1).

3. Extract texture property energy for each subband coefficients

4. Select subband with high energy and apply DWT again to get second level decomposition

5. Extract texture property energy for each subband coefficients at second level

6. Select subband with high energy and extract the first 128 bits as fingerprint features and use the following equation to extract the copyright image

$$S'_1 = \sum_{i,j=1}^{M} \begin{cases} 1 & Y' >> 0 \\ 0 & \text{otherwise} \end{cases}$$

Where S'_1 represents the extract Share1 and Y' is the watermarked bit.

7. The extracted Share 1 is superimposed on Share 2 using XOR (2, 2) VSS system to obtain the original copyright image.

5. EXPERIMENTAL RESULTS

The proposed watermarking model was tested with several cover, fingerprint and copyright images. This section reports the result obtained for one such set. Similar results were observed for all other images also. The cover image, copyright image and biometric image used is shown in Figure 4.

Cover Images **Biometric Image** **Copyright Image**

Figure 4 : Test Image and Secret Message

Experiments to test the robustness to withstand attacks were also conducted. Nine types of attacks were considered. They are compression at different quality factors, Gaussian and median filer, blurring, gamma, cropping, resizing, rotation and affine transformation. These were compared with the results when no attacks were performed. The proposed system was also compared with the watermarking scheme of [12]. This model is termed as Base System in the results. The quality metric Peak Signal to Noise Ratio (PSNR) was used for this purpose and is calculated using Equation 4.

$$PSNR = \log \frac{(2^n - 1)}{MSE} \quad (4)$$

Where n is the number of bits used for color representation and MSE is calculated using Equation 5.

Let f=I [I, J], f'=I' [I, J],

$$MSE = \frac{\sum_{R,G,B} \sum_{i=1}^{M} \sum_{j=1}^{N} (I[I,J] - I'[I,J])^2}{3MN} \quad (5)$$

Where M and N are the height and width of the image respectively, f represents the original image and f ' represents watermarked image, i and j represents the pixel position.

The results with respect to the PSNR value obtained between the original and watermarked image is shown in Table I.

Table I: Peak Signal to Noise Ratio

PSNR Between	Proposed System	Base System
Cover and Watermarked Image	45.91	43.67
Original copyright and Extracted Image	26.78	24.57

From the results projected it could be seen that the proposed system minimizes the distortion introduced by watermarking and the extracted watermark is very close to the original image. This is proved by the high PSNR value obtained. The proposed system showed a 4.88 per cent quality gain while comparing the PSNR obtained while comparing cover and watermarked image. Similarly, 8.25% accuracy was observed while comparing the original copyright and extracted copyright images. This proves that the proposed system is an improvement to the existing scheme.

According to [43], an improved denoising algorithm is recognized by a high PSNR or a lower MSE. In agreement with this, the results of the proposed systems with high PSNR prove that they are an improved version. Similarly, according to the report of [44], a PSNR value in the range 20-40 indicates that the resultant image is a very good match to the original image. In accordance with this report, the results of the proposed algorithm produce PSNR values in the range 25dB to 45dB proving that the proposed algorithms does not degrade the images with the insertion of watermark. Table II shows the affect of attacks using PSNR value.

Table II: Affect of Attacks

Attack	PSNR (dB)
No attack	45.91
JPEG (50%)	41.36
JPEG 2000 (50%)	42.69
Gaussian Noise (3 x 3)	39.23
Median Filter (3 x 3)	38.99
Blurring (3 x 3)	36.12
Gamma (0.5)	39.12
Cropping (10 pixels)	31.55
Resize (90%)	31.26
Rotation (10^o)	34.90
Affine Transform	36.46

Again the results prove that the proposed system is highly robust and can withstand most of the attacks. While considering the biometric text, the embedding process showed a very low error value (bpp) between 1.14 to 1.16bpp. This shows that the proposed system is efficient in terms of multiple watermarking also.

6. CONCLUSION

The present work proposed a multiple watermarking technique which combined wavelets based on texture properties to watermark copyright and authentication information inside a cover image. Experimental results proved that the proposed algorithm is efficient in terms of quality and further, the results also proved that storing watermarks using texture properties provides more robustness to the proposed technique. The present work uses a gray scale visual cryptographic method, which can be improved to color visual cryptography. Further, more efficient feature extraction technique can be used for fingerprint feature extraction process and its effect on the proposed scheme can be studied.

7. REFERENCES

[1] Piva, A., Bartolini, F. and Barni, M. (2002) Managing copyright in open networks, IEEE Transactions on Internet Computing, Vol. 6, Issue. 3, Pp. 18-26.

[2] Lin, E., Podilchuk, C., Kalker, T. and Delp, E. (2001) Streaming Video and Rate Scalable Compression: What Are the Challenges for Watermarking?, Proceedings the SPIE International Conference on Security and Watermarking of Multimedia Contents III, Vol. 4314, San Jose, CA, 22-25.

[3] Lu, C., Huang, S., Sze, C. and Liao, H. Y. M. (2000a) Cocktail watermarking for digital image protection," IEEE Transactions on Multimedia, Vol. 2, Pp. 209-224.

[4] Kim, Y., Moon, K. and Oh, I. (2003) A text watermarking algorithm based on word classification and inter-word space statistics, Proceedings Seventh International Conference on Document Analysis and Recognition, Pp. 775 -779.

[5] Xuehua, J. (2010) Digital Watermarking and its Application in Image Copyright Protection, International Conference on Intelligent Computation Technology and Automation (ICICTA), Pp.114 - 117.

[6] Checcacci, N., Barni, M., Bartolini, F. and Basagni, S. (2000) Robust video watermarking for wireless multimedia communications, Proceedings IEEEE Wireless Communications and Networking Conference 2000, WCNC. 2000, Vol. 3, Pp. 1530-1535.

[7] Hartung, F. and Kutter, M.(1999) Multimedia Watermarking Techniques, Proc. of IEEE, Tutorial, Survey, and Special Issue on Data Hiding & Security, Pp.1079-1107.

[8] Wang, C., Nie, X., Wan, X., Wan, W.B. and Chao, F. (2009) A Blind Video Watermarking Scheme Based on DWT," iih-msp, 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Pp.434-437,

[9] Mohammed, A.A. and Hussein, J.A. (2009) Efficient Video Watermarking Using Motion Estimation Approach, 2009 Eight IEEE/ACIS International Conference on Computer and Information Science (icis 2009), Pp.593-598.

[10] Jiang, J. and Weng, Y. (2008) Robust multiple watermarking in color images with correlation coefficient detector, Proceeding of the 8th IASTED International Conference on Visualization, Imaging and Image Processing (VIIP 2008), Palma de Mallorca, Spain, Pp.280-285.

[11] Dharwadkar, N.V. and Amberker, B.B. (2010) Watermarking Scheme for Color Images using Wavelet Transform based Texture Properties and Secret Sharing, International Journal of Information and Communication Engineering, No. 6, Issue 2, Pp. 94-101.

[12] Wong, P.H.W., Au, O.C. and Yeung, Y.M.(2003) Novel blind multiple watermarking technique for images, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 13, Issue 8, Pp. 813 - 830.

[13] Chen, W.Y., Lin, J.T., Lin, C.Y. and Liu, J.R. (2007) Multiple Watermarking Scheme Using Adaptive Phase Shift Keying Technique, The 23rd Workshop on Combinatorial Mathematics and Computation Theory, Vol. 46, No. 6, Pp.067002-1~12

[14] Wang, B., Sun, X., Ruan, Z. and Ren.H. (2011) Multi-mark: Multiple watermarking method for privacy data protection in wireless sensor networks, Information Technology Journal, Vol. 10, No. 4, Pp. 833-840.

[15] Sheppard, N.P., Safavi-Naini, R, and Ogumbona, P. (2001) On Multiple Watermarking, ACM Workshop Proceedings on Multimedia and Security – New Challenges, Pp. 1-3.

[16] Cox, I.J. , Kilian, J., Leighton, T. and Shamoon, T. (1997) Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing, Vol. 6, No. 12, Pp. 1673–1687.

[17] Mintzer, F. and Braudaway, G.W. (1999) If one watermark is good, are more better?, Proceedings of IEEE International Conference in Acoustics, Speech, and Signal Processing, Vol. 4, Pp. 2067–2069.

[18] Stankovic, S., Djurovic, I. and Pitas, I. (2001) Watermarking in the Space/Spatial-Frequency Domain Using Two-Dimensional Radon-Wigner Distribution, IEEE Transactions of Image Processing, Vol. 10, No. 4, Pp. 650-658.

[19] Hsu, C.T. and Wu, J.L. (1999) Hidden digital watermarks in images, IEEE Transactions on Image Processing, Vol. 8, No. 1, Pp. 58–68, Jan. 1999.

[20] Trichili, H., Boublel, M., Derbel, N., Kamoun, L. (2002) A new medical image watermarking scheme for a better telediagnosis, Proceedings of the IEEE International Conference on Systems, Man and Cybernetics 2002, Vol.1, Pp. 556–559.

[21] Sun, J., Cao, Z. and Hu, Z. (2008) Multiple Watermarking Relational Databases Using Image, 2008 International Conference on MultiMedia and Information Technology, Pp.373-376.

[22] Behnia, S., Teshnehlab, M. and Ayubi, P. (2010) Multiple-watermarking scheme based on improved chaotic maps, Communications in Nonlinear Science and Numerical Simulation, Vol. 15, Issue 9, Pp. 2469-2478.

[23] Liu, C.C. and Chen, W.Y. (2006) Multiple-watermarking scheme for still images using the discrete cosine transform and modified code division multiple-access techniques, Optical Engineering, Vol. 45, No.07, 077006

[24] Giakoumaki, A., Pavlopoulos, S., Koutouris, D., (2003) A medical image watermarking scheme based on wavelet transform, Proceedings of the 25th Annual International Conference of the Engineering in Medicine and Biology Society IEEE, Vol.1, Pp.856–859.

[25] Ratha, N.K., Connell, J.H. and Bolle, R.M. (2000) Secure data hiding in wavelet compressed fingerprint images, Proc.ACM Multimedia 2000 Workshops, Los Angeles, CA, Pp. 127-130

[26] Zebbiche, K. and Ghouti, L. et al. (2006) Protecting fingerprint data using watermarking, First NASA/ESA Conf. on Adaptive Hardware and Systems (AHS'06), Pp.451–456.

[27] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D.R. (1996) Visual cryptography for general access structures, Information Computation, Vol. 129, Pp.86-106.

[28] Naor, M. and Pinkas, B. (1997) Visual authentication and identification, Advances in Cryptology CRYPTO'97, Lecture Notes in Computer Science, Vol. 1294, Pp. 322–336.

[29] Yang, C.N. (2010) Visual cryptography: An introduction to visual secret sharing schemes, Department of Computer Science and Information Engineering National Dong Hwa University Shoufeng, Hualien 974, TAIWAN, Last accessed on July 04, 2010, http://sna.csie.ndhu.edu.tw/~cnyang/vss/sld001.htm

[30] Luo, H., Lu, Z.M. and Pan, J.S. (2008) Multiple watermarking in visual cryptography, IWDW 2007, LNCS 5041, Shi, Y.Q., Kim, H.J. and Katzenbeisser, S. (Eds.), Springer-Verlag Berlin Heidelberg, Pp.60-70.

[31] Yang, C. (2002) A note on Efficient Color Visual Encryption, Vol.18, Pp 367- 372.

[32] Arivazhagan, S. and Ganesan, L. (2003) Texture classification using wavelet transform, Elsevier, Pattern Recognition letter, Vol.24, Pp.1513-1521.

[33] Naor, M. and Shamir, A. (1995) Visual cryptography, Advances in Cryptology - EUROCRYPT '94, A. De Santis, ed., Lecture Notes in Computer Science, Vol. 950, Pp. 1-12.

[34] Tai, G.C., Chang, L.W. Visual Cryptography for Digital Watermarking in Still Images, Advances in Multimedia Information Processing - PCM 2004, Category – Watermarking I, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, vol. 3332, pp.50-57 (2005).

[35] Paul, N., Evans, D., Rubin, A., Wallach, D.: Authentication for remote voting, workshop on human-computer interaction and security systems, Fort Lauderdale, Florida, April (2003).

[36] Hawkes, L., Yasinsac, A., Cline, C.: An Application of Visual Cryptography to Financial Documents; technical report TR001001, Florida State University (2000).

[37] Bonnis, A., Santis, A.: Randomness in secret sharing and visual cryptography schemes, Theor. Comput. Sci, 314, pp 351-374 (2004).

[38] Naor, M., Pinkas, B.: Visual authentication and identification, Advances in Cryptology CRYPTO'97, Lecture Notes in Computer Science, vol. 1294, pp. 322–336 (1997).

[39] Houmansadr, A., Ghaemmaghami, S.: A Digital Image Watermarking Scheme Based on Visual Cryptography, International Symposium on Telecommunications, pp. 1-5 (2005).

[40] Zhang, Y. (1997) Adaptive Ordered Dither, Graphical, Models and Image Processing, Vol. 59, No. 1, Pp. 49-53.

[41] Velho, L. and Gomes, J. (1995) Stochastic screening dithering with adaptive clustering, Proceedings of SIGGRAPH-95, ACM Computer Graphics, Annual Conference Series, Pp. 273-276.

[42] Venkatesan, M., MeenakshiDevi, P., Duraiswamy, K. and Thyagarajah, K. (2008) Secure Authentication Watermarking for Binary Images using Pattern Matching, IJCSNS International Journal of Computer Science and Network Security, Vol.8, No.2, Pp. 241-250.

[43] Schneier, M. and Abdel-Mottaleb, M. (1996) Exploiting the JPEG compression scheme for image retrieval. IEEE Trans. Pattern Anal. Mach. Intell., Vol.18, No. 8, Pp. 849–853.

[44] Zhang, Y. (1998) Space-Filling Curve Ordered Dither, Elsevier, Computer & Graphics Journal, Vol. 22, No. 4, Pp. 559-563.