Chaos Encryption Based DWT-SVD Watermarking

Anumol Joseph¹, K. Anusudha²
(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 copyright 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:

\[ A = \mathbf{P} \mathbf{Q} \mathbf{R}^T \]  \hspace{1cm} (1)

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

\[ \lambda_1 \geq \lambda_2 \geq ... \geq \lambda_r \]  \hspace{1cm} (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.

\[ A^{k} = P^{k} Q^{k} R^{kT}, \quad k=1, 2 \]  

where $k$ represents one of two sub bands.

\[ W^{k} = P^{k} Q^{k} R^{kT} \]  

de

\[ Q^{k}_{WM} = Q^{k}_{W} + \alpha Q^{k}_{W} \]  

e

\[ A^{*k} = P^{k} Q^{k} R^{kT} \]  

f

\[ X_{n+1} = r X_{n} (1-X_{n}) \]  

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].
4.2.1 Encryption Algorithm

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

\[ \text{key } 1, \text{K} \times \text{key } 1 \times (1 - \text{key } 1). \]  

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.

\[ \text{key } 2, \text{K} \times \text{key } 2 \times (1 - \text{key } 2). \]  

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.

\[ \text{key } 3, \text{K} \times \text{key } 3 \times (1 - \text{key } 3). \]  

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

\[ P(i,j)=(1-t)^2 \times a(i,j) \times g0+2 \times t \times (1-t) \times b(i,j) \times g1+t^2 \times c(i,j) \times g2 \]  

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

\[ e=\text{round}(P \times 255). \]  

j) Encrypted image ‘E’ is obtained using the equation

\[ E=\text{mod}(tt \times A_{WM}+(1-tt) \times e,256). \]  

Where \( A_{WM} \) is the watermarked image and tt=0.001.

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)
Chaos Encryption Based DWT-SVD Watermarking

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

\[ F = (1 - tt) * e \]  \hspace{1cm} (14)

h) Where \( tt \) is a constant and its value is 0.001.

k) Decrypted image is obtained using the equation

\[ D = (E - F) / tt. \]  \hspace{1cm} (15)

Where ‘E’ is the encrypted image.

4.3 Algorithm – Extracting the watermark

a) Perform 3-level Haar wavelet transform on the decrypted image \( A_{WM}^k \).

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

\[ A_{WM}^k = P_{WM}^k Q_{WM}^k R_{WM}^k, \hspace{1cm} k = 1, 2 \]  \hspace{1cm} (16)

where \( k \) represents one of two sub bands.

c) The singular values of watermark images can be extracted as

\[ Q_{W}^k = (Q_{WM}^k Q_{WM}^k)^{1/\alpha} \]  \hspace{1cm} (17)

d) The watermark images can be obtained as

\[ W_{W}^k = P_{W}^k Q_{W}^k R_{W}^k \]  \hspace{1cm} (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 image.

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

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

\[ \text{NCC} = \frac{\sum_i \sum_j W(i,j)W'(i,j)}{\sqrt{\sum_i \sum_j W(i,j)^2} \sqrt{\sum_i \sum_j W'(i,j)^2}} \] (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>
<thead>
<tr>
<th>Attacks</th>
<th>NCC</th>
<th>NCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without attacks</td>
<td>0.9997</td>
<td>0.9996</td>
</tr>
<tr>
<td>Gaussian blur</td>
<td>0.8937</td>
<td>0.8144</td>
</tr>
<tr>
<td>Salt &amp; pepper noise</td>
<td>0.8096</td>
<td>0.8054</td>
</tr>
<tr>
<td>Speckle noise</td>
<td>0.8151</td>
<td>0.8162</td>
</tr>
</tbody>
</table>
Table 2: Normalized Correlation Coefficient Between Decrypted Image and Encrypted Image

<table>
<thead>
<tr>
<th>Attacks</th>
<th>NCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Without attacks</td>
<td>1</td>
</tr>
<tr>
<td>Gaussian blur</td>
<td>0.9911</td>
</tr>
<tr>
<td>Salt &amp; pepper noise</td>
<td>0.8198</td>
</tr>
<tr>
<td>Speckle noise</td>
<td>0.8352</td>
</tr>
</tbody>
</table>

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