International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:4, No:1, 2010

A Normalization-based Robust Image Watermarking Scheme Using SVD and DCT

Say Wei Foo, Qi Dong

Abstract**—**Digital watermarking is one of the techniques for copyright protection. In this paper, a normalization-based robust image watermarking scheme which encompasses singular value decomposition (SVD) and discrete cosine transform (DCT) techniques is proposed. For the proposed scheme, the host image is first normalized to a standard form and divided into non-overlapping image blocks. SVD is applied to each block. By concatenating the first singular values (SV) of adjacent blocks of the normalized image, a SV block is obtained. DCT is then carried out on the SV blocks to produce SVD-DCT blocks. A watermark bit is embedded in the high-frequency band of a SVD-DCT block by imposing a particular relationship between two pseudo-randomly selected DCT coefficients. An adaptive frequency mask is used to adjust local watermark embedding strength. Watermark extraction involves mainly the inverse process. The watermark extracting method is blind and efficient. Experimental results show that the quality degradation of watermarked image caused by the embedded watermark is visually transparent. Results also show that the proposed scheme is robust against various image processing operations and geometric attacks.

Keywords**—** Image watermarking, Image normalization, Singular value decomposition, Discrete cosine transform, Robustness.

I. Introduction

IMAGE watermarking is a process of embedding hidden information called watermark into original host image signals [1]-[5]. The embedded watermark is usually coded in binary format and it should not significantly degrade the visual quality of original host image signals. For robust image watermarking, the embedded watermarks must be robust enough to survive image processing operations and geometric attacks. The watermarks must be readily extracted from watermarked signal even if the image signals are subject to a variety of possible attacks.

Robust image watermarking schemes are usually performed in spatial domain, transform domain and compression domain. The schemes performed in spatial domain directly embed watermarks into pixel locations of host image [6]-[9]. This kind of watermarking method is the earliest and simplest watermarking techniques but it has low robustness against common image processing operations. The schemes performed in transform domain are based on the modification of frequency coefficients [10-18]. Discrete cosine transform (DCT), discrete Fourier transform (DFT) and discrete wavelet transform (DWT) are commonly used. High robustness can be achieved using these schemes. Schemes performed in compression domain make use of compressed signals such as vector quantization to hide the watermarks [16], [18].

In the design of image watermarking schemes, two important considerations must be made. First, there must be an appropriate trade-off between robustness and imperceptivity. In other words, the highest-possible robustness must be achieved without visible quality degradation. Second, the watermarking schemes must be able to detect the watermark embedding locations and extract the watermark accurately.

In recent years, watermarking schemes based on singular value decomposition (SVD) techniques have been shown to be powerful methods for robust image watermarking [15], [19]. This can be attributed to the facts that:

1) Singular value (SV) of a digital image is stable. The SVs remain intact when disturbances are added to an image.
2) SVD preserves both one-way and non-symmetric properties, which are not obtainable using DCT or DFT transformations.
3) SVs are able to represent intrinsic algebraic properties of a digital image.
4) SVD can be performed on both square and rectangular matrices.

However, schemes based on SVD alone cannot guarantee high robustness against geometric attacks. In this paper, we propose a novel normalization-based robust image watermarking scheme that utilizes the desirable features of SVD. The proposed scheme is performed in SVD-DCT composite domain. For the proposed scheme, the host image is first normalized to a standard form for subsequent processing. In the traditional SVD-based schemes, the watermark bits are embedded directly in the SVs. For the proposed scheme, the first SVs of adjacent blocks of the normalized image are concatenated to form a singular value (SV) block. DCT is then carried out on these SV blocks. A watermark bit is embedded in the high-frequency band of a SVD-DCT block by imposing a particular relationship between two pseudo-randomly selected DCT coefficients. An adaptive frequency mask is calculated to control local watermark embedding strength.

Say Wei Foo is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore (e-mail: eswFoo@ntu.edu.sg).
Qi Dong is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore (e-mail: DONG0041@e.ntu.edu.sg).

The rest of this paper is organized as follows. Image normalization procedures are covered in Section II. In Section III, the proposed watermarking scheme is described in detail. The experimental results are shown in Section IV and the concluding remarks are presented in Section V.

II. Image Normalization

The general concept of image normalization using moments is well-known in pattern recognition [15], [17]. In this section, we describe a moment-based normalization process that achieves invariance properties against geometric attacks. The geometric attacks include rotation, scaling and translation of an image. These distortions can be represented by affine transformations. An affine transformation with scaling parameters (a, b), rotation angle φ and translational parameters (T_x, T_y) is given by

$$\begin{bmatrix} x_a \\ y_a \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} T_x \\ T_y \end{bmatrix} \quad (1)$$

where (x, y) is a pixel coordinates of an input image and (x_a, y_a) are the corresponding pixel coordinates of the transformed image. The affine transform parameters can be calculated from image moments. The image moment m_{pq} of an input image $I(x, y)$ with the size of $N_1 \times N_2$ is defined in two dimensional Cartesian coordinates as

$$m_{pq} = \sum_{y=0}^{N_2-1} \sum_{x=0}^{N_1-1} x^p y^q \cdot I(x, y) \quad (2)$$

The central moment μ_{pq} is given by

$$\mu_{pq} = \sum_{y=0}^{N_2-1} \sum_{x=0}^{N_1-1} (x - \bar{x})^p (y - \bar{y})^q \cdot I(x, y) \quad (3)$$

The covariance matrix based on the central moments is given by

$$\begin{pmatrix} \mu_{20} & \mu_{11} \\ \mu_{11} & \mu_{02} \end{pmatrix} \quad (4)$$

Based on the covariance matrix, the rotation angle φ is calculated as

$$\varphi = \frac{1}{2} \tan^{-1}[2\mu_{11}/(\mu_{20} - \mu_{02})] \quad (5)$$

The two eigenvalues of covariance matrix are given by

$$\lambda_i = \frac{1}{2}\left[(\mu_{20} + \mu_{02}) \pm \sqrt{4\mu_{11}^2 + (\mu_{20} - \mu_{02})^2}\right] \quad i = 1,2 \quad (6)$$

Based on the eigenvalues, the scaling parameters are calculated as

$$a = (\lambda_1\lambda_2)^{0.25}/\sqrt{\lambda_1}\ , b = (\lambda_1\lambda_2)^{0.25}/\sqrt{\lambda_2} \quad (7)$$

Using the equations derived, any transformed image can be converted to a normalized form by identifying the transform parameters, $(a, b), \varphi$ and $(\bar{x}, \bar{y})$. To demonstrate this normalization procedure, an original host image given in Fig. 1(a), is put through the procedures. Two images after general affine transformations are shown in Fig. 1(b) and Fig. 1(c). These three different images yield the same normalized image, as shown in Fig. 1(d), based on which subsequent watermark embedding and extracting are performed. It is known that the normalized image has invariance properties against different affine transformations. The embedded watermark in the normalized image can be accurately synchronized under a variety of possible affine transformations.

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

Fig. 1 Demonstration of image normalization

III. Proposed Watermarking Scheme

A. Watermark Embedding Process

For the proposed watermarking scheme, the host image is first normalized to a standard form. The first SVs of adjacent blocks of the normalized image are concatenated to form a SV block. This block is transformed into the frequency domain using DCT. A watermark bit is embedded in the high-frequency band of a SVD-DCT block in pseudo-randomly selected positions. The watermark embedding process is repeated over the whole normalized image. In other words, after the last watermark bit has been embedded, the embedding process begins with the first watermark bit again, until all the positions that can be embedded are occupied.

The SVD-DCT blocks can be obtained following the steps below.

1) Divide the normalized image into non-overlapping 4×4 sub-image blocks.
2) Perform SVD on each block to produce 4 SVs.
3) Concatenate the first SVs from adjacent 16 blocks to form a 4×4 SV block.
4) For each SV block, DCT is performed to obtain its corresponding SVD-DCT block.

The result is a 4×4 SVD-DCT coefficient block from 16 adjacent 4×4 sub-image blocks of the normalized image. A SVD-DCT block with 16 DCT coefficients in the zigzag order is shown in Fig. 2, where the shaded positions are potential positions for watermark embedding.

1	2	6	7
3	5	8	13
4	9	12	14
10	11	15	16

Fig. 2 Illustration of a SVD-DCT block

The watermark bits are embedded as follows.

1) Produce an adaptive frequency mask for each SVD-DCT block.
2) Use the mask to adjust local watermark embedding strength.
3) Select one pair of coefficients to be modified in the potential positions of the SVD-DCT block.
4) Modify the relationship between the two coefficients in the selected pair according to the specific watermark bit.

Before watermark embedding,, two secret keys are first generated. One is an encryption key [15] which is used to encrypt the original ownership information. After encryption, the original ownership information becomes a pseudo-random bit sequence. The other key is a position key [18] which is used to pseudo-randomly select one coefficient pair from the potential positions in the SVD-DCT block. The aim is to reduce the probability for an attacker to detect and alter the embedded watermark bits. These two secret keys must be available to extract watermark bits and recover original ownership information. In this way, the security of proposed scheme is enhanced.

To achieve an appropriate tradeoff between the robustness against a variety of possible attacks and the visual transparency of embedded watermark, the high-frequency band of SVD-DCT block is chosen for watermark embedding. This is because the DCT block in the proposed scheme is derived from the visual important components (first SV) of the normalized image. Embedding watermarks in the high-frequency bands of SVD-DCT blocks can preserve high visual quality of watermarked images. This differs from the traditional methods that embed watermarks in the mid-frequency band of DCT blocks [18].

The watermarking embedding process is implemented by changing the difference of the magnitudes of two selected coefficients. Only one pair of coefficients in the 8 potential positions in Fig. 3 is used for watermark embedding. In so doing, an attacker would not know which one pair of coefficients is embedded with watermark bit, and attacking on all the 8 coefficients will cause significant quality degradation to the original normalized image.

In the watermark embedding process, the difference between the magnitudes of two coefficients of a selected pair is first computed as follows.

$$D(x_1, y_1, x_2, y_2) = |F(x_1, y_1)| - |F(x_2, y_2)| \quad (8)$$

where F is the SVD-DCT block matrix; (x_1, y_1) and (x_2, y_2) are the coordinates of two coefficients of the selected pair. It is found that the high-frequency coefficients in the SVD-DCT block are close enough so that $D(x_1, y_1, x_2, y_2)$ can be considered as a zero-mean random Gaussian process [9]. Let the two modified coefficients be denoted by $F'(x_1, y_1)$ and $F'(x_2, y_2)$. These coefficients are modified to make the difference $D'(x_1, y_1, x_2, y_2)$ positive if the watermark bit to be embedded is "1" and negative if the watermark bit to be embedded is "0". Details of the process are given in the following paragraphs.

In the case of embedding watermark bit "1",

(1) If $D(x_1, y_1, x_2, y_2) \geq 0$, no operation is performed.

(2) If $D(x_1, y_1, x_2, y_2) < 0$, the following operations are carried out if one of the coefficients, $F(x_1, y_1)$ and $F(x_2, y_2)$, is nonzero.

$$\begin{cases} F'(x_1, y_1) = sgn\big(F(x_1, y_1)\big) \cdot \left(\frac{|F(x_1, y_1)| + |F(x_2, y_2)|}{2} + 0.5 \cdot mask\right) \\ F'(x_2, y_2) = sgn\big(F(x_2, y_2)\big) \cdot \left(\frac{|F(x_1, y_1)| + |F(x_2, y_2)|}{2} - 0.5 \cdot mask\right) \end{cases}$$

(3) If $F(x_1, y_1) = F(x_2, y_2) = 0$, then

$$\begin{cases} F'(x_1, y_1) = 0.5 \cdot mask \\ F'(x_2, y_2) = -0.5 \cdot mask \end{cases}$$

The parameter *mask* in the above equations is the frequency mask described in the next part. It is used to adaptively adjust the local watermark embedding strength of each SVD-DCT block.

In the case of embedding watermark bit "0",

(1) If $D(x_1, y_1, x_2, y_2) < 0$, no operation is performed;

(2) If $D(x_1, y_1, x_2, y_2) \geq 0$, the following operations are carried out if one of the coefficients, $F(x_1, y_1)$ and $F(x_2, y_2)$, is nonzero.

$$\begin{cases} F'(x_1, y_1) = sgn\big(F(x_1, y_1)\big) \cdot \left(\frac{|F(x_1, y_1)| + |F(x_2, y_2)|}{2} - 0.5 \cdot mask\right) \\ F'(x_2, y_2) = sgn\big(F(x_2, y_2)\big) \cdot \left(\frac{|F(x_1, y_1)| + |F(x_2, y_2)|}{2} + 0.5 \cdot mask\right) \end{cases}$$

(3) If $F(x_1, y_1) = F(x_2, y_2) = 0$, then

$$\begin{cases} F'(x_1, y_1) = -0.5 \cdot mask \\ F'(x_2, y_2) = 0.5 \cdot mask \end{cases}$$

After watermark embedding, the inverse DCT is first performed on the modified SVD-DCT blocks. The SV blocks consisting of 4×4 first SVs are then constructed followed by the reconstruction of 16 adjacent 4×4 sub-image blocks of each corresponding SV block. Note that, watermark information is embedded only in the first SVs and other SVs are kept unchanged. Inverse SVD is performed on all blocks and the watermarked normalized image is obtained by concatenation of all 4×4 sub-image blocks in spatial domain. The final watermarked image is obtained by restoring to the original image size and position before normalization.

B. Frequency Masking

The degree of modification of SVD-DCT coefficients is directly proportional to the quality degradation of watermarked image. The modification threshold of each SVD-DCT block, which is block adaptive, can be used to determine the local watermark embedding strength and guarantee the visual transparency of embedded watermark. To achieve the highest-possible robustness without significant quality degradation, it is necessary to calculate a frequency mask to measure the modification threshold of each block. A frequency mask contains a lot of frequency components and several methods were developed to calculate the mask [20,21]. In the proposed watermarking scheme, the calculation of frequency mask is kept simple to reduce computational load. The parameter $mask$ as mentioned above is introduced to represent the frequency mask and it is an average value of the sum of the absolute values of the SVD-DCT coefficients, whose indices are from 9 to 16, representing the coefficients in the high-frequency band as shown shaded in Fig. 3.

To measure the modification threshold of each block, a linear frequency mask is calculated as follows.

$$mask = \frac{1}{8}\sum_{i=9}^{16} |F(i)| \quad (9)$$

where F is the SVD-DCT block matrix. As mentioned above, this frequency mask is able to adjust the local watermark embedding strength of each block. Hence highest-possible

robustness can be achieved without significant quality degradation for the proposed scheme.

The complete flow of operations of the proposed watermark embedding process is given in the block diagram form shown in Fig. 3.

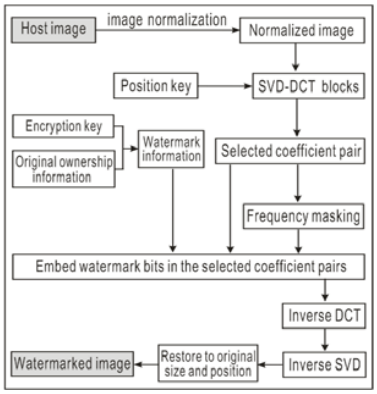


Fig. 3 Block diagram of watermark embedding process

C. Watermark Extracting Process

For the proposed scheme, watermark extraction is blind, that is, the original host image is not required for watermark extraction. The steps taken to extract the embedded watermark bits are detailed in the following.

(1) Normalization procedures are applied on the watermarked image which is possibly distorted or attacked. As a result, a normalized watermarked image is obtained.

(2) SVD-DCT operations are carried out on normalized image to obtain the SVD-DCT blocks.

(3) Using the position key, the embedding positions of the selected coefficient pair in each SVD-DCT block are identified.

(4) The difference between two coefficients of each selected pair is computed as follows:

$$D^*(x_1, y_1, x_2, y_2) = |F^*(x_1, y_1)| - |F^*(x_2, y_2)| \qquad (10)$$

where $F^*(x_1, y_1)$ and $F^*(x_2, y_2)$ are the two coefficients of a selected pair that might carry watermark information.

(5) Since the watermark bit stream is repeatedly embedded, accuracy of watermark extraction can be enhanced using "majority vote". For this purpose, the sum of $D^*(x_1, y_1, x_2, y_2)$ values for all selected coefficient pairs of a given watermark bit repeatedly embedded is first computed as follows.

$$B_i = \sum_{\Phi_i} D^*(x_1, y_1, x_2, y_2) \qquad (11)$$

(6) The extracted watermark bit is determined according to the value of B_i as follows.

$$W_i' = \begin{cases} 1 & if\ B_i \geq 0 \\ 0 & if\ B_i < 0 \end{cases} \qquad (12)$$

(7) The original ownership information in binary format is recovered using the encryption key.

D. Security Considerations

For the schemes proposed in [12] and [14], the watermark embedding positions are deterministic. For such schemes, a simple attack, such as adding perturbations to the embedding positions or statistical attack, will bring about significant watermark detection errors. For the proposed watermarking scheme, $K_1 = 2$ coefficients are selected for embedding out of the $K_2 = 8$ potential positions. Suppose that the size of watermark is N_w and the maximum capacity for watermark embedding is N_C, then the probability of successfully extracting $K_1/2$ watermark bit without the position key is

$$P = \sum_{i=\lceil N_C/(2N_w)\rceil+1}^{\lceil N_C/N_W \rceil} \left(\frac{(K_2-K_1)!}{K_2}\right)^i \left(1 - \frac{(K_2-K_1)!}{K_2}\right)^{\left\lceil \frac{N_C}{N_W} \right\rceil - i} \binom{\lceil N_C/N_W \rceil}{i} \qquad (13)$$

and the probability of successfully extracting all N_w watermark bits is

$$P_w = (P)^{\frac{N_W}{K_1/2}} (1-P)^{\lfloor \frac{N_C}{N_W} \rfloor} \qquad (14)$$

For illustration, suppose that N_w=32 and N_c=256, then $P \approx 6.8 \times 10^{-12}$and $P_w \approx 7.3 \times 10^{-56}$. Thus, tremendous computational efforts are required to identify the embedding positions without knowing the position key. On the other hand, if the attackers resort to averaging the magnitude of the coefficients over all the potential positions for embedding in each SVD-DCT block, the visual quality of the attacked watermarked image will be severely affected. For the host Lena image, the attacked image is shown in Fig.4, Peak Signal-to-Noise Ratio (PSNR) value in this case is only 17.6dB.

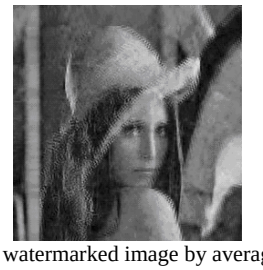
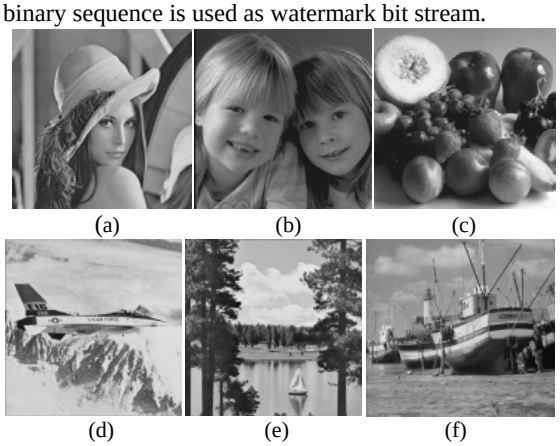


Fig. 4 Attacked watermarked image by averaging operation

IV. Performance of Proposed Scheme

Experiments are carried out to assess the performance of the proposed watermarking scheme. The six 256×256 gray-level images used as original host images are shown in Fig. 5. A 32-bit binary sequence is used as watermark bit stream.



(a) (b) (c)

(d) (e) (f)

Fig. 5 Original host images (a) Lena (b) Girls (c) Fruits (d) Plane (e) Lake (f) Boat

A. Visual Quality Evaluation

All host images are first normalized, after which the watermark bit stream is embedded into the normalized images. The final watermarked image of Fig. 5(a) Lena is shown in Fig. 6(a). The difference between watermarked and host image is considered as quantization errors. For ease of displaying, the values of quantization errors are normalized to the range of [-127,128] and rounded to the nearest integers. And the difference image is shown in Fig. 6(b).

(a) (b)

Fig. 6 (a) Watermarked image (b) Difference image

Perceptually, the watermarked image shown in Fig. 6(a) is visually the same as the original host image. The numbers of occurrence for the values of quantization errors are plotted in the histogram shown in Fig. 7.

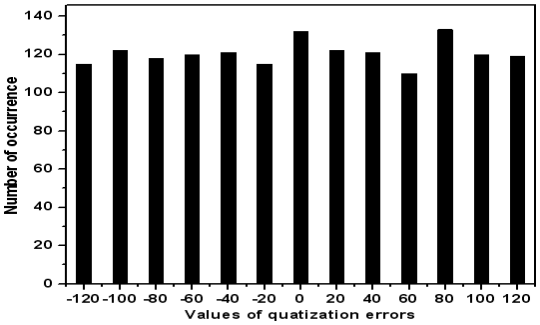


Fig. 7 Histogram of quantization errors

We can see that the values of quantization errors are more or less evenly spread across the range and they are close to uniform distribution. Hence, it is difficult for an attacker to detect the existence of embedded watermark using statistical analysis [3], [11]. Similar results are obtained for the other five host images.

For objective measure of visual quality, PSNR is used. The PSNR values of all six images are tabulated in Table I.

TABLE I
PSNR OF WATERMARKED IMAGES

	Lena	Girls	Fruits	Plane	Lake	Boat
PSNR(dB)	43.3	45.1	45.5	39.2	48.2	46.4

Based on the PSNR values of watermarked images, which are all higher than 39dB, it can be concluded that degradation of visual quality caused by the embedded watermark is insignificant.

B. Robustness Evaluation

The robustness of the proposed scheme against attacks is assessed. For this purpose, the following attacks are used.

1) JPEG compression with the following quality factors: (a) 10, (b) 15, (c) 20, (d) 25, (e) 30, and (f) 35.
2) Median filtering with the following sizes: (a) 4×4, (b) 5×5, (c) 6×6, (d) 7×7, (e) 8×8, and (f) 9×9.
3) Noise addition: (a) Uniform noise (0.2), (b) Uniform noise (0.3), (c) Gaussian noise (0.2), (d) Gaussian noise (0.3), (e) Salt & pepper noise (0.05), and (f) Salt & pepper noise (0.08).
4) Common image processing operations: (a) Spatial sharpening with the kernel of $\begin{pmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{pmatrix}$, (b) Spatial sharpening with the kernel of $\begin{pmatrix} 0 & -2 & 0 \\ -2 & 6 & -2 \\ 0 & -2 & 0 \end{pmatrix}$, (c) Gaussian filtering with kernel of $(1/8)\begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 1 & 1 \end{pmatrix}$, (d) Gaussian filtering with kernel of $(1/16)\begin{pmatrix} 2 & 2 & 3 \\ 1 & 3 & 5 \\ 3 & 1 & 4 \end{pmatrix}$, (e) Frequency mode Laplacian removal (FMLR) attack, and (f) Color quantization. Color quantization is similar to GIF compression.
5) StirMark bending strength (a) 2, (b) 3, (c) 4, (d) 5, (e) 6, and (f) 7.
6) Line and column removal: (a) (2, 5), (b) (5, 2), (c) (3, 6), (d) (6, 3), (e) (7, 8), and (f) (8, 7). The two numbers in the pairs are respectively the number of rows and columns removed. The removed rows or columns are equidistant.
7) Scaling by the following factors: (a) 0.6, (b) 0.75, (c) 0.8, (d) 1.1, (e) 1.2, and (f) 1.5
8) Rotation by the following angles: (a) -25°, (b) -15°, (c) -10°, (d) 25°, (e) 35°, and (f) 45°
9) Change of aspect ratio: (a) (0.8, 1.1), (b) (0.9, 1.1), (c) (1.1, 0.8), (d) (1.1, 0.7), (e) (1.2, 0.9), and (f) (1.2, 1.0), where each pair of numbers indicate the amount of scaling in *x* and *y* directions, respectively.
10) Sharing; (a) (5%, 1%), (b) (2%, 5%), (c) (1%, 3%), (d) (5%, 3%), (e) (2%, 2%), and (f) (5%, 5%), where each pair of numbers indicate the amount of shearing in *x* and *y* directions, respectively.
11) General affine transformations: (a) matrix transformation $\begin{pmatrix} 1.2 & 0.3 \\ -0.2 & 0.8 \end{pmatrix}$, (b) matrix transformation $\begin{pmatrix} 1.1 & 0.1 \\ -0.3 & 0.9 \end{pmatrix}$, (c) matrix transformation $\begin{pmatrix} 1.0 & 0.5 \\ -0.1 & 0.7 \end{pmatrix}$, (d) matrix transformation $\begin{pmatrix} 1.2 & 0.9 \\ -0.8 & 0.2 \end{pmatrix}$, (e) Horizontal flipping, and (f) Vertical flipping.

12) Combination attacks: (a) JPEG 15+Rotation 35°, (b) JPEG 20+Scaling 0.9, (c) JPEG 25+Scaling 1.2, (d) Median filtering 5×5+ Rotation 25° (e) Median filtering 6×6+Scaling 0.8, and (f) Median filtering 7×7+Scaling 1.1.

The watermarked images are put through the listed attacks. Watermark extracting process as detailed is then carried out to extract the watermark bits. The accuracy of watermark extraction is measured using extracting bit error rate (BER), defined as the ratio between the number of incorrectly extracted bits and the total number of embedded watermark bits. The average BER value of all six attacked images subjected to the same type of attack is calculated. All average values are tabulated in Table II.

TABLE II
AVERAGE BER VALUES

Attacks	(a)	(b)	(c)	(d)	(e)	(f)
(1)	0.102	0.034	0.026	0.01	0	0
(2)	0	0.009	0.022	0.039	0.055	0.115
(3)	0	0.008	0.025	0.03	0.046	0.051
(4)	0.013	0.008	0.011	0.01	0.023	0.038
(5)	0	0.005	0.031	0.049	0.086	0.133
(6)	0	0	0	0.003	0	0.002
(7)	0.01	0	0	0	0	0.051
(8)	0	0	0	0	0	0
(9)	0	0	0	0	0	0
(10)	0	0	0	0.023	0	0.012
(11)	0	0.05	0.029	0.018	0	0
(12)	0.027	0.01	0.01	0.03	0.033	0.048

Based on the BER values, it is observed that the proposed scheme is robust against most of the attacks including image processing operations and geometric attacks, except when StirMark bending strength is very high.

V. CONCLUSION

In this paper, a novel robust image watermarking scheme is described. The host image is first normalized. A 4×4 SV block is constructed by concatenating first SVs of 16 adjacent 4×4 image blocks in the normalized image. DCT is then performed on SV blocks and watermark bits are embedded in the high-frequency DCT coefficients. An adaptive frequency mask is calculated to adjust local watermark embedding strength. The watermark extracting method is blind. Fidelity loss of watermarked image is very low. Experimental results show that the proposed scheme is very robust against various image processing operations and geometric attacks.

Although the proposed scheme is described for embedding watermark in image, it can be readily adapted for audio watermarking and other forms of watermarking.

REFERENCES

[1] S.W. Foo, H.S. Muh, and N.M. Mei "Image watermarking using time-frequency compression expansion" *IEEE International Symposium on Circuits and Systems*, 2004, pp. 201-204.

[2] S.W. Foo, X. Feng, and M. Li "A blind imagewatermarking scheme using peak point extraction", *IEEE International Symposium on Circuits and Systems*, 2005, pp. 4409-4412.

[3] M. Acevedo, "Image watermarking: properties, techniques and evaluation. *Multimedia security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, Idea Group Publishing*. Pennsylvania, 2005.

[4] S.W. Foo, Y.T. Hee, and H.D. Yan, "An adaptive image watermarking system", *IEEE Tencon 2005*, pp. 509-513.

[5] N. Cvejic and T. Seppänen, "Audio watermarking: requirement, algorithms, and benchmarking". *Digital watermarking for digital media, Information Science Publishing*, Pennsylvania, 2005.

[6] J. Foote, J. Adco, and A. Girgensohn, "Time base modulation: a new approach to watermarking audio" *[Electronic Version], Palo Alto Laboratory. California*. 2003.

[7] M.A. Suhail, "Digital watermarking for protection of intellectual property". *Multimedia security: steganography and digital watermarking techniques for protection of intellectual property, Idea Group Publishing*. Pennsylvania, 2006.

[8] P. Bassia, W.T. Pitas, "Robust Audio Watermarking In Time Domain", *EUSIPCO 1998, 8-11 Sept., Patras, Greece*, pp. 25-28.

[9] D. Gruhl, A. Lu, and W. Bender, "Echo Hiding for Watermarking", in *Proc. Information Hiding Workshop*, University of Cambridge, U.K., 1999, pp. 295-315.

[10] K. Seits, and T. Jahnke, "Digital watermarking: an introduction". In *Seits, J, Digital watermarking for digital media, Information Science Publishing*. Pennsylvania, 2006.

[11] R. Garcia, "Digital Watermarking of Audio Signals Using a Psychoacoustic Auditory Model and Spread Spectrum Theory", *107th Convention, Audio Engineering Society, New York*, 1999.

[12] H.J. Kim, Y.H. Choi & J.W. Seok and K.H. Hong. "Audio Watermarking Techniques: Intelligent Watermarking Techniques". *Chapter 8, 185-218*, 2005.

[13] J, Seitz, S.H. Michale, "Digital Watermarking for Digital Media," *Information Science Publishing*, 2005.

[14] N. Cvejic and T. Seppänen, "Increasing robustness of LSB audio steganography by reduced distortion LSB coding," *Journal of University Computer Science, vol 11, p56*, 2006.

[15] C. Hsieh. & P. Tsou. "Blind Cepstrum Domain Audio Watermarking Based on Time Energy Features". *4th Int. Conf. on Digital Signal Processing*, 705-708, 2004.

[16] K.N. Garcia. "Digital Watermarking of Audio Signals Using a Psychoacoustic Auditory Model and Spread Spectrum Theory". *107th Convention, Audio Engineering Society, preprint 5073*, 2006.

[17] L. Wu, P.C. Su and M. Kuo "Robust Audio Watermarking for Copyright Protection". *SPIE's 44th Annual Meeting Advanced Signal Processing Algorithms, Architectures, and Implementations IX*. 2003.

[18] B. Vladimir, K.E. Rao. "An Efficient Implementation of the Forward and Inverse MDCT in MPEG Audio Coding". *IEEE Signal Processing Letters*, Vol.8, No.2, 2005.

Say Wei Foo, Associate Professor, School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798. E-mail: eswFoo@ntu.edu.sg. Say Wei Foo has served in various capacities in the Institution of Engineers, Singapore (IES) and is the President of IES from 2004-2006. He is also a board member of the Professional Engineers Board (Singapore) and a member of the ASEAN Academy of Engineering and Technology. He is currently an Associate Professor. His research interests include image processing, information hiding and speech signal processing.

Qi Dong, Ph.D. candidate, School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798. E-mail: DONG0041@ntu.edu.sg. He is currently a Ph.D. candidate. His research interests include information hiding, digital watermarking and signal processing.