IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 3, Ver. II (May - Jun. 2014), PP 45-50
www.iosrjournals.org

Chaos Encryption Based DWT-SVD Watermarking

Anumol Joseph[1], K. Anusudha[2]
[1]*(Department of Electronics Engineering, Pondicherry University, India)*

Abstract : *The progress in computer network technology, processing, reproducing and distribution of digital images has becomes very easy. Apart from its advantages, it also gives an opportunity to the attacker or illegal user. Two major approaches available to protect digital images are watermarking technique and encryption technique. This paper presents a combined watermarking and encryption method to further improve the security of the images. It uses Discrete Wavelet Transform (DWT) – Singular Value Decomposition (SVD) watermarking technique and chaotic encryption method. After embedding the two watermark images into the host image it is encrypted and transmitted. At the receiver side it is decrypted and the watermarks are recovered. Simulation results prove that the proposed method is simple and more secure.*

Keywords: *Discrete Wavelet Transform, Normalized Correlation Coefficient (NCC), Singular Value Decomposition*

I. Introduction

The significance of multimedia communication and information security are tremendously increasing day by day. It will continue to play important roles in the information era. The main aim is to provide secure delivery of multimedia data. Cryptography and watermarking are the two techniques which provide the security. Watermarking technique is mainly used for copy right protection. In this case the host image is the object of communication and the protection of its ownership is the aim of the hiding technique. On the other side, cryptography encrypts the messages: it focuses on rendering information not intelligible to any unauthorized entity who might intercept them. Here the data is kept secretly and securely.

The main characteristics of watermarking technique are robustness, transparency and capacity. Transparency implies the imperceptibility of the technique. After insertion of watermark into the original image it should not be distorted [1, 2]. Robustness is related to attacks. If the watermarked image can withstand the attacks then the scheme is said to be robust [3, 4]. Capacity refers to the amount of data are inserted to the cover image. More capacity means one can hide large amount of information.

The proposed method uses a hybrid DWT-SVD-based watermarking scheme that requires less computation effort to yield better performance. Two images are watermarked in the intermediate frequency bands of the cover image after third level DWT decomposition. It is done by changing the singular values of the LH and HL bands of the host image. The watermarked image is then encrypted using chaos based encryption technique to improve security of images.

The paper is organized as follows. Section II discusses about DWT. Section III explains the SVD. Proposed system is described in section IV. Section V gives the simulation results and section VI projects the performance analysis. Finally section VII gives the conclusion.

II. Discrete Wavelet Transform

Wavelet domain is identified as an important domain for watermarking technique .Wavelet contains small waves. Discrete Wavelet Transform is based on small waves of limited duration and varying frequency [5]. It is a frequency domain technique in which the host image is transformed into frequency domain and then its coefficients are modified in accordance with the transformed coefficients of the watermark. DWT provides both spatial and frequency description of the image [6]. It decompose an image in basically three spatial directions horizontal, vertical and diagonal in result separating the image into four different components namely LL, LH, HL and HH.

III. Singular Value Decomposition

Let A be a general real matrix of order m x n and its SVD is the factorization:

$$A=PQR^T \tag{1}$$

Where P and R are orthogonal (unitary) matrices and Q = diag ($\lambda_1, \lambda_2, ..., \lambda_r$), where λ_i, i = 1 to r are the singular values of the matrix A with $r = min(m, n)$ and it satisfies:

$$\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_r \tag{2}$$

The first r columns of P and R are the left and right singular vectors of A respectively. There are many advantages to use SVD in digital image processing. Firstly, the SVD transformation can be applied to an image processing is performed. Lastly singular values contain intrinsic algebraic properties of an image.

IV. Proposed System

The proposed scheme combines DWT-SVD watermarking and chaotic encryption method. Two watermark images are embedded in the LH and HL bands of the cover image after third level DWT decomposition. The embedding is done by modifying the singular values in LH and HL bands of the cover image with the singular values of the watermark images. Embedding is followed by chaotic encryption method to improve the security. Fig.1 shows the proposed system.

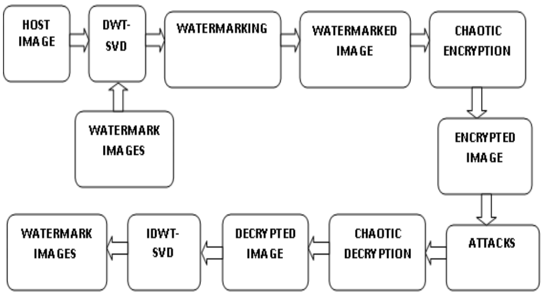


Fig. 1: Proposed system

4.1 Algorithm – Embedding the watermark

a) Apply 3-level Haar wavelet transform on the host image A.

b) Perform SVD to HL and LH sub bands of the host image.

$$A^k = P^k\, Q^k\, R^{kT} \quad , \quad k=1, 2 \tag{3}$$

where *k* represents one of two sub bands.

c) Apply first level Haar wavelet transform to the watermark images.

d) Perform SVD to HL, LH sub bands of watermark image 1 and watermark image 2 respectively.

$$W^k = P_W^k Q_W^k R_W^{kT} \tag{4}$$

e) Modify the singular values in HL and LH subbands of the host image with the singular values in HL and LH sub bands of the watermark image 1and watermark image 2 respectively.

$$Q_{WM}^k = Q^k + \alpha Q_W^k \tag{5}$$

f) Obtain the modified DWT coefficients

$$A^{*k} = P^k\, Q_{WM}^k\, R^{kT} \tag{6}$$

g) Apply inverse DWT using two sets of modified DWT coefficients and two sets of non modified DWT coefficients to obtain the watermarked image A_{WM}[11,12].

4.2 Encryption

The chaos-based encryption was first introduced in 1989 [8]. Chaotic system has many properties such as sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity, etc. It motivated many researchers to work in this field. One of the simple chaos functions for cryptography applications is the logistic map. It is defined as:

$$X_{n+1} = r\, X_n\, (1-X_n) \tag{7}$$

Where X_n takes values in the interval [0, 1] and r is in the range of 3.5 to 4. Fig. 2 shows the encryption-decryption block diagram [10].

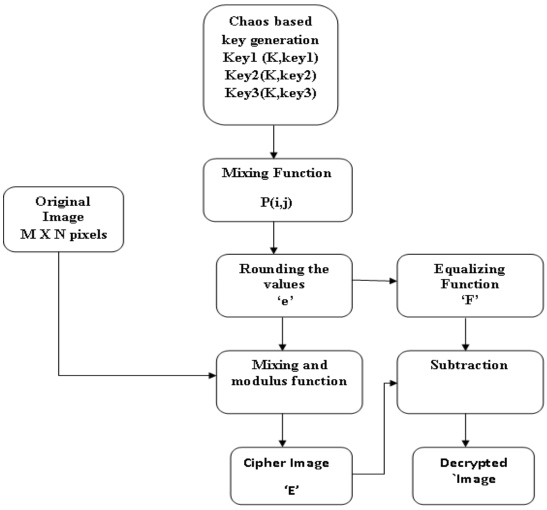


Fig. 2: Encryption and decryption

4.2.1 Encryption Algorithm

a) Iterate the logistic map equation key 1 into 'h' times.

$$\text{key } 1 = K*\text{key } 1*(1-\text{key } 1). \tag{8}$$

Where K =3.925,'h' is the size of the image the initial value of key 1 is 0.1.

b) The set of Key 1 values are stored in a(i,j)

c) Iterate the logistic map equation key 2 into 'h' times.

$$\text{key } 2 = K*\text{key } 2*(1-\text{key } 2). \tag{9}$$

Where the initial value of key 2 is 0.2

d) The set of Key 2 values are stored in b(i,j)

e) Iterate the logistic map equation key 3 into 'h' times.

$$\text{key } 3 = K*\text{key } 3*(1-\text{key } 3). \tag{10}$$

Where the initial value of key 3 is 0.3

f) The set of Key 3 values are stored in c(i,j)

g) Set the constants t=0.4,g0=0.2,g1=0.5,g2=0.3.

h) Substitute the value of a,b,c in the equation

$$P(i,j)=(1-t)^2*a(i,j)*g0+2*t*(1-t)*b(i,j)*g1+t^2*c(i,j)*g2 \tag{11}$$

i) Rounding the value of 'P' after multiplying with 255 using the equation,

$$e=\text{round}(P*255). \tag{12}$$

j) Encrypted image 'E' is obtained using the equation

$$E=\text{mod}(tt*A_{WM}+(1-tt)*e,256). \tag{13}$$

Where A_{WM} is the watermarked image and tt=.001.

4.2.2 Decryption algorithm

a) Iterate the logistic map equation key 1(8) into h times.

b) The set of Key 1 values are stored in a(i,j)

c) Iterate the logistic map equation key 2(9) into h times.

d) The set of Key 2 values are stored in b(i,j)

e) Iterate the logistic map equation key 3 (10) into h times.

f) The set of Key 3 values are stored in c(i,j).

g) Set the constants t=0.4;w0=0.2;w1=0.5;w2=0.3;

h) Substitute the value of a,b,c in the equation (11)

i) Round the value of P after multiplying with 255 using the equation (12)

j) Substitute the above rounded value in the following equation.

$$F=(1-tt)*e \tag{14}$$

h) Where tt is a constant and its value is 0.001.
k) Decrypted image is obtained using the equation

$$D=(E-F)/tt. \tag{15}$$

Where ‘E’ is the encrypted image.

4.3 Algorithm – Extracting the watermark

a) Perform 3-level Haar wavelet transform on thedecrypted image A^{*}_{WM}.
b) Perform SVD to the HL and LH sub bands of the decrypted image.

$$A^{*k}_{WM}=P^{*k}\,Q^{*k}_{WM}R^{*kT}\ ,\quad k=1,2 \tag{16}$$

where k represents one of two sub bands.
c) The singular values of watermark images can be extracted as

$$Q^{*k}_{W}=(Q^{*k}_{WM}-Q^{k})/\alpha \tag{17}$$

d) The watermark images can be obtained as

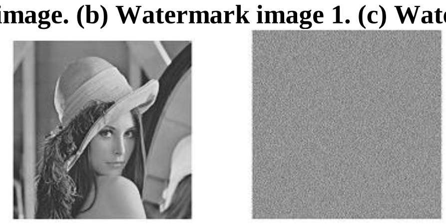
$$W^{*k}=P^{k}_{W}\,Q^{*k}_{W}\,R^{kT}_{W} \tag{18}$$

V. Simulation Results

The proposed algorithm is implemented using MATLAB. An 8-bit gray scale ‘Lena’ of size 512 x 512 is selected as host image. Two gray level images of size 128x128 are used as watermark images. Fig. 3 shows the host image and watermark images. Fig. 4 shows the watermarked image, encrypted image, decrypted image and extracted watermarks without noise attacks. It can be seen that the proposed method preserves the perceptual quality of the watermarked mage.

(a) (b) (c)

Fig. 3:(a) Host image. (b) Watermark image 1. (c) Watermark image 2.

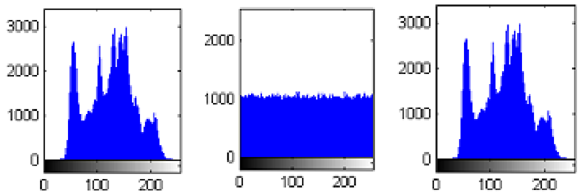


(a) (b)

© (d) (e)

Fig.4: (a) Watermarked image (PSNR=∞). (b) Encrypted image.(c)Decrypted image.(d)Extracted watermark image 1. (c) Extracted watermark image 2.

Histogram is a graphical representation of the tonal distribution in a digital image. It gives the number of pixels for each tonal value. Figure 5 shows the histogram of the watermarked image, encrypted image and the decrypted image. From the figures it is understood that the proposed method perfectly decrypt the encrypted image.

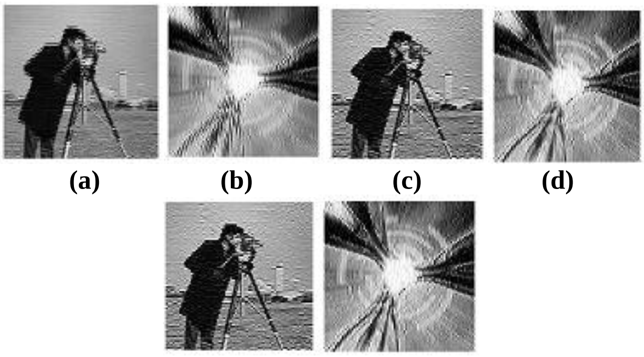


(a) (b) (c)

Fig.5: Histogram (a) watermarked image (b) encrypted image (c) decrypted image

VI. Performance Analysis

To investigate the robustness of the algorithm, the encrypted image is subjected to various types of attacks such as salt and pepper noise, speckle noise and Gaussian blur attacks. Salt and pepper noise is also called impulse noise and it can be caused by sudden and sharp disturbances in the image signal. It appears as randomly occurring white and black pixels over the image. Salt and pepper noise attack is also essentially a high pass filter function. Gaussian blurring is a process that averages the value of pixels over an area using weighing coefficients derived from a Gaussian function. It is often used to reduce noise or to reduce pixilation in an image. Speckle noise is a granular noise that inherently presents in and degrades the quality of the active radar and Synthetic Aperture Radar (SAR) images. It causes difficulties for image interpolation in SAR images. The extracted watermarks after different noise attacks are shown in the Fig.6.



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

(e) (f)

Fig-6: Extracted watermarks (a) watermark image 1 after Gaussian blur. (b) Watermark image 2 after Gaussian blur. (c) Watermark image 1 after Salt & Pepper noise. (d) Watermark image 2 after Salt & Pepper noise. (e) Watermark image 1 after Speckle noise. (f) Watermark image 2 after Speckle noise.

For comparing the similarities between the original and extracted watermarks, the correlation coefficient was employed. The normalized coefficient (NCC) gives a measure of the robustness of watermarking and its peak value is 1.

$$NCC=\frac{\sum_i \sum_j W(i,j).W'(i,j)}{\sqrt{\sum_i \sum_j W(i,j)}\sqrt{\sum_i \sum_j W'(i,j)}} \quad (19)$$

Where *w* and *w'* represents the original and extracted watermark respectively [9]. Table 1 shows the NCC values between extracted watermarks and original watermarks. Table 2 shows the NCC values between decrypted image and the encrypted image. It can be observed that the proposed method is robust to various attacks.

Table 1: Normalized Correlation Coefficient Extracted Watermarks and Original Watermarks

Attacks	NCC	NCC
Without attacks	0.9997	0.9996
Gaussian blur	0.8937	0.8144
Salt & pepper noise	0.8096	0.8054
Speckle noise	0.8151	0.8162

Table 2: Normalized Correlation Coefficient Between Decrypted Image and Encrypted Image

Attacks	NCC
Without attacks	1
Gaussian blur	0.9911
Salt & pepper noise	0.8198
Speckle noise	0.8352

VII. Conclusion

The proposed method combines the watermarking and encryption techniques to improve the security of the digital images. It utilizes the advantages of DWT, SVD in the watermarking technique and chaos in the encryption technique. In this method two watermark images are embedded in the HL and LH bands of the host image after three levels DWT decomposition of the host image using Haar wavelet by modifying the singular values of the host image with that of watermark images. The watermarked image is then encrypted and then sends to the receiver. In this the key generation is based on chaotic logistic maps. Proposed encryption method has wide key space and high key sensitivity. Performance analysis shows that it is able to recover the watermarks after Gaussian blur, Salt & pepper noise and speckle noise attacks.

References

[1] W. Bender, D. Gruhl, N. Morimoto and A. Lu, Techniques for data hiding,, IBM Systems Journal, vol.35, no. 3&4, pp.313-336, 1996.

[2] I. J. Cox, J. Killian, F. T. Leighton and T. Shamoon,Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing, vol. 6, no. 12,pp. 1673-1687,December 1997.

[3] J. J. K. 0 Ruanaidh, W. J. Dowling and F. M. Boland, Watermarking digital images for copyright protection, IEEE Proceedings - Vision, Image and Signal Processing, vol. 143,no. 4, pp. 250-256, August 1996.

[4] M. D. Swanson, M. Kobayashi and A. H. Tewfik, Multimedia data-embedding and watermarking techniques, Proceedings of the IEEE, vol. 86, no. 6, pp.1064-1087, June1998.

[5] Chunlin Song, SudSudirman, MadjidMerabti, Recent Advances and Classification of Watermarking Techniques in Digital Images, ISBN: 978-1-902560-22-9 © 2009 PGNet

[6] Vaishali S. Jabade,Dr. Sachin R. Gengaje, Literature Review of Wavelet Based Digital Image Watermarking Techniques, International Journal of Computer Applications (0975 – 8887) , Volume 31– No.1, pp. 28-35, October 2011

[7] M. MohamedSathik, S. S. Sujatha, A Novel DWT Based Invisible Watermarking Technique for Digital Images, International Arab Journal of e-Technology, Vol 2, no. 3, pp. 167-173, January 2012.

[8] R. Matthews, Cryptologia 8 (1989) 29.

[9] Chunlin Song , Sud Sudirman, Madjid Merabti, A robust region-adaptive dual image watermarking technique, Elsevier Journal of Visual communication and image reconstruction, pp. 549–568, Feb. 2012.

[10] Yupu Dong; Jiasheng Liu; Canyan Zhu; Yiming Wang; Image encryption algorithm based on chaotic mapping, 3rd IEEE International Conference on Computer Science and Information Technology ,Volume: 1,pp.:289 – 291,Oct.2010.

[11] Anumol Joseph,K.Anusudha, Singular Value Decomposition Based Wavelet Domain Watermarking ,IEEE International Conference on computer communication and informatics,Jan.2014.

[12] Anumol joseph,K.Anusudha ,A Robust Watermarking Technique Based on DWT SVD, Proceedings of International conference on mathematical computer engineering,Nov.2013