Medical Image Encryption Using Block-Based Scrambling and Discrete Wavelet Transform

S. Kulasekaran[1], Feminna Sheeba[2], B. Saivigneshu[2], C. Dayalan[2], and P. Cyril Rex[2]

[1] Healthcare Technology Innovation Centre, Chennai, India
[2] Department of Computer Science, Madras Christian College, Chennai, India

Abstract— **In today's age of manifold advances in the field of medical imaging, a significant amount of sensitive and personal information related to patients is being transmitted electronically via images. With the advent of e-Health and Telemedicine in the vast field of medicine, there is a need to guarantee the authenticity and validity of the images being exchanged. The much-need security of medical images imposes the conditions of confidentiality, reliability and availability, and these can be attained by various Image Authentication methods and one such authentication is Image Encryption. The proposed work aims at an Image Encryption technique, which is a combination of Tiling, Scrambling and Image Transformation and Encryption of the image. The proposed architecture for encryption and decryption of a medical image is using a symmetric key, which gives the size of the tiles and the hash code of the image. The encryption algorithm divides the image into tiles of arbitrary size, scramble them using a scrambling technique and transform the scrambled image using Discrete Wavelet Transform (DWT). The hash code in the key is used to find out if tampering has taken place during transmission of the medical image.**

Keywords— **Red blood cells, Morphology, Houghman Transformation, watershed, extreme points.**

I. Introduction

The recent advances in the field of medical imaging and transmission of images across networks, include transmission of significant amount of sensitive and personal information of patients as images, With the advent of e-health and telemedicine, there is a need for authentication and validation of images being exchanged across networks. Moreover such medical images have to be confidential, reliable and securely available which can be attained with image authentication. Image authentication verifies the originality of an image by detecting malicious manipulations. This can be attained by various ways including encryption, cryptography, digital signatures and watermarking.

A method is suggested which can distinguish malicious manipulations from JPEG lousy compression regardless of how high the compression ratio is [1]. **A**n image scrambling encryption algorithm which makes use of one-dimensional chaos system for shuffling the pixel bits with the bit-plain of size M×8N is suggested in [2]. Detailed cryptanalytic results suggest that the image scrambling scheme can only be used to realize perceptual encryption [3]. Cryptography enables significant information to be stored or transmitted over non-secure networks, so that only authorized recipients can read it. Message authentication techniques are used in image integrity and authentication systems. Hash functions, private or public key systems and digital signatures are also used. The problem of a digital signature is that a conventional signature is physically attached to the signed document and that a conventional signature is authenticated by comparing it with a certified one [4]. In the recent times image authentication is achieved by the technique of watermarking. A spatial domain watermarking where the embedding is done in the non-region of interest is suggested in [5]. In order to gain robustness against attacks a frequency domain watermarking was suggested in [6]. In order to keep the images in perfect condition without any loss of information, the original image should be recovered upon the extraction of the embedded watermark [7] [8][9].

The proposed work aims at authentication of images, where the image is split into equal sized blocks, scrambling of the blocks, transforming the image and reversing the process at the receiving end. A key is generated during the watermarking process, which is used as a secret key for reversing.

II. Methodology

The source image is first split into various blocks or tiles with an arbitrary size. Scrambling algorithms which involves interchanging the first and third quadrants in each block is applied. This scrambled image is then transformed using the discrete wavelet transform. This transformed image is sent across the networks. In this process, a key is generated. This key is used to restore the original image in the receiving end. This is done by inversing the process by

J. Goh and C.T. Lim (eds.), *7th World Congress on Bioengineering 2015*,
IFMBE Proceedings 52, DOI: 10.1007/978-3-319-19452-3_17

using the secret key that was generated during transmission. The images when transmitted in networks may be tampered by unauthorized users. This tampering can be detected by obtaining the hash value of the image and matching it with the one that is in the key.

III. Results and findings

A prototype application was developed do test the image authentication method. 50 images were used for testing. One of the source images used is shown in Fig 1. The image was converted to a square image by adding black pixels to the width and height of the image as shown in Fig.2. The image was divided into various blocks of size 16 x 16. Each of the blocks was scrambled by interchanging the first and fourth quadrants. This is shown in Fig.3. The scrambled image was then transformed using DWT transformation [6] [10][11][12], which is shown in Fig. 4. A key was generated with the block size and the hash code of the image.

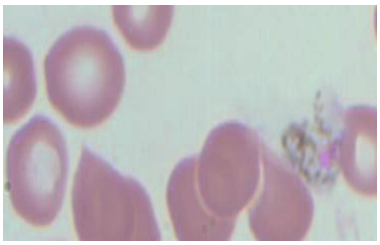

Fig.1 Source image

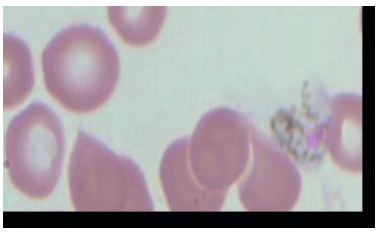

Fig.2 Square Image

Fig.3 Scrambled Image

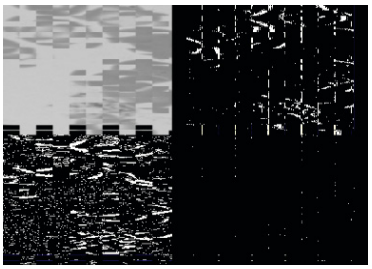

Fig.4 DWT Transformed Image.

In the receiving the image was decrypted using the secret key. Inverse DWT was applied to get the scrambled image, which is shown in Fig. 5. This image was then unscrambled which is shown in Fig 6. The hash code of the unscrambled was calculated and matched with the hash value in the Key. It was found that both were the same meaning that the image was not tampered.

Fig.5 Scrambled Image

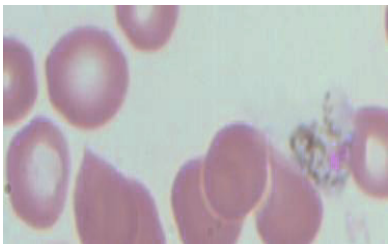

Fig.6 Unscrambled Image

IV. CONCLUSION

Image authentication is the need of the hour as images are sent across the networks for taking second opinion from clinicians. Also the images have to be stored for future study. Hence tampering of images can be found out using

the image authentication method discussed. The method gave expected results which could be easily incorporated in applications involving telemedicine and e-health.

REFERENCE

1. Jianfeng Lua , Meng Wanga , Junping Daib,Qianru Huanga , Li Lia,∗ and Chin-Chen Changc d, Multiple Watermark Scheme based on DWT-DCT Quantization for Medical Images Journal of Information Hiding and Multimedia Signal Processing 2015 ISSN 2073-4212 Ubiquitous International Volume 6, Number 3, May 2015

2. Liang Zhao, Avishek Adhikari, Di Xiao, Kouichi Sakurai, Cryptanalysis on an Image Scrambling Encryption Scheme Based on Pixel Bit, Conference: Digital Watermarking - 9th International Workshop, IWDW 2010, Seoul, Korea, October 1-3, 2010, DOI: 10.1007/978-3-642-18405-5_5

3. Shujun li, chengqing li, kwok-tung lo, guanrong chen Cryptanalysis of an image scrambling scheme without bandwidth expansion, Circuits and Systems for video technology IEEE transactions, volume:18, issue: 3, pp. 338 – 349, 2008, doi: 10.1109/tcsvt.2008.918116

4. Adil Haouzia & Rita Noumeir, Methods for image authentication: a survey Multimed Tools Appl (2008) 39:1–46, Springer Science + Business Media, LLC 2007, DOI 10.1007/s11042-007-0154-3

5. Feminna, S., H.M.T. Thomas, and J.J. Mammen, Segmentation and Reversible Watermarking of Peripheral Blood Smear Images. Proc. IEEE Conference on Bio Inspired Computing: Theories and Applications 2010. 2: 1373-6.

6. Feminna, S., Robinson T., J.J. Mammen , H.M.T. Thomas and Atulya K. Nagar.: White Blood Cell Segmentation and Watermarking. In: Proceedings of the IASTED International Symposia Imaging and Signal Processing in Healthcare and Technology, ISPHT 2011,Washington DC, USA (2011).

7. M.Sreerama Murty, D.Veeraiah, 3A.Srinivas Rao, Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis, Signal & Image Processing : An International Journal (SIPIJ) Vol.2, No.2, June 2011

8. Imen Fourati Kallel, Mohamed Salim Bouhlel, Jean-Christophe Lapayre, “Improved Tian’s Method for Medical Image Reversible Watermarking”, GVIP Journal, Volume 7, Issue 2, August 2007.

9. Feminna, S., Robinson T., Joy John Mammen and Atulya K. Nagar, Detection of plasmodium falciparum in peripheral blood smear images. In: Proceedings of BICTA 2012, 202 (2013) 289–298

10. FeminnaSheeba,Robinson Thamburaj,Atulya K. Nagar, Image Authentication using Reversible Watermarking, Proc. *Conference* on Mathematics in Engineering & Business Management (*ICMEB 2012*) Volume 2. pp.408-410

11. Gonzalez, Woods, Digital Image Processing 3ed (Prentice Hall 2008)

12. .Gonzalez, Woods,Eddins, Digital Image Processing using Matlab (Pearson Education 2009)