A Visual Cryptography based Watermarking Scheme Incorporating the Concepts of Homogeneity Analysis and Singular Value Decomposition

Priyanka Singh
Motilal Nehru National Institute of Technology
Allahabad, India

Suneeta Agarwal
Motilal Nehru National Institute of Technology
Allahabad, India

ABSTRACT
A visual cryptography based watermarking scheme incorporating the concepts of singular value decomposition (SVD) and the homogeneity analysis of the cover image is proposed here. Firstly, feature vectors are created from the singular values of the homogeneous blocks and thereby classified using the k-medoid clustering technique. A master share is then constructed based on the clustering result and thereafter, combined with the secret binary image (watermark) ownership share is build up. This ownership share is registered with the certificate authority in case to resolve any dispute regarding rightful ownership of the image in future. A two-out-of-two visual cryptography scheme is being used in the proposed methodology and robustness validated by applying comprehensive set of attacks. The peak signal to noise ratio (PSNR) and normalized cross correlation (NCC) metric values are used for evaluation of the scheme. Higher values of these metrics establish the appropriateness of the proposed methodology as compared to the other state of art schemes for copyright protection.

General Terms
Algorithms, Security, Watermarking

Keywords
Homogeneity Analysis, Singular Value Decomposition (SVD), Visual Cryptography (VC), Peak Signal to Noise Ratio (PSNR), Normalized Cross Correlation (NCC).

1. INTRODUCTION
The era of the Internet eased the rapid transmission and exchange of lots of data without any bound through networked systems at convenience. However, the advantage of connectivity brings with the disadvantages of illegal tampering, duplication of works, violation of intellectual property rights of digital data, such as document, image, audio, and video etc. Hence, the issue of protection of the rightful ownership of digital data arises as one of the recent issues. Many researches are already ongoing in the field to propose techniques to protect the intellectual property rights for digital images. Digital watermarking is one such technique, that embeds a meaningful signature or some owner information called as the watermark into the cover host image for authenticating, copyright protection, copy protection etc. This hidden watermark is later on extracted to prove the rightful ownership of the host data.

The original cover image may or may not be required during the extraction process like in many cases such as image monitoring, it may not be available, thus techniques able to retrieve watermarks without requiring the original image would furnish better solutions. An effective watermarking scheme must satisfy certain conditions like robustness, imperceptibility, unambiguousness, low computational complexity, capacity and security. A trade off has to be maintained among the requirements like imperceptibility conflicts with robustness to achieve optimum solution for intended applications. The watermarking schemes can be broadly classified into two categories: one is the spatial-domain approach [1-4] and other, the transform-domain approach. In the spatial domain techniques, the watermark is embedded by directly modifying the pixel values of the cover image whereas, in transform domain techniques, the watermark is embedded by modifying the frequency coefficients of the cover image which may be transformed into domains like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transformation DWT) [5-8]. The robustness of frequency domain techniques is usually high compared to the spatial domain schemes whereas the computational complexity of spatial domain techniques is lower.

2. RELATED WORK
Many watermarking schemes have been proposed in the past decades to meet the requirements. Some are remarkable in some aspects while lack at others. A trade off need to be maintained between them depending on the application. In [6], a technique was proposed where 1000 DCT coefficients were selected except DC one for embedding the watermark. The main drawback was the requirement of the original cover image to extract the watermark. A wavelet-based technique has been proposed in [7] where the scrambled watermark was embedded into the middle frequency coefficients of the wavelet domain. It fulfilled the requirements of security and blindness at the same time. The robustness of the wavelet-based technique was further improved in [8] by embedding the watermark into low sub-band wavelet coefficients of visually insensitive locations.

Many lossless watermarking techniques have also been proposed [10–16] to maintain good image quality. Visual cryptography [13–15] is such one kind of lossless watermarking scheme which furnishes the requirement by utilizing the codebook concept to divide an image into several different sharing images and produce the same by stacking when a dispute for ownership arises.Visual cryptography serves as a good technique against tampering of digital media and proving its rightful ownership and gained much attention for researchers in recent years. Many watermarking schemes based on visual cryptography have already been proposed [19-26]. The basic idea is to generate two shares of the watermark

exploiting the local statistics of the pixel values of the watermark. One is registered with the certified authority and other share generated from a suspected watermarked image. Consequently, these two shares are stacked up to reveal the watermark and visually decrypt it to prove the rightful ownership. A visual cryptographic watermarking scheme based on the concept of generation of two based on the pixel values of the binary watermark, its global mean and also, the mean of some random pixels within the image was proposed in [20-21]. Other scheme comparing the global mean of the pixels values has been proposed in [22]. A most significant bit watermarking embedding (MWE) and pixel watermarking embedding (PWE) scheme has been proposed in [23-25].

In this paper, a copyright protection scheme using two out of two visual cryptography technique is proposed. Firstly, homogeneity analysis of the cover image is done and thereby, feature extracted from it that is used to build the master share. After the master share construction, a ownership share is constructed combining the secret image (watermark) and the master share. This ownership share is registered with the certificate authority (CA). Whenever a dispute arises regarding the rightful owner of a image, the master share is build up from the suspected image. Along with the registered ownership share, a secret image is extracted that helps to prove the ownership and resolves the dispute.

The paper is organized as follows: Basic concepts of the quad tree based image segmentation, Singular Value Decomposition and visual cryptography are outlined in section 3. Section 4 gives an insight into the proposed watermarking methodology and experimental results along with analysis are given in section 5. Conclusions along with the scope of future work are drawn in section 6.

3. BRIEF OVERVIEW OF THE CONCEPTS USED

3.1 Quad Tree based Image Segmentation

The Quad Tree based Image Segmentation method partitions the image into regions based on discontinuities in intensity levels or distribution of pixel properties, such as intensity values. It iteratively subdivides the entire image region into smaller quadrant regions and forms a tree structure where each node has exactly four descendants.

The partitioning must satisfy the following conditions:

i. $\bigcup R_i = R$

ii. $R_i \bigcap R_j = \phi$ for all i and j, $i \neq j$

iii. R_i is a connected region, i=1,2,.....n

iv. $P(R_i)$ = TRUE, for i=1,2,....n

where , $P(R_i)$ is the homogeneity criteria, a logical predicate defined over R_i and ϕ is the null set.

The parent node represents the entire image region and its four descendants signify the disjoint sub regions within the large region. The segmentation process continues dividing until the blocks meets the homogeneity criterion set by the user. The defined criteria is tested for each block and only if it doesn't satisfy, then it is further subdivided otherwise left as a whole region. Large regions represent less valuable information in an image like the absence of edges, the background area etc. whereas critical information signified by the small regions. The appropriate sites for watermark embedding would be these small sites. In the proposed methodology, threshold value for the quad tree decomposition was set as 10.Thereafter, 4x4 blocks passing the homogeneity criteria were selected for further watermark embedding.

3.2 Singular value decomposition (SVD)

The singular value decomposition (SVD) technique finds application in solving a lot of problems, such as data compression, pattern analysis and signal processing. The singular values do not change much due to the various tampering attacks and hence the image quality doesn't deteriorate much by slightly changing the singular values of the cover image. From the linear algebra viewpoint, the SVD decomposition of any discrete image matrix A of size mxn can be represented as:

$$A=USV^T$$

where, U and V are orthogonal matrices ($U^T U=I, V^T V=I$) of size mxm and nxn respectively.

The columns of U and V matrices called as left and right singular vectors represent the horizontal and the vertical details in an image. The diagonal matrix S with size mxn, has nonzero elements arranged in decreasing order called as singular values of the matrix represent the luminance values of the image layers.

3.2 Visual cryptography (VC)

Visual cryptography is the main idea in the proposed copyright protection scheme. The concept of visual cryptography technique was firstly proposed by Naor and Shamir [17] and meant for the security of a secret image. In a (k, n) VC scheme, a secret image is divided into n different sharing images and can be recovered from k or more than k sharing images. However, with the increase in number of sharing images, the management becomes harder [13]. Hence, in the paper, a simple and secure (2, 2) visual cryptography technique is adapted for the proposed scheme. According to the concept of Naor and Shamir scheme, each pixel of the secret image is replaced by 2x2 pixels. Hence, a secret image with M by N pixels can be divided into two sharing images with 2M by 2N pixels and can be recovered by stacking the two sharing images.

4. THE PROPOSED METHODOLOGY

In the proposed copyright protection scheme, there are two phases: the ownership share construction phase and the ownership identification phase. The steps of the embedding

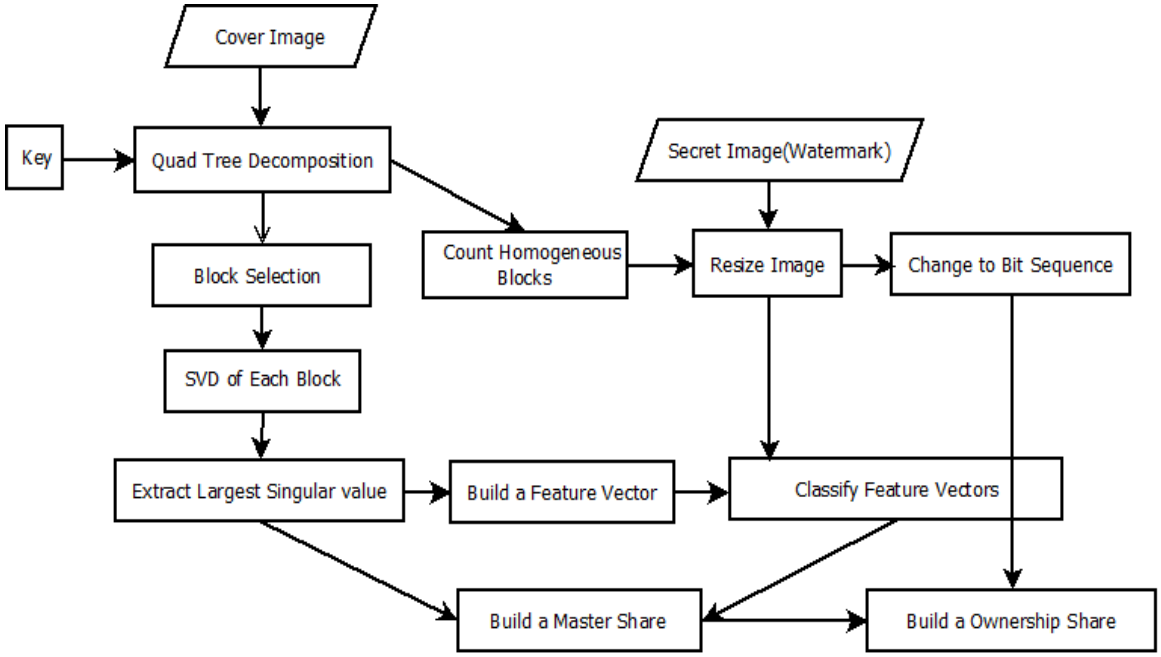


Fig.1: Watermark Embedding Methodology of the Proposed Scheme

phase and the extraction phase are shown in Fig. 1 in Fig. 2 and described as follows:

4.1 Ownership share construction

In this phase, a color cover image C to be protected and a secret binary image S is taken up. Thereupon, the homogeneity analysis of the blue channel of the cover image is done using the quad tree based image segmentation and appropriate homogeneous blocks are chalked out as the sites for watermark embedding. Singular value decomposition of each block is computed to extract the singular values. The singular values are then arranged to compose a feature vector. Thereupon, these feature vectors are clustered using k-mediod clustering and master share constructed based upon the clustering result. Then along with the secret binary image, the ownership share is constructed. This ownership share is then registered with the certificate authority and in case of dispute it is used in ownership identification phase. The step by step algorithm is enlisted as below:

Ownership share construction algorithm

Input: A color host image C of size M1xM2 pixels, a binary secret image P of size N1xN2 pixels.

Output: An ownership share O of size 2N1x2N2 pixels.

1. The homogeneity analysis of the blue channel of the cover image is done using quad tree based image segmentation with some user defined criteria. For instance, in the experiments done, it was fixed as 10 that is, the difference between the maximum and minimum gray level value of the block elements must be less than 10.

Thereafter, blocks of appropriate size are selected from the decomposed image, depending upon the level of segmentation needed for the particular problem. We have selected blocks of 4x4 pixels in the proposed methodology.

2. The watermark is resized depending upon the count of the homogeneous blocks in the above step say of size N1xN2 pixels.

3. Singular value decomposition (SVD) computed for each 4x4 pixels homogeneous block and singular values extracted from it.

4. The singular values from each 4x4 pixels homogeneous block B_i are arranged in a feature vector g_i and these vectors are classified using k-medoid clustering into two classes C_1 and C_2 .

5. Construct a master share M of size 2N1x2N2 pixels by dividing into 2x2 sized non-overlapping blocks m_i and content of each block determined as follows:

Master share generation rule

If $g_i \in C_1$

Then $m_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Else

$m_i = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

where, “0” and “1” within a block represent black pixel and white pixel respectively.

6. Generate the ownership share O of size 2N1x2N2 pixels mapping the secret image P and the master share M. It is divided into non-overlapping blocks o_i ($1 <= i <= N1xN2$) of size 2×2 and content filled in each block according to the following ownership share generation rule:

Ownership share generation rule

If p_i =1,

$o_i = m_i$

Else

$o_i = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} - m_i$

where, p_i denotes bit in the secret watermark image.

The generated ownership share O has to be registered with the certificate authority. In case of dispute of ownership, it is used for the rightful ownership verification of a suspected image. The homogeneity criteria set for the decomposition of the cover image must be kept securely by the copyright owner as the private key K .

4.2 Ownership identification

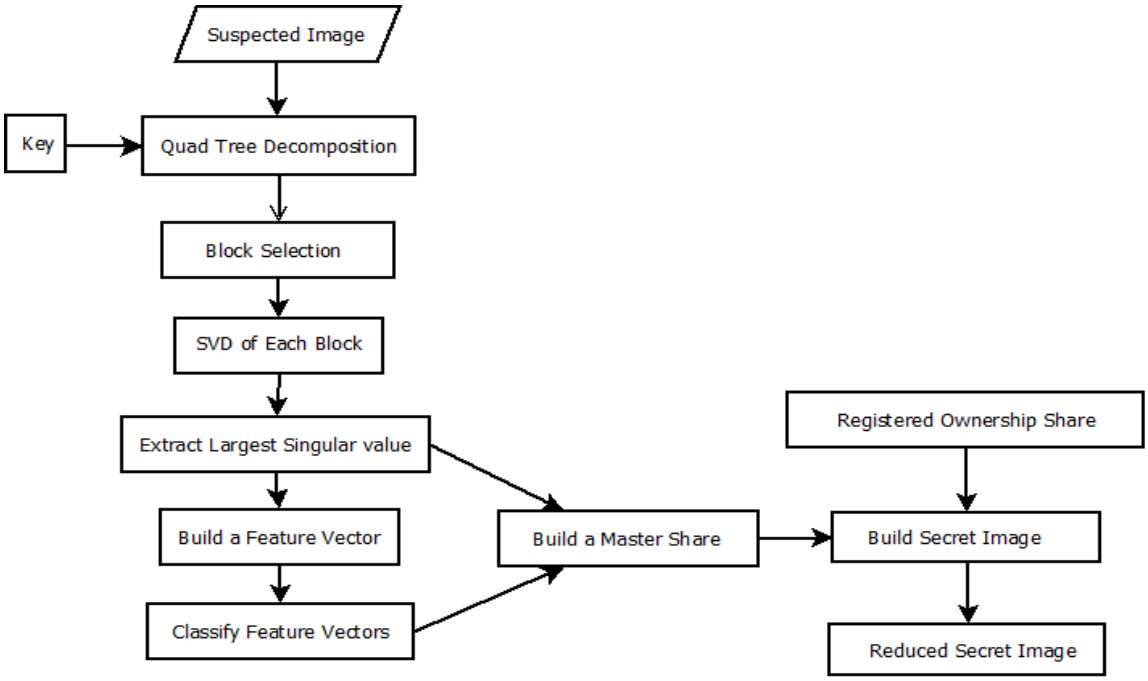


Fig. 2: Watermark Extraction Methodology of the Proposed Scheme

In the ownership identification phase, a master share M' is constructed from the suspected cover image C' by following the same procedure as used at the time of the ownership share construction phase. Thereafter, the obtained master share M' is stacked with the ownership share O registered with the CA and secret hidden image S' is revealed. The retrieved secret image is further reduced to obtain a reduced secret image Sq of same size as the original used at the embedding time. The detailed step by step procedure of the identification procedure is enumerated below.

Ownership identification algorithm

Input: A suspected cover image C' of size M1xM2 pixels, an ownership share O of size 2N1x2N2 pixels, a private key K.

Output: A retrieved secret image S' of size 2N1x2N2 pixels and a reduced secret image Pq of size N1xN2 pixels.

1. The homogeneity analysis of the suspected cover image C' is done using quad tree based image segmentation using the same homogeneity criteria, used at the time of embedding.

2. Apply SVD to each 4x4 pixels homogeneous block and extract the singular values.

3. Construct feature vectors g'_i from each 4x4 pixels homogeneous block B'_i and classify them into classes C_1 and C'_2 using the k-medoid clustering technique.

4. According to the clustering result, build up a master share M' using the same rule as at the time of embedding.

5. Retrieve the secret image S' by stacking the master share M' and the ownership share O kept by the CA.

6. Reduce the secret image P' by dividing it into 2x2 non-overlapping blocks p'_i (1<=i<=N1xN2) and following the process to obtain a reduced secret image Pq by the following rules:

$$Pq = \begin{cases} 1 & \text{if } \sum_m \sum_n p'_i \leq 2 \\ 0 & \text{if } \sum_m \sum_n p'_i > 2 \end{cases}$$

5. EXPERIMENTAL RESULTS AND ANALYSIS

The color cover images of size 512x512 and binary images of size 64x64 pixels were used as the test images for the proposed methodology as shown in Fig.3 and Fig.4. The 4x4 pixels sized homogeneous blocks were used in the experiments performed and homogeneity criteria set as 10 i.e. the difference between the maximum and the minimum pixel value within a homogeneous block must be less than 10.

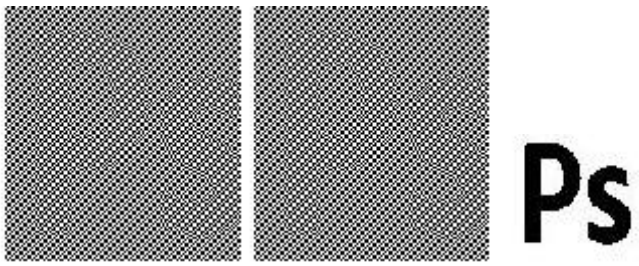
(a) (b) (c) (d)

Fig. 3: Cover Images Used

(a) (b) (c)

Fig. 4: Set of Binary Images used as Watermark

The performance of the proposed scheme on Fig. 3(a) is depicted in Fig.5 where Fig. 5(a) and 5(b) shows the master share and the ownership share and 5(c) is the reduced secret image.



(a) Master Share (b) Ownership Share (c) Stacked and Reduced Secret Image

Fig. 5: Sample Result of the Proposed Scheme

The quantitative evaluation of the proposed scheme is performed using peak signal-to-noise ratio (PSNR) and normalized cross correlation (NCC) metrics. The imperceptibility of the watermarked image from the original image is indicated by the Peak-Signal-to-Noise-Ratio (PSNR) metric defined as follows:

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{MSE} (dB)$$

$$\text{MSE} = \frac{1}{M1 \times M2} \sum_{i=1}^{M1} \sum_{j=1}^{M2} \| C_{i,j} - C'_{i,j} \|$$

where, $C_{i,j}$ and $C'_{i,j}$ represents pixel value of original cover image and the attacked image of size $M1 \times M2$.

High PSNR values signify higher similarity between the original cover image and the watermarked image. Also, the similarity of the extracted and the original watermark has been measured with the Normalized Cross Correlation (NCC) metric value defined as follows:

$$\text{NCC} = \frac{[W_{ij} \times W'_{ij}]}{[W_{ij} \times W_{ij}]}$$

where W_{ij} and W'_{ij} are the pixel values at the (i,j)th position in the original and extracted watermark.

The NCC values range from 0 to 1. Higher values indicate good robustness against various attacks and greater similarity between the original watermark and the extracted watermark and vice versa. The proposed methodology has been validated by applying comprehensive set of attacks on the watermarked image. Some are depicted in Fig. 6 to Fig. 10 and NCC metric values tabulated in table 1.

(a) Attacked Cover Image (PSNR=26.04 dB) **(b) Extracted Watermark (NCC=1)**

Fig. 6: Experimental Result under Salt & Pepper Noise Attack

(a)Attacked Cover Image (PSNR=26.07 dB) **(b) Extracted Watermark (NCC=1)**

Fig. 7: Experimental Result under Rotation Attack

(a)Attacked Cover Image (PSNR=39.97dB) **(b) Extracted Watermark (NCC=1)**

Fig. 8: Experimental Result under Gaussian Filter Attack

(a)Attacked Cover Image (PSNR=18.73dB) **(b) Extracted Watermark (NCC=1)**

Fig. 9: Experimental Result under Histogram Equalization Attack

(a)Attacked Cover Image (PSNR=33.99dB) **(b) Extracted Watermark (NCC=1)**

Fig. 10: Experimental Result under Median Filtering Attack

6. CONCLUSION AND FUTURE SCOPE

A visual cryptography based watermarking scheme incorporating the concepts of homogeneity analysis and singular value decomposition has been proposed in the present paper. The cover image is segmented using quad tree based decomposition to chalk out homogeneous sites based on some homogeneity criteria. Thereafter, singular values of these homogeneous blocks are extracted to build feature vectors which are further classified by the k-medoid clustering technique. Based on the clustering result, the master share is constructed and along with the secret image, the ownership share is build up that is registered with the certificate authority to resolve disputes regarding ownership verification of the image in future. The scheme allows verification of the watermark possible even by the naked human eyes without requiring the original cover image or involving any sort of computation. The proposed methodology is found to be robust against various attacks like histogram equalization, filtering, scaling, noise addition, JPEG lossy compression, rotation etc. In future, k out of n visual cryptography scheme may be incorporated to extend to various applications like fingerprinting etc.

Table 1. Attacks Applied on Watermarked Image

Attacks	**NCC Value**	**PSNR Value**
Salt & Pepper Noise (variance=0.01)	1	26.04
Rotation (60 degrees)	1	26.07
Gaussian Filter	1	39.97
Median Filter (3×3)	1	33.99
Speckle Noise (variance=0.01)	1	27.83
Cropping	1	60.37
Wiener Filter (3×3)	1	34.18
Laplacian Filter	1	7.21
Histogram Equalization	1	18.73
Gaussian Noise (variance=0.01)	1	21.08
Resize (512 to 128 to 512)	1	32.40

JPEG	1	16.01
Average Filter (3 × 3)	1	30.78

Table 2. Comparative NCC Values with other existing schemes

Attacks	**Proposed Scheme**	**M.S.Wang et.al. Scheme**
Salt & Pepper Noise (variance=0.01)	1	0.989
Rotation (60 degrees)	1	Not Tested
Gaussian Filter	1	0.989
Median Filter (3 × 3)	1	0.987
Speckle Noise (variance=0.01)	1	0.989
Cropping	1	Not Tested
Wiener Filter (3 × 3)	1	Not Tested
Laplacian Filter	1	0.989
Histogram Equalization	1	0.985
Gaussian Noise (variance=0.01)	1	0.989
JPEG	1	0.61
Average Filter (3 × 3)	1	0.78

7. REFERENCES

[1] Yu, Y.H., Chang C.C., and Hu, Y.C. 2005. Hiding secret data in images via predictive coding, Pattern Recognition 38 (5), 691–705.

[2] Chu, S.C., Roddick, J.F., Lu, Z.M., and Pan, J.S. 2004 A digital image water-marking method based on labeled bisecting clustering algorithm, IEICE Transactions on Fundamentals E87-A (1), 282–285.

[3] Chang, C.C., Chen T.S., and Chung, L.Z. 2002 A steganographic method based upon JPEG and quantization table modification, Information Sciences 141, 123–138.

[4] Wu, D.C., and Tsai, W.H. 2003 A steganographic method for images by pixel-value differencing, Pattern Recognition Letters 24, 1613–1626.

[5] Hsu C.T., and Wu, J.L. 1998 Multiresolution watermarking for digital images, IEEE on Circuits and Systems II: Analog and Digital Signal Processing, vol. 45(8), 1097–1101.

[6] Cox, I.J., Kilian J., Leighton, F.T., and Shamoon, T. 1997 Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing 6 (12) , 1673–1687.

[7] Wang, Y., Doherty, J.F., and Van Dyck, R.E. 2002 A wavelet-based watermarking algorithm for ownership verification of digital images, IEEE Transactions on Image Processing 11 (2), 77–88.

[8] Joo, S., Suh, Y., Shin J., Kikuchi H., and Cho, S.J. 2002 A new robust watermark embedding into wavelet DC components, ETRI Journal 24 (5), 401–404.

[9] Das, T.K., and Maitra, S. 2004 Cryptanalysis of correlation-based watermarking schemes using single watermarked copy, IEEE Signal Processing Letters 11 (4), 446–449.

[10] Celik, M.U., Sharma, G., Tekalp, A.M., and Saber, E. 2005 Lossless generalized-LSB data embedding, IEEE Transactions on Image Processing 14 (2), 253–266.

[11] Tian, J. 2003 Reversible data embedding using a difference expansion, IEEE Transactions on Circuits and Systems for Video Technology 13 (8), 890–896.

[12] Fridrich, J., Goljan, M., and Du, R. 2002 Lossless data embedding for all image formats, Proceedings of SPIE Photonics West 4675, Electronic Imaging, Security and Watermarking of Multimedia Contents (San Jose, California), 572–583.

[13] Wang, C.C., Tai, S.C., and Yu, C.S. 2000 Repeating image watermarking technique by the visual cryptography, IEICE Transactions on Fundamentals E83-A (8) , 1589–1598.

[14] Hsieh, S.L., and Huang, B.Y. 2004 A copyright protection scheme for gray-level images based on image secret sharing and wavelet transformation, Proceedings of International Computer Symposium, 661–666.

[15] Chang, C.C., and Chung, J.C. 2002 An image intellectual property protection scheme for gray-level images using visual secret sharing strategy, Pattern Recognition Letters 23, 931–941.

[16] Lee, W.B., and Chen, T.H. 2002 A public verifiable copy protection technique for still image, Journal of Systems and Software 62, 195–204.

[17] Naor, N., and Shamir, A. 1995 Visual cryptography, advances in cryptology: Eurocrypt'94, LNCS 950, 1–12.

[18] Lou, D.C., and Sung, C.H 2004 A steganographic scheme for secure communications based on the chaos and Euler theorem, IEEE Transactions on Multimedia 6 (3) , 501–509.

[19] Chang, C.C., Hsiao, J.Y., and Yeh, J.C. 2002 A color image copyright protection scheme based on visual cryptography and discrete Fourier transform, Imaging Science Journal, 50, 133-140.

[20] Hsu, C.S., and Hou, Y.C. 2005 Copyright protection scheme for digital image using visual cryptography and sampling methods, Optical Engineering, 44(7), 077003-1-77003-10.

[21] Hsu, C.S., and Hou, Y.C. 2005 A visual cryptography and statistics based method for ownership identification of digital images, World Academy of Science and Technology, 2, 172-175.

[22] Singh, K.M. 2009 Dual Watermarking Scheme for Copyright Protection", International Journal of Computer Science and Engineering System, ISSN 0973 4406, 3(2).

[23] Hwang, R.J. 2000 A digital image copyright protection scheme based on visual cryptography, Tamkang journal of Science and Engineering, 3(2), 97-106.

[24] Sleit, A., and Abusitta, A. 2008 A visual cryptography based watermark technology for individual and group images, Systems, Cybernetics and Informatics, 5(2), 24-32.

[25] Surekha, B., and Swamy, G.N. 2011 A spatial domain public image watermarking, International Journal of Security and Applications, 5(1), 1-11.

[26] Wang, M.S., and Chen, W.C. 2009 A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography, Computer Standards and Interfaces, 31, 757-762.