International Journal of Control and Automation
Vol. 9, No. 11 (2016), pp.295-304
http//dx.doi.org/10.14257/ijca.2016.9.11.25

A Grayscale Images Watermark Authentication System Based on SVD

Xu Zhan[1, 3], Ping He[1, 2] and Yue-Rong Lei[1,3]

[1] *School of Automation and Electronic Information, Sichuan University of Science & Engineering, Zigong, Sichuan 643000, People's Republic of China*
zhanxuu@163.com
[2] *Department of Electromechanical Engineering, Faculty of Science and Technology, E11, University of Macau, Avenida da Universidade, Taipa, 999078, Macao Special Administrative Region of the People's Republic of China. pinghecn@126.com; pinghecn@qq.com*
[3] *Artificial Intelligence Key Laboratory of Sichuan Province, Sichuan University of Science & Engineering, Zigong, Sichuan 643000, People's Republic of China*

Abstract

*The paper proposes a grayscale images watermark authentication system based on SVD. The grayscale image is divided into the pieces of size 16*16. Each small piece is made into DCT transform and extracted low frequencies to generate the watermark image. Then, the watermark image is made in Arnold scrambling algorithm and embedded in SVD algorithm. The hash algorithm is used to generate authentication code. In the authentication stage, when the image was tampered and attacked, the system can effectively lock the tamper region.*

Keywords:*-SVD, authentication, lock tampering*

1. Introduction

Digital watermarking technology is more and more widely used in many fields, such as digital video, music and so on, to protect intellectual rights. According to the ability against the attack, digital watermarking technology is classified to robust watermarking, fragile watermarking technology and semi-fragile watermarking technology. The watermark image can be extracted although the images are under attack if the watermark image is used in robust watermarking technology. If used in fragile watermarking technology, the watermark image may not be extracted under attack. The semi-fragile watermarking technology can resist some attacks such as adding noise, jpeg compression, *etc*. and locate the tamper area. So it is widely used in many fields[1-8].

The digital watermarking technology is divided to two technologies, one is information security technology and the other is image watermarking technology. In information security technology, the image is encrypted to hide data to prevent unauthorized access. In the image watermarking technology, the watermark image is embedded into the original image. And the system should detect whether the image is tampered when suffering attack. The watermark image also should not degrade the carrier image's quality and should be invisible. The image authentication techniques are classified into two groups. One group is the techniques of embedding the watermark image in spatial domain, and the other one is the techniques of embedding the watermark image in frequency domain.

Our proposed system is in frequency domain method. The grayscale image is divided into the pieces of size 16*16. Each small piece is made into DCT transform and extracted low frequencies to generate the watermark image. Then, the watermark image is made in Arnold scrambling algorithm and embedded in SVD algorithm. The hash algorithm is used to generate authentication code. In the authentication stage, when the image was tampered and attacked, the system can effectively lock the tamper region.

ISSN: 2005-4297 IJCA

2. DCT

The Discrete Cosine Transform (DCT) is associated with the Fourier Transform, it is similar to the Discrete Fourier Transform (DFT for Discrete' Fourier Transform), but only use the real number.

The original image is made in Discrete Cosine Transform(DCT) transform. The formula is shown in the following.

$$F(0,0)=\frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\,,\qquad u=0,v=0 \tag{1}$$

$$F(u,0)=\frac{2}{\sqrt{N}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\left[\frac{\pi}{2N}(2x+1)u\right],\quad v=0,\ u=1,2,\cdots,N-1 \tag{2}$$

$$F(0,v)=\frac{2}{\sqrt{N}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\left[\frac{\pi}{2N}(2y+1)v\right],\quad u=0,\ v=1,2,\cdots,N-1 \tag{3}$$

$$F(u,v)=\frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\left[\frac{\pi}{2N}(2x+1)u\right]\cos\left[\frac{\pi}{2N}(2y+1)v\right] \tag{4}$$

$$u,v=1,2,\cdots,N-1$$

And the formula of Inverse Discrete Cosine Transform (IDCT) is shown in the following.

$$\begin{aligned}f(x,y)=&\frac{1}{N}F(0,0)\\&+\frac{2}{\sqrt{N}}\sum_{u=1}^{N-1}F(u,0)\cos\left[\frac{\pi}{2N}(2x+1)u\right]\\&+\frac{2}{\sqrt{N}}\sum_{v=1}^{N-1}F(0,v)\cos\left[\frac{\pi}{2N}(2y+1)v\right]\\&+\frac{2}{N}\sum_{u=1}^{N-1}\sum_{v=1}^{N-1}F(u,v)\cos\left[\frac{\pi}{2N}(2x+1)u\right]\cos\left[\frac{\pi}{2N}(2y+1)v\right]\end{aligned} \tag{5}$$

Discrete cosine transform is often used by signal processing and image processing, is used to signal and image (still images and motion images) data compression. This is due to the discrete cosine transform has a strong focus on "energy" features, most of the natural signals (including the voice and image) of the energy is concentrated in the low frequency after the discrete cosine transform, and the high-frequency information is just the profile and edges information. The low-frequency information is used as the watermark image in this paper.

3. The Singular Value Decomposition Algorithm

Singular value decomposition is important matrix decomposition in linear algebra and is widely used in many fields, such as signal processing, statistics, *etc*. Digital images can be expressed as a lot of nonnegative scalar matrix. SVD(singular value decomposition) is a numerical technology to make the matrix diagonalization and has been widely applied to image coding and other signal processing. The singular value decomposition has the feature that an image of the singular value has quite good stability in image processing, When the image suffer slight disturbance, its singular value is not going to be changed. A digital image can be composed of a lot of nonnegative scalar matrix in linear algebra. A image matrix is expressed as $X\in R^{N*N}$, where R is real number domain. The singular value decomposition of X is shown in the following.

$$X = USV^T \tag{6}$$

Where $U\in R^{N*N}$ and $V\in R^{N*N}$ are the orthogonal matrix, $S\in R^{N*N}$ is the diagonal matrix. The diagonal elements are satisfied the following formula.

$$l_1 \geq l_2 \geq \ldots \geq l_r \geq l_{r+1} = \ldots = l_N = 0 \quad (7)$$

Where r is the rank of X; $l_i (1 \leq i \leq N)$ is called the singular value of X.

The singular value is the inner algebraic features of the image and can be used as one of image features. The singular value has good stability. when the image is slightly disturbed, the singular values of image is not going to change.

4. Arnold Transform

The image is made as a binary function in planar region in Arnold transform.

$$Z = F(x, y), (x, y) \in R \quad (8)$$

Where R usually is a rectangle. Any element of R reprents the information of the image. The discrete Amold transform formula is shown in the following.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ N) \quad (9)$$

(x, y) represents an element of the image when their position did not change. (x', y') represents an element of the image when their position changed. The watermark image is transformed from clear to fuzzy in Arnold transform. After extracting the watermark, the original watermark image is get in Arnold transform. The Arnold period transformation table is shown in the following.

Table 1. The Arnold Period Transformation Table

The image size	period
32*32	24
64*64	48
128*128	96
256*256	192

5. A Grayscale Images Watermark Authentication System Based On SVD

5.1. Generating the Watermark Image

input: the original grayscale image, the private key(K)

output: the watermark image

i. the original image is divided into 16 *16 pieces,

ii. the each piece is made into DCT transform and the low frequencies is extracted to generate the watermark image.

iii. the watermark image is made in Arnold scrambling algorithm.

iv. the watermark image the lowest bit is replaced by the private key(K),

v. the watermark image is obtained

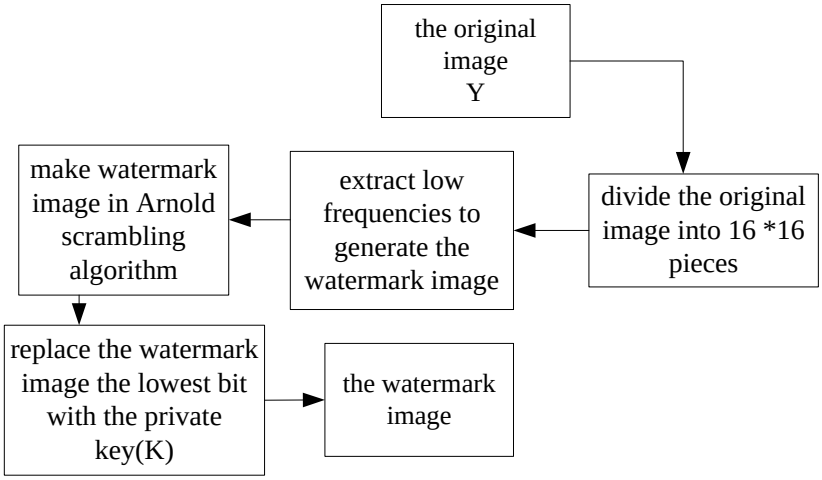

Figure 1. Generating the Watermark Image

5.2. Embedding the Watermark Image

input: the original grayscale image(Y), the watermark image, the private key(K'),the public key(Qkey)

output: the watermarked image(Y*), message authentication code(M)

i. Y is made in the SVD algorithm,

$$Y = USV^T \tag{10}$$

ii. the watermark image is superimposed on the diagonal matrix S to get a new matrix S', $S' = S + \alpha W$ (11)

ii. the new matrix S' is made into the singular value decomposition,

$$S' = U_1 S_1 V_1^T \tag{12}$$

where U1, V1 are keys,

iii. the watermarked image is obtained,

$$Y^* = US_1V^T \tag{13}$$

v. the message authentication code is generate, M*= encrypt (hash(Y, Y*),K'),where K' is a key,

vi. I= encrypt（Y,Y*,M*,Qkey）

vii. the information I is sent in the common channel.

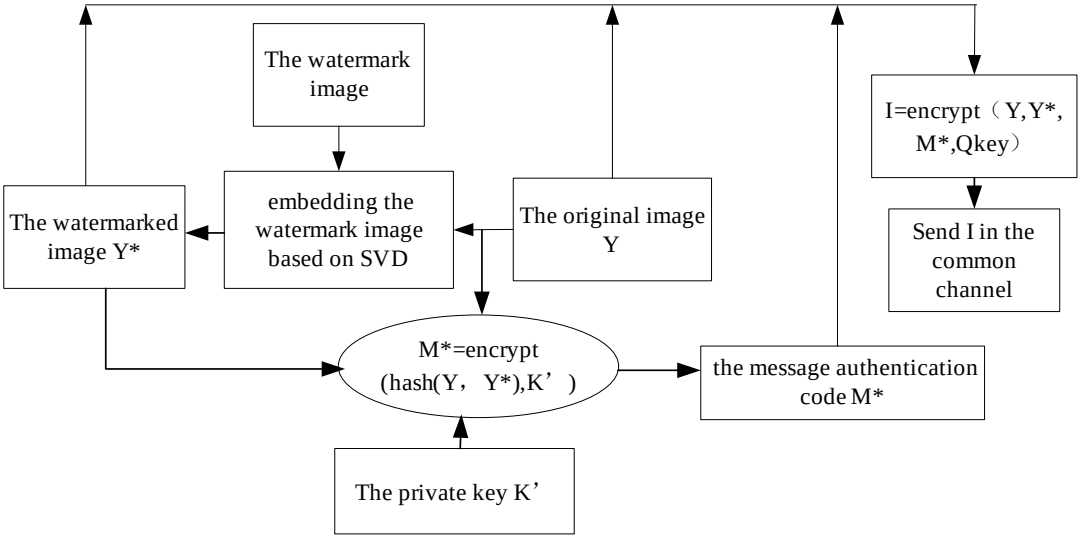

Figure 2. Embedding the Watermark Image

5.3. Extracting the Watermark Image and Image Authentication

input: the information I, the private key(Pkey)

output: authentication information

i. (Y, Y*,M*)= decrypt (I,Pkey);

ii. M’= encrypt (hash(Y， Y*),K’), where K’ is a key,

iii. M’ is compare with M* , if they are same, the image is intact, if not, the image was tampered.

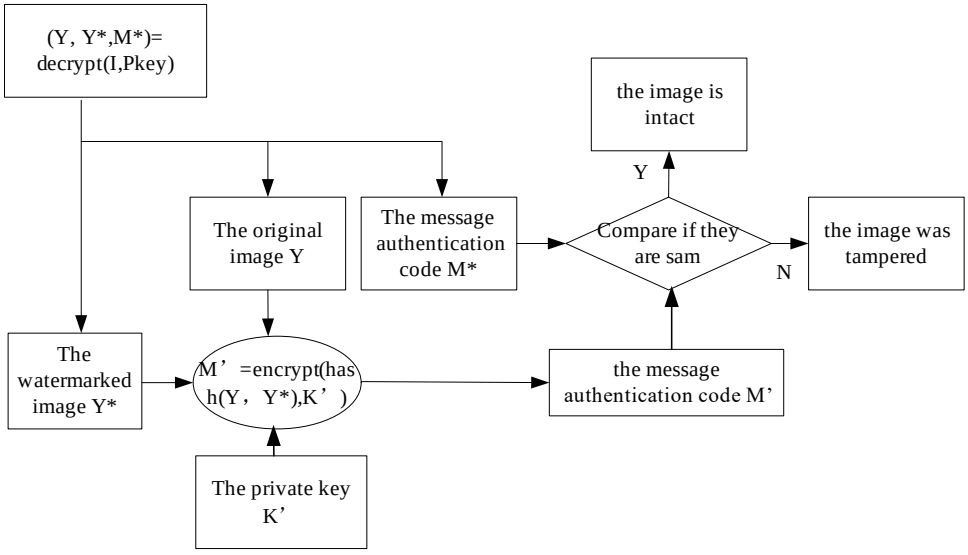

Figure 3. Extracting the Watermark Image and Image Authentication

5.4. Tamper Localization

If the image was tampered, the tampered place should be localized. The step is shown in the following.

input: the original image Y, and the watermarked image Y*

output: localize the tampered place

i. generate the new watermark image W' with size m*n from the original image Y ,

ii. extract the watermark image W* with size m*n from the watermarked image Y*,

a. make the watermarked image Y* the singular value decomposition,

$$Y^* = U^* S_1^* V^{*T} \tag{14}$$

b. calculate the intermediate matrix,

$$D^* = U_1 S_1^* V_1^T \tag{15}$$

c. obtain the watermark image,

$$W^* = \frac{1}{\alpha}(D^* - S) \tag{16}$$

iii.XOR W* and W' to locate the tampered place.

6. Experiment

In order to test the system' robustness and imperceptibility, we did the experiment. The image lena of size 512*512 is used as the original image. Figure 4-9 are shown the original mage, the watermarked image, the watermark image and the extracting watermark image before or after Arnold algorithm. Table 2 is shown the results of NC.

Figure.4 The Original Image

Figure 5 The Watermarked Image

Figure 6. The Watermark Image of Insertion

Figure 7. The Watermark Image of Extraction

Figure 8. The Embedding Watermark Image In Arnold Algorithm

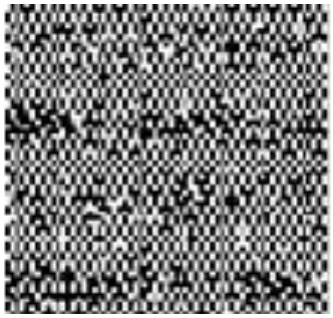

Figure 9. The Extract Watermark Image In Arnold Algorithm

Table 2. Data of the Image

	name	Size(pixel)	
Fig.5	the original image	512*512	NC=0.98
Fig.6	the watermarked image	512*512	
Fig.7	the watermark image of insertion	256*256	NC=0.99
Fig.8	the watermark image of extraction	256*256	

From the table 1, the results are shown the proposed system has good imperceptibility.

In order to test the robustness of the system, the detecting the noise and preventing be tampered test is made in the experiment. Figure 10 to Figur.15 are shown the images of adding t noise and being tampered, the results of locking the place of the image being tampered.

Figure 10. The Image of Adding Saltand Pepper Noise

Figure 11. Locking the Tamper Region

Figure 12. The Image Of Adding Gaussian Noise

Figure 13. Locking the Tamper Region

Figure 14. The Image of Being Tampered

Figure 15. Locking the Tamper Region

From the Figure 10 to Figure 15, we know the system can effectively lock tampered region when the image was tampered.

7. Conclusion

A grayscale images watermark authentication system based on SVD is proposed. In order to test the robustness of the system, we did experiment. The result is shown that the system can make the image invisible and when the image was tampered, the system can effectively lock tampered region.

Acknowledgments

This work was jointly supported by Research Foundation of Department of Education of Sichuan Province(Grant nos. 14ZA0203 and 14ZB0210), Open Foundation of Enterprise Informatization and Internet of Things Key Laboratory of Sichuan Province (Grant nos. 2014WYJ01 and 2013WYY06), Open Foundation of Artificial Intelligence Key Laboratory of Sichuan Province (Grant nos. 2014RYY02, and 2013RYJ01), Science Foundation of Sichuan University of Science & Engineering (Grant no. 2014PY14).

References

[1] Y.S. Liu, "Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map", optics and laser technology, vol. 60, no. 2, **(2013)**, pp. 111-115.
[2] M.R. Abuturab, "An asymmetric color image cryptosystem based on Schur decomposition in gyrator transform domain", optics and Lasers in Engineering, vol. 58, no.42, **(2014)**, pp. 39-47.
[3] Y. Zhou, W. Cao and C. Chen, "Image encryption using binary bitplane", signal processing, vol. 100, no.7, **(2014)**, pp. 197-207.
[4] Q. Ran, T. Zhao, L. Yuan, J. Wang and L. Xu, "Vector power multiple-parameter fractional Fourier transform of image encryption algorithm", Optics and Lasers in Engineering, vol. 62, no.6, **(2014)**, pp.80–86.
[5] D. Sharma and R. Saxena, "A Novel Image Encryption Scheme based on Multiple Parameter Discrete Fractional Fourier Transform", International Journal of Computer Applications, vol. 93, no.20, **(2014)**, pp. 93:9-16.

[6] T. Ran, L. Jun and W. Yue, "Optical image encryption based on the multiple-parameter fractional Fourier transform", Optics Letters, vol. 33, no.6, **(2008)**, pp.581-583.
[7] J. Lang, "Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform", Optics Communications, vol. 285, no.7, **(2012)**, pp. 929–937.
[8] Q.H. Alsafasfeh and A.A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal & Information Processing, vol. 2, no.3, **(2011)**, pp. 238-244.
[9] K. Wang，L. Zou，A. Song and Z. He, "On the security of 3D Cat map based symmetric image encryption scheme", Physics Letters A, vol.343, no.6, **(2005)**, pp. 432-439.
[10] K. Wang，J. Chen，W. Zhou，Y. Zhang and Y. Yan, "Direct Growth of Highly Mismatched Type II ZnO/ZnSe Core/Shell Nanowire Arrays on Transparent Conducting Oxide Substrates for Solar Cell Applications", Advanced Materials, vol.20, no.17, **(2008)**, pp. 3248-3253.
[11] Y.F. Zhu，G.H. Zhou and H.Y. Ding， "Synthesis and characterization of highly-ordered ZnO/PbS core/shell heterostructures", Superlattices and Microstructures, vol.50, no.5, **(2011)**, pp. 549–556.
[12] S.Kandula and P. Jeevanandam, "Visible-light-induced photodegradation of methylene blue using ZnO/CdS heteronanostructures synthesized through a novel thermal decomposition approach", Journal of Nanoparticle Research, vol.16, no.6, **(2014)**, pp. 1-18.
[13] J.Z. Kong and A.D. Li, "Photo-degradation of methylene blue using Ta-doped ZnO nanoparticle", Journal of Solid State Chemistry, vol.183, no.6, **(2010)**, pp. 1359–1364.
[14] V. Luca and M. Osborne, "Photodegradation of Methylene Blue Using Crystalline Titanosilicate Quantum-Confined Semiconductor", Chemistry of Materials, vol.18, no2.6, **(2006)**, pp. 6132-6138.

Authors

Xu Zhan, she received the B.S. Degree in Electronic Information from Sichuan normal University, in Chengdu, Sichuan, People's Republic of China and the M.S. Degrees in Signal Processing from Sichuan University in Chengdu, Sichuan, China, in 2004 and 2007, respectively. She is currently a lecturer with the School of Automation and Electronic Information, Sichuan University of Science & Engineering, in Zigong, Sichuan, China, from 2009. His research interests include Technology and application of microcontrollers, signal processing.

Ping He, he was born in Nanchong, Sichuan, People's Republic of China, in October 1990. He received the Bachelor degree of Engineering from the School of Automation and Electronic Information, Sichuan University of Science & Engineering at Zigong, Sichuan, China, in June 2012. He received the Master degree of Engineering from the School of Information Science & Engineering, Northeastern University at Shenyang, Liaoning, China, in July 2014. He is currently a PhD degree candidate and Research. Assistant in the Department of Electromechanical Engineering, Faculty of Science and Technology, University of Macau, Taipa, 999078, Macao Special Administrative Region of China, from September 2014. His main research interests include Control of PDEs, Synchronization of complex networks, Consensus of multi-agent systems, nonlinear systems.

Yue-Rong Lei, he received the B.S. Degree in Automatic Control from Sichuan University of Science & Engineering, in Zigong, Sichuan, People's Republic of China in 2008, He is currently an Associate Professor with the School of Automation and Electronic Information, Sichuan University of Science & Engineering, in Zigong, Sichuan, China, from 2008. His research interests include Technology and application of microcontrollers, Intelligent control and Chaos control.