Security of Medical Images by Discrete Sine Transform Encryption Algorithm

Shaifi Goyal, Reecha Sharma

Abstract-Image encryption is an application of security on digital images. Digital medical images contains vital information about patient personal data and need to be safe and protected.This paper presents the used of watermarking algorithm with encryption by discrete sine transform in the medical field as the demand for security is getting higher day by day. Furthermore, Hash (key) has been used to strengthen the security and chaotic sequences are used to image encryption by DST domain. In medical images ROI in an area that contains important information. This algorithm has very good effect and can resist against the common and geometrical attacks. Experimental results demonstrate that watermarking with encryption scheme is robust to signal processing operation such as rotation, JPEG compression and median filter.

Index Terms— DST, Medical image, watermarking, chaotic table.

1 INTRODUCTION

Medical image watermarking algorithm is suitable method used for enhancing security, authentication, reliability and confidentiality of medical data, which is crucial and used for further diagnosis and reference. Image encryption algorithm protects the data from an unauthorized access. Encryption is a tool of security that aims to provide protection in the ciphers of any kind of messages. The applications of digital multimedia have grown tremendously in the last five years, security and legal issues became more and more important. Watermarking, which is the embedding of a signal (known as the watermark) into the original multimedia element is one method that has been proposed for the protection of digital media elements such as audio, video, and images. [2]

Chaotic systems are nonlinear dynamic behaviour; they are sensitivity to the initialize conditions and generate highly complicated signals. Because chaotic systems have good properties, chaotic systems are widely used in communications, optimization, control and image processing et al. In 1989, Matthews used discrete chaotic dynamical systems in cryptography firstly [1]. He derived a one-dimension chaotic map, which is used to generate a sequence of pseudo-random numbers. Image encryption has its own specifications such as en-cryption speed, compatibility to image format and compression standards, and real-time implementation etc., therefore requires a special design of the encryption algorithm.

In this paper, I propose an encryption algorithm based on image watermarking with encryption by DST domain. By setting the key to prevent recover and repair the watermark in the unauthorized situation. This transform helps in the selection of regions on basis of their sine energies. Data is hidden behind the region of not interest (RONI).

The simulation results show that the encrypted images are robustness for noise disturbing and geometrical attack. We have also improved the normalised cross- correlation of an image based on chaotic system.

The proposed study aims to explore the possibility of using chaotic or chaos-based encryption techniques by DST to protect medical images and provides high level of security in efficient and reliable way.

The rest of the paper is organized as follows. Section 2 gives detailed analysis of the proposed algorithm. The effect of noise on the decryption process is discussed in Section5. The last section gives the concluding remarks.

2. THE ALGORITHM

2.1 Image encryption algorithm

Step1. Loading Image

Loaded the image of CT brain in the matlab. Here we use brain image as a binary medical image and is of size 128×128.

Step2. Data Reading

Logical data is a binary data which have been hide using original image. Here 'copy right' image is a logical image of size 32×32.

Step3. Sine transformation

In the sine transform values in the chaotic table can be regarded as a feature vector of the medical image.DST coefficients reflects the visual characteristics of medical image.

DST presents a new approach for image encryption based on the chaotic table. Discrete sine transform is energy based theory. It is well known for analysis of signal or images in ROI and RONI. Region of interest contains useful information and must be secured from attacks or noises.

For medical images DST is defined as:

$$y(k)=\sum_{n=1}^{N} x(n)\sin\left(\pi \frac{kn}{N+1}\right), \quad k= 1, 2, 3,4....N \qquad (1)$$

Here n is pixel number, k is number of pixels in a size of image, N is natural number.

For both joint photographic group(JPEG) and moving expert group(MPEG) we use DST.A watermarking algorithm that uses DST is more compatible.

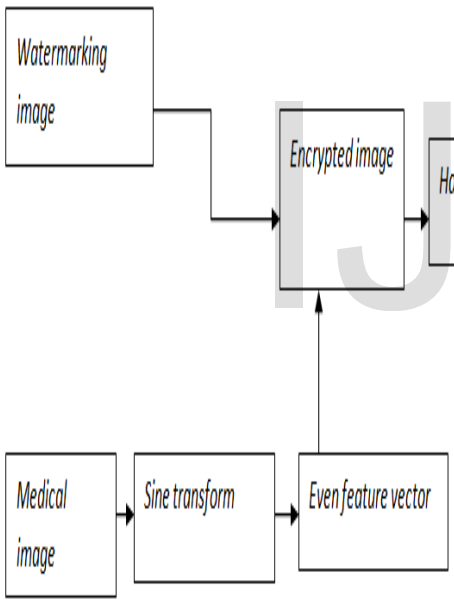
2.2 WATERMARKING DESIGN ALGORITHM

Step1. Generate chaotic sequences.
Chaotic sequence is related to the position of pixels. Chaotic table have a addresses of the pixel of two dimensional image. Binary encrypted image can be achieved as the chaotic sequence by mathematical computation. Position of the pixel stores sine energy values of an image. Sortrows of an image sine values in ascending order.

Step2. Hiding a logical image
Acquire even feature vector of original medical image.
Empty the LSB for hiding the data. Even feature vector is calculated by taking the mod of a two dimensional image.

Step3.Scrambled image
Now scrambled the image by taking the difference between the image and mod image. Absolute the image for positive values.

The proposed algorithm flowchart



Fgure1. The diagram of watermarking algorithm with encryption by DST.

3 Decryption algorithm
Decrypt the original watermarking image
The original image can be extracted from watermarked image. Chaotic sequence can be deciphered with the private key. By using HASH function of cryptography we can recover the original watermarking image. Hidden information can be restore without any distortion which is large advantage to safety of the medical image.

4 Watermarking evaluating algorithm
The Normalised cross-correlation(NC) is used to measure the quantitative similarity between the extracted and embedded watermarking which is defined as

$$NC = \frac{\sum_i \sum_j W(i,j)\, W'(i,j)}{\sum_i \sum_j W^2(i,j)} \quad (2)$$

where W denotes the embedded original watermarking and w′ denotes extracted image. Higher the value of NC , more will be the similarity between the extracted and original image.
The peak signal to noise ratio is defined as:

(3)

$$PSNR = 10 \lg \left[\frac{MN \max_{i,j} \left(I(i,j)\right)^2}{\sum_i \sum_j \left(I(i,j) - I'(i,j)\right)^2} \right]$$

where I(i,j), I′(i,j) denote the pixel value of coordinates(i,j) in the original image and watermarked image respectively .M,N represents the rows and the columns of pixel respectively.

5 RESULTS

To verify our proposed algorithm, we carried out are simulation in Matlab2011b platform. We have choosen medical image as original image (1≤i≤128,1≤j≤128).The size of the logical image (binary image) as(1≤i≤32,1≤j≤32).

Without any common attacks and geometric attacks the difference between the embedded watermarking image and original image is of ideal case. The quality of embedded image has hardly any change.

1) When no attack
The encrypted image is the exact replica of original image.

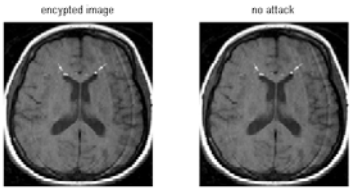


Figure2: (a) Encrypted image (b) The Watermarked image without attacks.

The following are common attacks added to medical image.
2) Rotation attack
The rotation attack at 20 degree is added to watermarked image to check the scheme is good robust against the common attacks.This parameter helps to validate the effectiveness of proposed algorithm.Figure3 shows that medical image is rotated at 20^0.Furthermore, fig.(b) depicts that the watermarked image can be extracted with NC=1.It proves that our proposed

algorithm has a strong robustness against rotation attack.

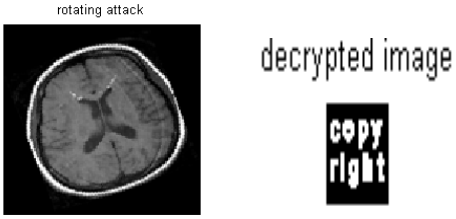


Figure3 .under rotation attack (20^0) (a) an image with rotation attack;(b) the decrypted image.

(3) JPEG attack

The JPEG compression process is done by using a percentage of image quality as a parameter to measure. The medical image undergoes our proposed algorithm that is by discrete sine transform. Brain image with PSNR=40.3350 under JPEG attack (8%) is shown in figure (a).Here decrypted image is extracted with NC=1.This shows that our scheme can resist against JPEG attack.

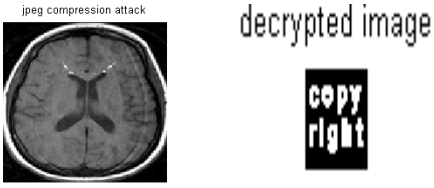


Figure4. under JPEG attack(8%) (a) an image under JPEG attack;(b) the decrypted watermarked image with NC=1.

(4) Median 3×3 attack

In a watermarked image, median filter (3×3) attack is added to validate the effectiveness of our proposed algorithm. Figure (a) shows that that medical image undergoes median attack. Moreover fig(b) that watermarked image can be extracted with NC=1. It states that there is similarity between the embedded watermarking image and the original image and hence proposed algorithm has strong robustness against median(3×3) attacks.

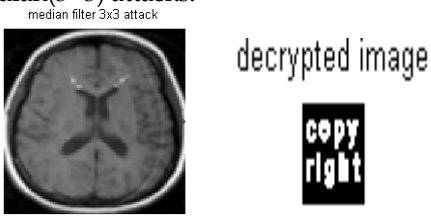


Figure5. under Median 3×3 attack (a) an image under Median 3×3 attack;(b) the decrypted watermarked image with NC=1

TABLE I
Change of NC by DST to different attacks

Image Processing	MSE	PSNR	NC
Original image	0.0305	63.2940	1
Rotation(200)	6.0606e+003	10.3056	1
JPEG compression	6.0198	40.3350	1
Median filter (3×3)	184.6567	25.4672	1
No attack	0	Infinite	1

6. CONCLUSION

In this paper, encryption with DST achieves maximum degree of robustness against various attacks. we present an image encryption algorithm based on chaotic systems by discrete sine transform. The proposed algorithm has enough cipher key space to resist different kinds of attacks.It achieves maximum degree of robustness in the encrypted data. Medical Images often are attacked by the noises and a series of other attacks in the transmission or other processes. From the decrypted images, it can be seen that this algorithm has good anti-attack capability for the Rotation, JPEG compression and median filter. The algorithm has good encryption efficiency and safety seen from the simulation results.

ACKNOWLEGMENT

I would like to thank Reecha Sharma from the Faculty of Electronic Engineering UCoE, Punjabi University, Patiala for her efforts during the course of this work and the arrangement of this paper.

References

[1] Jiu-Lun FAN , Xue-Feng ZHANG1,2 ," Image Encryption Algorithm Based on Chaotic System".

[2] Shanshan Zhang, Xiaohong Wang, Shizheng Zhou, "The Research of Image Watermarking Encryption Algorithm ,"2011 Fourth international Joint Conference on Computational Sciences and Optimization,pp.821-824.

[3] Ensherah A. Naeem1, Mustafa M. Abd Elnaby 1, and Mohiy M. Hadhoud 2," Chaotic Image Encryption in Transform Domains." 2009 IEEE, pp.71-76.

[4] Meghdad Ashtiyani, Parmida Moradi Birgani , Hesam M. Hosseini," Chaos-Based Medical Image Encryption Using Symmetric Cryptography".

[5] Shanshan Zhang, Xiaohong Wang, Shizheng Zhou, "The Research of Image Watermarking Encryption Algorithm ,"2011 Fourth international Joint Conference on Computational Sciences and Optimization,pp.821-824.

[6] Weiwei Xiao, Zhen Ji. Jihong Zhang. Weiying Wu, "A watermarking algorithm based on chaotic encryption," Proceedings of IEEE Tencon02,pp.545-548.

[7] Chen Dongming, Zhu Zhiliang, Yang Guangming," An improved Image Encryption Algorithm Based on Chaos," the 9th International Conference for Young Computer Scientists 2008 IEEE, pp.2792-2796.

[8] Chunhua Dong,JingBing Li*,Mengxing Huang,Yong Bai, "The Medical Image Watermarking Algorithm with Encryption By DCT and Logistic," 2012 Ninth Web Information Systems and Applications Conference ,pp.199-124.