Internet of Medical Things Application in Encryption of Medical Images Based on Synchronization of Multi-state Chaotic Systems

Ali Akbar Kekha Javan, Assef Zare

Department of Electrical Engineering, Gonabad Branch, Islamic Azad University, Gonabad, Iran

Abstract

Introduction: Studies on the security and interoperability of Internet of medical things (IoMT) in health are still scarce. The most important effects of the IoMT on health care are the ability to exchange information and reduce hospitalization and health care costs. The main challenges of the IoMT in healthcare are security and protection of privacy, among which encryption of images is very important in the field of communication and security. The main purpose of this study was to design a secure channel for encrypting and sending medical data.

Methods: This study presents a new method for encrypting medical images to preserve patient information by synchronizing two chaotic systems. The use of chaotic signals as carriers of medical images greatly enhances security and greatly reduces the possibility of detection. The idea of synchronization of chaotic systems was presented in multi states with fixed time delay. In this idea, with the help of Lyapunov's theory of stability, a controller was designed to establish the stability of the closed-loop system. Then, according to the synchronization idea and its error, a chaotic masking method was proposed to encrypt patient images. The simulation and accuracy of the results of the presented method were investigated in MATLAB software version 2020.

Results: The simulations were performed on medical color images and CT, MRI, and X-ray images. Encrypted and recovered images were obtained by the proposed system. To evaluate the performance of the proposed method, various criteria including image histogram, signal-to-noise rate, correlation, and entropy of information were evaluated. The results showed the excellent image encrypting efficiency of the proposed method.

Conclusion: Using the proposed method, medical images were encrypted based on a secure protocol, and then with satisfactory quality, images were recovered after transmission.

Keywords: Medical image encryption, Internet of things, Chaos theory, Delayed chaos systems, Multi-state synchronization

Introduction

In many developed countries today, large numbers of medical images are stored electronically. The expansion of electronic storage of medical images, on the one hand, and the existence of wired and wireless networks in most places, on the other hand, have made it possible to easily access and share images among medical personnel. At the same time, the easy distribution of images poses a major threat to the preservation of patient information. In such a situation, an effective tracking strategy against unauthorized distribution of medical images should be used. Protecting a patient's privacy by keeping his or her medical records confidential has always been an important issue in managing patients' medical records. In many developed countries today, a large number of medical images are stored electronically, which makes it easy to archive and access patient images. On the other hand, it is also possible to publish these images easily. Medical images play an important role in the medical field, both in the diagnosis and in the proper treatment of these diseases. There are different types of medical images, including magnetic resonance imaging (MRI), computed tomography (CT) scan, X-ray images, etc.

In this regard, a multi-parameter cosine number conversion was proposed. Experiments have shown that the design is...
resistant to covert attacks. Medical image cryptography was performed based on elliptical cryptography and chaos theory. The performance of the two system encryptions is evaluated in the categories of security analysis and duration of the run. The results are reliable and can be used in research fields. The protection of medical images has been studied using a genetic algorithm. Performance analysis shows that the proposed design has good statistical characteristics and key sensitivity and can resist differential, and entropy attacks, presenting a new encryption scheme for protecting medical images. It has high efficiency and shows the robustness of defending some impulse noise and data loss. There are two types of operations to implement the pixel adaptive diffusion: bitwise exclusive or (XOR) and modulo arithmetic. The former has high efficiency in hardware platforms while the latter can achieve fast speed in software platforms. Simulations and evaluations show that both encryption schemes using bitwise XOR and modulo arithmetic have high-security levels and can achieve much faster speeds. Digital images and communication encryption in medicine have been proposed based on chaotic gravitations in the frequency field by combining integer wavelet transform and deoxyribonucleic acid (DNA) sequences in the space field. A partial cryptographic algorithm for medical images based on secret response code and hidden reversible data technology was proposed. Another type of medical image encryption was proposed using a fractional discrete cosine transform with a chaotic function. The results showed that the proposed key flow generator was able to successfully meet the security needs of CT imaging for Covid patients. Medical image cryptography has also been studied based on the adaptive robust multiple synchronizations of Chen hyper-chaotic systems.

The Internet of Things (IoMT) is an ecosystem that combines physical objects, software, and hardware to interact with each other. The challenges of population aging, the scarcity of health care resources, and rising medical costs make IoMT-based technologies essential in health care. The healthcare sector is always looking for new approaches to provide services, reduce costs, and improve the quality of healthcare. Therefore, the reliance of this sector on IoT technology will increase. Choosing the correct data model is essential for data analysis. Efficient tools and technologies are needed to analyze the data. Medical data, including medical images, medical signals, etc. are recorded digitally, and this has led to the transfer of this information between specialist physicians to facilitate the process of diagnosis and treatment of many patients. One way to exchange information between medical professionals is through the IoMT. Communication technologies such as wireless loyalty (Wi-Fi), Bluetooth, radio frequency identification (RFID), and low-power wireless personal networks are often used in various IoT models, which among these, image encryption in communication and security fields are very important. The IoMT can implement cryptographic models and security fields for specific purposes. Of course, with the growth of the IoT and the increase in communications and data exchanges, security problems are also increasing. Information and network security must be met with characteristics such as identification, reliability, integration, and undeniability. Encryption (important information that must be exchanged or stored in insecure environments) therefore plays an important role in information security. In the following, the definitions of the systems used and their necessity and application in cryptography will be explained.

The concept of chaos is one of the new and fundamental concepts of modern science that can be reflected in many real-world phenomena, including systems that have seemingly random and disordered behavior and systems that have certain behaviors. Chaotic systems have properties such as non-linearity, extreme sensitivity to initial conditions, non-repetition of the path and its interruption, etc. In general, the problem of synchronization of chaotic systems means that two chaotic systems oscillate equally and simultaneously with each other. In synchronization of chaotic systems, the states of a master system are followed by the states of a slave system. The smaller the error of this tracing, the better the synchronization.

According to previous research, chaos theory has been used in the cryptography of medical images. However, in the application of medical image cryptography, no attention has been paid to multiple synchronizations with fixed time delays. This study presents a new method for encrypting medical images to preserve patient information by synchronizing two chaotic systems. The use of chaotic signals as carriers of medical images greatly enhances security and greatly reduces the likelihood of detection. In the following, the proposed method is implemented on Lorenz chaotic systems and various medical images are encrypted using chaotic masking. The efficiency of this method was evaluated by histogram analysis, correlation analysis, number of pixel change rate (NPCR), unified average changing intensity (UACI), peak signal to noise ratio (PSNR) and information entropy.

Methods
In this section, at first, the scheme of synchronizing multiple chaotic systems with fixed delay time was explained, in which medical images are carried on the signals of the chaotic system, then it was explained how we used the synchronization scheme to apply image encryption using a chaotic masking method.

Synchronization of Multi-state Chaotic Systems
The chaotic stimulus system is described as follows:
The slave chaotic systems are with control function as follows:

\[
\begin{align*}
\dot{x}_i(t) &= f_i(x_i(t)) + F_i(x_i(t - \tau_i)) + H_i(x_i(t))\theta_i(t) + u_{i,i}(t) \quad i = 2, 3, \ldots, N \\
\end{align*}
\]

In which \(x_i(t)\) system state vector of \(i\)\(^{th}\) system, \(f_i(x_i(t)) = [f_{i1}, f_{i2}, \ldots, f_{in}]\) continuous function, \(F_i(x_i(t - \tau_i))\) continuous function, \(\tau_i\) system delay that was unknown, \(H_i(x_i(t)) = [H_{i1}, H_{i2}, \ldots, H_{in}]\) matrix function, \(\theta_i(t) = [\theta_1, \theta_2, \ldots, \theta_n]\) are basic and unknown parameters of slave system \(i\)\(^{th}\), and \(u_{i,i}(t) = [u_{i1,i}, u_{i2,i}, \ldots, u_{in,i}(t)]\) are control functions of the slave system \(i\)\(^{th}\), which is suggested by the designer to Trace the master system.

Figure 1 shows the block diagram of the synchronization model between a master system and several slave systems.

**Encryption of Medical Images by the Chaotic Masking Method**

Encryption is the disorder of information that is incomprehensible to anyone. Encryption technology deprives unauthorized persons of the ability to view, read, and interpret messages. Encryption is used to protect data in public networks such as the Internet. In the chaotic masking method, an information signal is added to the linear combination of the chaotic signals. If \(M(t)\) is the original signal (medical image) carried by the master system and \(F(t)\), the transmission message is defined as follows:

\[
F(t) = M(t) + \sum_{i=1}^{n} \eta_i z_i(t)
\]

Where \(z_i(t)\) is \(i\)\(^{th}\) component of the master system, and the signal \(M(t)\) (medical image) is masked by the chaotic signal. The signal \(F(t)\) from the transmitter is sent to the receiver by a secure channel. Using the proposed controller and multi-mode synchronization of chaotic systems, the message signal (medical image) can be recovered from the received signal with the help of the following equation:

\[
\dot{M}(t) = F(t) - \sum_{i=1}^{n} \eta_i y_i(t)
\]

Where \(y_i(t)\) is \(i\)\(^{th}\) component of the slave system. According to the concept of synchronization, the following formula can be obtained:

\[
\dot{M}(t) = M(t) + \sum_{i=1}^{n} \eta_i z_i(t) - \sum_{i=1}^{n} \eta_i y_i(t)
\]

Using the chaotic masking method, a medical image is encrypted and decrypted using the proposed synchronization scheme. Simulation is with the use of MATLAB software version 2020. Encryption and decryption are applied after the synchronization of chaotic signals. For this purpose, we considered a medical image, and with the help of the reshape command, we converted the medical image matrix into a columnar array and used it as a message signal. We performed the encryption steps and then obtained the recovered signal (medical image) using the reshape command.

Figure 2 shows a block diagram of medical image encryption using proposed chaotic masking and multiple adaptive synchronizations. In this research, a secure cryptographic channel for medical images based on multistate chaotic systems with time delay and disturbance was presented. In this channel a multistate chaotic system is presented as the master system, as well as two slave chaotic systems based on the primary conditions estimate and the master system parameters.

**Results**

In this section, we describe the chaotic system as the system which carries the medical image and then explain the criteria for measuring the cryptographic parameters of medical data.

**Basic and Follower Multi-state Chaotic System**

One Lorenz chaotic system was considered as the master and two Lorenz chaotic systems were considered as slave, which are as follows:

\[
\begin{align*}
\dot{x}_{11} &= \theta_{11} (x_{12} - x_{11}) \\
\dot{x}_{12} &= \theta_{12} x_{12} - x_{11} x_{13} - x_{12} (t - \tau_1) \\
\dot{x}_{13} &= x_{11} x_{12} - \theta_{13} x_{13}
\end{align*}
\]

Where \(\theta_{ij}\) are system parameters. At the beginning of synchronization, we have:

\[
\dot{e}_{11} = 10, \dot{e}_{12} = 28, \dot{e}_{13} = \frac{8}{3}, i = 1, 2, 3
\]
Figure 3 shows the two-dimensional and three-dimensional phase curves of the Lorenz chaotic system, which indicates that the system is chaotic:

In the simulations, at first, these chaotic systems were synchronized, and then the encryption and decryption steps are performed.

**Statistical Metrics**

In order to demonstrate the efficiency of the proposed method, a variety of statistical parameters including the histogram of the original image and the recovered image, correlation, NPCR, PSNR, and information entropy for medical color images were calculated. The mentioned parameters are common criteria that have been used in various studies.1,2

The histogram is used to exhibit image pixels distribution. The more exactly the histogram curves match, the more successful the cryptographic scheme is. The correlation relationship between the input and encrypted images has been shown in Figure 4. This parameter indicates the degree of similarity and information protection between the input and output images. NPCR parameter was utilized to indicate the resistance of the encryption algorithm against differential attacks. The UACI parameter was utilized to prove the robustness of the encryption algorithm against differential attacks, and PSNR (the ratio of the peak power of a signal to the noise power) was used to represent the quality of the input and encrypted image.

Entropy is one of assessment parameters in image encryption. The entropy value for randomly generated images will be eight. The closer the entropy of an encryption method is to eight, the less predictable it is.1

**Experiment Results**

In the following, we use medical images including CT, MRI, and X-ray color images for cryptography. The size of all images was 300 × 300, and they were noise-free. Figure 4 shows the encrypted, recovered images as well as the histograms of the original and recovered images in the new method of synchronizing the correct order chaotic system. According to Figures 4 and 5, the proposed method has a successful performance in cryptography and recovery of medical images.

The images used to conduct the experiments included standard benchmark images and then color medical images. Various statistical parameters are presented in the following sections to demonstrate the efficacy of the proposed method.

Histograms for input and reconstructed images are shown in Figure 5. The method of synchronizing the proposed corrected order system encoded medical images successfully. The histograms of the input and reconstructed images are very similar, as it can be seen.

Figures 4 and 5 show that the images are well recovered. It is also observed that the histogram curve of the recovered image matches the histogram of the original
image. For each image, medical, statistical parameters such as histogram, cryptography, NPCR, UACI, PSNR, and information of entropy were calculated. The calculated statistical parameters have been presented in Table 1 for standard medical images.

Discussion
According to our results, color images acquired acceptable entropy, which means better encryption. The best entropy value was 7.2802, which is close to the standard eight, which indicates the successful operation of the encryption channel of the introduced images. The histogram difference between the input and recovered images was better in color images, and its minimum value was 356.6484, indicating the quality of the recovered image and the efficiency of the proposed design. Also, the correlation of the input and recovered images was very close to one, which is excellent, and in general, indicates the proper performance of this model for encrypting medical images, either in color or gray.

As mentioned, various studies have assessed the encryption of medical images in different ways, including genetic algorithms, elliptical chaos, discrete cosine fractional conversion with disturbing performance, etc. for color images and CT, EEG, MRI (Table 2). Each of them described their method based on some of the previously mentioned criteria. In this study, for the first time, we used multiple correct order chaotic systems with time delay and disturbance and tested this combination for CT, MRI, and color images, which was shown to be extremely successful according to the standard criteria.

According to Table 2, it can be perceived that the method proposed in this article has a high efficiency compared to other methods already applied. Medical data entails important information from patients and therefore their transferring and receiving are of particular significance. Medical information involves images, signals, and other data.

In the research of Moafimadani et al, a chaotic method based on the combination of bits was used to encrypt medical images and they used entropy, histogram, etc. to evaluate the proposed method. One of the differences of the recent work with our study was that they did not use time delay and did not evaluate unknown parameters. In Lima and colleagues’ study, cryptography of medical images was performed using a three-dimensional finite field rotation operator, and they used the parameters of covariance, NPCR, UACI, etc. to evaluate the performance, but the system model was not studied in multiple modes. In a study conducted by Benssalah et al, they encrypted medical images based on the chaos theory and elliptic curves, in which a single-state approach was used with no time delay or uncertainty.

Conclusion
According to the evaluation of the parameters, the proposed method for cryptography of medical images was successful and indicated the efficiency of the cryptographic channel, showing that no information was leaked in the transmission path. This proposed method can be used to encrypt other medical images such as COVID, EEG, and cardiac signals. Another feature of the chaotic system is that it is easy to change the parameters, replace the types
Table 1. Statistical Metrics for Medical Images Without Noise

<table>
<thead>
<tr>
<th>Images</th>
<th>Histogram</th>
<th>Correlation</th>
<th>Differential Attack</th>
<th>PSNR</th>
<th>Information Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Standard</td>
<td>Encrypted</td>
<td>NPCR (%)</td>
<td>UACI (%)</td>
<td></td>
</tr>
<tr>
<td>Image 1*</td>
<td>74440.2265</td>
<td>74083.5781</td>
<td>0.9998</td>
<td>97.69</td>
<td>51.9108</td>
</tr>
<tr>
<td>Image 2</td>
<td>146661.6640</td>
<td>145352.8125</td>
<td>0.9994</td>
<td>99.94</td>
<td>42.5356</td>
</tr>
<tr>
<td>Image 3</td>
<td>125273.1015</td>
<td>135212.5234</td>
<td>0.9927</td>
<td>98.68</td>
<td>32.9563</td>
</tr>
<tr>
<td>Image 4</td>
<td>383457.8828</td>
<td>361655.2265</td>
<td>0.9998</td>
<td>99.69</td>
<td>50.6989</td>
</tr>
<tr>
<td>Image 5</td>
<td>98919.3515</td>
<td>120134.3515</td>
<td>0.9999</td>
<td>99.97</td>
<td>48.8672</td>
</tr>
<tr>
<td>Image 6</td>
<td>51902.2109</td>
<td>51890.2656</td>
<td>0.9999</td>
<td>99.61</td>
<td>49.1591</td>
</tr>
</tbody>
</table>

Abbreviations: NPCR, number of pixel change rate; UACI, UACI, unified average changing Intensity; PSNR, peak signal to noise ratio.
*The number of each image corresponds to that mentioned in Figure 4.
of chaotic and hyper-chaotic systems, or use varying time delay. Other combinations of chaotic systems can also be combined with other types of cryptographic channels, which demonstrates the flexibility of the method in encrypting images.

Acknowledgments
This work is done for the Ph.D. dissertation in Islamic Azad University of Gonabad.

Competing Interests
The authors have no conflict of interest to declare.

Ethical Approval
Not applicable.

References

Table 2. Comparison of Already Proposed Methods with the Model Presented in This Study

<table>
<thead>
<tr>
<th>Disturbance</th>
<th>Unknown Parameters</th>
<th>Type of Delay</th>
<th>Encryption Method</th>
<th>Types of Data</th>
<th>Dataset</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not studied</td>
<td>Not studied</td>
<td>Not studied</td>
<td>Chaotic systems to protect medical data</td>
<td>Color Images</td>
<td>Medical images</td>
<td>1</td>
</tr>
<tr>
<td>Not studied</td>
<td>Not studied</td>
<td>Not studied</td>
<td>Chaos-based theory, elliptic curves</td>
<td>Gray scale images</td>
<td>Medical images</td>
<td>2</td>
</tr>
<tr>
<td>Not studied</td>
<td>Not studied</td>
<td>Not studied</td>
<td>Features of genetic algorithms</td>
<td>Gray Scale Images</td>
<td>Medical image</td>
<td>4</td>
</tr>
<tr>
<td>Not studied</td>
<td>Not studied</td>
<td>Not studied</td>
<td>Pixel adaptive diffusion: bitwise XOR</td>
<td>Gray scale images</td>
<td>Medical images</td>
<td>5</td>
</tr>
<tr>
<td>Not studied</td>
<td>Not studied</td>
<td>Not studied</td>
<td>Chaotic 3D Lorenz attractor</td>
<td>Gray scale images</td>
<td>Medical images</td>
<td>6</td>
</tr>
<tr>
<td>Not studied</td>
<td>Not studied</td>
<td>Not studied</td>
<td>3D-CNT basis vectors, Pixel adaptive diffusion: bitwise XOR</td>
<td>Gray scale images</td>
<td>Medical images</td>
<td>2</td>
</tr>
<tr>
<td>Not studied</td>
<td>Not studied</td>
<td>Not studied</td>
<td>Hyper chaotic system, which adopts DNA dynamic coding</td>
<td>Gray scale images</td>
<td>Bench mark</td>
<td>7</td>
</tr>
</tbody>
</table>

Approved Approved Constant - unknown Multi-Mode Synchronization of Fractional-Order Chaotic Systems Color images Medical images Our proposed method