Volume 3, Issue 6, June 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

The Medical Image Watermarking Algorithm with Encryption by Discrete Sine Transform

Shaifi Goyal*
UCoE, Punjabi University, Patiala, Punjab, India

Reecha Sharma
UCoE, Punjabi University, Patiala, Punjab, India

Abstract— Abstract-This paper deals with the image watermarking encryption technology based on DST domain by converting data or information from its original data into some other form so that image can be protected from unauthorised access. Encryption is employed to enhance its reliability and security. Furthermore, Hash (key) has been used to strengthen the security and highlights that how chaotic system is rich in significance of image protection by DST domain. In medical images ROI in an area that contains important information and must be stored without any distortion. Even feature vector of image has been used as a part of sign sequence for DST coefficients. Experimental simulations show that effect of decrypted image has low computational complexity and strong robustness even when encrypted image undergoes various attacks.

Keywords— DST, Medical image, watermarking, chaotic table, ROI.

I. INTRODUCTION

Image encryption is a wide research. With the fast growth of economy a large number of encryption algorithm have been developed for the protection of images from unauthorised access. With the development of computer technology many digital services, such as Medical, Military, and Space imaging systems require reliable security in storage and transmission of digital images. The rapid use of Internet in the digital world today, the security of digital images has become more and more important. The prevalence of multimedia technology in our society has promoted digital images to play a more significant role, which demands a serious protection of user privacy. When medical images are transmitted in the hospitals, it requires strict confidentiality, reliability and authentication. Patient information is hidden in medical images by digital watermarking algorithm. Even when medical images undergo various attacks it can still extract the watermarking which can protect the patient personal information.

In the medical images, Region of interest (ROI) contains useful data and must be protected from noise and shear transformation attacks. Discrete sine transform (DST) has been used in the field of digital watermarking for medical images by changing coefficients in the sine domain to embed in the watermark. This transform helps in the selection of regions on basis of their sine energies. Data is hidden behind the region of not interest (RONI). This paper put forward a new medical image encryption algorithm based on chaotic sequences and discrete sine transform. The simulation results shows that the encrypted images are strong robustness against common (noises) and geometric (shape changes) attacks. Watermarking algorithm reduces the tedious work for selecting ROI. In addition, we have also improved the normalised cross- correlation of an image based on chaotic system. Section II presents encryption theory, section III presents algorithm for encryption by DST, and section IV represents experimental results of proposed algorithm.

II.THE MEDICAL ENCRYPTION THEORY

Medical images, should be encrypted before they are sent over networks. Image encryption can also be used to protect privacy. When such images are sent over a network, an eavesdropper may duplicate or reroute the information. By encrypting these images, a degree of security can be achieved. The image encryption technique envolves four goals for medical images: Confidentiality: Confidentiality refers to the protection of information from unauthorized access. Data integrity: It ensures that information has not been manipulated in an unauthorized way. Authentication means that there should be evidence that information belongs to correct person. Non-repudiation: It means that the receiver can prove to everyone that the sender did indeed send the message [4].

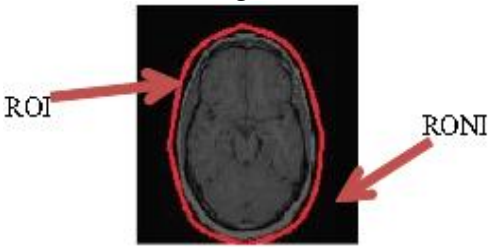


Figure 1. The ROI of medical image

A. The Discrete Sine Transform (DST)

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:

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

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

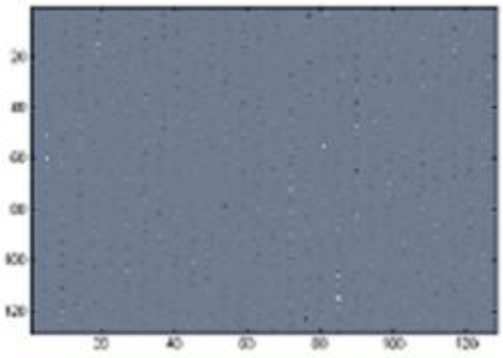
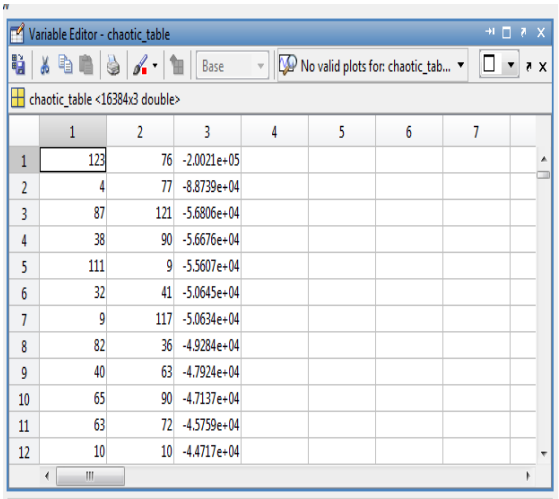


Figure2. Energy density image

In the matlab simulink colormap fuction is used for displaying color images by using colormap function energy density can be known .In an image where there is more white dot means that more data is encypted here, higher will be the energy and least white or black dot means less encrypted data is present.

B. The Chaotic System

Chaotic systems are encryption system, which depends on maps for image encryption. Chaotic system is performed in various domains, to make full use of their characteristics in each domain. They have a property that they are very much sensitive to initial conditions and parameters. Encryption is important tool to protect the data from various attackers. Chaos improves the security of image transmission and easy way to achieve the encryption system.



Variable Editor - chaotic_table

Base | No valid plots for: chaotic_tab...

chaotic_table <16384x3 double>

	1	2	3	4	5	6	7
1	123	76	-2.0021e+05				
2	4	77	-8.8739e+04				
3	87	121	-5.6806e+04				
4	38	90	-5.6676e+04				
5	111	9	-5.5607e+04				
6	32	41	-5.0645e+04				
7	9	117	-5.0634e+04				
8	82	36	-4.9284e+04				
9	40	63	-4.7924e+04				
10	65	90	-4.7137e+04				
11	63	72	-4.5759e+04				
12	10	10	-4.4717e+04				

Figure 3: chaotic Table

Chaotic table involves the position of pixels, where values of sine energy are stored in an ascending order. For example at 123×76 pixel energy is -2.0021e+05.

III. THE ALGORITHM

A. 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.

Figure4. Original image

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.

Figure5. Logical image.

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.

B. *Watermarking design algorithm*

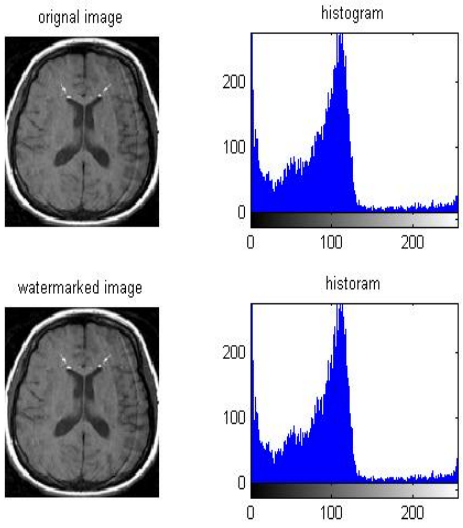
Step1. *Generate chaotic sequences.*

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. Sort rows of an image sine values in an 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. Histogram represents energy density of pixels.



(a) (b)

Figure6. (a)Watermarked image,(b) histogram represents energy pixel an image.

Step3.*Scrambled image*

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

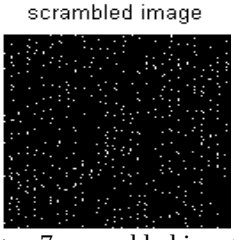
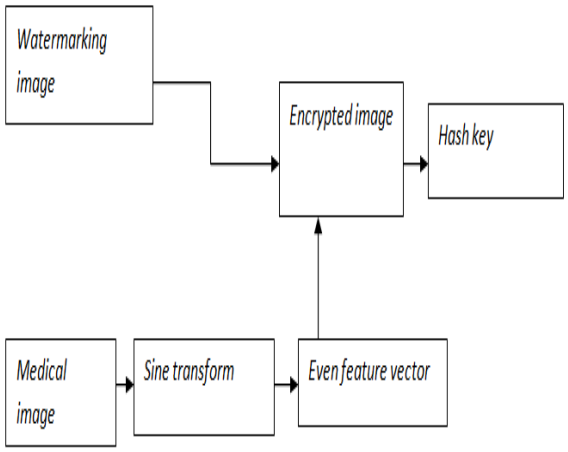


Figure7. scrambled image.



Fgure8. The diagram of watermarking algorithm with encryption by DST.

C. *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.

D. *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

$$NC = \frac{\sum_i \sum_j W(i,j)\, W'(i,j)}{\sum_i \sum_j W^2(i,j)} \quad (1)$$

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[4].

The peak signal to noise ratio is defined as:

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

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.

IV. RESULTS

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

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.

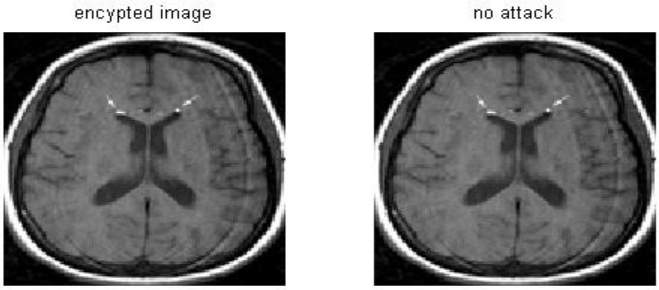
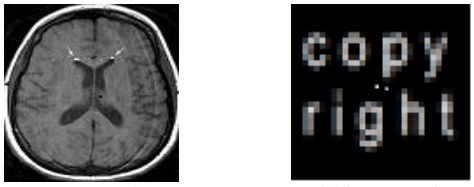


Figure9: (a) Encrypted image (b) The Watermarked image without attacks.

The following are common attacks added to medical image.

2) Adding Gaussian noise

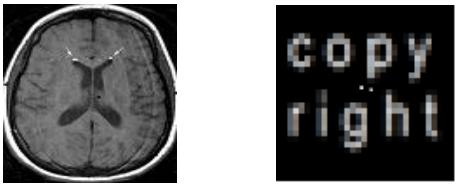
When Gaussian noise is added in the medical image at 3% the PSNR=35.6481and watermarked image is extracted with NC=1.The results shows that our proposed algorithm has strong robustness against noise attacks.



Gaussian noise at 3% NC=1

2) Scaling attacks

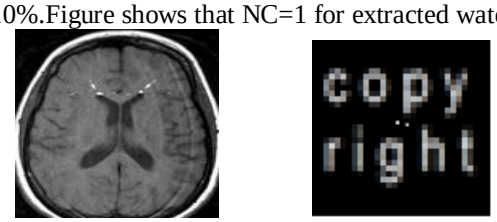
we scaled the image upto 50% that means medical image will be shrunk with a scale factor of 0 .5.Watermarked image can be extracted with NC=1.It states that there is similarity between the embedded watermarking image and the original image and hence proposed algorithm has strong robustness against scaling attacks.



Scaling factor=0.5 NC=1

3) Cropping attacks

The cropping attacks are common attacks and are added to test the robustness of the algorithm. Here we crop the medical image from Y axis with the ratio of 10%.Figure shows that NC=1 for extracted watermarked image.



Cropping=10% NC=1

TABLE I
Change of NC by DST to different attacks

Image Processing	***MSE***	***PSNR***	***NC***
Original image	0.0305	63.2940	1
Gaussian noise(3%)	17.7122	35.6481	1
Scaling (50%)	23.0321	34.5075	1
Cropping in y direction(10%)	891.0968	18.6316	1
No attack	0	infinite	1

V. Conclusion

In this, we have presented a new approach for chaotic system image encryption in DST domain. Experimental results shows that encryption with DST achieves maximum degree of robustness against various attacks. Images in this domain are much more secure than other domain. In addition, we use chaotic table to generate chaos sequence which can encrypted the watermarking image. Hence, this proposed algorithm is very much useful for medical images.

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

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

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

[4] 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.

[5] S. Li, X. Zheng, X. Mou, and Y. Cai, "Chaotic Encryption Scheme for Real-time Digital Video," In Real-Time Imaging VI, Proceedings of SPIE vol. 4666, pp. 149–160, 2002.

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

[7] 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.

[8] X Zhang and W. Chen," A New Chaotic Algorithm for Image Encryption" Proceedings of the International Conference on Audio, Language and Image Processing (ICALIP), pp, 889 – 892, 2008.

