

A Blind Watermarking Technique for Color Image based on SVD with Circulation

Hongqin Shi, Fangliang Lv[†], Yiqin Cao

School of Software, East China Jiaotong University, Nanchang, Jiangxi, China

Email: shihongqin@163.com

[†]Corresponding author. Email address: shihongqin@163.com

Abstract—Digital watermarking is a method for protecting copyrighted materials such as digital images. This paper presents a new color watermark embedding technique with circulation, based on non-overlapping Singular Value Decomposition (SVD) for hiding important information in images. First, the real-color original image is decomposed into three components R, G and B. The blue component and the watermark performed by Chebyshev chaotic map are divided into non-overlapping blocks, respectively. Then an SVD is performed on each partitioned blocks. Second, the Singular Values (SVs) of watermark are embedded into the singular value matrix of blue component with circulation. Extracting any consecutive four rows and columns from the blocked watermarked image can get complete watermark information. Every watermark bits have been embedded several times and their embedding position are consecutive in the selected original image. That is why, our proposed scheme is naturally secure to geometric attacks and compound attacks, and it is also strongly robust against common image processing attacks.

Index Terms—Copyrighted materials, Circulation, Chebyshev chaotic map, Singular values

I. INTRODUCTION

Watermarking has been studied extensively for many years, which is a technique to invisibly embed secret information into the image, audio or video data. Basic properties of a digital watermarking technique are imperceptibility, robustness and the ability to provide a definite proof of ownership [1-6]. In the recent years, color image watermarking has been becoming one of the research hot topics [7-9]. The color image has two advantages: the first one is to hide more amounts of data; the second one is to attain higher fidelity. The color perception depends not only on the luminance but also on the chrominance. Thus, by using color watermarking, both the capacity and the fidelity can be increased relative to gray watermark image. There are two types of methods to recover the original hidden image: The first one needs help of original image, which is called half blind watermarking. The second one does not need the original image. Only those who have the key can detect and extract the right watermark, which makes the approach have high security level is called blind watermarking.

Recently, one kind of watermarking, which is based on SVD, is popularly proposed. The SVD performs an

optimally matrix decomposition in a least-square domain for matrices in real number domain [10-14]. A blind extraction method for gray image watermark based on DWT and SVD was proposed in [15]. Firstly, one binary watermark image was embedded into the host image using the technology of wavelet transform and singular value decomposition. And then, a fragile watermark was further embedded into LSB of the above watermarked image to reduce the fragile watermark's influence towards robustness. Although, the combination of the two watermarks achieves a double protection for the host image but how to solve the large calculation amount is a problem. Y. J. Cai et al [5] proposed a technique in which each bit of the scrambling watermark was embedded into the relative size of the first singular values of one couple blocks, which was the non-overlapping blocks of host channel implemented by DWT and SVD. A watermark in [10] was encrypted by Tent chaotic sequence, and then the cover image is decomposed by SVD, the encrypted watermark is embedded into the singular values of the cover image, and the watermark can be extracted without the original image. R. Agarwal et al [11] present a data-hiding algorithm that exploits the singular value decomposition (SVD) representation of the data, which compute the SVD of the host image and the watermark, then embed the watermark in the singular vectors of the host image. Reference [16] suggests a gray-scale watermark algorithm based on SVD, the pixel value of watermark is embedded into the blocks of largest singular value by the quantization. Peng et al. [17] proposed a new semi-fragile watermarking scheme for color image authentication based on spatiotemporal chaos and SVD, in which the watermark is embedded directly into the SVs (singular values) of the blocks within wavelet sub-band. In order to enhance the security, spatiotemporal chaos is employed to select the embedding positions for each watermark bit as well as for watermark encryption. A New SVD based Hybrid Color Image Watermarking for Copyright Protection was proposed in reference [18], dual color host and watermark image are decomposed into directional sub-bands using contour-let transform. And then applied Singular value decomposition to mid frequency sub-band coefficients. The singular values of mid frequency sub-band coefficients of watermark are embedded into singular values of mid frequency sub-band coefficients of host color image in red, green and blue

color spaces simultaneously based on spread spectrum technique. C.F. Tsai et al [19] propose one scheme, which first calculates the frequency coefficient of luminance within the original color image using DCT. And then decomposes the coefficient to computes its singular value. The scheme embeds the watermark into the singular value of the DCT coefficient blocks within an original color image and does not require the original image when performing extraction of watermark procedure. The above algorithm can achieve a high-quality watermarked image.

Based on the methods above, a novel blind digital watermarking algorithm for color image based on SVD with circulation was presented. Firstly, performed Chebyshev chaotic map on the watermark image and then partitioned it into non-overlapping blocks. Secondly, the real-color original image was decomposed into R, G and B components, and then the blue component was divided into equally non-overlapping blocks and implemented with SVD, respectively. The human eye is less sensitive to changes in the blue component. That is why the watermark embedded into blue channel. Thirdly, every scrambling watermark blocks implemented with SVD, respectively, were embedded into the singular value matrix of blue component blocks with circulation.

The rest of this paper is organized as follows. The proposed watermarking scheme is depicted in section 2. The detailed watermark embedding and extraction procedures are presented in Section 3. Subsequently, Section 4 we present our numerical simulations including the robustness to several possible attacks. Finally, conclusions are given in Section 5.

II. RELATED WORK

A. Chebyshe Maps

Chebyshev maps have important properties of excellent cryptosystem [20]. The expression of Chebyshev maps as in (1).

$$X_{n+1} = \cos(k \cos^{-1} X_n) \quad -1 \leq X \leq 1 \quad (1)$$

Where k is the degree of Chebyshev maps, if $k \geq 2$, the Lyapunov exponent of Chebyshev maps is positive, which predicates that Chebyshev maps are chaotic. Its invariant probability distribution density is as in (2).

$$\rho(X) = \frac{1}{(\pi\sqrt{1-X^2})} \quad (2)$$

Chebyshev maps are a classic chaotic system with the sensitivity of initial state, the real number sequences generated by which are orthogonal each other. The auto-correlation function of real-valued sequences generated by the Chebyshev maps is δ function. Moreover, it can generate a huge number of different sequences using only slightly different initial values. The parameter k and initial state value X_0 are regarded as the key of proposed watermarking system. Chaotic maps generated by a single real-valued chaotic sequence cycle from initial

value X_0 are limited. To avoid this situation, several chaotic sequences are cascaded to generate longer period of ones. The first chaotic sequence X_1 , which length is N_1 , was generated by initial value X_0 and then the second chaotic sequence X_2 , which length is N_2 , was generated by initial value X_1 , will analogize in turn. The complexity of chaotic system is decided by the level of cascaded. According to the computation, the system use two cascading chaotic sequence. Since the binary sequence is used as a spreading sequence in actual digital spread spectrum communication system, to take 0 as the threshold value, using threshold approach to binary chaotic sequence as in (3).

$$\text{sgn}(X) = \begin{cases} 1 & x \in [0, 1] \\ -1 & x \in [-1, 0] \end{cases} \quad (3)$$

Given a set of initial values, computing with (1) can get a certain length of real-valued sequences, threshold with (3) then obtained binary chaotic spreading sequence group.

B. Singular Value Decomposition

SVD is an important tool in linear algebra, which is widely applied in many research fields such as principal component analysis, canonical correlation analysis and data compression. Indeed, the main properties of the SVD from the viewpoint of image processing applications are: firstly, the SVs of an image have a very good stability, i.e., when a small perturbation is added to an image, its SVs do not change significantly. Secondly, SVs represent intrinsic algebraic image properties [10].

From the perspective of linear algebra, a digital image can be viewed as a matrix composed of a number of nonnegative scalars, singular value decomposition (SVD) belongs to an orthogonal transformation, it can make the image matrix diagonalization.

Let $X \in \mathbb{R}^{m \times n}$ denote an image matrix, two orthogonal matrixes: $U = [u_1, u_2, u_3, \dots, u_m] \in \mathbb{R}^{m \times m}$ and $V = [v_1, v_2, v_3, \dots, v_n] \in \mathbb{R}^{n \times n}$, there exist a factorization of the form as (4)

$$X = USV^T \quad (4)$$

Where $S \in \mathbb{R}^{m \times n}$ is a matrix of all elements are zero except for its diagonal elements, u_i and v_i are called the singular value vectors and the diagonal elements shown as (5)

$$\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \dots \geq \lambda_r \geq \lambda_{r+1} = \dots = \lambda_N = 0 \quad (5)$$

Where r is rank of X , λ_i ($i=1, 2, \dots, N$) is uniquely determined by the SVD and called the singular values of X . Use of SVD in digital image processing has some advantages. First, the size of the matrices from SVD transformation is not fixed. It can be a square or a rectangle. Secondly, singular values in a digital image are less affected if general image processing is performed. Bigger singular values not only preserve most energy of an image but also resist against attacks

W ₀	W ₁	W ₂	W ₃	W ₄	W ₅	W ₆	W ₇	W ₈	W ₉	W ₁₀	W ₁₁	W ₁₂	W ₁₃	W ₁₄	W ₁₅
W ₄	W ₅	W ₆	W ₇	W ₈	W ₉	W ₁₀	W ₁₁	W ₁₂	W ₁₃	W ₁₄	W ₁₅	W ₀	W ₁	W ₂	W ₃
W ₈	W ₉	W ₁₀	W ₁₁	W ₁₂	W ₁₃	W ₁₄	W ₁₅	W ₀	W ₁	W ₂	W ₃	W ₄	W ₅	W ₆	W ₇
W ₁₂	W ₁₃	W ₁₄	W ₁₅	W ₀	W ₁	W ₂	W ₃	W ₄	W ₅	W ₆	W ₇	W ₈	W ₉	W ₁₀	W ₁₁
W ₀	W ₁	W ₂	W ₃	W ₄	W ₅	W ₆	W ₇	W ₈	W ₉	W ₁₀	W ₁₁	W ₁₂	W ₁₃	W ₁₄	W ₁₅
W ₄	W ₅	W ₆	W ₇	W ₈	W ₉	W ₁₀	W ₁₁	W ₁₂	W ₁₃	W ₁₄	W ₁₅	W ₀	W ₁	W ₂	W ₃
W ₈	W ₉	W ₁₀	W ₁₁	W ₁₂	W ₁₃	W ₁₄	W ₁₅	W ₀	W ₁	W ₂	W ₃	W ₄	W ₅	W ₆	W ₇
W ₁₂	W ₁₃	W ₁₄	W ₁₅	W ₀	W ₁	W ₂	W ₃	W ₄	W ₅	W ₆	W ₇	W ₈	W ₉	W ₁₀	W ₁₁

Figure 1. System of circulation.

Generally, the matrix S has many small singular values. Finally, singular values possess intrinsic algebraic image properties.

C. System of Circulation

In this work, we propose a novel method to embed and extract watermark information with circulation. The main procedure includes three steps as follows.

Step1: The watermark image is equally divided into non-overlapping $p \times p$ blocks W_t ($t=0,1, 2, \dots, p^2-1$) and p is a positive integer.

Step2: The original image is equally divided into non-overlapping $m \times n$ blocks A_{ij} ($i=0,1, 2, \dots, m-1$) ($j=0, 1, 2, \dots, n-1$), m is an integer multiple of p and $n \geq p$.

Step3: Modifying the singular value to embed the watermark information with circulation and get new value. Every watermark block was embedded in one original block with circulation. The first column of every row of original image matrix A_{ij} was embedded with W_t ($t = (i \bmod p) \times p$) and the next column was embedded

with $W_{((t++) \bmod p^2)}$. Wherein mod denoting module operation.

For example, the watermark image was divided into non-overlapping 4×4 blocks W_t ($t=0, 1, 2 \dots 15$) and the original image was blocked to non-overlapping 8×16 blocks A_{ij} , ($i=0, 1, 2 \dots 7$) ($j=0, 1, 2 \dots 15$) (shown as in Fig. 1). Every box represents one carrier image block and the symbol W_t ($t=0, 1, 2 \dots 15$) denotes watermark block.

Extracting any consecutive four rows and four columns shown as the coloring regions can get complete watermark information from the embedded blocks. That is why the algorithm can effectively resist the cropping attacks.

III. WATERMARK EMBEDDING AND EXTRACTION

Let O be the original image of size $M \times M$, W is the watermark image of size $N \times N$. The relation between original image and the watermark image

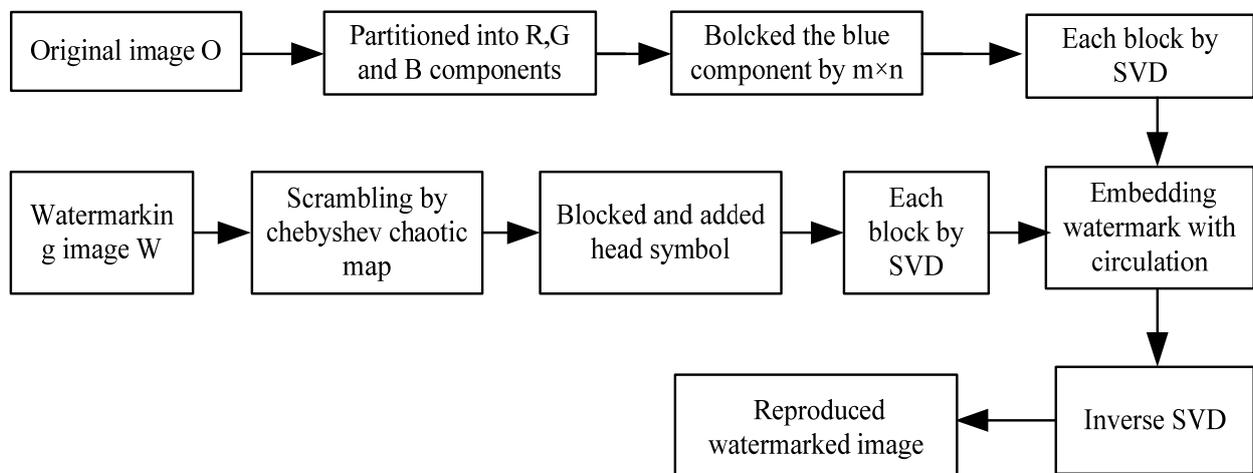


Figure 2. Watermark embedding process.

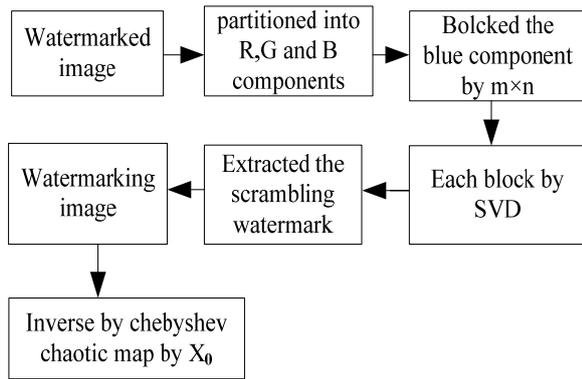


Figure 3. Watermark extraction process.

meets $O = 2^k \times W$, the sizes of O are integer multiple of W, where k is positive integer. The proposed method in this paper is illustrated in Fig. 2.

The concrete embedding procedure is as bellows:

Step1: Based on the theory that a RGB color image is the composition of R, G and B components, the real-color original image O is decomposed into three components R, G and B components, respectively.

Step2: Partition the blue component into a set of non-overlapping blocks with same size O_{ij} .

$$O_{ij} = \frac{(M \times M)}{2^n \times 2^4} \quad (6)$$

Where n is a positive integer.

Step3: W is encrypted by Chebyshev chaotic maps using (1) for taking the initial value X_0 to get $N_1 \times X_1$. (N_1 is the length of scrambling sequence X_1)

Step4: Setting X_1 as new initial value by Chebyshev

chaotic maps again get X_2 which length is $N_1 \times N_2$.

Step5: Using threshold approach for the last binary chaotic sequence in (3) to get encrypted watermark W' .

Step6: Partition the W' into a set of non-overlapping blocks with size W'_d ($d=0,1,\dots,15$).

Step7: Perform an SVD on each block O_{ij} . Let the matrix X, with elements x_{ij} , ($i=0,1,2,\dots,m-1$) and ($j=0,1,2,\dots,n-1$), represent the block O_{ij} , which needs to be watermarked.

$$X = U_X S_X V_X^T = A_X V_X^T \quad (7)$$

Step8: The encrypted watermark W'_d , added heading symbol to identify its order. Let Q represent the matrix of W'_d to be embedded. The computation for SVD of Q is as follows:

$$Q = U_Q S_Q V_Q^T = A_Q V_Q^T \quad (8)$$

Where $A_{X(Q)} = U_{X(Q)} S_{X(Q)}$ are also called the principal components in the language of principal component analysis. Now, we add the scaled eigenvector V_Q of watermark to that of the original image.

$$V' = V_X + \alpha V_Q \quad (9)$$

Where α is the scale factor, it is used to control the watermark embedding strength.

Step9: Perform inverse SVD for A_X and V' to recover watermarked matrix X' .

$$X' = A_X V'^T \quad (10)$$

Repeat step7-step9 with circulation as shown in Fig. 2, until all watermark blocks are embedded into the blue component blocks with circulation.

Step10: Rearrange the watermarked blue component blocks back to one. Then recombine the watermarked B



Figure 4. Original images (the first line) Watermarked images (the second line).



Figure 5. Watermarking image Scrambling watermarking image.

and original R, G to obtain the watermarked image.

Extraction algorithm is a straightforward reversal of the embedding algorithm (shown as Fig. 3).

Step1: The watermarked image is firstly decomposed into three components R, G and B.

Step2: Divide the blue component into non-overlapping blocks having the same size used in the embedding process.

Step3: Select any consecutive four rows and four columns of the blocks. Perform SVD on the sixteen selected blocks to get SVs.

Step4: Obtains the matrices that contain the watermark using (4) and extract the possibly corrupted watermark block using the follows:

$$V_o^{rT} = (A_x^{-1} X' - V_x^{rT}) / \alpha \tag{11}$$

$$Q' = A_o V_o^{rT} \tag{12}$$

Step5: Rearrange watermark block components to reproduce the scrambling watermark image by the head symbol embedded in every W'_d .

Step6: Perform threshold approach to reverse chaotic sequence and reconstruct the watermark W by Chebyshev chaotic maps with initial value X_0 .

IV. EXPERIMENTAL RESULTS

In order to study the sensitivity of this watermarking method for different images and sizes, we have used four sets original images in the simulations, such as Baboon, F16, Peppers and Lena, respectively. The sizes of original images in the experiences are 512×512 and the block sizes are 16×16 , 32×32 and 64×64 , respectively. Several experiments are presented to demonstrate the performance of the proposed approach. Some of these original images and their watermarked images have been shown in Fig. 4, respectively. It is virtual impossible to distinguish the differences between the original image and the watermarked one from visual effect. The watermark image of size 32×32 and the block sizes are 4×4 (shown in Fig. 5).

Normalized correlation (NC), a similarity indicator specified in (13), is used to evaluate the similarity between the original watermarking W and the extracted watermarking W' retrieved from an attacked and watermarked image.

$$NC = \frac{\sum_{i=1}^M \sum_{j=1}^N |W + W'| \div 2}{M \times N} \tag{13}$$

Where M and N represent the length and width of the

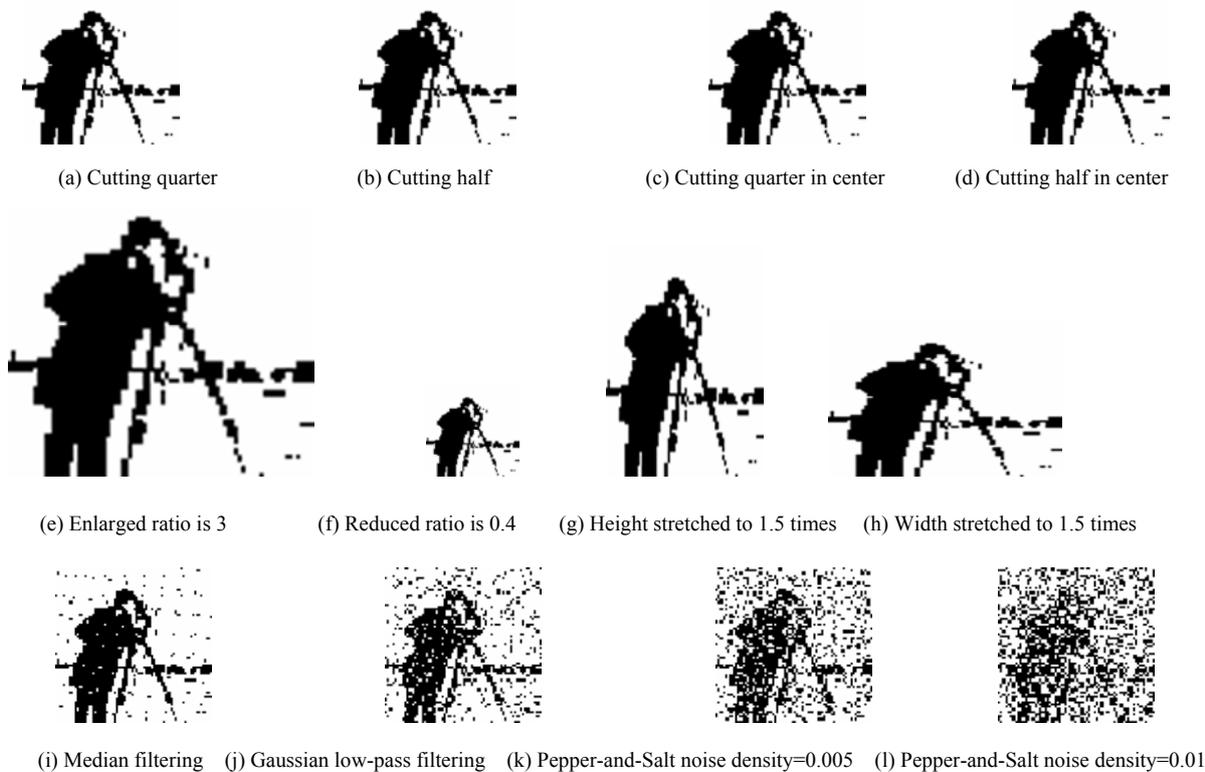


Figure 6. the extracted watermark images from different attacks.

watermark image respectively, higher NC value stands for high resemblance between W and W' . Additionally, another quantitative index, Peak Signal-to-noise (PSNR) is used to evaluate the quality of the watermarked image to the original image. The higher PSNR value indicates a watermarking method produces few differences between original image and watermarked image.

For the sake of clarity and simplicity, only one original image blocked by 16×16 , Lena is used to analysis in the following discussion.

A. Cropping Attacking

Image cropping is very frequently used in real life, which is a lossy operation. Too much cutting will make the image meaningless and unvalued, so the degree of cropping attack will not be much in the general case. Four different cropping attacks are carried out to the watermarked image, respectively. The experimental results are shown in Fig. 6 (a), (b), (c) and (d). The proposed algorithm is resistant to a large extent cropping attack, which has wonderful performance in the experiments.

B. Scaling Attack

The great majority of watermarking algorithm resist against scaling attack in the interval $[0.5, 2]$, but the proposed algorithm can be resistant to any size scaling attacks. The extracted watermarking images are shown in Fig. 6 (e) and (f), after the watermarked image is enlarged or reduced in size.

C. Aspect Ratio Adjustment Attack

In some applications, the watermarked image may be stretched more in one spatial dimension than another.

This type of distortion is sometimes referred to as aspect ratio adjustment. The most watermarking algorithms can not resist against aspect ratio adjustment attack, the proposed scheme in this paper has strong robust against that one. Fig. 6 (g) and (h) show the extracted watermarks after the watermarked image stretched by width or height. The results indicate that the extracted watermarks are originally the same as the embedded watermarks, which have stretched by the same way.

D. Conventional Attack

The most common manipulation in digital image is filtering. The extracted watermarks, after applying median filtering and Gaussian low-pass filtering, are shown in the Fig. 6 (i) and (j). It can be observed that the extracted watermark is still recognizable after applying the above filters.

Addition of noise is another method to estimate the robustness of the watermark. Generally, addition of noise is responsible for the degradation and distortion of the image. The watermark information is also degraded by noise addition and results shown some difficulties in watermark extraction. Fig. 6 (k) and (l) show the extracted results of adding Pepper-and-Salt noise with 0.005 and 0.01 to the watermarked Lena image, respectively. The embedded watermark can be extracted and detected from the watermarked image of added noise. It can be observed that extracted watermark is a noisy image, which nearly can not be recognizable when adding Pepper-and-Salt noise upon 0.01.

E. Robustness to JPEG Compression

JPEG compression attack is one of the common attacks that should be verified in watermarking algorithm. In this

TABLE I

NC RESULT VALUES OF THREE IMAGES UNDER DIFFERENT ATTACKS

Attack type	Pepper NC			Baboon NC			F16 NC		
	16×16	32×32	64×64	16×16	32×32	64×64	16×16	32×32	64×64
Cutting quarter	1.0000	1.0000	0.9987	0.9996	0.9999	1.0000	0.9968	0.9989	1.0000
Cutting half	1.0000	0.9999	0.9996	1.0000	1.0000	0.9998	1.0000	0.9998	1.0000
Cutting quarter in center	0.9034	1.0000	0.9996	0.9141	0.9978	1.0000	0.9124	0.9979	1.0000
Cutting half in center	0.9787	0.9997	1.0000	0.8896	0.9974	1.0000	0.9056	0.9933	1.0000
Aspect Ratio Adjustment height to 2 times	1.0000	0.9998	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Aspect Ratio Adjustment width to 2 times	1.0000	1.0000	0.9995	1.0000	0.9997	0.9999	1.0000	1.0000	0.9998
Scaling Attack ratio is 4	0.9998	1.0000	0.9999	1.0000	0.9999	1.0000	0.9998	1.0000	1.0000
Scaling Attack ratio is 0.3	0.9998	0.9999	1.0000	1.0000	1.0000	0.9997	1.0000	1.0000	0.9998
JPEG QF=90	0.9997	0.9979	0.9988	0.9981	0.9960	0.9953	0.9941	0.9869	0.9886
JPEG QF=30	0.9172	0.8785	0.9132	0.9147	0.9236	0.9311	0.9044	0.9187	0.9425
JPEG QF=20	0.7578	0.7395	0.7586	0.7790	0.7883	0.8133	0.8252	0.7872	0.8121
Median filtering 5×5	0.8792	0.8922	0.8783	0.8786	0.8937	0.8846	0.8886	0.8794	0.8563
Gaussian low pass filtering 5×5	0.9801	0.9691	0.9824	0.9791	0.9775	0.9849	0.9861	0.9838	0.9756
Pepper and Salt noise 0.005	0.8227	0.8361	0.8016	0.8142	0.8312	0.8152	0.8144	0.8365	0.8013
Pepper and Salt noise 0.01	0.7385	0.7172	0.7331	0.7242	0.7007	0.7247	0.7181	0.7160	0.7403

experiment, the watermarked images are compressed with different compression factors from 10 to 100 increasing in steps of 10. We show the watermark extracted from JPEG compressed Lena image with various quality factors (QF). Briefly, JPEG quality factor is an indication of the distortion, such that 100% quality factor corresponds to least distortion. Table II gives NC values of different QF under JPEG compression. It is variously that the algorithm is strongly resistant to JPEG compression.

TABLE II
RESULTS OF DIFFERENT QF UNDER JPEG COMPRESSION

QF (%)	100	90	80	70	60
NC	1	0.9987	0.9968	0.9954	0.9947
QF (%)	50	40	30	20	10
NC	0.9871	0.9662	0.9039	0.7667	0.6247

V. CONCLUSIONS

In this paper, a blind watermark algorithm for color image based on SVD and chaos with circulation was proposed. The proposed scheme takes advantage of image scrambling and blocked with circulation to improve the robustness and security of current watermark schemes. During the embedding procedure, the watermark is cropped into small watermarks by 4×4 and the original image blocked by 16×16, 32×32 and 64×64. Each small watermark is embedded into one single blocked with circulation. The perceptual quality and the watermarking capacity are greatly improved by this way.

The original image is not needed during the extraction and detection procedure. Experimental results and attacks analysis show that the watermark algorithm is transparent and robust against some image processing operations, such as JPEG compression, median filtering, additive noise and some cropping attacks. The deficiency of the algorithm is consistency between extraction and embedment, in which the blocks must be implemented in the same manner. Otherwise, the watermark cannot be correctly detected.

ACKNOWLEDGEMENT

This work was supported by the National Natural Science Foundation of China under grant no. 61365008, East China Jiaotong University Research Fund no.11RJ04, 13RJ01.

REFERENCES

[1] I. J. Cox, M. L. Miller, J. A. Bloom, "Digital Watermarking," *Journal of Electronic Imaging*, Vol.11, No.3, pp.153-154, 2002.
 [2] P.Moulin and R. Kotter, "Data-hiding codes," *Proc. IEEE*, vol. 93, no.12, pp. 2083-2016, Dec. 2005.

[3] Liyun Wang, Hefei Ling, Fuhao Zou, Zhengding Lu, "Real-Time Compressed- Domain Video Watermarking Resistance to Geometric Distortions," *IEEE MultiMedia*, Vol.19, No.1, pp.70-79, 2012.
 [4] M.K. Dutta, P. Gupta, V.K. P, "Audio Watermarking Using Pseudorandom Sequences Based on Biometric," *Journal of computers*, Vol.5, No.3, pp.372-379, 2010.
 [5] C. Wang, S.H. Liu, F. Jiang, Y. Liu, "A Robust Scalable Spatial Spread-Spectrum Video Watermarking Scheme Based on a Fast Downsampling Method," *Journal of computers*, Vol.7, No.9, pp.2256-2261, 2012.
 [6] R.Z. Liu, T.N. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia*, Vol.4, No.1, pp.121-128.
 [7] A. Tremeau, D. Muselet, "Recent Trends in Color Image Watermarking ," *Journal of Imaging Science and Technology* Vol.53, No.1, pp.010201(1-15), 2009.
 [8] T.Y. Wang, H.W. Li, "A Novel Robust Color Image Digital Watermarking Algorithm Based on Discrete Cosine Transform," *Journal of computers*, Vol.8, No.10, pp.2507-2511, 2013
 [9] H.H. Tsai, D.W. Sun "Color image watermark extraction based on support vector machines," *Information Sciences*, Vol.177, No.2, pp.550-569, 2007.
 [10] J.H. Song, J.W. Song, Y.H. Bao, "A Blind Digital Watermark Method Based on SVD and Chaos," *Procedia Engineering*, Vol.29, pp.285-289, 2012.
 [11] R. Liu and T. Tan, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership," *IEEE Transactions on Multimedia*, vol. IV. No.1, 2002, pp. 121-128.
 [12] R. Agarwal, M.S. Santhanam, "Digital Watermarking in the Singular Vector Domain," *International Journal of Image and Graphics*, Vol.8, No.3, pp.351-368, 2008.
 [13] M. Wang, W. Chen, "A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography," *Computer Standards & Interfaces* Vol.31, No.4, pp.757-762, 2009.
 [14] C.C. Chang, P. Tsai, C.C. Lin, "SVD-based digital image watermarking scheme," *Pattern Recognition Letter*, Vol.26, No.10, pp.1577-1586, 2005.
 [15] J. Chen, "Image Robust-Fragile Dual Watermarking Algorithm Based on DWT and SVD," *Journal of Soochow University (engineering science edition)*, Vol.31, No.6, pp.42-48, 2011. (in Chinese).
 [16] X.H. Ma, X.F. Shen, "A Novel Blind Grayscale Watermark Algorithm Based on SVD," *International Conference on Audio, Language and Image Processing*, Shanghai, pp.1063-1068, 2008.
 [17] Z.N. Peng, Y.J. Huang, W.B. Liu, "Color Image Authentication based on Spatiotemporal Chaos and SVD," *Chaos, Solitons and Fractals*, 2008, Vol.36, No.5, pp.946-952.
 [18] C. Venkata Narasimhulu, K. Satya Prasad, "A New SVD based Hybrid Color Image Watermarking for Copyright Protection using Contourlet Transform Decomposition," *International Journal of Computer Applications*, Vol.20, No.8, pp.18-27, 2011.
 [19] C.F. Tsai, W.Y. Yang, "Real-Time Color Image Watermarking Based on D-SVD Scheme," *Lecture Notes in Computer Science*, Vol.4872, pp.289-297, 2007.
 [20] S.P LIU, "Degrees of Irreducible Maps and the Shapes of Auslander-Reiten Quivers," *The Journal of the London Mathematical Society*, Vol. s2-45, No.1, pp. 32-54.

Hongqin Shi was born in Hebei province of China in 1970. She received her BEng. degree and MEng. degree in electronics in computer science from Hebei University of Science and Technology of China and Haerbin University of Science and Technology of China in 1991 and in 2004, respectively.

She has published some 15 papers in journals. She is at present a lecturer at East China Jiaotong University of China. Her current research interests in digital watermark and information security.

Fangliang Lv born in 1972, engineer of East China Jiaotong University, His main research interests include information security.

Yiqin Cao born in 1968, Professor of East China Jiaotong University, His main research interests include information security and wireless sensor networks.