Medical image security using modified chaos-based cryptography approach

Methaq Talib Gatta and Shahad Thamear Abd Al-latief
Computer Science Department, University of Mustansiriya, Baghdad, Iraq

Abstract. The progressive development in telecommunication and networking technologies have led to the increased popularity of telemedicine usage which involve storage and transfer of medical images and related information so security concern is emerged. This paper presents a method to provide the security to the medical images since its play a major role in people healthcare organizations. The main idea in this work based on the chaotic sequence in order to provide efficient encryption method that allows reconstructing the original image from the encrypted image with high quality and minimum distortion in its content and doesn’t effect in human treatment and diagnosing. Experimental results prove the efficiency of the proposed method using some of statistical measures and robust correlation between original image and decrypted image.

1. Introduction

Recently; hospitals and medicinal appliances produce images in digital forms with the ability of storing and transfer these images electronically which improves the efficiency of the health care services institution [1]. These images plays a prime role in evaluate the oddity in the human body and have its importance to provide accurate diagnosing with only a still image “A Picture worth Thousand Words”[2]. With the remarkable development in communication technologies and the need of fast and secure treatments from remote location lead to phenomenal growth in the number of medical images that are transmitted daily [3] in to the open network, this result in many threat to these images by malicious attacks so the security of these medical image is essential and require reliable, fast and powerful security system [4]. There is no single encryption algorithm that is suitable for all image types, many popular encryption standard have been proposed such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), these standards are designed to the textual data encryption and the message can be decrypted by using the same key used for encryption so it is poorly suitable to the image encryption because it doesn’t meet the image requirements such as redundancy, high data capacity, strong correlation between pixels [5]. There are many researchers noticed the strong relationship between the chaos theory and the cryptography systems which can be used to achieve the desired level of image security because of the chaotic system strong properties such as high sensitivity to the initial conditions and parameters, aperiodicity, etc. any successful cryptosystem must have the diffusion and confusion effects, in order to be robust against several attacks[6], the chaos-based cryptography can achieve these two effects[7]. In this work the one dimensional standard chaotic logistic map 1D(SLM) is used for medical images cryptography by acting as a random numbers generator that input to the chaos-based cryptography modified algorithm steps depending on some determined number of iterations and specific algorithm for each step to have the desired level of security. Many researchers try to design image cryptography systems by using chaos, in [8] Zhang et al. proposed medical image protection scheme based on Arnold cat map to shuffle the image pixels and use the logistic map to change
the pixels values by a chosen number of the rounds for encryption and have proven its efficiency and security. In [9] Zhang et al. proposed a way to compress and encrypt the medical images which the plain image is compressed and encrypted by chaos-based Bernoulli measurement matrix, which is generated by the control of the Chebyshev map and perform a second level of protection by encrypt the result by permutation-diffusion type chaotic cipher, in [10] Rakesh S et al. present image encryption based on block scrambling using the chaotic Arnold cat map and also scramble the whole image again using the same map then the image is encrypted using a chaotic sequence generated using symmetric keys. In [11] Goce et al. present a block encryption algorithm based on two well-known chaotic maps exponential and logistic and have proven its efficiency against most of attacks rather than brute force attack.

2. Modified Method

This paper introduces the modified chaos-based cryptography algorithm by the use of the traditional architecture by Fridrich [12] in order to protect the security of medical images. The modification is presented through used the chaotic map rather than the two dimensional baker map as used in Fridrich’s work; it is a symmetric block encryption. This architecture mainly consist of two main stages: confusion and diffusion for medical image pixels where confusion applied to changing pixels locations in the original medical image and diffusion step applied to perform a transformation on pixels to change their values to remove correlation between pixels [13], 1D chaotic map is used as a key generator that known as standard logistic map (SLM) and its control parameter and initial value as a secret key for the cryptography process. Block diagram of the medical image encryption process shows in 'figure 1'.

![Figure 1. Block diagram of medical image encryption process.](image)

The input for the proposed encryption process is a gray-scale image that is get of image database [14]. The medical image in this work can take different size of rows and columns. The main steps of image encryption process shows in algorithm 1:

**Algorithm 1. Medical image encryption process**

Input: Encrypted medical image, initial value, parameters.
Output: Encrypted medical image.

Begin:
Step 1: Read the desired gray-scale medical image and save its pixels into a 2D array that suits the cryptography process.

Step 2: Use the 1D standard logistic map as a random key generator and its initial condition and its control parameter as image encryption secret key which given in equation (1).

\[ x_{n+1} = \mu x_n (1 - x_n) \] (1)

Where \( \mu \) is the system control parameter and the system is chaotic when \( 0 < \mu \leq 4 \) and \( x_0 \in [0, 1] \), this work uses \( x_0 = 0.4 \) and \( \mu = 3.87 \) as the secret key value.

Step 3: Confuse the pixels position in the array by using the random values generated from the 1D standard logistic map and change the pixels positions depending on modified confusion equation.

Step 4: Diffuse the pixels of the image depending on the random values generated from the 1D standard logistic map by performing some transformation on the image pixels using modified equation to give them new values that produce the ciphered image with uniform histogram shape.

Step 5: Iterate steps (3) and (4) until all image pixels are visited.

End

After complete the image encryption process, the encrypted image can be sent through communication network or stored in database with secure mode. At the other side, the decryption process is applied on encrypted image by inverse order of the encryption process. The main steps of image decryption process are shown in algorithm (2):

**Algorithm 2. Medical image decryption process**

Input: Encrypted medical image, initial value, parameters.

Output: Original medical image.

Begin:

Step 1: Read the gray-scale ciphered image and store it into a 2D array of pixels.

Step 2: Enter the same key used in encryption into the key generator which it is the initial value and the control parameter of the 1D standard logistic map, same values that are used in the encryption process.

Step 3: The pixels of the image are diffused by perform inverse transformation and return the value of each pixel to its original value.

Step 4: Confuse the pixels in inverse order and return pixels into their original positions in the original image.

Step 5: Iterate steps (3) and (4) for all image pixels.

End

3. Experimental Results

In this section, some results are described to show the performance and security of the proposed algorithm. The experiments are performed on three MRI medical images with the use of MATLAB 2016b programing language.

3.1. Histogram Analysis

In the following experiments, the original, ciphered, and recovered images and their histograms are described in figure 2. It’s obvious that the histogram of the ciphered image is completely different from the histogram of the original one and almost has a uniform distribution.
statistical attacks difficult because the ciphered image doesn’t provide any chance to employ any kind of it.

Figure 2. Experimental results of the modified encryption method: from the first to the fifth column are: original image, histogram of the original image, ciphered image, histogram of the ciphered image, and the recovered images, respectively.

3.2. Entropy Analysis
It is important property founded in information theory by Shannon [6] to give idea about them, the randomness and the unpredictability of an information source. Equation (2) used to calculate the entropy value [15].

$$H(m) = - \sum_{m=0}^{2^{N-1}} p(m) \log_2 p(m)$$

Where $p(m_i)$ is the probability of existence of the gray level value of pixel $m_i$ in the $m$ image and the log is taken to represent them in term of bits; since the gray-scale image pixel values is 256 gray levels then its contain 8 bits so the ideal entropy value to the secure cryptosystem must be 8 [16]. The entropies of the introduced medical images and their ciphered version are presented in table 1. It is evident that the entropies of the ciphered images are extremely close to the theoretical value of 8 which make the system able to resist the entropy attacks.

Table 1. Entropies of the original images and ciphered images.

| Tested image | Original image | Ciphered image |
|--------------|----------------|----------------|
| MRI-brain    | 4.7571         | 7.9993         |
| MRI-sinuses  | 5.1074         | 7.9993         |
| MRI-neck     | 6.1344         | 7.9994         |

3.3. Time Analysis
The required time in image encryption process is very important aspect and depends on the used encryption method complexity. This work uses Java v8 in medical image cryptography algorithm implementation. Table 2, illustrate time analysis result of the previous three medical images.
| Tested image | Encryption process | Decryption process |
|--------------|--------------------|-------------------|
| MRI-brain    | 0.282 sec          | 0.422 sec         |
| MRI-sinuses  | 0.421 sec          | 0.337 sec         |
| MRI-neck     | 0.671 sec          | 0.419 sec         |

4. Conclusions
In this paper medical image cryptography method is presented that based on chaos theory by using one of the most simple and popular one dimensional chaotic map which named standard logistic map. The results that have been shown proved that this method has an acceptable level of security rather than it is robust against statistical attacks and entropy attack.

References
[1] Zhang R and Liu L 2010 Security models and requirements for healthcare application clouds IEEE 3rd Inter. Con. on Cloud Com. USA 268-75.
[2] Vimala S and Nath B 2015 A survey on medical images Inter. J. Research in Science Eng. Tech. IJRSET 02 673-79
[3] Puech W and Rodrigues J M 2004 A new crypto-watermarking method for medical images safe transfer 12th Eur. Con. Signal Proc. Australia 1481-84.
[4] Mohan A K Saranya M R and Anusudha K 2014 Separable reversible data hiding using chaotic encryption and histogram shifting Inter. J. Simulation Sys. Tech. IJSSST 15.
[5] Pareek N K, Patidar V and Sud K 2006 Image encryption using chaotic logistic map Image Vis. Computing 24 926-34
[6] Shannon C 1949 Communication theory of secrecy systems Bell Labs Tech. J. 28 656-715.
[7] Kocarev L 2001 Chaos-based cryptography: a brief overview IEEE Circuits Sys. Mag. 21 6-21.
[8] Zhang L B, Zhu Z L, Yang B Q, Liu W Y, Zhu H F and Zou M Y 2015 Cryptanalysis and improvement of an efficient and secure medical image protection scheme Mathematical Pro. Eng.
[9] Zhang L B, Zhu Z L, Yang B Q, Liu W Y, Zhu H F, Zou M Y 2015 Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach Mathematical Pro. Eng.
[10] Rakesh S., Kaller A, Shadakshari B C and Annappa B 2012 Image encryption using block based uniform scrambling and chaotic logistic mapping Inter. J. Cryptography and Information Security IJCIS 02 49-57.
[11] Jakimoski G and Kocarev L 2001 Chaos and cryptography: block encryption ciphers based on chaotic maps IEEE Trans. Circuits and Systems I: Foun. Theo. App. 48 163-9.
[12] Fridrich J 1998 Symmetric ciphers based on two-dimensional chaotic maps Inter. J. Bifurcation and chaos 08 1259-84.
[13] Misra A, Gupta A and Rai D 2011 Analyzing the parameters of chaos based image encryption schemes World Appl. Programming 01 294-99.
[14] Gaata M and Hantoosh F 2016 An Efficient Image Encryption Technique using Chaotic Logistic Map and RC4 Stream Cipher Inter. J. Modern Trends Eng. Research (IJMTER) 03.
[15] Ponnain D and Chandranbabu K 2016 Security analysis of an image encryption algorithm based on paired interpermuting planes and a modified scheme Optic-Inter. J. Light and Electron Opt. 127 8111-23.
[16] Ahmad J and Fawad A 2012 Efficiency analysis and security evaluation of image encryption schemes Inter. J. Video and Image Processing N.W. Sec. 12 25.