A SVD Feature based Watermarking Algorithm for Gray-level Image Watermark

Wei Wang
College of Computer Science and Technology, Jilin University, Changchun, China
Computer School, Dalian Nationalities University, Dalian, China
Email: wangwei@dlnu.edu.cn

Wenhui Li
College of Computer Science and Technology, Jilin University, Changchun, China
Email:wang09@mails.jlu.edu.cn

Yongkui Liu
Computer School, Dalian Nationalities University, Dalian, China
Email: ykliu@dlnu.edu.cn

Borut Žalik
Computer School, University of Maribor, Maribor, Slovenia
Email: borut.zalik@um.si

***Abstract*—In this paper, a novel gray-level image watermarking algorithm based on Singular Value Decomposition (SVD) feature and neural network is presented for copyright protection. Firstly, a new method which encodes the gray-level secret information into bit string is used. It uses the eigenvalues of SVD to extract the most valuable features of the watermark image and reduces lots of redundant information. Then based on human visual system's characteristic, the SVV (Singular Value and Variance) method is adopted to analyze the host image and choose the regions suitable for watermark embedding. Finally, the back propagation neural network is utilized for watermark recovery. Relying on the information contained in the extracted eigenvalues, the neural network is trained to recognize the original watermark. The application of the proposed scheme makes the gray-level watermark capable of transparent hiding. Results demonstrate that our method is robust to the intentional attacks and performs better than traditional methods.**

***Index Terms*—SVD, Neural Network, Watermarking, Singular Value**

I. Introduction

Digital watermarking is a technique that embeds secret information, such as identifiers, words, image logos and so on imperceptibly into multimedia data to prove data ownership. The special application of digital watermarking technique requires that the embedded watermark should be not only transparent to observers, but also robust enough so that it cannot be easily destroyed or removed after some digital image processing or attacks [1].

According to the practical application, the digital watermarking technologies can be classified into three types including image watermarking algorithm [1], audio watermarking algorithm [2] and video watermarking algorithm [3]. More recent research have turned their attention to image watermarking algorithms and developed many methods including spatial domain method, frequency domain method, physiological model method and so on [4-6].

According to the watermark detection method whether needs original host image, image digital watermarking algorithms can be classified into non blind watermarking algorithm and blind watermarking algorithm [7-9]. Non blind watermarking technology refers to the detection method needs original host image, while blind watermarking algorithm means that the watermark extraction doesn't need original image. In the process of non blind watermark extraction, it is hard to find the original image rapidly and accurately in the massive image database, so it affects the efficiency of watermark extraction. Therefore, blind watermarking algorithm has great research significance and practical value in the current research region of image digital watermark. In this paper, a blind watermark algorithm is developed to realize the digital copyright protection.

Nowadays there are many existing watermarking algorithms based on image watermarks [10-12]. Some methods embed the watermark information through changing the relative relationships of pixel values in spatial domain or the coefficient values of frequency domain [13]. Yoo et al. [13] has proposed a method

This work was supported by the Fundamental Research Funds for the central Universities of China and the National Natural Science Foundation of China (NO.61300089)
Corresponding author: Wenhui Li

doi:10.4304/jcp.9.6.1497-1502

which chooses some intermediate frequency coefficients after discrete wavelet transform and changes the average value of these neighboring coefficients to embed the BCD code of student identifier. The other methods are using coefficient quantization to realize the hiding of watermark. In literature [14], the DCT coefficients are quantified firstly and then be modified according to the value of embedded watermark.

In fact, the visual masking effect is also an important evaluation index of watermarking algorithm. Many algorithms only pay attention to specific watermark information hiding method, while ignoring the position of information hiding. According to Human Visual System (HVS) [15], embedding information in texture areas with high visual masking effect, can not only realize the watermark information hiding, but also can improve the robustness of information hiding. In [16] the authors present a watermarking approach which embeds the singular values (SVs) of the original image into the watermark to attain the lossless objective. The scheme degrades the quality of the embedded watermark image by replacing SVs of the watermark image with those of the original one to some acceptable degree in advance [1]. So in this paper a novel algorithm which uses the characteristics of the Singular Values (SV) to adaptively select watermark hiding position suitable for information hiding in the host image is proposed. The algorithm can not only achieve the purpose of information hiding, but also has large quantitative range of coefficients value changing to ensure the robustness of the algorithm. In addition, because more and more watermarks are gray-level images, this paper proposes a grayscale image watermark algorithm based on the scheme of literature [1]. The overview of the algorithm is shown in Figure 1.

The rest of this paper is organized as follows: Section II introduces our algorithm of watermark preprocessing and host image analyzing in detail. In Section III, we describe the watermark embedding algorithm, extraction algorithm and watermark recovery algorithm respectively. Experimental results are exhibited in Section IV. Finally, conclusions are given in Section V.

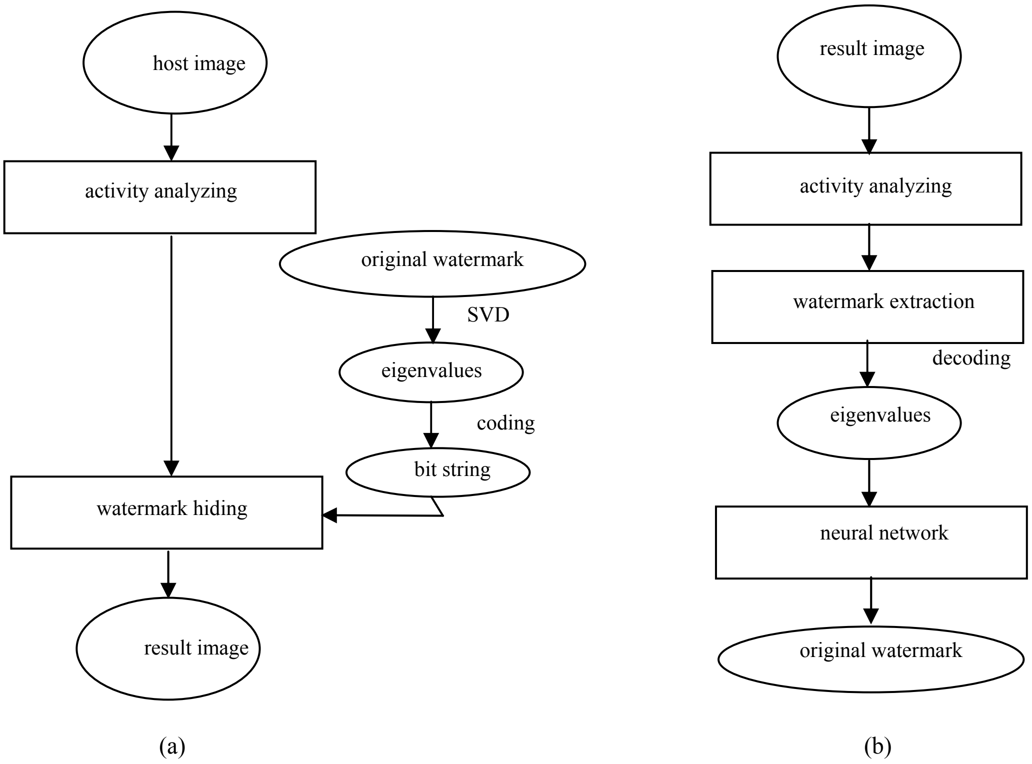

Figure 1. An overview of the proposed watermarking scheme. (a) embedding scheme. (b) extraction scheme

II. IMAGE PREPROCESSING

2.1 Singular Value Decomposition

Singular Value Decomposition (SVD) is one of the most powerful numeric analysis techniques and its application in image compression and image watermarking field is also compelling [17-18].

Let A be a grayscale image with size of m×n. Every real matrix A can be decomposed into three matrices as $A = USV^T$ by SVD, where U and V are orthogonal matrices with size of m×m and n×n respectively, S is a diagonal matrix with the same size as A and with larger singular value entries in decreasing order satisfying $\lambda_{1,1} \ge \lambda_{2,2} \ge \cdots \ge \lambda_{r,r} > \lambda_{r+1,r+1} = \cdots = \lambda_{t,t} = 0$, r is the rank of A ($r \le t,\ t = \min(m,n)$).

$$A=\begin{bmatrix} u_{1,1}, & \cdot\ \cdot\ \cdot, & u_{1,m} \\ u_{2,1}, & \cdot\ \cdot\ \cdot, & u_{2,m} \\ & \cdot & \\ & \cdot & \\ u_{m,1}, & \cdot\ \cdot\ \cdot, & u_{m,m} \end{bmatrix} \begin{bmatrix} \lambda_{1,1}, & 0, & \cdot & \cdot & \cdot, & 0 \\ 0, & \lambda_{2,2}, & \cdot & \cdot & \cdot, & 0 \\ & & \lambda_{r,r}, & \cdot & & \\ & & \cdot & \lambda_{t,t}, & & \\ 0, & 0, & \cdot & \cdot & \cdot & 0 \end{bmatrix} \begin{bmatrix} v_{1,1}, & \cdot\ \cdot\ \cdot, & v_{1,n} \\ v_{2,1}, & \cdot\ \cdot\ \cdot, & v_{2,n} \\ & \cdot & \\ & \cdot & \\ v_{n,1}, & \cdot\ \cdot\ \cdot, & v_{n,n} \end{bmatrix}^{\mathrm{T}} = \sum_{i=1}^{r} \lambda_i u_i v_i^{\mathrm{T}} \quad (1)$$

2.2 Watermark Preprocessing

Most existing digital watermarking methods concentrated on the embedding methods of binary image as the watermark. Along with the development of multimedia and digital watermarking technique, more and more gray-level image watermark algorithms are needed because the gray-level image can take more information. In this paper we improve the method described in [1] and embed the watermark into the host image. The detail of the method is as follows.

Step 1: Perform SVD on the watermark image and extract the first 20 values of matrix S which are called eigenvalues in this paper [1].

Step 2: For every eigenvalue marked as Xi(1<=i<=20), firstly we use the floor(X) function to get the greatest integers less than or equal to X, and then we convert every decimal bit of Xi into binary number[1].

For example, if the eigenvalue Xi is '5379', the result will be ‘0101 0011 0111 1001’ after the operation of step 2.

Step 3: Because most eigenvalues are no more than 10000, we make a length limitation of the encoded eigenvalue to 16 bits. If there are some encoded strings more than 16 bits, from left to right, we mark the first bits which are not belong to the 16 bits as W_high, the length of W_high is recorded as N, and then the first N bits of the encoded minimal eigenvalue is replaced by W_high. The W_high and the original code are separated by the string of ‘1111’ which is not equal to any decimal bit form 0 to 9[1].

For example, if there is an eigenvalue ‘25379’ and its bit string is ‘0010 0101 0011 0111 1001’, a minimal eigenvalue ‘14’ and its bit string is ‘0000 0000 0001 0100’, after Step 3, W_high is marked as ‘0010’, the two eigenvalues are marked as ‘0101 0011 0111 1001’ and ‘0010 1111 0001 0100’ separately.

Step 4: Horizontally concatenates the corresponding binary bit string according to the descending order of the 20 eigenvalues and save as W_encoded which will be embedded into the host image as secret information [1].

2.3 Host Image Analyzing

Based on human visual system’s characteristic, the human eyes have different sensitivity to noise in areas with different luminance and texture. So we analyze the host image before watermark embedding to ensure the imperceptibility of the proposed watermarking scheme. In this paper we adopt the SVV (Singular Value and Variance) method to analyze the host image. The method is described as follows:

Step 1: Divide the host image into 8×8 sub-blocks in spatial domain.

Step 2: Compute each sub-block’s variance V1 and find the maximum value V_max among them. Define the normalized variance as $A1 = V1/V\_\max$.

Step 3: Perform singular value decomposition (SVD) on each sub-block and then computer E of the obtained S matrix.

$$[U\,S\,V] = svd(A), \qquad E = S(1,1)/S(2,2) \quad (2)$$

where A stands for the matrix of the sub-block, svd denotes the operation of SVD, U, S and V are the three result components of SVD transformation. S(1,1) and S(2,2) denote the two maximum values in the diagonal matrix S.

Step 4: Find the maximum value of E marked as E_max and define the normalized E as $A2 = E/E\_\max$.

Step 5: Calculate activity factor AF of each sub-block as

$$AF = \alpha 1 \times A1 + \alpha 2 \times A2 \quad (3)$$

where $\alpha 1$ and $\alpha 2$ are the weights of A1 and A2 with $\alpha 1 + \alpha 2 = 1$.

Step 6: Sort all the sub-blocks’ activity factors in decreasing order. The sub-blocks which have large magnitude of activity factors have complex texture and median luminance and are suitable for embedding watermark with imperceptibility.

After analyzing the host image using our method, we have obtained the activity factors of all the sub-blocks. The high magnitude of activity factor means the corresponding sub-block is not only suitable for embedding watermark but also robust to the attacks. So we select the best sub-blocks which have large values of activity factors and good visual masking effect to embed watermark.

III. Watermarking Algorithm

3.1 Embedding Algorithm

In this sub-section, we employ singular value decomposition to embed watermark into the selected sub-blocks of host image after the preprocessing of the SVV method. Our algorithm is robust because the maximum SV is stable to the attacks that always encountered in digital image processing. SVD_based algorithm is described as follows:

Step 1: Perform SVD on each selected 8×8 sub-block.

Step 2: Choose the maximum SV marked as S(1, 1) in the diagonal matrix S.

Step 3: Use dither modulation method to insert one bit watermark signal into each sub-block according to Formula (4).

$$\begin{array}{lll} L = fix(S(1,1), Q) & & \\ if & W\_encoded\ (i) == 1 & S(1,1) = L \times Q \\ else & W\_encoded\ (i) == 0 & S(1,1) = L \times Q + Q/2 \end{array} \quad (4)$$

where L denotes the integer part of the result of S(1, 1)/Q, W_encoded denotes the watermark bit and Q denotes the quantization step.

Step 4: Perform the inverse SVD on each sub-block to get the modified sub-image.

Step 5: Embed the watermarked sub-image back into the original host image.

3.2 *Extraction Algorithm*

Watermark extraction algorithm is the exact inverse process of embedding algorithm. Watermark could be extracted without the original host image as soon as we get the secret keys.

Step 1: The value of extracted bit for a given sub-block is calculated according to Formula (5).

$$\begin{array}{ll} Z = \mathrm{mod}(\ S * (1,1), Q\ ) & \\ if\ (Z - Q/2) < Q/4 & W\_\mathrm{recover}\ \ (i) = 0 \\ else & W\_\mathrm{recover}\ \ (i) = 1 \end{array} \quad (5)$$

where Z stands for the modulus after division of S*(1, 1) and Q, Q is transmitted as secret key.

Step 2: Decode the obtained W_recover according to the inverse order of coding and record the result as W_Decoded. W_Decoded denotes the eigenvalues of the watermark.

Step 3: Use Neural Network to regain the hidden watermark.

In this paper, we utilized the method based on back propagation (BP) neural network (NN) for watermark recovery [19-20]. Relying on the information that the extracted eigenvalues contained, the neural network is applied to recognize the original watermark. This method is able to associate the accurate content of watermark, which contributes a lot to the work of tracing multimedia data distribution.

3.3. *Neural Network Training*

In this sub-section, the work of training neural network is done to make it possess the capability of memorizing the characteristics of different watermarks. First, a huge number of watermarks are collected as the training set which we have performed different kinds of attacks on them with distinct factors. Then we take each watermark as data matrix X and get the first 20 eigenvalues after performing SVD as the neural network input feature. Every unique output node is assigned to every different watermark. The 20 eigenvalues marked as $B_k = (a_1, a_2, \cdots, a_p)$ while the NN output marked as $Y_k = (y_1, y_2, \cdots y_q)$ form the training-pair patterns, where p stands for the number of input nodes, q denotes the number of output nodes and k is the total number of training patterns of training set. The structure of the BP neural network is three layers including an input layer with 20 nodes, a hidden layer with 35 nodes, and an output layer with q nodes which can be easily changed in the training process according to the actual number of different watermarks.

3.4. *Watermark Recovery based on the BPNN*

The trained neural network performs a highly adaptive ability of recognition. Take the regained 20 eigenvalues which were extracted from the host image following the instruction of the former sections as input pattern and feed them to the BP neural network. The exact original watermark will be recognized by the network according to the identifier of output pattern.

IV. Results and Discussion

Figure 2 and Figure 3 are the result images of test images ‘Barbara’ and ‘Baboon’ of size 512×512. Figure 4 and Figure 5 show the original gray-level watermark of size 64×64 , 128×128. Taking ‘Baboon’ image for example, in the experiment we first calculate each sub-block’s activity factor according to the image’s texture and gray information. The watermarks as shown in Figure 4(a) and Figure 5(a) are respectively embedded into the selected sub-blocks using our algorithm. In the process of embedding, the weights value of $\alpha 1$ and $\alpha 2$ used in the experiments are set to 0.1 and 0.9 respectively, and the quantization step used is set to 55.

The PSNR (peak signal-to-noise ratio) is used in this paper to access the imperfectability of our algorithm, as follows:

$$PSNR = 10 \times \log_{10}\left(\frac{M \times N \times \max(I^2(i,j))}{\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - I*(i,j)]^2}\right) \quad (6)$$

where I(i, j) denotes the gray value of host image pixel, I*(i, j) denotes the gray value of watermarked image pixel, M and N are the height and width of host image.

Because of the encoding processing for the watermarks of the proposed algorithm, the sizes of the watermarks are independent on our embedding scheme. Table 1 shows the PSNR results of different watermarked host images which have hidden different sizes of watermarks. All the results of PSNR are capable to insure the fidelity of the watermarked host images.

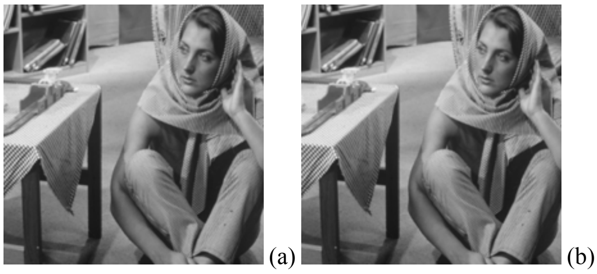

Figure 2. (a) Original host image ‘Barbara’. (b) Watermarked image

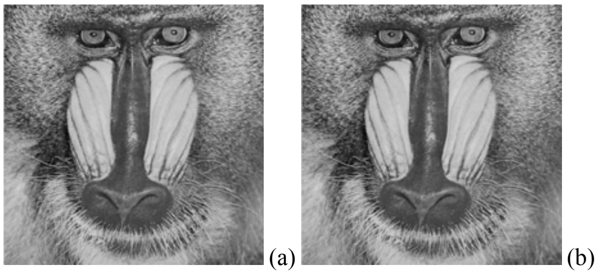

Figure 3. (a) Original host image ‘Baboon’. (b) Watermarked image

Figure 4. (a) Original watermark 'Logo' of size 64×64. (b) Watermark extracted from Figure 3(b) after watermark recovery

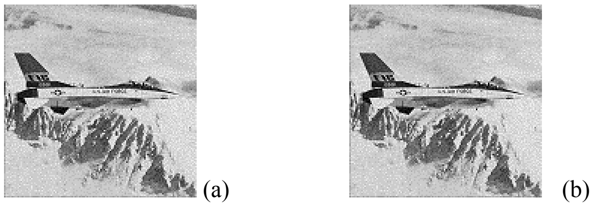

Figure 5. (a) Original watermark 'Airplane' of size 128×128. (b) Watermark extracted from Figure 3(b) after watermark recovery

TABLE 1.
THE PSNR OF DIFFERENT WATERMARKED HOST IMAGES FREE OF ANY ATTACKS

Host image Watermark		Barbara	Baboon
Logo	64×64	41.7439	42.4396
Airplane	128×128	41.6653	42.8744

TABLE 2.
THE RESULT OF WATERMARK RECOVERY AFTER JPEG 30% ATTACK BASED ON BPNN

after JPEG 30% attack	Barbara	Baboon
Watermark total number	20	20
Right recognized number	20	19
Wrong recognized number	0	1
Precision	100%	95%

TABLE 3.

THE RESULT OF WATERMARK RECOVERY AFTER MULTIPLE ATTACKS BASED ON BPNN

after crop 50% + Noise 2%	Barbara	Baboon
Watermark total number	20	20
Right recognized number	18	19
Wrong recognized number	2	1
Precision	90%	95%

In the watermark recovery sub-section, the extraction results are first decoded into the regained eigenvalues of the watermark, and then fed to the BPNN. Figure 4 (b) and Figure 5 (b) show the result original watermarks that recognized by the NN. In the experiment, the eigenvalues of 20 gray-level watermark images are extracted and trained in the proposed BPNN. Table 2 and Table 3 shows the watermark recovery results after different attacks based on BPNN, where 'JPEG 30%' means JPEG compression with quality factor of 30% , 'crop 50% + Noise 2%' means crop the watermarked image with the ratio of 50%, and then add the Pepper and Salt noise with the density of 2%. The precision for different attacks indicates that the proposed algorithm is robust and the watermark recovery for gray-level watermark images is flexible and applicable.

V. CONCLUSION

In this paper, a novel technique of digital image watermarking has been discussed. Our method is a new algorithm that employs the SVD to encode the gray-level watermark and extract watermark. We have utilized the characteristics of singular values and variance to preprocess the host image and then embed the watermark into the selected sub-blocks. Results demonstrate the excellent performance on both robustness and transparency of our scheme.

REFERENCES

[1] Wei Wang, Chengxi Wang, "A Watermarking Algorighm for Gray-level Watermark based on Local Feature Region and SVD", *International Congress on Image and Signal Processing*, 2008, 650-654.

[2] Shuo-Tsung Chen, Huang-Nan Huang, Chur-Jen Chen, Kuo-Kun Tseng, Shu-YiTu, "Adaptive audio watermarking via the optimization point of view on the wavelet-based entropy", *Digital Signal Processing*, 23 (2013) 971–980.

[3] Th. Rupachandra Singh, Kh. Manglem Singh, Sudipta Roy, "Video Watermarking Scheme based on Visual Cryptography and Scene Change Detection", *International Journal of Electronics and Communications*, Volume 67, Issue 8, August 2013, Pages 645–651.

[4] Frederic Lusson, Karen Bailey, Mark Leeney, Kevin Curran. "A Novel Approach to Digital Watermarking, exploiting Colour Spaces", *Signal Processing*, 93 (2013) 1268–1294.

[5] F. Qi, J. Wu, G. Shi, "Extracting Regions of Attention by Imitating the Human Visual System", *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, 2009, 1905–1908.

[6] S.P. Mohanty, P. Guturu, "A Novel Invisible Color Image Watermarking Scheme using Image Adaptive Watermark Creation and Robust Insertion-Extraction", *ACM Transactions on Multimedia Computing Communications and Applications*, 5(2), 2008, 1–24.

[7] Yong C Kim, et al. "Two-Step Detection Algorithm in a HVS-based Blind Watermarking of Still Images". *Lecture Notes in Computer Science*, Springer-Verlag Heidelberg, 2003, 2613: 235-248.

[8] Huang Jiwu, G F Elmasry. "An Algorithm for Meaningful Watermarks Based on Matched Filtering", *ACTA ELECTRONICA SINICA*, 2001, 29 (4), 447-451.

[9] Yongwon Jang, Intaek Kim, et al. "Blind Watermarking Algorithm Using Complex Block Selection Method". *Lecture Notes in Computer Science*, Springer-Verlag Heidelberg, 2001, 2195: 996.

[10] M.V.S.S. BABU. "A Robust Watermarking Algorithm for Image Authentication", *International conference of information and network technology*, 2012, 200-207.

[11] Wei Wang, Wenhui Li, Chengxi Wang, Huijie Xin. "A Novel Watermarking Algorithm based on SURF and SVD", *TELKOMNIKA*, VOL. 11, No 3, 2013, 1560-1567.

[12] Tai-yue Wang, Hong-wei Li, "A Novel Robust Color Image Digital Watermarking Algorithm Based on Discrete Cosine Transform", *Journal of Computers*, VOL.8, NO.10, 2013, 2507-2511.

[13] Kil-Sang Yoo, et al. "A Wavelet-based Blind Watermarking Technique for Real-time Watermark Interpretation". *Lecture Notes in Computer Science*, Springer-Verlag Heidelberg, 2003, 2668: 348-355.

[14] Piva A, Barni M, et al. “DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image”. *Proceedings of International Conference on Image Processing*, USA, 1997. 520-523.

[15] Huiyan Qi, Dong zheng, Jiying Zhao, “Human visual system based adaptive digital image watermarking”, *Signal Processing*, 88(2008) 174-188.

[16] Jieh Ming Shieh, Der Chyuan Lou, Ming Chang Chang. "A semi-blind digital watermarking scheme based on singular value decomposition". *Computer Standards & Interfaces*, 28(2006), 428-440

[17] E. Ganic, A. M. Eskicioglu. "Robust DWT-SVD domain image watermarking: embedding data in all frequencies". *Proceedings of the 2004 Multimedia and Security Workshop on Multimedia and Security*, 2004, 166-174

[18] CAI Yong-mei, GUO Wen-qiang, DING Hai-yang, "An Audio Blind Watermarking Scheme Based on DWT-SVD", *Journal of Software*, VOL.8, NO.7, 2013, 1801-1808.

[19] Yinghua Lu, Wei Wang, Jun Kong. "A robust watermarking algorithm based on SVD and neural network". *2005 Asia-Pacific workshop on visual information processing, IEEE SMC Society Hong Kong Chapter*, Hong Kong, 165-170.

[20] HE Dong-xiao, ZHOU Chun-guang, LIU Miao, MA Jie, "Approach for Constructing Neural Network Ensemble Applied to Handwritten Digit Recognition", *Journal of Jilin University*, 2009, 47(6), 1211-1216.

Wei Wang was born in 1981. She is a lecturer in College of Computer Science and Technology, Dalian Nationalities University, Dalian, China. Her major research interests include computer vision, image processing and information security.

Wenhui Li was born in 1961. He is a Professor and doctor supervisor in College of Computer Science and Technology, Jilin University, Changchun, China. His major research interests include computer vision, image processing and computer graphics.

Yongkui Liu was born in 1961. He is a professor in Computer Science Department, Dalian Nationalities University, Dalian, China. He obtained his PhD degree in CAD and computer graphics from Zhejiang University in 1999. His research interests include computer Graphics, pattern recognition and image processing.

Borut Žalik is a professor of Computer Science in University of Maribor, Slovenia. He obtained PhD degree in computer science in 1993 from the University of Maribor, Slovenia. He is the head of Laboratory for Geometric modeling and multimedia algorithms. His research interests include computational geometry, geometric data compression, scientific visualization and geographic information systems. He is an author or co-author of more than 70 journal and 90 conference papers.