Medical Image Encryption and Decryption Based on DCT Domain

Deepshikha Mehra, S R Dogiwal
Department of Computer Science and Engineering,Swami Keshvanand Institute of Technology, Management and Gramothan, Jaipur-302017(INDIA)
Email- dogiwal@gmail.com
Received 07.05.2018 received in revised form 04.09.2018, accepted 06.09.2018

Abstract:Cryptography plays an important role in Medical Images and its applications because of its ability to adapt to Encryption, Decryption and watermarking. Often, in this paper, to insure the medical information is secure. First of all use Scrambling algorithm to hide the patient information and require a authentication to access a real image. For watermarking, a Discrete Cosine Transform is applied to non-overlapping block size 8 x 8 image pixels. After that, a DCT coefficient values are apply to each block for position identification of embed message in medical image. To improve high capacity and imperceptibility in watermarking step, a Two Dimension Barcode ECC200 standard is used to convert message before embed to cover image. Experimental results demonstrate that the proposed scheme achieves better performance imperceptibility.

Keywords:DCT, Digital Watermarking, Two-Dimensional Data Matrix Bar Code, Encryption, Decryption.

1. INTRODUCTION

Images processing is very important for various applications in remote sensing, office automation, scientific application, bio-medical, criminology, astronomy, space application and military application. When processing images for these applications, uncertainty.

In Digital image area use the encryption, decryption and watermarking has widely used for information hiding can be done either in spatial domain or in frequency domain, in frequency domain embedding has higher imperceptibility. High PSNR (Peak Signal to Noise Ratio) more than in spatial domain but not robust against different kinds of geometry attack and so many different techniques and methods are in researching for improve this area to resolve the problems[8]. With rapid development of computer technology and a lot of information is transmitted through digital transformation media. Medical image is important personnel information's of patient and its required to protection. So the protection of view and access for extract required information given by access key and medical images are consider in this propose. The image Watermarking scheme has two common types, one is extraction step and another one is embedding step.

Mei Jiansheng and Tan Xiaomei [1] proposed a technique where the information of digital watermarking which has been discrete cosine transformed convert into the high frequency band of the image which has been wavelet transformed.

M.P. Turuk A.P. Dhande P. [2] Proposed to provide the security for text data and ECG signals are encrypt before interleaving in the frequency domain. Predictive coding techniques like differential pulse code and adaptive delta modulation are used for ECG signal encryption and compression. The quantitative and qualitive assessment of the watermarked images is carried out using PSNR and normalized MSE. The experimental results on different medical images (MRI, XRAY, MRA and CT scane) are tabulated, which shows that the DFT based interleaving technique is efficient as it preserves imperceptibility better than DCT.

Prabakaran G and Dr.Bhavani R[3] present a viable steganography technique using Integer Wavelet Transform (IWT) to protect the MRI medical image into a single container image. The container image was taken and flip left was applied and obtained the dummy container image. Then the patient's medical diagnosis image was taken as secret image and Arnold transform was applied and obtained a scrambled secret image.

S. Nithya, K. Amudha [4] proposes AES (Advanced encryption standard), SHA 256 and arithmetic compression techniques. The ROI of medical image is irregularly shaped and it is an area which contains important patient information. The protection of medical image information and the whole image of SHA 256 is embedded in the least significant bits of the ROI. The compression of recovered SHA 256 image and extracted water marking for medical validations. Fragile watermarking scheme [6] can detect and recover the tampered images. The watermarking technique being developed a secure, confirm and simplify technique for verification, safety, privacy protection, copyright protection and safety management for digital transformation.

Many algorithms have been researching to encrypt the high information in the original image but quality of watermarked image will worse when increasing information. This approach proposes concept and algorithm to apply watermarking and image encryption and decryption for medical image to match with real situation require.

2. METHODS

1.1 Discrete Cosine Transform (DCT)

DCT represents the data in terms of frequency band space other than one dimension space[5][7]. It is useful because it affects the way more and more people, so that part which has not been apparent can be recognized and thrown away. Watermarking technique using DCT is stronger than local domain technologies.

$$F(m,n) = (\frac{2}{\sqrt{MN}})C(M)C(N)\sum_{X=0}^{M-1}\sum_{Y=0}^{N-1} f(x,y)x \cos\frac{2x+1}{2M}$$
$$\pi m \cos(\frac{2y+1}{2N})\pi n \quad (1)$$

$$F(x,y) = (\frac{2}{\sqrt{MN}})\sum_{X=0}^{M-1}\sum_{Y=0}^{N-1} F(m,n)C(m)C(n)x\cos(\frac{2x+1}{2M})$$
$$\pi m \cos(\frac{2y+1}{2N})\pi n \quad (2)$$

Where C(m)C(n) $=\frac{1}{\sqrt{2}}$, F(m,n) and F(x,y) represent the image pixels value in form of DCT and Spatial domain. M, N is the image's size. In many researches transform image by DCT then divided into non-overlapped m x m block.

2.2 Arnold Transform

Arnold transformations is a simple chaotic map and mainly used for image scrambling using shifting the position of pixels instead change values. The Arnold transformation function represent as in Eq.3. [4][5][6]

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod1 \quad (3)$$

Where (x mod 1) is a fractional part of x for real values. To increase the reliability of scramble, Arnold transformation is given with two other parameters a, b represent as in Eq. 4.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod1 \quad (4)$$

Where a, b are real values call control parameters. [6] Both values are greater than 1 will increase stronger of chaotic. This is another technique for increase less visible by repeating loop of Arnold transformation.

2.3 Two-Dimensional Barcode (Data Matrix Barcode)

Data Matrix Barcode [11] was invent in mid of 1980stoeliminate the limit of the One-Dimension Barcode for data capacity and size. Data Matrix Barcode in this research use ECC200 standard, which has error checking and error correction algorithm, able to recognition up to sixty percent damaged by using Reed-Solomon error correction. This is matrix barcode which can be constructed as a square or rectangular symbol. The size of image depend on the amount of information. Maximum data capacity of number and alpha is 3,116 and 2,335 characters respectively. The specification is follow in ISO/IEC 16022 standard. [12] Data Matrix Barcode is composed of two separate parts, the finder pattern, which is used by the scanner to locater the symbol, and the encoded data itself. The solid dark is called the "L finding pattern". It is primarily used to determine the size, orientation and distortion of the symbol. Two-Dimensional Barcode ECC200 standard is the best type compare with other standards for the smallest size with the same data information. Fig. 1 shows a structure of this barcode. Fig. 2 shows readability of Data Matrix Barcode although shape distortion, image rotation attack and damaged barcode.

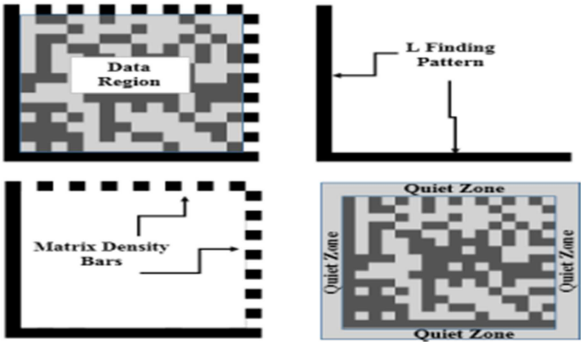


Figure 1: Data Matrix Bar Code

2.4 Steganography

Steganography is the [9]process of hiding sensitive and privateinformation within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because they are similar wayand both are used to secure sensitive information [10].Steganography involves hiding information so it appears that no information is hidden at all [13]. If a person or persons access or views the object that they have hidden information inside of that, he or she will have no idea that there is any hidden information; therefore the person will not attempt to decrypt information. Steganography Process:

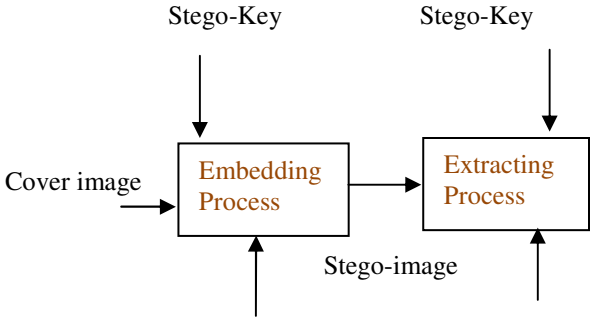


Figure 2: Steganography Process

3. PROPOSED METHOD

Since, in the present world there is measure requirement of successful algorithms to prevent illegal stealing of multimedia contentapplications such as Medical images of patient data. The main objective to secure the medical data by a new sound method to store the sensitive information of patients to prevent the stealing from others. In this work using the watermarking, steganography and DCT, to designed algorithm which has given the best outcome result in Encryption and Decryption of image. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The DCT has special property in which the most of the visually significant part of the object is concentrated in just a few coefficient of the DCT.

The proposed Methodology Workflow follows:

3.1 Watermark Embedding Process

The embedding process consists of following steps:

1. Collect the information of patient data and convert the data into Two-Dimensional Barcode format,to improve the high capacity of watermark with image size m x n.
2. Create the 1st scrambling method by using Arnold Function from the original watermark image then we got the watermark image after scrambling.
3. Apply DCT into block.
4. Consider position for embed information perform two level IDCT decomposition and perform image encryption.

3.2 Watermark Extraction Process

The watermark image is extracted process by follows steps:

1. Input security password that identified by patient or people who have the authorization.
2. Perform extraction watermark by reverse from embedding step then confirm barcode readability.

3.2 Watermark Extraction Process

The watermark image is extracted process by follows steps:

1. Input security password that identified by patient or people who have the authorization.
2. Perform extraction watermark by reverse from embedding step then confirm barcode readability.

3.3 Image Encryption

1. Get the patient details from edit text.
2. Converting details into a matrix.
3. Converting the id-matrix into character matrix using a zero matrix of 11x11 elements
4. Take image from database and resize in 480x480 resolutions.
5. Use bit set function on image
6. Apply 2-D DCT (Discrete Cosine Transform) on image.
7. Apply Arnold Function on image.
8. Encrypted Image.

The watermark image is extracted process by follows steps:

3.4 Image Encryption

1. Get the Password from Patient.
2. And compare password the Database.
3. Apply Inverse Arnold Function.
4. Apply Inverse Discrete Cosine Transform.
5. Apply unsigned 8-Bit format.
6. Decrypted Image

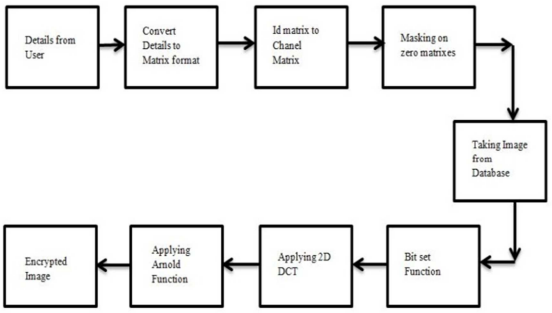


Figure 3: Encryption Block diagram

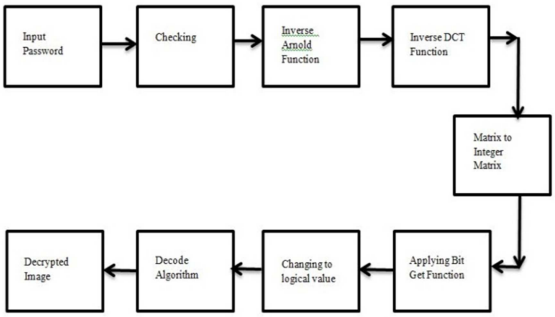


Figure 4 : Decryption Block diagram

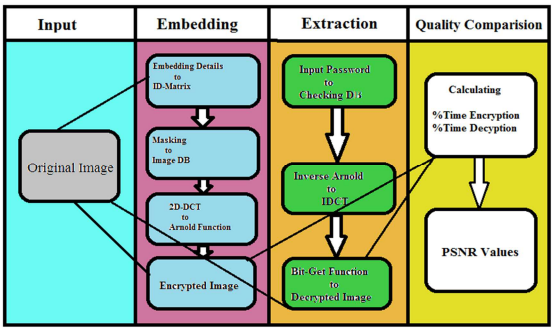


Figure 5 : Process behind the Work

4. EXPERIMENTAL RESULT

The performance of proposed algorithms has been studied by means of MATLAB simulation

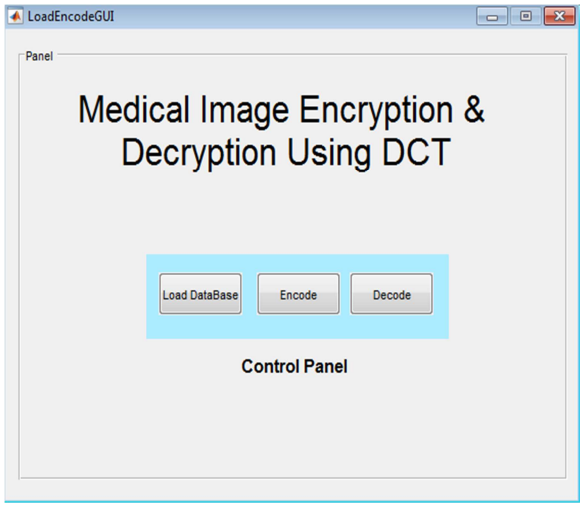


Figure 6 : GUI Model

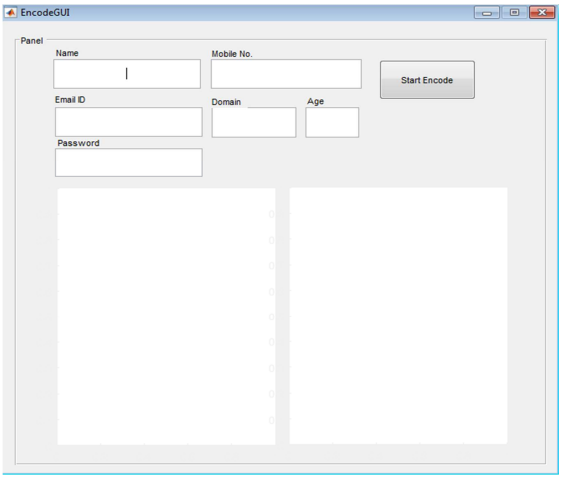


Figure 7 : Patient Information Application

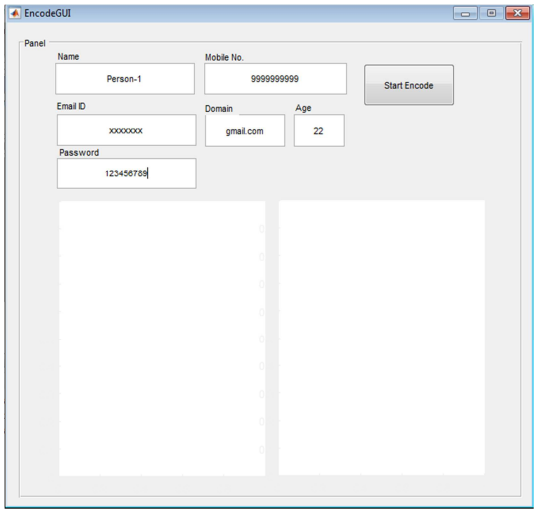


Figure 8 : Inserting Patient Data in Database

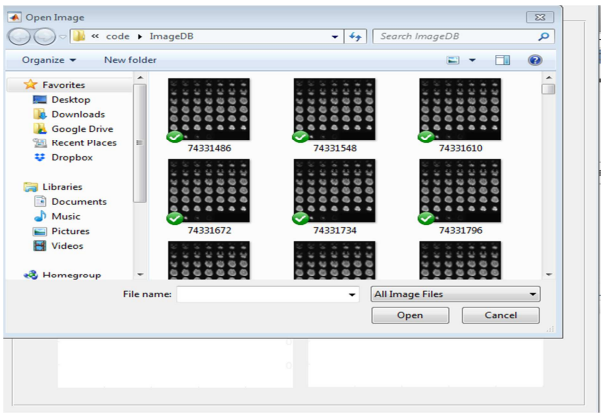


Figure 9 : Loading Medical Image to Store in Database

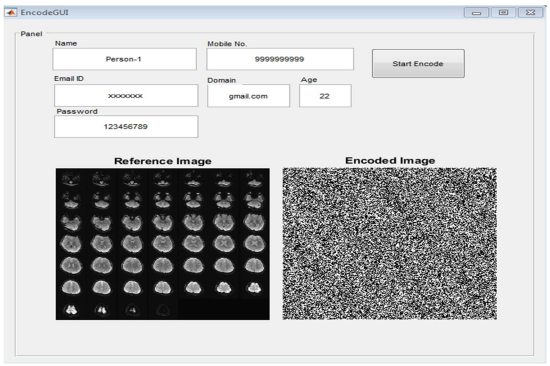


Figure 10 : Encrypted Image

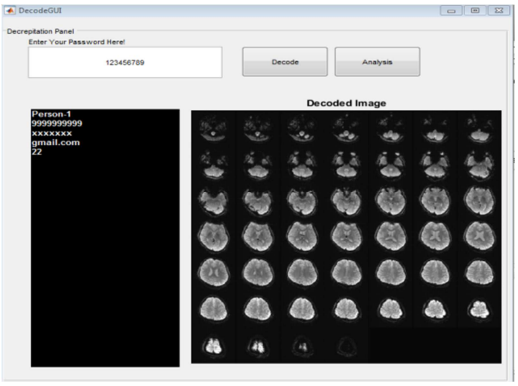


Figure 11: Inserting Patient key to Decryption

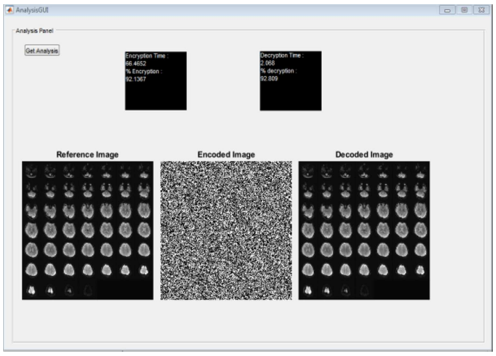


Figure 12 : Decryption Image With Data

5. CONCLUSION AND FUTURE WORK

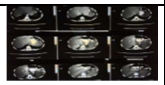
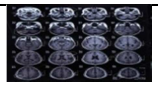
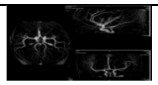
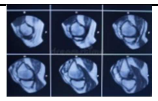
In this work, Medical Image Encryption and Decryption by using DCT is provided. It strengths the image attacks, which shows the fake patient data. It achieves the Encryption and Decryption of image with Image-imperceptibility versus robustness. Using DCT method with watermarking method to create PSNR value of any image >70% and we got successful encryption and decryption of image with high PSNR value.

Using the combination of DCT and Watermarking and steganography, the implementation of securing Patient data from stealing can be achieved with standard results achieved as follows:

1) This paper has proposed a medical image encryption and decryption scheme based on DCT by apply scramble process technique to increase high embed capacity with maintain high PSNR which is an important information for medical image.
2) This paper also proposed additional operation of image encryption after complete embed by use unique security key for patient to decrypt the real image.

In this work images are not 100% accurate till date. As future aspect medical images protection based on DCT and bar code approach proposed here can be further improved PSNR values. So in the future it can be implemented to secure for attacks.

Table I. Accuracy obtained by different medical images

S. No.	Name	Picture	% Enc time	% Dec	Dec time	PSNR
1	Abdomen		11.67	92.64	2.02	71.66
2	Brain		8.07	84.64	2.07	70.04
3	Brain		5.46	69.50	2.10	78.89
4	Foot		9.17	78.90	2.06	76.94
5	Hand		11.30	77.61	2.05	76.55
6	Knee		7.8	97.49	2.6	70.20

REFERENCES

[1] Mei Jiansheng, Li Sukang and Tan Xiaomei "A Digital Watermarking Algorithm Based On DCT and DWT" , ISBN 978-952-5726-00-8 (Print), 978-952-5726-01-5 (CD-ROM)

[2] Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09)

[3] M. P. Turuk, A. P. Dhande, P. P.Kalgaonkarl, "Performance Evaluation of Frequency Domain Techniques for Efficient Storage of Patient Information with Medical Images", Las Vegas,NV, vol. 3, pp. 112-118, June 1997.

[4] Prabakaran G, Dr. Bhavani R, Rajeswari P. S. "Multi Secure and Robustness for Medical Image Based Steganography Scheme", DOI: 10.1109/ICCPCT. 2013. 6528835 Conference: Conference: Circuits, Power and Computing Technologies (ICCPCT), 2013

[5] S. Nithya and K. Amudha, "Watermarking and encryption in medical image through roi-lossless compression," *2016 International Conference on Communication and Signal Processing (ICCSP)*, Melmaruvathur, 2016, pp. 0610-0614. doi: 10.1109/ICCSP.2016.

[6] Ross J. Anderson, Fabien A.P. Petitcolas, "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, May 1998.

[7] Gavin Longmuir,"Privacy and Digital Authentication",http://caligula.anu.edu.au, May, 2000.

[8] Sanwta Ram Dogiwal, Y.S.Shishodia, Abhay Upadhyaya "Super Resolution Image Reconstruction Using Wavelet Lifting Schemes and Gabor Filters", Published in Confluence, Fifth International conference 2014, 978-1-4799-4236-7/14/$31.00© IEEE.

[9] Sanwta Ram Dogiwal, Y S Shishodia, Abhay Upadhaya "Efficient Lifting Scheme Based Super Resolution Image Reconstruction Using Low Resolution Images " Published in Springer International Publishing, Vol. No. 27, pp. 259-266. 2014.

[10] Brain Fitzgerald, Fuping Gao, Damien O'Brien, Sampsung Xiaoxiang Shi, "Copyright Law, Digital Content and the Internet in the Asia-Pacific", Sydney University Press, March, 2008.
[11] Frank hartung, Martin kutter, "Multimedia Watermarking Techniques" for Avoiding Unauthorized Replication", IEEE, 1999.
[12] Wolfgang R.B., Delp E.J., "A watermarking technique for digital imagery: Furtherstudies", Proc. Int. Conf. on. Imaging Science, Systems and Technology, Las Vegas,NV, vol. 3, pp. 112-118, June 1997.
[13] Vipula Singh, "Digital Watermarking: A Tutorial Cyber", Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), January 2011.
[14] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", 3rd International Conference on Industrial Informatics (INDIN 2005), IEEE, 2005.