Image Watermarking Scheme based on Visual Cryptography in Discrete Wavelet Transform

Th. Rupachandra Singh
Assam University
Department of Information Technology
Silchar - 788011, India

Kh. Manglem Singh
NIT Manipur
Department of Computer Science & Engineering
Imphal- 795001, India

Sudipta Roy
Assam University
Department of Information Technology
Silchar - 788011, India

ABSTRACT
Multimedia security and copyright protection have become wide interest due the explosion of data exchange in the Internet and the extensive use of digital media. We propose an image watermarking scheme based on visual cryptography in discrete wavelet transform. A complete survey of the current image watermarking technologies was done and has been noticed that majority of the existing schemes are not capable of resisting all attacks. We propose the idea to use different parts of a single watermark into different regions of the image for generation of the owner's share from the low frequency subband of the original image based on the binary watermark, and comparing the global mean value of pixels in the same subband and the local mean of the same subband, and generation of the identification share based on comparing the global mean and the local mean of the low frequency subband of the controversial image. These two shares after stacking can reveal the copyright ownership. Experiments are conducted to verify the robustness through a series of experiments.

General Terms
Watermarking

Keywords
Digital watermarking, visual cryptography, global mean, local mean.

1. INTRODUCTION
The growth of the digital multimedia technology and the successful development of the Internet have not only allowed people to process, deliver and store digital content more easily, but also have gifted the facility of copying it rapidly and perfectly without loss of quality, with no limitation on the number of copies, tempering with and redistributing illegally without authorization. This kind of advantages raises the issue of how to protect copyright ownership of digital data. Cryptography is not a solution, because data after decryption can always be distributed in plain form without any restriction, even by the authorized customer. A better solution to this problem is to integrate the security information directly into the content of the digital data in inseparable form during its useful lifespan, and digital watermarking is such an effective way to protect copyright of the digital multimedia data even after its transmission. Watermarking is the process that enables data called a watermark, digital signature, tag, or label into a multimedia object such as audio, image or video in perceptually invisible or inaudible manner without degrading the quality of the object, such that watermark can be detected or extracted later to make an assertion about the object [1-4]. The embedded information can be a serial number or random number sequence, ownership identifiers, copyright messages, control signals, transaction dates, information about the creators of the work, bi-level or gray level images, text or other digital data formats [5]. Digital watermarking gives value-added protection on the top of data encryption and scrambling for content protection and effective digital rights management [6].

Typically watermark contains information about the origin, ownership, destination, copy control, transaction etc. Watermarking has many different applications such as copyright protection, transaction tracking, copy control, ownership identification, authentication, forensic analysis, playback screening, legacy system enhancement and database linking etc [7-9]. Copyright protection of digital data is defined as the process of proving the intellectual property rights to a court of law against the unauthorized reproduction, processing, transformation or broadcasting of digital data [7]. It can embed information about the owner of the object, which can be used for resolving rightful ownership. Each digital object has a unique watermark identifying the buyer of the object, which requires a very high level of robustness for fingerprinting for traitor tracking so that buyers can be traced. For copyright-related applications, the embedded watermark is expected to be robust to various kinds of malicious and non-malicious attacks, provided that the manipulated content is still valuable in terms of perceptual quality [10]. Although some significant progresses have been done recently, one of the major problems in the practical watermarking methods is the insufficient robustness of the existing watermarking algorithms against geometrical attacks such as sharpening, lightening, darkening, cropping, blurring, distorting, scaling, jittering, rotation and, removal attacks such as denoising, quantization, remodulation, filtering, JPEG compression, collusion, print-copy-scanning, cryptographic attacks and protocol attacks. Majority of geometrical and removal attacks come under malicious attacks. Malicious attacks attempt to remove or disable watermark [11].

A wide variety of image watermarking schemes has been proposed and each addresses many different application scenarios. Depending on the work domain in which the watermark is hidden, the watermarking schemes can be classified into two categories: spatial-domain watermarking schemes and frequency-domain watermarking schemes. In a spatial domain watermarking scheme, the watermark is embedded by directly modifying the spatial characteristics, such as pixel values and statistical traits. In contrast, frequency-domain watermarking schemes first transform an image into frequency domains, such as discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT), Fourier Mellin transform

(FMT), fractal transform etc. The watermark is then embedded by altering the frequency coefficients. Since low and middle frequency coefficients are less likely to be affected by common signal processing than high frequency coefficients, the watermark is preferably embedded into the low and middle frequency coefficients.

In our work, a copyright protection scheme based on visual cryptography (VC) in discrete wavelet transform domain is proposed. The proposed scheme generates the owner's share based on the binary watermark, local mean and global mean of the low frequency subband of the original image, and the identification share based on the local mean and global mean of the low frequency subband of the controversial image.

This paper is organized into five sections. Section 2 gives a survey of current image watermarking technologies. Section 3 describes the details of the proposed watermarking scheme. Section 4 gives the experimental results, followed by the conclusions in Section 5.

2. RELATED WORKS

Watermarking system can be characterized by a number of properties [12] such as embedding effectiveness, fidelity, data payload, blind or informed detection, false positive rate, robustness, security, cipher and watermark keys, modification and multiple watermarks, cost, temper resistance, unobtrusiveness, reading detection, unambiguous, sensitivity, scalability etc.

The simplest watermarking in the spatial domain is the least significant bit (LSB), which flips the chosen pixels in the image. An improvement to the basic LSB substitution is to embed watermark at random location, which is generated by a pseudo-random number generator based on a given seed or key. The algorithm may withstand cropping attack, but is vulnerable by replacing the LSBs with a constant. Watermark embedding can use the correlation properties of additive pseudo-random noise patterns as applied to an image [13]. Watermarking schemes in the spatial domain are less robust than those in frequency domain [14].

Transform domain techniques offerthe advantages of special properties of alternate domains to address the limitations of spatial domain and support the additional features. Threshold-based correlation watermarking scheme [13] is worse than the LSB-based watermarking scheme. Discrete cosine transform based watermarking scheme is more robust to lossy compression [16]. Discrete Fourier transform with template matching [17] watermarking can resist a number of attacks including removal, rotation and shearing. Discrete wavelet transform based watermarking is the most robust to noise addition [18].

Watermarking techniques based on visual cryptography and either discrete wavelet transform or discrete cosine transform have been proposed for copyright protection of the images [19-25]. These schemes generate two shares of the watermark based on watermark and local statistics of the pixel values. One share is registered to the certified authority. The other share is generated from the suspected watermarked image. These two shares are stacked together for the visual decryption to reveal watermark in case of dispute. Hsu and Hou proposed random average watermarking embedding (RAWE) scheme using visual cryptography for generation of shares based on the pixel value of the binary watermark, the global mean of the pixels in the image and the mean of some random pixels from the image [20,21]. An alternative to their method is pixel watermarking embedding (PWE) scheme that compares the global mean with the pixels in the image [22]. Hwang proposed most significant bit watermarking embedding (MWE) scheme that uses visual cryptography for generation of shares based on the pixel value of the binary watermark and most significant bit of pixel value of the image [23-25].

3. PROPOSED IMAGE WATERMARKING SCHEME

The proposed image watermarking is based on the binary watermark, global mean and local mean of the low frequency subband of the image. The image is decomposed into four subbands – low frequency subbandLL_1, mid frequency subbands LH_1 and HL_1, and high frequency subband HH_1. Only the low frequency subband LL_1 is used in our work. The global mean $\mu_g$of the image is found by taking the mean of all pixels in the same subband. The local mean μ_l is found by taking the mean of the pixels values surrounding a specified pixel including itself. The binary watermark in conjunction with the global mean and local mean are used to generate owner's share based on visual cryptography that checks whether the pixel value of the binary watermark is zero or not, and compares the pixel value of the global mean of the subband with the local mean corresponding to a pixel value. Details are given in the following section.

3.1 Generation of Owner's Share

The global mean $\mu_g$is compared with the local mean μ_l corresponding to pixel value at the location(m,n), which is generated by a random number generator seeded by a key K, where $m = 0,1,2,3,\dots,M$ and $n = 0,1,2,3,\dots,N$ and $M \times N$ is the size of the subband of the image. The owner's share O is generated based on the pixel value of the binary watermark value W, which may be either 0 or 1 at the location(i,j), and comparison between the global mean μ_g and the local mean μ_l. The generation of owner's share is shown in Figure 1.

Rule	Comparison between μ_l and μ_g	Watermark $W(i,j)$	Owner's Block $\boldsymbol{O}$
1	$\mu_l < \mu_g$	0	
2	$\mu_l < \mu_g$	1	
3	$\mu_l \geq \mu_g$	0	
4	$\mu_l \geq \mu_g$	1	

Figure 1 Generation of Owner's share

Algorithm for generation of owner's share:

Input: Low frequency subbandLL_1 of the image of size $M \times N$, binary watermark W of size$P \times Q$ and a key K for generation of random location (m,n).

Output: An owner's share O of size $2P \times 2Q$

1. Compute the global mean μ_g of the subband LL_1.

2. Generate a list of two-dimensional random number pair (m,n) over the interval $[(0,0),(M-1,N-1)]$ seeded by the key *K*.
3. For each local mean $\mu_l$surrounding the random location (m,n) and the global mean μ_g from Column 2 in Figure 1, and each watermark value $W(i,j)$at location $(i,j)$from Column 3 in Figure 1, generate the owner's block $\boldsymbol{o}$ from Column 4 in Figure 1.
4. Repeat 3 until all pixels of the watermark *W* are processed.

Each block of $\boldsymbol{o}$contains $\boldsymbol{o}(2i,2j), \boldsymbol{o}(2i+1,2j), \boldsymbol{o}(2i,2j+1)$and $\boldsymbol{o}(2i+1,2j+1)$binary subpixels respectively. The ownership share *O* is made up of blocks of $\boldsymbol{o}$. The private *K* and the owner's share must be kept secretly by the copyright owner for proving his ownership.

3.2 Generation of Identification Share

The copyright owner should use the same key *K* used in the generation of owner's share for obtaining the correct sequence of pixel values from the low frequency subband $LL_1^{'}$ of the probably controversial image. The comparison between the global mean $\mu_g^{'}$and the local mean $\mu_l^{'}$surrounding the random location $(m,n)$is used to generate the identification share *M* and it is explained in Figure 2 by the following algorithm.

Rule	Comparison between $\mu_l^{'}$ and $\mu_g^{'}$	Identification Block$\boldsymbol{m}$
1	$\mu_l^{'} < \mu_g^{'}$	
2	$\mu_l^{'} \geq \mu_g^{'}$	

Figure 2 Generation of identification share.

Algorithm for generation of identification share

Input: Low frequency subband$LL_1^{'}$ of the controversial image of size $M \times N$and the key *K*for generation of random location (m,n).

Output: Identification share *M* of size $2P \times 2Q$

1. Compute the global mean $\mu_g^{'}$ of the low frequency subband $LL_1^{'}$ of the probably controversial image.
2. Generate a list of two-dimensional random number pair (m,n)over the interval $[(0,0),(M-1,N-1)]$seeded by the key *K*.
3. For each local mean $\mu_l^{'}$at random location (m,n) and the global mean $\mu_g^{'}$ from Column 2 in Figure 2, and each sub-watermark value $W(i,j)$at location $(i,j)$from Column 2 in Figure 2, generate the master block m from Column 3 in Figure 2.
4. Repeat 3 until the end of all random locations generated by *K*is exhausted.

4. EXPERIMENTAL RESULTS

Lena, Kodak, Barbara, Goldhill, Airplane, Lake, Mandrill and Pepper color images of size $512 \times 512$are used for conducting the experiments, and are shown in Figure 3. The performance of the proposed video watermarking scheme is evaluated through several attacks such as median filtering, scaling, JPEG compression, injection of impulse noise, injection of Gaussian noise, blurring, sharpening, Gamma correction, cropping, rotation attacks etc. We use the normalized correlation (NC) to measure the similarity of the revealed watermark and the original watermark to evaluate our scheme in the experiments. Peak signal to noise ratio (PSNR) is used to see the quality of images after attacks. The proposed scheme is named as the Average watermarking in discrete wavelet transform embedding (AWDE) and is compared with the following VC based watermarking schemes.

(I) Random average watermarking embedding
(II) Most significant bit watermarking embedding (MWE)
(III) Average watermarking embedding (AWE)
(IV) Pixel watermarking embedding (PWE)

Figure 4 gives the graphical plots of comparing the proposed scheme with other schemes under consideration on Lena image under different attacks. Figure 4(a) shows the results of comparing the proposed scheme with other schemes under median filtering attack at different values of window sizes, ranging from 2×2 to 10×10. It is found that the proposed scheme AWDE achieves better performance than the RAWE, MWE and PWE in term of NC values by a wide margin, and better than the AWE marginally.

Figure 4(b) shows the results of comparing the proposed scheme with other schemes under scaling attack, which down-scales the image to [4, 100] and, then up-scales to the previous values. It is found that the proposed scheme achieves better performance than the than the RAWE, MWE, PWE and AWE.

Figure 4(c) shows the results of comparing the proposed scheme with other schemes under JPEG compression attack at different values of quality, ranging from 10 to 100. It is found that the proposed scheme achieves better performance than the RAWE, MWE, PWE and AWE. It is because compression does not affect the low frequency components, and generation of shares use low frequency subband of the image.

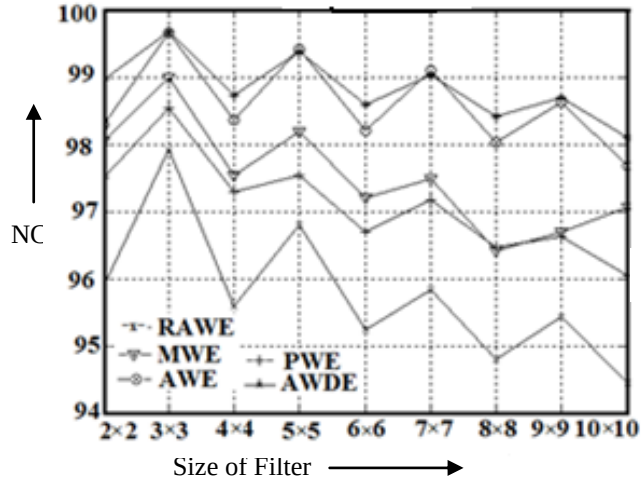
Figure 4(d) shows the results of comparing the proposed scheme with other schemes under impulse noise attack at different values of impulse noise ratios, ranging from 10% to 90%. It is found that the proposed scheme achieves better performance than the RAWE, MWE, PWE and AWE. It is because the high frequency components in subbands are affected by the impulse noise, while the low frequency components in subband is the least affected.

Figure 4(e) shows the results of comparing the proposed scheme with other schemes under Gaussian noise attack at different values of Gaussian noise at zero mean and different local variances from 0.01 to 0.1. It is found that the proposed scheme achieves better performance than the RAWE, MWE, PWE and AWE. It is because the high frequency components in subbands are affected by the Gaussian noise.

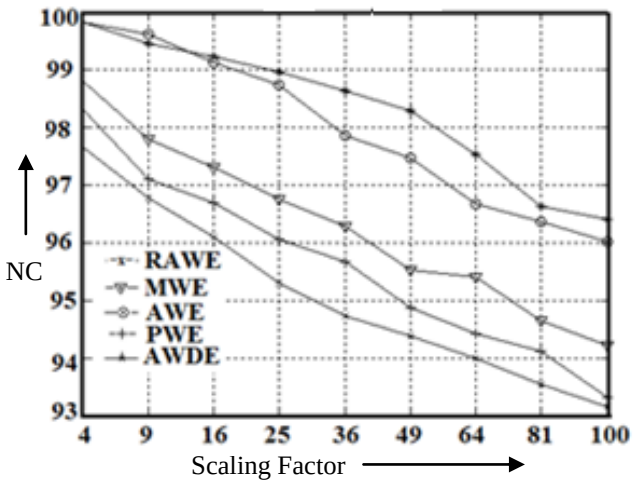
(a) (b) (c) (d)

(e) (f) (g) (h)

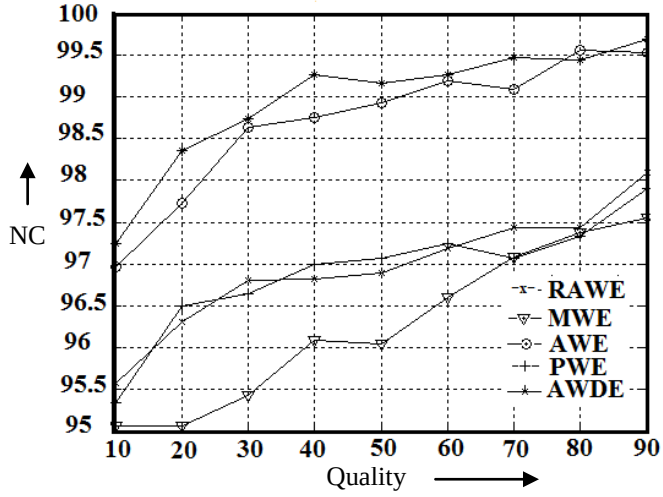
Figure 3 Representative Images: (a) Lena, (b) Kodak, (c) Barbara, (d) Goldhill, (e) Airplane, (f) Lake, (g) Mandrill and (h) Pepper.



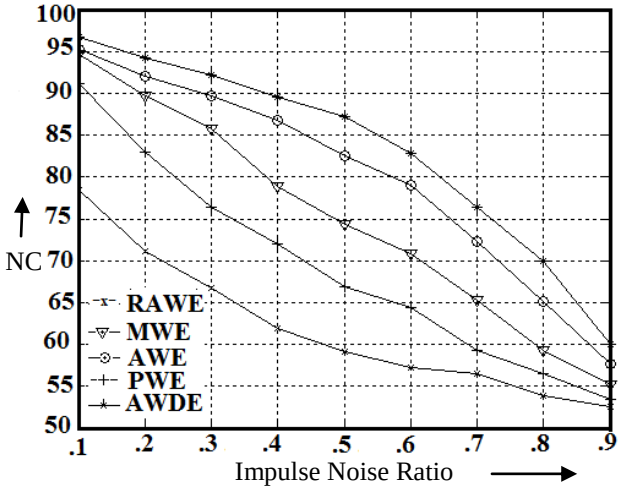
(a) Filtering Attack



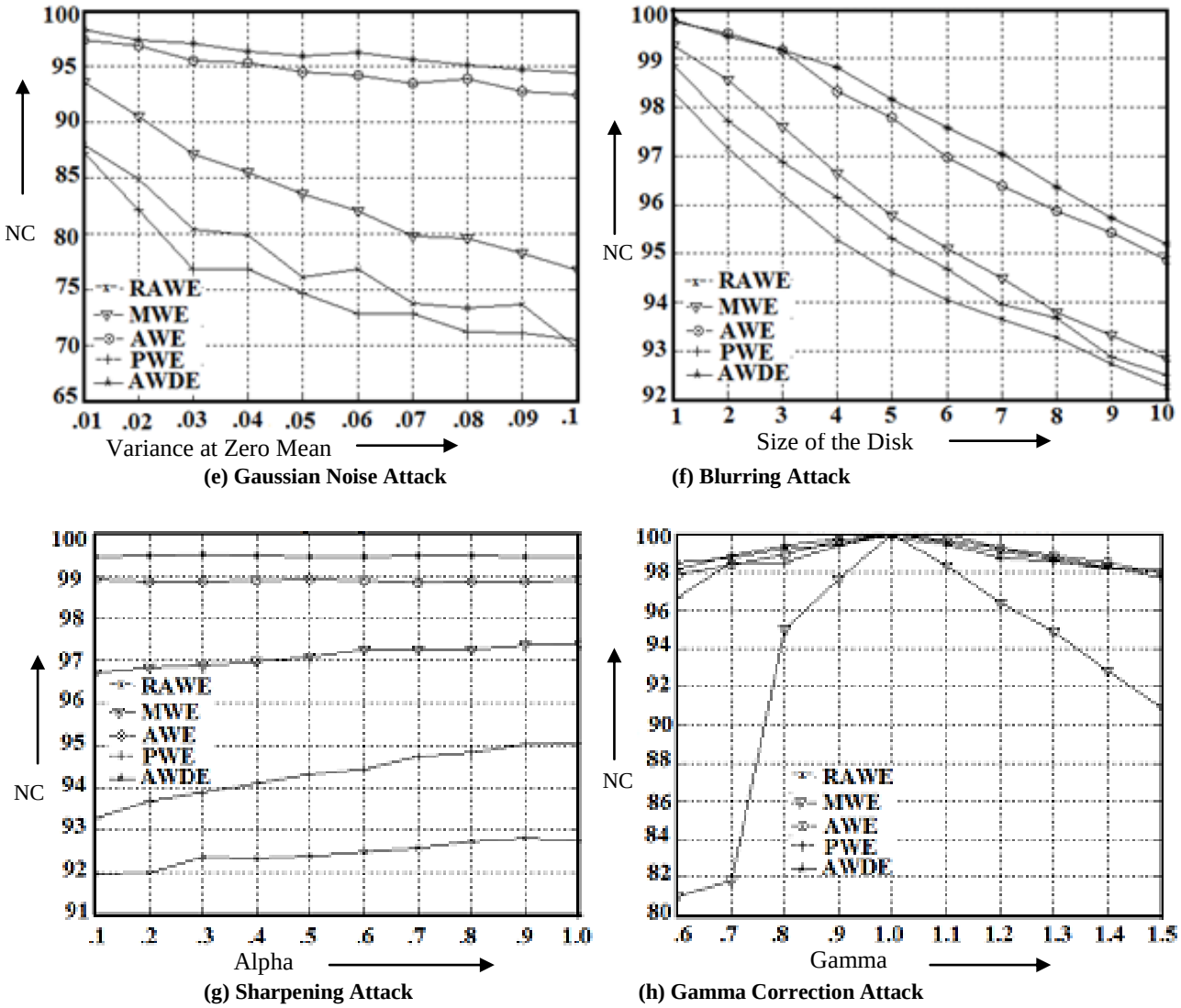
(b) Scaling Attack



(c) Compression Attack



(d) Impulse Noise Attack



(e) Gaussian Noise Attack **(f) Blurring Attack**

(g) Sharpening Attack **(h) Gamma Correction Attack**

Figure 4: Experiment Results under Different Attacks

Figure 4(f) shows the results of comparing the proposed scheme with other schemes under blurring attack at different values of disk, ranging from 1 to 10. It is found that the proposed scheme achieve better performance than the RAWE, MWE, PWE and AWE. It is because blurring does not affect the low frequency components.

Figure 4(g) shows the results of comparing the proposed scheme with other schemes under sharpening attack. It is found that the proposed scheme achieves better performance than the RAWE, MWE, PWE and AWE.

Figure 4(h) shows the results of comparing the proposed scheme with other schemes under Gamma correction attack. The value of the Gamma less than 1 gives brighter frames and value greater than 1 gives darker frames. It is found that the proposed scheme achieves better performance than the than the RAWE, MWE, PWE and AWE.

Experimental results indicate that the proposed image watermarking scheme is resistant to several attack such as filtering, scaling, JPEG compression, injection of impulse noise, injection of Gaussian noise, blurring, sharpening, Gamma correction, cropping, rotation attacks etc. Hence the proposed scheme can be used in various practical applications.

Table 1 gives the results of comparing the proposed scheme with other schemes under consideration on Lena image by applying Stirmark version 4.0 under 14 different attacks. It is observed that the proposed scheme gives better results than the RAWE, MAWE, AWE and PWE by a wide margin for all attacks mentioned in Stirmark except the cropping attack.

5. CONCLUSIONS

This paper proposes an image watermarking scheme based on visual cryptography in discrete wavelet transform. Experiments are conducted to demonstrate that the proposed scheme is robust against median filtering, scaling, JPEG compression, injection of impulse noise, injection of Gaussian noise, blurring, sharpening, Gamma correction, cropping, rotation attacks etc. The proposed scheme can identify the ownership without the original host image and it does not alter the host image to hide the invisible watermark. It is not possible to recover the invisible identification share without the secret key in the proposed scheme. The security requirement of the proposed algorithm is achieved with the visual cryptography.

Table 1 : Comparison of Different Watermarking Schemes on Lena image using Stirmark version 4.0

Attack Class	RAWE	MWE	AWE	PWE	AWDE
Affine	89.72	95.50	96.16	95.55	98.19
Convolution filter	78.02	79.44	82.12	78.85	86.23
Cropping	53.05	61.42	49.90	52.44	44.92
JPEG Compression	96.06	97.26	98.68	96.11	99.24
PSNR	96.26	96.97	99.21	97.14	99.73
Rescaling	96.48	96.38	99.21	96.77	99.30
Removal of line	96.19	96.65	98.41	96.72	98.43
Random Distortion	80.34	87.45	85.42	83.91	89.59
Rotation	81.12	89.25	88.94	87.69	92.18
Rotation + Cropping	93.21	94.84	96.14	95.04	97.11
Rotation + Scaling	93.31	94.97	95.87	95.14	97.07
Self Similarity	96.65	97.11	99.24	97.36	99.63
Add Noise	55.10	43.09	73.73	52.12	81.68
Median Filter	97.41	96.09	98.95	97.38	99.51

6. REFERENCES

[1] F. Petticolas, Information hiding techniques for steganography and digital watermarking, StefenKatzenbeisser, Artech house books, ISBN 158053-035-4, Dec. 1999.

[2] F. Hartung and M. Kutter, Multimedia watermarking techniques, Proceedings of the IEEE, vol. 87, no. 7, July 1999.

[3] S. Voloshynovkiy, S. Pereira, T. Pun, J. Eggers and J. Su, Attacks on digital watermarks: classification, estimation-based attacks and benchmarks, IEEE communications Magazine 39, 9 (August) 2001, pp. 118-126.

[4] A. Sequeira and D. Kundur, Communications and information theory in watermarking: A survey, In proc. of SPIE Multimedia systems and application IV, vol. 4518, pp. 216-227.

[5] J.O. Ruanaidh, H. Peterson, A. Herrigel, S. Pereira and T. Pun, Cryptographic copyright protection for digital images based on watermarking techniques, Elsevier Theoretical Computer Science, vol 226, no. 1, pp. 117-142, 1999.

[6] S.P. Mohanty and B.K. Bhargava, Invisible watermarking based on creation and robust insertion-extraction of image adaptive watermarks, ACM Journal, vol. 5, no. 2, Article 12, pp. 1-24, February 2008.

[7] I.J. Cox and M. Miller, Electronic watermarking: The first 50 years, EURASIP Journal of Applied Signal Processing, vol. 2002, Issue 2, pp. 126-132, 2002.

[8] R. Barnett, Digital watermarking: Application techniques and challenges, IEE Electronics and Communication Engineering Journal, pp. 173-183, 1999.

[9] W. Bender, W Butera, D. Gruhl, R Hwang, F.J. Paiz and S. Pogers, Applications for data hiding, IBM Systems Journal, vol. 39, Issue 3 and 4, pp. 547-568, 2000.

[10] J. Hussein and A. Mohammed, Robust video watermarking using multi-band wavelet transform, IJCSI, vol. 6, no. 1, 2009.

[11] Kh. Manglem Singh, Dual Watermarking Scheme for Copyright Protection, *International Journal of Computer Science and Engineering System*, ISSN 0973 4406, Vol. 3, No. 2, April-July 2009.

[12] M. Kutter and F. Hartung, "Introduction to watermarking techniques", Proc. Information Techniques for steganography and Digital Watermarking, S.C. Katzenbeisser et al. Eds, North Wood, MA: Artec House, pp. 97-119, Dec. 1999.

[13] G. Langelaar, I. Setyawan and R. Lagendijk, "Watermarking digital image and video data", IEEE Signal Processing Magazine, vol. 17, pp. 20-43, Sep. 2000.

[14] N. Memon, "Analysis of LSB based image steganography technique", IEEE Proc. ICIP, vol. 3, pp. 1019-1022, Oct. 2001.

[15] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I. Pitas, "Performance analysis of correlationbased watermarking schemes employing markov chaotic sequences," *IEEE Trans. on Signal Processing*, vol. 51, pp. 1979 – 1974, 2003.

[16] F. Duan, I. King, L. Xu and L. Chan, "Intra-block algorithm for digital watermarking", IEEE Proc. ICPR, vol. 2, pp. 1589-1591, Aug. 17-20, 1998.

[17] S. Pereira and T. Pun, "Robust template matching for affine resistant to image watermarks", IEEE Trans. On Image Processing, vol. 9, issue 6., pp. 1123-1129, Jun. 2000.

[18] I. Hong, I. Kim and S. Hem, "A blind watermarking technique using wavelet transform", IEEE Proc. ISIE, vol. 3, pp. 1946-1950, 2001.

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

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

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

[22] Kh. Manglem Singh, Dual Watermarking Scheme for Copyright Protection, *International Journal of Computer Science and Engineering System*, ISSN 0973 4406, Vol. 3, No. 2, April-July 2009.

[23] R-J. Hwang, A digital image copyright protection scheme based on visual cryptography, Tamkang journal of Science and Engineering, vol. 3, no. 2, pp. 97-106, 2000.

[24] A Sleit and A. Abusitta, A visual cryptography based watermark technology for individual and group images, Systems, Cybernetics and Informatics, vol. 5, no. 2, pp.24-32, 2008.

[25] B. Surekha and G.N. Swamy, A spatial domain public image watermarking, International Journal of Security and Applications, vol. 5, no. 1, pp. 1-11, 2011