Dual Image Watermarking Scheme based on Singular Value Decomposition and Visual Cryptography in Discrete Wavelet Transform

B. Pushpa Devi
Department of IT,
Assam University, Silchar

Kh. Manglem Singh
Department of CSE,
NIT Manipur, Imphal

Sudipta Roy
Department of IT,
Assam University, Silchar

ABSTRACT
There is wide interest in multimedia security and copyright protection due to the explosion of data exchange in the Internet and the extensive use of digital media. An image watermarking scheme based on singular value decomposition and visual cryptography in discrete wavelet transform is proposed. We start with a survey of the current image watermarking technologies, and have noticed that majority of the existing schemes are not capable of resisting all attacks. We propose the idea to use of singular value decomposition and visual cryptography in discrete wavelet transform such that the primary watermarking scheme based on singular value decomposition in the discrete wavelet transform is empowered by the secondary watermarking scheme based on visual cryptography in discrete wavelet transform. Experiments are conducted to verify the robustness through a series of experiments.

Keywords
Digital watermarking, singular value decomposition, visual cryptography, discrete wavelet transform.

1. INTRODUCTION
The growth of the digital multimedia technology and the successful development of the Internet are boons that 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 has alerted the issue of how to protect copyright ownership. Classical protection such as cryptography is not a solution, because data after decryption can always be available and 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 or anything that can reveal something about the object [5]. Digital watermarking provides 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 of the object, ownership of the person who possesses it, destination, copy control against illegal reproduction, transaction without owner's consent 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 embeds information about the owner of the object and uses 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 addressing 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 dual watermarking scheme having primary watermarking scheme that is based on singular value decomposition (SVD) in DWT, and secondary watermarking scheme, based on visual cryptography (VC) in DWT is proposed. The secondary watermarking scheme is the back up of the primary watermarking one. These two schemes are complementary to each other.

This paper is organized into five sections. Section 2 gives a survey of current image watermarking technologies. Section 3 gives a preliminary basic of the proposed method. Section 4 describes the details of the proposed primary watermarking scheme. Section 5 describes the secondary watermarking scheme. Section 6 gives the experimental results, followed by the conclusions in Section 7.

2. RELATED WORKS

Watermarking system can be characterized by a number of defining 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. Various types of watermarking methods have been proposed for different applications and these can be classified into two categories: either spatial domain or frequency domain using discrete Fourier transform, discrete wavelet transform, Fourier Mellin transform, fractal transform etc.

The simplest watermarking in the spatial domain is to flip the least significant bit (LSB) of the chosen pixels in the image. A more robust watermark is to superimpose a watermark over an area of the image. An improvement to the basic LSB substitution is to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given seed or key. The algorithm may survive cropping attack, but is vulnerable to replacing the LSBs with a constant. Another technique for watermark embedding is to exploit 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].

The main strength offered by the transform domain techniques is that they can take advantages of special properties of alternate domains to address the limitations of pixel based methods and/or to 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 compromised 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 [11]. 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 [22-24]. Rupachandra et al. proposed the average watermarking in discrete wavelet transform embedding (AWDE) [25].

In the recent years, singular value decomposition based image watermarking schemes have been proposed [26-32]. The SVD-based watermarking scheme is found to be weak against cropping attacks [33] and the DWT-SVD based scheme is able to remove this disadvantage. Liu et al. proposed a multi-scale full-band image watermarking scheme by merging DWT-based and SVD-based techniques utilizing the advantages of both [34].

(a) (b)

Fig 1: The original image (a) is divided into 4 sub bands (b) through 1-scale level wavelet transformation.

3. PRELIMINARY BASICS

3.1. Introduction to discrete wavelet transforms

Discrete wavelet transform is a mathematical tool for representation of multiresolution images to view the image's spatial and frequency characteristics [35]. Figure 1 shows a 1-scale Haar wavelet transform, where an image I of size $M_0 \times N_0$ pixels is decomposed into four subbandsLL_1, LH_1, HL_1 and HH_1 having size $M \times N$. The subband LL_1, which represents the course overall shape is the low frequency component, which contains the most of energy of the image. The subbands labeled LH_1, HL_1, and HH_1 contain the higher frequency detail information.
The wavelet transform can be applied to obtain next courser scale by decomposing the subband LL_1 and the process can be repeated as many times as required.

The first four Haar subbands are represented by the following equations [36].

$$LL_1(i,j) = \frac{1}{4}\sum_{x=0}^{1}\sum_{y=0}^{1} I(2i+x, 2j+y) \qquad (1)$$

$$LH_1(i,j) = \frac{1}{4}\sum_{x=0}^{1} I(2i+x, 2j) - \frac{1}{4}\sum_{x=0}^{1} I(2i+x, 2j+1) \quad (2)$$

$$HL_1(i,j) = \frac{1}{4}\sum_{y=0}^{1} I(2i, 2j+y) - \frac{1}{4}\sum_{y=0}^{1} I(2i+1, 2j+y) \quad (3)$$

$$HH_1(i,j) = \frac{1}{4}\{I(2i,2j) + I(2i+1,2j+1)\, I(2i+1,2j) - I(2i,2j+1)\} \quad (4)$$

where $I(i,j)$ is the pixel value at the coordinate (i,j) of I and $LL_1(i,j), LH_1(i,j), HL_1(i,j)$ and $HH_1(i,j)$ are the coefficients at the coordinates of the subbands LL_1, LH_1, HL_1 and HH_1 respectively. Similarly, the other higher subbands can be found.

3.2 Introduction to singular value decomposition

Suppose that the singular value decomposition is applied to a real matrix A. For convenience, assume that A is an $N \times N$ square matrix with rank $r \leq N$. The SVD of A can be represented by

$$A = UDV^T = \begin{bmatrix} u_{1,1} \dots \dots u_{1,N} \\ u_{2,1} \dots \dots u_{2,N} \\ \dots \dots \dots \dots \dots \\ u_{N,1} \dots . u_{N,N} \end{bmatrix} \begin{bmatrix} \sigma_1 & 0 \dots . \dots 0 \\ 0 & \sigma_2 \dots . \quad 0 \\ \dots . \dots \dots \dots \dots \\ 0 \dots \dots \dots \sigma_N \end{bmatrix} \begin{bmatrix} v_{1,1} \dots \dots v_{N,N} \\ v_{2,1} \dots \dots v_{2,N} \\ \dots \dots . \dots \dots \dots \\ v_{N,N} \dots v_{N,N} \end{bmatrix}^T \quad (5)$$

where U and V are $N \times N$ orthogonal matrices such that $UU^T = ID$ and $VV^T = ID$, (ID denotes an identity matrix of size $N \times N$ and D is an $N \times N$ singular, diagonal matrix with diagonal entries σ_i's (singular values) satisfying $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r > \sigma_{r+1} = \cdots = \sigma_N = 0$.

The columns of U are called left-singular vectors and the columns of V are called right-singular vectors.

3.3 Visual cryptography

Naor and Shamir introduced visual cryptography in their seminal paper [37] in which a secret image (printed text, notes, picture etc.) is encrypted in a perfectly secure way such that the secret can be decoded directly by the human visual system. It is a method of sharing a secret image among a group of participants, where certain group of participants is called as qualified group who may combine their shares of the image to obtain the original, and certain other group is defined as forbidden group who cannot obtain any information on the secret image, even if they combine knowledge about their parts. Figure 2 illustrates how an image is divided into shares for a 2-out-of-2 VC. The image is encoded into a pair of subpixels in each of the two shares. If a pixel p is white, one of the two columns tabulated under the white pixel in Figure 2 is selected. If p is black, one of the two columns tabulated under the black pixel is selected. In each case, the selection is performed by randomly flipping a fair coin, such that each column has 50% probability to be chosen. If p is white, the superposition of the two shares always outputs two black and two white subpixels, no matter which column of subpixel pair is chosen during encoding. If p is black, it yields four black subpixels.

Pixel	White		Black	
Probability	50%	50%	50%	50%
Share 1				
Share 2				
Stack of Share 1&2				

Fig 2: A simple 2-out-of-2 VC.

4. PROPOSED PRIMARY WATERMARKING SCHEME

The proposed primary watermarking scheme (PWS) is based on the singular value decomposition in the discrete wavelet transform. The low frequency subband LL_1 is divided into non-overlapping block B_k of size 4×4, singular value decomposition is applied to the block resulting in two orthogonal matrices U_k and V_k and a diagonal matrix D_k. A pixel multiplied by a pre-defined threshold T from the binary watermark is inserted in each diagonal matrix. The embedding and extracting algorithms are presented in detail below.

4.1 Embedding Algorithm

Input: Block B_k, where $k = 0,1,2,3, \dots, \frac{N \times N}{16} - 1$, binary watermark W, and its coordinate (i,j) generated by a random number generator seeded by a key K_1.

Output: A watermarked image I'.

1. Let $k = 0$.
2. Perform SVD on the block B_k, generating the corresponding U_k, D_k and V_k matrices. Let $D_k = \begin{bmatrix} \sigma_1 & 0 & 0 & 0 \\ 0 & \sigma_2 & 0 & 0 \\ 0 & 0 & \sigma_3 & 0 \\ 0 & 0 & 0 & \sigma_4 \end{bmatrix}_k$
3. If $W(i,j) == 1$
$$\sigma_4 = \begin{cases} \sigma_2 - \sigma_3, & \text{if} \sigma_3 > (\sigma_2 - \sigma_3) \\ 0, & \text{otherwise.} \end{cases}$$
and $\sigma_2 = \sigma_2 + T$ such that a new diagonal matrix WD_k is obtained, where T is a threshold.
4. Perform inverse SVD on U_k, WD_k and V_k to reconstruct the watermarked block $WB_k = U_k WD_k V_k^T$.
5. Let $k = k + 1$. Go to Step 2 until all binary pixels of the watermark have been embedded into the image.
6. Combine all watermarked blocks WB_k to form the watermarked image I'.

4.2 Extracting Algorithm

Input: Watermarked block WB_k, where $k = 0,1,2,3, \dots, \frac{N \times N}{16} - 1$, and the coordinate (i,j) of extracted watermark generated by a random number generator seeded by a key K_1.

Output: The extracted watermark EW.

1. Let $k = 0$.

2. Perform SVD on the block WB_k generating the corresponding UW_k, DW_k and VW_k matrices. Let
$$DW_k = \begin{bmatrix} \sigma w_1 & 0 & 0 & 0 \\ 0 & \sigma w_2 & 0 & 0 \\ 0 & 0 & \sigma w_3 & 0 \\ 0 & 0 & 0 & \sigma w_4 \end{bmatrix}_k$$
where $\sigma w_1, \sigma_{w2}$, σw_3 and σw_4 are singular values of the block WB_k.
3. The extracted watermark is given by
$$EW(i,j) \begin{cases} 1, \text{if } \sigma w_2 - \sigma w_3 > T/2. \\ 0, \quad \text{otherwise.} \end{cases}$$
4. Let $k = k + 1$ and go to Step 2 until all watermark bits are extracted.

5. PROPOSED SECONDARY WATERMARKING SCHEME

The proposed secondary image watermarking scheme (SWS) is based on the binary watermark W and global mean of the low frequency subband of the primary watermarked image I'. The image I' is decomposed into four subbands – low frequency subband LL_1', mid frequency subbands LH_1' and HL_1', and high frequency subband HH_1'. The global mean μ_g of the subband LL_1' is found by taking the mean of all pixels in the subband LL_1'. The binary watermark in conjunction with the global mean and local pixel value in LL_1' 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 subband with the global mean μ_g. Details are given in the following section.

5.1 Generation of Owner's Share

The global mean μ_g is compared with the pixel value in corresponding to pixel value in LL_1' at the location (m,n), which is generated by a random number generator seeded by a key K_2, where $m = 0,1,2,3,\dots,N$ and $n = 0,1,2,3,\dots,N$. 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 pixel value in LL_1' at random location (m,n). The generation of owner's share is shown in Figure 3.

Algorithm for generation of owner's share:

Input: Low frequency subband LL_1' of the image of size $N \times N$, binary watermark W of size $P \times Q$ and a key K_2 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 $[(0,0),(N-1,N-1)]$ seeded by the key K_2.
3. For each pixel value in LL_1' at the random location (m,n) and the global mean μ_g from Column 2 in Figure 3, and each watermark value $W(i,j)$ at location (i,j) from Column 3 in Figure 3, generate the owner's block ***o*** from Column 4 in Figure 3.
4. Repeat 3 until all pixels of the watermark W are processed.

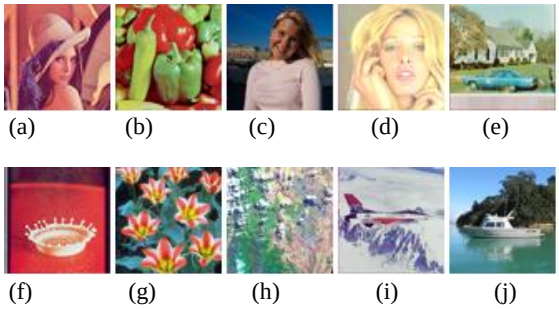
Each block of o contains $o(2i,2j), o(2i+1,2j), o(2i,2j+1)$ and $o(2i+1,2j+1)$ binary subpixels respectively. The ownership share O is made up of blocks of o. The private K_2 and the owner's share must be kept secretly by the copyright owner for proving his ownership.

Rule	Comparison between $LL_1'(m,n)$ and μ_g	Watermark $W(i,j)$	Owner's Block ***o***
1	$LL_1'(m,n) < \mu_g$	0	
2	$LL_1'(m,n) < \mu_g$	1	
3	$LL_1'(m,n) \geq \mu_g$	0	
4	$LL_1'(m,n) \geq \mu_g$	1	

Fig 3: Generation of owner's share.

Rule	Comparison between $LL_1''(m,n)$ and μ_g'	Identification Block ***m***
1	$LL_1''(m,n) < \mu_g'$	
2	$LL_1''(m,n) \geq \mu_g'$	

Fig 4: Generation of identification share.



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

(f) (g) (h) (i) (j)

Fig5: (a) Lena, (b) Pepper, (c) Kodak, (d) Tiffany, (e) House, (f) Splash, (g) Tulips, (h) Terrain,(i) Airplane and (j) Boat.

5.2 Generation of identification Share

The copyright owner should use the same key K_2 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 μ_g' and the pixel value in LL_1'' at the random location (m,n) is used to generate the identification share M and it is explained in Figure 4 by the following algorithm.

Algorithm for generation of identification share

Input: Low frequency subband LL_1'' of the controversial image and the key K_2 for generation of random location (m,n).

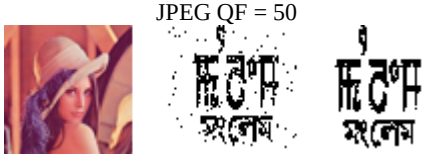
Output: Identification share M of size $2P \times 2Q$

1. Compute the global mean μ_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 $[(0,0),(N-1,N-1)]$ seeded by the key K_2.

3. For each pixel value in LL_1'' at the random location (m,n) and the global mean μ_g' from Column 2 in Figure 4, and each sub-watermark value $W(i,j)$at location $(i,j)$from Column 2 in Figure 4, generate the master block m from Column 3 in Figure 4.
4. Repeat 3 until the end of all random locations generated by $K_2$is exhausted.

6. EXPERIMENTAL RESULTS

Lena, Pepper, Kodak, Tiffany, House, Splash, Tulips, Terrain, Airplane and Boat color images of size 512×512were used for conducting the experiments, and are shown in Figure 5. The performance of the proposed image watermarking scheme is evaluated through several attacks such as JPEG compression, Rotation, Median filtering, cropping, scaling, impulse noise injection, Gaussian noise injection, blurring, sharpening and Gamma correction attacks. Stirmark version 4.0 was used to test the robustness of the proposed watermarking scheme [38]. 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.



JPEG QF = 50

PSNR=32.04 dB NC=95.94NC=99.26

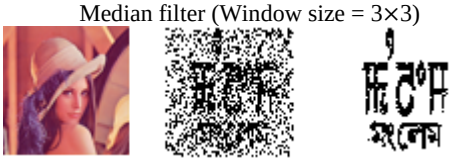
(a)

Rotation 5°

PSNR=14.57 dB NC = 40.35 NC=90.77

(b)

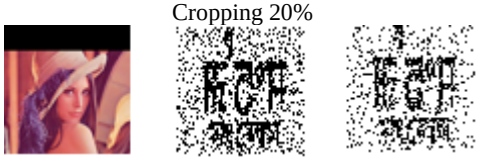
Median filter (Window size = 3×3)



PSNR=35.74dB NC = 58.03 NC=98.38

(c)

Cropping 20%



PSNR=11.94 dB NC = 82.42 NC=85.66

(d)

Scaling (Factor = 3 × 3)

PSNR=26.28 dB NC = 71.46 NC=98.04

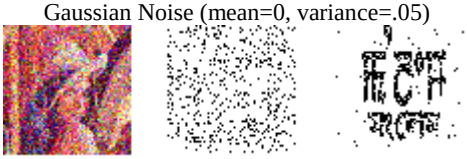
(e)

Impulse noise (Ratio = 30%)

PSNR=15.58 dB NC = 76.31 NC=90.77

(f)

Gaussian Noise (mean=0, variance=.05)



PSNR=18.24 dB NC = 74.31 NC=95.72

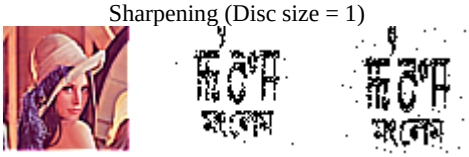
(g)

Blurring (Disc size = 1)

PSNR=36.40 dB NC = 93.92 NC=98.92

(h)

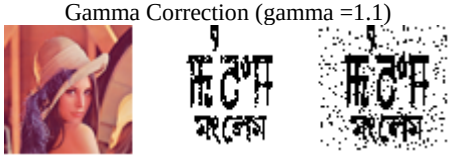
Sharpening (Disc size = 1)



PSNR=23.79dB NC = 96.04 NC=97.21

(i)

Gamma Correction (gamma =1.1)



PSNR=31.45 dB NC = 98.80 NC=92.18

(j)

Fig6: Extracted watermarks from attacked watermarked image under various attacks.

Extracted watermarks from the watermark image after applying various attacks are shown in Figure 6. The watermarked image was compressed using lossy JPEG compression. Figure 6(a) shows the extracted watermarks under JPEG attack for a quality factor (QF) of 50, and NCs values of PWS and SWS are 95.94% and 99.26% respectively for PSNR value of 32.04 dB. The result indicates that the proposed method is able to survive against JPEG compression attack.

The watermarked image was rotated clockwise by an angle of 5° followed by bilinear interpolation for adjusting image to its previous size. Figure 6(b) shows the extracted watermarks and NCs values of PWS and SWS are 40.35% and 90.77% respectively for PSNR value of 14.57 dB. The result indicates that the proposed PWS is not able to survive rotation attack, while the SWS can withstand such attack.

The watermarked image was filtered using median filter. Figure 6(c) shows the extracted watermarks under this attack for a window size of 3×3, and NCs values of PWS and SWS are 71.21% and 97.85% respectively for PSNR value of 32.74 dB. The result indicates that extracted watermarks are visible and distinguishable, but the performance of the PWS is poor and that of the SWS is comparatively good.

Table 1: Comparison of spatial domain and DWT domain on Lena image

Attack	Spatial domain		DWT domain	
	PWS	**SWS**	**PWS**	**SWS**
JPEG QF=50	73.12	92.89	95.94	99.26
Rotation Angle 5^o	28.78	72.77	40.35	90.77
Median filter 3×3	20.01	92.89	58.03	98.38
Cropping 20%	34.88	79.27	82.42	85.66
Scaling size3×3	43.11	89.11	71.46	98.04
Impulse noise 30%	76.34	80.66	76.31	90.77
Gaussian noise var=.05	72.80	68.82	74.31	95.72
Blurring Disc=1.0	25.14	94.16	93.92	98.92
Sharpen Disc=1.0	96.19	89.13	96.04	97.21
Gamma gamma=1.1	99.90	99.82	98.80	92.18

The watermarked image was cropped at the upper portion by 20% as shown in Figure 6(d). NCs values of PWS and SWS are 82.42% and 85.66% respectively for PSNR value of 11.94 dB. The result indicates that the proposed method is able to survive against cropping attack.

The watermarked image was downscaled by a factor of 3×3 and then upscale by the same factor. Figure 6(e) shows the extracted watermarks under scaling attack, and NCs values of PWS and SWS are 71.46% and 98.04% respectively for PSNR value of 26.28 dB. The result indicates that the proposed PWS is not able to survive scaling attack, while the SWS can withstand such attack.

Table 2: Comparison of spatial domain and DWT domain on Pepper image

Attack	Spatial domain		DWT domain	
	PWS	**SWS**	**PWS**	**SWS**
JPEG QF=50	84.66	97.46	94.23	99.34
Rotation Angle 5^o	30.71	76.04	42.40	93.35
Median filter 3×3	26.09	97.36	70.55	99.41
Cropping 20%	34.27	83.08	81.25	90.28
Scaling size3×3	19.70	95.80	51.70	98.46
Impulse noise 30%	73.29	72.70	76.53	81.64
Gaussian noise var=.05	69.06	70.99	70.33	91.21
Blurring Disc=1.0	43.89	97.97	94.09	99.43
Sharpen Disc=1.0	97.26	92.94	74.16	96.63
Gamma gamma=1.1	97.80	100	95.89	94.14

The watermarked image was injected with impulse for a noise ratio of 30%. Figure 6(f) shows the extracted watermarks against impulse noise attack, and NCs values of PWS and SWS are 76.31% and 90.77% respectively for PSNR value of 15.58 dB. The result indicates that the proposed PWS is not able to survive impulse noise attack at higher value of impulse noise ratios, while the SWS can withstand such attack.

Table 3: Comparison of spatial domain and DWT domain on Kodak image

Attack	Spatial domain		DWT domain	
	PWS	**SWS**	**PWS**	**SWS**
JPEG QF=50	81.51	97.70	96.28	99.78
Rotation Angle 5^o	32.91	84.47	42.40	96.94
Median filter 3×3	25.07	96.94	66.21	99.70
Cropping 20%	34.17	82.05	83.17	92.94
Scaling size3×3	19.50	96.4	46.75	99.56
Impulse noise 30%	74.09	83.64	76.24	93.65
Gaussian noise var=.05	71.46	78.66	72.02	96.87
Blurring Disc=1.0	38.86	97.38	95.84	99.82
Sharpen Disc=1.0	97.99	93.45	95.87	98.02
Gamma gamma=1.1	99.07	98.92	98.46	96.85

The watermarked image was injected with Gaussian noise for zero mean and 0.05 variance. Figure 6(g) shows the extracted watermarks under impulse noise attack, and NCs values of PWS and SWS are 74.31% and 95.72% respectively for PSNR value of 18.24 dB. The result indicates that the proposed PWS is not able to survive Gaussian noise attack at lower PSNR values, while the SWS can withstand such attack.

The watermarked image was blurred as shown in. Figure 6(h) for a disc size of 1 and NCs values of PWS and SWS are 93.92% and 98.92% respectively for PSNR value of 36.40 dB. The result indicates that extracted watermarks are visible and distinguishable, and the performances of both the PWS and SWS are comparatively good.

The watermarked image was sharpened as shown in Figure 6(i) for disc size of 1. NCs values of PWS and SWS are 96.04% and 97.21% respectively for PSNR value of 23.79 dB. The result indicates that extracted watermarks are visible and distinguishable, and the performances of both the PWS and SWS are comparatively good.

The watermarked image was Gamma corrected as shown in Figure 6(j). NCs values of PWS and SWS are 98.80% and 92.18% respectively for PSNR value of 31.45 dB. The result indicates that extracted watermarks are visible and distinguishable, and the performances of both the PWS and SWS are comparatively good.

Table 4: Performance against Stirmark attacks

Attack	PSNR (db)	PWS	SWS
Affine transformation AFFINE_1	21.72	50.51	88.20
Convolution CONV_1	9.44	69.09	59.52
Cropping CROP_75	13.05	38.69	81.90
JPEG Compression JPEG_50	24.92	34.22	86.40
PSNR attack PSNR_50	25.44	76.97	87.64
Rescaling RESC_50	24.96	56.22	87.23
Removal of lines RML_50	24.87	66.18	87.20
Random distortion RNDDIST_0.95	16.16	35.03	88.96
Rotation ROT_5	11.41	37.98	89.35
Rotation+Cropping ROTCROP_2	24.17	52.49	87.25
Rotation+Scaling ROTSCALE_2	19.96	37.69	85.66
Self-Similarity SS_1	25.34	68.43	87.79
Add Noise NOISE_20	8.27	74.70	68.70
Median Filter MEDIAN_3	24.01	47.26	85.08

Tables 1, 2 and 3 show the comparison of the proposed watermarking scheme with its counterpart in spatial domain using Lena, Pepper and Kodak image against 10 different attacks. It was found that the PWS in spatial domain is the weakest to survive the attack, followed by the PWS in DWT domain. The results show that the performance of the watermarking is better in DWT domain than spatial domain in the respective schemes.

Table 4 gives the performance of the proposed scheme on Lena image by applying Stirmark version 4.0 against 14 different attacks. It was observed that the proposed secondary watermarking scheme gave good results against various attacks given in Stirmark benchmark software.

7. CONCLUSIONS

This paper proposes an image watermarking scheme based on the singular value decomposition and visual cryptography in discrete wavelet transform. Experiments are conducted to demonstrate that the proposed scheme is robust against JPEG compression, Rotation, Median filtering, cropping, scaling, impulse noise injection, Gaussian noise injection, blurring, sharpening and Gamma correction attacks. The proposed scheme can identify the ownership without the original host image. The secondary watermarking scheme shows very promising performance and it acts as a backup for the primary watermarking scheme. It was also shown that the performance of the watermarking scheme is better in discrete wavelet transform than in spatial domain. It is not possible to recover the watermarks without the keys.

8. 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 water- marking 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, vol.39, no. 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 correlation based 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 and 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 and 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] 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.

[23] 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.

[24] 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, and 2011.

[25] Th. Rupachandra Singh, Kh. Manglem Singh and Sudipta Roy, Image Watermarking Scheme Based on Visual Cryptography in Discrete Wavelet Transform, *International Journal of Computer Applications*, ISSN 0975 - 8887, Vol. 39, No. 1, pp. 18-24, February 2012.

[26] R. Liu and T. Tan, An SVD-based Watermarking scheme for protecting rightful ownership, *IEEE Transaction on Multimedia*, vol. 4, no. 1, pp. 121-128, 2002.

[27] C.C. Chang, P. Tsai and C.C. Lin, SVD-based digital image watermarking scheme, *Pattern Recogn*. Lett.Vol. 26, pp. 1577-1586, 2005.

[28] K-L. Chung, W-N.Yang, Y-H.Huang, S-T.Wu and Y-C. Hsu, On SVD-based Watermarking Algorithm, *Elsevier, Applied Mathematics and Computation*, vol. 188, pp. 54-57, 2007.

[29] G.H. Golub and C. Reinsch, Singular value decomposition and least squares solutions, *NumerischeMathematik*, vol. 14, pp. 403-420, 1970.

[30] K.L. Chung, C.H. Shen and L.C. Chang, A novel SDV- and VQ-based image hiding scheme, *Pattern Recognition Letters*, vol. 22, no. 9, pp. 1051-1058, 2001.

[31] K. Konstantinides, B. Nataranjan and G.S. Yovanof, Noise estimation and filtering using blocked-based singular value decomposition, *IEEE Transaction on Image Processing*, vol. 10, no. 3, pp. 479-483, 1997.

[32] J.F. Yang and C.L. Lu, Combined techniques of singular value decomposition and vector quantization for image coding, *IEEE Transaction on Image Processing*, vol. 4, no. 8, pp. 1141-1146, 1995.

[33] M. Prasad R. and S. Koliwad, A Comprehensive survey of contemporary researches in watermarking for copyright protection of digital images, *IJCSNS*, vol. 9, no. 4, pp. 91-107, April 2009.

[34] J-C. Liu, C-H.Lin, L-C.Kuo and J-C. Chang, Robust multi-scale full-band image watermarking for copyright protection, Lecture Notes in Computer Science, *Springer Berlin, Heidelberg*, vol. 4570, pp. 176-184, 2007.

[35] R.C. Gonzalez, R.E. Woods and S.L. Eddins, *Digital Image Processing with MATLAB*, Pearson, Fifth edition 2009.

[36] T-H. Chen, C-C.Chang, C-S.Wu and D-C. Lou, On the security of a copyright protection scheme based on visual cryptography, *Elsevier Computer Standard & Interfaces*, vol. 31, pp.1-5, 2009.

[37] M. Naor and A. Shamir, Visual Cryptography, in "Advances in Cryptology – Eurocrypt '94", A. De Santis ed., vol. 950 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, pp. 1–12, 1995.

[38] http://www.peticolas.net/fabien/software/StirMarkBenchmark_4_0_129.zip (lasted accessed July 2008)