Watermarking Based Fresnel Transform, Wavelet Transform, and Chaotic Sequence

Ahmed S. Hadi, Baydaa M. Mushgil, and Heba M. Fadhil

University of Baghdad, Al-Khwarizmi College of Eng., Information and Communication Dept.

Abstract: In this paper a watermarking based on Fresnel transform, discrete wavelet transform with support of chaotic sequence will be present. Where the Fresnel transform is applied to the host image according to the distance parameter (D) in order to encrypt it. After that the DWT will be applied to the encrypted image to create a channel for embedding the copywrite information that encrypted by using chaotic sequence. The initial condition of this sequence is consider as key (k2), the Fresnel transform is depending on distance parameter “D” which is considered as a key (k1), and the embedding into the approximation coefficient of the DWT is accomplished by key (k3). So we have three concatenated keys that eavesdropper have to discover in order to decrypt the copywrite information which is considered a robust to the eavesdropper.

Key words: Watermarking, Fresnel Transform, Discrete Wavelet Transform, and Chaotic Sequence.

INTRODUCTION

The fast developments of business on the internet multimedia such as videos, sounds, and images, increases the need to protect this multimedia from unauthorized access and keep the rights of the owners of this multimedia. The process of embedding the information about the owners in a way that is invisible and undetectable by eavesdropper in the multimedia is called a watermarking [1,2].

In [3,4] the host image is Fresnel transformed with various distance depend on distance parameter (D) in order to obtain a channel for embedding the copywrite information. The distance parameter (D) represents the key of encryption. The eavesdropper can obtain the protected data by finding D, and scan the channels for embedded information.

In [5] a chaotic sequence is generated according to logistic map, which is used to encrypt the copywrite information, and then embedded in the middle sequence coefficients of the DWT domain. The eavesdropper can obtain the DWT, scan its domain for encrypted data, and rescan for the key of encryption to decrypt this data.

Our proposed method will combine the DWT and chaotic sequence with the Fresnel transform, where the Fresnel transform is applied to the host image according to predefined distance parameter D, which is the key of encrypting this image (K1). Then we find the DWT for the transformed image in order to isolate the detailed coefficients from the approximation coefficients. At the same time a chaotic sequence is generated by using Logistic Map. The initial condition of this sequence is considered as the key (k2) that will be used to encrypt the copywrite information. The chaotic sequence must have the same length of the copywrite information. Then the encrypted data is embedded into the approximation coefficient of the DWT of the transformed image according to key (k3).

This paper is organized as follows; in section two the theory of DWT, Fresnel transform, and chaotic sequence will be present. The proposed method with its simulation will be present in section three and four respectively. Finally section five will contains the conclusion.

2. Theory of the Discrete Fresnel Transform, Discrete Wavelet Transform, and Chaotic Sequence:

2.1 Discrete Fresnel Transform: [3] Fresnel transform describes the wave propagation in the Fresnel diffraction region as shown in Fig.1 the distance between planes f(x1, y1) and f(x2, y2) depends on the distance parameter D, this parameter can diffuse the image in original plane f(x1, y1). Distance parameter plays as the key of encryption of the image because if the value of D is increased or decreased it will diffuse the image to be just a noisy image. Fig.2 explains the effect of parameter D. While Fig.3 shows the computation of Fresnel transform.

2.2 Discrete Wavelet Transform (DWT) for 2-D Signal: A 2-D DWT is equivalent to two one dimensional DWT in series. It’s implemented as 1-D row transform followed by 1-D column transform on the data obtained from the row transform as shown in Fig. 4. Where h(n)&g(n) are the lowpass filter and
Fig. 1: Fresnel Transform of a 2-D Model

Fig. 2: Fresnel Transform for Different Distance Parameter (D).

Fig. 3: The Flow of Calculation of Fresnel Transform

Fig. 4: One Level Filter Bank for Computation of 2-D DWT.
highpass filter which splits the signal into two subspaces, the low pass filter generates the details of the signal (XL) and the high pass filter generates the noise signal (XH). XLL, XHL, X LH, and X HH are the details-sub signal, noise detail subsignal, detail noise subsignal and noise subsignal respectively. The embedding of message will be in the noise subsignal in order not to effect on the original signal \( [6] \).

An example for implementing the 2-D DWT Harr type is shown in fig.5. Fig.5.b and fig.5.c shows the one and the two level 2-D DWT respectively for the original image shown in fig.5.a. The first Quarter of the first sub image in the left upper corner of fig.5.c represents the details of original signal the right lower corner represent the noise sub image where our secret message will be embedded \([7]\).

2.3 Chaotic Sequence: The chaotic sequence depends on the initial condition where a sequence with closely initial condition will give different sequence \([8]\). So that the initial condition of the chaotic sequence represents the key of encryption in crypto system. In this paper a chaotic sequence using logistics map \([9]\) will be used to encrypt the message. The logistic map is defined as:

\[
X(n+1) = rX(n) \mod(p)
\]

\( n = 0, 1, \ldots, x_0 \in [0, q], r = \frac{p}{q} > 1, \text{ and } p \text{ is a co-prime to } q \)

The map is chaotic for all \( r \) and has lyapunov exponent \( \lambda = \log r > 0 \).

3. Proposed Method: Our proposed methods is shown in fig.6, as shown in this figure the host image must be first encrypted by Fresnel transform according to D parameter (which is considered as k1) then a two level 2-D DWT is applied to the encrypted host image to creates a channels for embedding. At the same time the text message is encrypted by chaotic sequence that have been generated according to a specific initial point (which is considered as k2) then the text message is Exclusively ORed (XOR) with the chaotic sequence to generate the encrypted text message, knowing that the chaotic sequence length must equal to the length of the message.

The encrypted message is embedded into the noise subspace of the encrypted split host image. The embedding is done according to predefined positions (this positions is considered as k3).

After all that inverse 2-D DWT then the inverse Fresnel transform is applied to the encrypted split host image to get the watermarked image.

4. Simulation of Proposed Method: The simulation of our proposed method will be planned into six parts as follows:

4.1 Encrypting of the Host Image: Consider the image shown in Fig.7(a) this image will be encrypted by Fresnel transform according to \( D=50 \) as shown in Fig.7(b). As shown in Fig.7(b), it is difficult to recognize the original image, however \( D \) must be chosen so that the inverse Fresnel transform gives us the original image with no observable changes in it.

4.2 2-D DWT: To prepare this encrypted image for embedding it must be split into signal and noise subspaces which are done by two level 2-D DWT, as shown in Fig.8. For higher security we took second level of the 2-D DWT.

4.3 Encryption of the Text Message: Consider the text message “University of Baghdad” that we want to watermark in the host image, first we have to convert it to binary number, and then we have to generate a chaotic sequence with same length of the binary sequence of the message. The chaotic sequence is generated according to logistic map with initial condition 0.5. Finally, the binary sequence of the message is Exclusively ORed (XOR) with the chaotic sequence, which is the encrypted message.

4.4 Embedding the Encrypted Message: The encrypted message will be embedded in the second level of the noise subspace of the encrypted split image. The embedding will be in any predefined position with different order. Knowing that the two levels 2-D DWT results in 128*128 coefficients, which means that the second noise subspace (HH2) will be in positions (32,32) to (64, 64). In this example we will embed in main diagonal of HH2, that is in (32, 32) to (52, 52), because the length of the message is 20. Hence \( k_3=\{(32, 32), (33, 33), \ldots, (52, 52)\} \). The encrypted split image after embedding is shown in Fig. 9.

4.5 Reconstruction of Watermarked Image: Inverse 2-D DWT and inverse Fresnel transform is applied respectively to the encrypted split image. The obtained image is the final watermarked image (Fig. 10) as we can see it's not affected by encryption.

4.6 Reconstruction of the Text Message: Reconstruction of text image can be done if and only if we have the three predefined keys, k1 (D), k2 (initial condition for the chaotic sequence), and k3 (map of embedding).
Fig. 5: 2-D DWT for One and Two Levels.

Fig. 6: The proposed Algorithm

Fig. 7: a) Original Image, b) Fresnel Transform Image for D=50
Fig. 8: The Two Level 2-D DWT of the Fresnel Image.

Fig. 9: The encrypted split image after embedding

Fig. 10: The Original Image after Decryption.
The Fresnel transform is applied to the watermarked image by using k_1, to get the domain used for embedding.

The obtained image is transformed by two level 2-D DWT to get the space of embedding. Then, the binary embedded sequence is reconstructed from specified positions of the noise subspace according to k_3. Finally the message will be output of bit XOR operation between the reconstructed sequence and the regenerated chaotic sequence according to K_2.

5. Conclusions: If we assume that, the eavesdropper knows the encryption process, then in order to obtain the text message, the eavesdropper has to know keys k_1, k_2, and k_3. The chaotic sequence initial value (k_2) is very sensitive to any change in its value, so that the eavesdropper have to obtain exactly its value which is difficult and time consuming. The distance parameter “D” (k_1) of Fresnel transform is also required a long time to obtain its value, where any change in its value will change the image obtained. Finally, the mapping of the two level 2-D DWT (k_3) is required to scan all the noise subspace to obtain the required encrypted message which is also a time consuming process.

REFERENCES


