DWT BASED ENCRYPTION TECHNIQUE FOR MEDICAL IMAGES

JOSHUA CALEB DAGADU, JIAN-PING LI, FADIA SHAH, NADIR MUSTAFA, KAMLESH KUMAR

[1]International Centre for Wavelet Analysis and Its Applications, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, P. R. China
E-MAIL: joscaldag@yahoo.com, jpli2222@uestc.edu.cn

Abstract:

The security of medical images has attracted much attention recently, especially when these images are hosted by third party cloud service providers and therefore must be sent through the communication networks. A key challenge in the cloud computing paradigm is the design of efficient security schemes that help address the issues of confidentiality, integrity and authentication. Consequently, we propose a fast and robust encryption technique for gray scale medical images for real time applications. Our technique first compresses the medical image in the discrete wavelet transform (DWT) domain before encrypting with an algorithm based on basic pixel permutation and randomness. In the DWT domain, correlation and redundancy are reduced while random pixel permutation with encryption key provides confusion and diffusion. Our simulation results demonstrate the potentials of our technique.

Keywords:

Image compression; medical imaging; encryption; pixel permutation; DWT; redundancy; pixel correlation

1. Introduction

Medical images are at the heart of health information systems. They form critical components of medical diagnostic procedures due to the fact that, aside of providing means of evaluation and management of patients' diagnosis and treatment effects, they also offer a non-invasive method of viewing anatomical cross sections of internal organs and other features of patients. The current advancements in healthcare delivery systems, remote access to medical data and cloud storage of health and imaging data are key to effective healthcare delivery. The very critical nature of health services and the myriad advantages and opportunities provided by software, storage and transmission technologies make it possible for a more efficient healthcare delivery; hence the popularity of tele-diagnosis, tele-surgery and tele-consultation [1].

With the adoption of cloud storage of medical images, the need to enhance the security of these images has increased due to the increase in malicious activities on cyber critical infrastructure, not excepting those of the health sector. Unsecured storage coupled with unsecured transfer of medical images such as Magnetic Resonance Imaging (MRI) scans between a cloud medical database and a health center means a low level of confidentiality and integrity to patients' information. Consequently, measures have to be put in place to ensure confidentiality, integrity and availability of medical images outsourced to cloud database service providers.

Various promising approaches for securing medical images have been proposed; however, much more needs to be done towards the attainment of a satisfactory efficiency level. According to [2], existing security mechanisms used in medical image systems are mostly based on the conventional encryption schemes such as DES, RSA, AES, and IDEA. However, due to some intrinsic features of images such as high redundancy, bulk data capacity, and strong correlation among adjacent pixels, these encryption techniques are not ideal for practical image encryption. "Only a few image encryption algorithms, exclusively designed for digital gray scale medical images are seen in the literature"; besides, the existing colour image encryption schemes have low encryption rates and most of them are lossy in nature [1]. Hence, it is desirable to provide rigorous security approaches for securing medical images.

In this paper, we exploit the strengths of the DWT and pixel permutation to provide a fast and robust scheme for encrypting medical images. Our approach reduces image size, pixel correlation and redundancy, which increases encryption speed and reduces success of plaintext attacks. The rest of the paper is organized as follows: In section 2 we explain the Haar DWT; in section 3, we introduce pixel permutation and cryptography; in section 4, we discuss our proposed methodology. We discuss experimental results in section 5 and finally conclude in section 6.

2. Haar DWT Image Compression

Compression has two elementary components namely

redundancy reduction and irrelevancy reduction. Redundancy reduction removes duplication from the signal source image while irrelevancy reduction removes signal portions that are unnoticed by the signal receiver, the Human Visual System (HVS) [3]. DWT compression reduces the redundancy in the image and makes it difficult for plaintext attacks that are based on data redundancy. The Haar wavelet transform uses a scale function $\phi(t)$ and a wavelet $\psi(t)$ for representing a large number of functions $f(t)$. The representation is the infinite sum [4]

$$f(t)=\sum_{k=-\infty}^{\infty} c_k \phi(t-k)+\sum_{k=-\infty}^{\infty}\sum_{j=0}^{\infty} d_{j,k}\psi\left(2^j t-k\right) \quad (1)$$

Where c_k and $d_{j,k}$ are coefficients that are to be calculated.

The basic scale function $\phi(t)$ is the unit pulse

$$\phi(t)=\begin{cases}1, & 0 \le t < 1,\\ 0, & \text{otherwise.}\end{cases} \quad (2)$$

The function $\phi(t-k)$ is a copy of $\phi(t)$ that is shifted k units to the right. Likewise, $\phi(2t-k)$ is a copy of $\phi(t-k)$ scaled to half the width of $\phi(t-k)$. The shifted copies are used in approximating $f(t)$ at different times t while the scaled copies are used in approximating $f(t)$ at higher resolutions.

The basic Haar wavelet is the step function

$$\psi(t)=\begin{cases}1, & 0 \le t < 0.5,\\ -1, & 0.5 \le t < 1.\end{cases} \quad (3)$$

From this, it is clear that the general Haar wavelet $\psi\left(2^j t-k\right)$ is a copy of $\psi(t)$ that is shifted k units to the right and is scaled in a way that its total width is $1/2^j$. Both $\phi(2t-k)$ and $\psi\left(2^j t-k\right)$ are nonzero in an interval of width $1/2^j$ which is their support. Because this interval is short, these functions are said to have compact support [4].

An image comprises of pixels that are represented by numbers [5]. When averaging and differencing as explained in [3] and [4] are performed on the image matrix, we obtain a new matrix that represents the same image in a more concise form.

When the reverse operations of averaging and differencing are performed on the final matrix, the original image can be obtained. Threshold values influence the quality of the compressed image. Due to the very sensitive nature of medical images, threshold values must be set carefully to preserve image diagnostic quality.

3. Pixel Permutation and Cryptography

Permutation techniques are essential building blocks when combined with random generators for the purposes of image encryption.

A permutation process of n degree refers to the operation of replacing an arrangement $\{p_i \mid i=1,2,\ldots,n, p_i \in S\}$ by another arrangement $\{q_i \mid i=1,2,\ldots,n, q_i \in S\}$ represented as [6]

$$\phi=\begin{pmatrix} p_1 p_2 \cdots p_n \\ q_1 q_2 \cdots q_n \end{pmatrix} \quad (4)$$

Where $n!$ of such permutations are possible and S denotes any non-empty set. The reverse of this permutation process is

$$\phi^{-1}=\begin{pmatrix} q_1 q_2 \cdots q_n \\ p_1 p_2 \cdots p_n \end{pmatrix} \quad (5)$$

Formally, permutation is a one-to-one mapping of any non-empty set S onto S and the set that contains all of such mappings is denoted by S_n with $n!$ members if S has n elements. Based upon this definition, a permutation aided cryptographic process can also be seen as:

Definition: If any data matrix X is transformed to a cipher matrix $\psi_z=\phi_z(X)$ where ϕ_z is any permutation operation, then the original matrix X can be obtained again from the inverse operation of ψ_z That is, $\phi_Z^{-1}(\psi_Z)=\phi_Z^{-1}(\phi_Z(X))=X$ since $\phi_z^{-1}\phi_z$ forms an identity [6]. In most permutations, all the elements may not be displaced; leading to some residual intelligence which could help attackers. Hence, only certain permutation patterns (keys) that increase the level of security are considered. According to [7], good permutation keys have some properties that help reduce intelligible information.

There are three basic permutation techniques for image matrices namely bit permutation, block permutation and pixel permutation. In pixel permutation, groups of pixels are selected from the image. The pixels in each group are permuted using selected keys [6]

4. Methodology

Our approach differs from previous works in the sense that we first exploit the property of the DWT to reduce redundancy and pixel correlation in the image; then we use sub and full image permutations by image decomposition to

provide both diffusion and confusion. We make use of random permutation with different keys in the encryption and decryption processes.

Figure 1 is the block diagram of the encryption process.

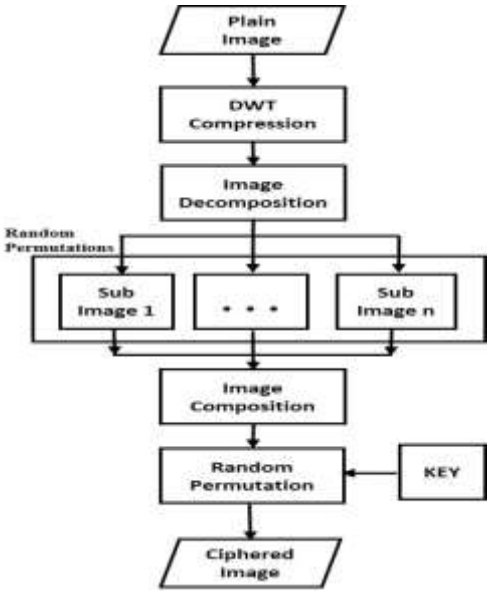

Fig.1 Block diagram of encryption process

4.1. Compression Process

Compression is achieved by applying a linear transform (DWT) to de-correlate the image data, quantizing the transform coefficients and entropy coding the quantized values [3].

Thresholding modifies wavelet coefficients that are close or equal to zero so that the sequence of wavelet coefficients contains long strings of zeros. This makes it possible for storage and transmission in much less space [8]. The quantizer reduces the number of bits needed to store the transformed coefficients by reducing the precision of the values and this is the main source of compression in the encoder. The entropy encoder additionally compresses the quantized values in a lossless manner to give a better compression entirely [3].

The inverse of the DWT reconstructs the image exactly as the original once the threshold value is set to 0.

4.2. Encryption

The compressed image becomes the input (Plain Image) of the encryption process. Algorithms 1 and 2 are the encryption and decryption algorithms.

Algorithm 1 Encryption

Input: Plain image **(I),** key **(K),** iterations **(R)**
Output: Cipher image **CI**
I← read (plain image)
S ($I_1, I_2, I_3, \ldots, I_n$) ← Decompose (I)
for each $I_i \in S$ where i = {1, 2, 3,…, n} **do**
    [M, N] = Size (I_i)
    E = entropy (I_i)
    Mn = mean (I_i)
    Compute sub key (sk_i) with E and Mn
    Generate random numbers with sk_i
    for J = 1 to MN, Step X
        if (pixels not permuted > 2) **then**
            Random permute 2 pixels
        end if
        Track pairs of permuted pixels
        Track sk_i
    end for
end for
EI ← Re-compose sub images (S)
CI← random permute pixels in EI using K, R times
Return CI

Algorithm 2. Decryption

Input: Cipher image (C**I),** key **(K),** sub keys (**sk_i), R**
Output: Plain image **I**
CI← read (cipher image)
EI← inverse permute pixels in CI using K, R times
S ($I_1, I_2, I_3, \ldots, I_n$) ← Decompose (EI)
for each $I_i \in S$ where i = {1, 2, 3,…, n} **do**
    Generate random numbers with sk_i
    for J = 1 to MN, Step X
        if (exists pixels not reversed) **then**
            inverse permute those pixels
        end if
        Track reversed pixels
    end for
end for
I ← Re-compose sub images (S)
Return I

The sub key of each sub image is generated with its entropy and arithmetic mean. The main key, K is a 64 bit key provided as input. For decryption, all the keys are provided as inputs.

5. Results and Discussions

Figure 2 shows one result of the experiment. Sub-figures a, b, c, d; e, f, g and h represent the original, encrypted, decrypted and reconstructed images; histograms

of original, encrypted, decrypted and reconstructed images respectively. The decrypted image is initially in its compressed form and can be reconstructed exactly as the original. For the purposes of showing the efficiency and potentials of this technique, we only show the result after one iteration. It is evident from figure 2 and table 1 that, after just one iteration, a good level of encryption is attained. Increasing the number of iterations produces an evenly distributed histogram but reduces encryption speed.

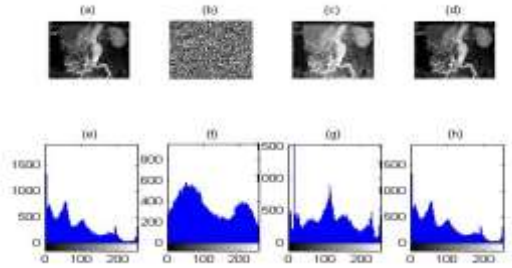

Fig.2 X-ray of the Aorta

In images, neighbouring pixels are highly correlated. A less correlation between adjacent pixels provides a stronger ability to resist statistical attacks. The following equations as explained in [9] are used to calculate the correlation coefficient between adjacent pixels

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{6}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2 \tag{7}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{8}$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{9}$$

We randomly selected 2000 pairs of adjacent pixels from both original and encrypted images and calculated their horizontal, vertical and diagonal correlation coefficients. Table 1 shows two of the results

Table 1 Correlation between adjacent pixels

Image	Correlation	Original	Encrypted
Knee 226X300	Horizontal	0.9729	-0.0070
	Vertical	0.9932	-0.0015
	Diagonal	0.9741	0.0054
Aorta 300X300	Horizontal	0.9284	-0.0109
	Vertical	0.9420	-0.0014
	Diagonal	0.8773	0.0006

6. Conclusion

We have proposed an encryption technique based on DWT compression and pixel permutation for gray scale medical images. In this approach, pixel correlation and redundancy are reduced; and diffusion and confusion are adequately provided. Our approach has exhibited good computational speed and a security good enough for real time and mobile applications where protection is needed mainly against casual attackers and plaintext attacks. It could be applied to non-regions of interest in selective encryption approaches where the region of interest is encrypted with a more robust algorithm such as the DES.

Acknowledgements

This paper was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, and the Scientific Research Project of Chengfei Group.

References

[1] N. K. Pareek and V. Patidar, "Medical image protection using genetic algorithm operations," Soft Comput., vol. 20, no. 2, pp. 763–772, 2016.

[2] M. A. F. Al-Husainy, "A novel encryption method for image security," Int. J. Secur. Its Appl., vol. 6, no. 1, 2012.

[3] K. H. Talukder and K. Harada, "Haar wavelet based approach for image compression and quality assessment of compressed image," arXiv Prepr. arXiv1010.4084, 2010.

[4] D. Salomon, A guide to data compression methods. Springer Science & Business Media, 2013.

[5] G. Beylkin, R. Coifman, and V. Rokhlin, "Fast wavelet transforms and numerical algorithms I," Commun. pure Appl. Math., vol. 44, no. 2, pp. 141–183, 1991.

[6] A. Mitra, Y. V. S. Rao, S. R. M. Prasanna, and others, "A new image encryption approach using combinational permutation techniques," Int. J. Comput. Sci., vol. 1, no. 2, pp. 127–131, 2006.

[7] S. R. M. Prasanna, M. E. Ashalatha, S. R. Nirmala, and K. N. Haribhat, "Study of permutations in the context of speech privacy," Proc. of ECCAP, pp. 99–106, 2000.

[8] P. S. Ritu, "A Review of Data Compression Technique."

[9] E.-S. M. El-Alfy, S. M. Thampi, H. Takagi, S. Piramuthu, and T. Hanne, Advances in Intelligent Informatics. Springer, 2015.