A Prediction based Encryption Approach for Telemedicine Applications

G. Vallathan¹, T. Rajani², Eelandula Kumaraswamy³, C. Srinivas⁴

¹, ², ⁴ Nalla Malla Reddy Engineering College, Hyderabad, India.
³Sumathi Reddy Institute of Technology for Women, Warangal, Telangana State, India.

Abstract. The rapid progression of health care technologies systems and transmission strategies makes it reliable to gain, dispense and manage data over medical devices and as well improves conventional hospital information systems (HIS) to deliver effective health care services. When the medical information is communicated through wireless network, there exists a high chance of modifying the information. Before examining the patient, the physician has to check for the integrity of received medical image. A futuristic tele healthcare framework has been proposed to ensure the security, for offering complete healthcare services at reduced cost. In this paper, the proposed framework encompasses the integration of three modules viz. Prediction, Padding and Chaotic map encryption. This work offers an enhanced security for both patient medical data as well as medical scan images to a great extent. Two processes are involved in the padding sequence namely: forward and backward snail tour. After the snail tour process, the adjacent pair of pixels in the original image is XORing in order to make it ready for further process using the chaotic map encryption algorithm. Three operations have been carried out in chaotic approach namely: permutation, diffusion and substitution. This encryption method arises, a valid confusion and diffusion in the image pixels such that, the security of the images/data is enhanced. The performance of the proposed approach is assessed and compared with existing schemes such as ECC and Chaotic map encryption on a set of MRI/CT medical images. Experimental outcomes demonstrate that the proposed framework offers robustness in terms of security, quality and reliability which alleviate misdiagnosis at the physician end in telemedicine applications.

Keywords: PRSP Prediction, Padding, Chaotic map encryption, permutation, diffusion, substitution

1. Introduction

For the past decade, an attractive improvement in communication technologies has generated much demand for securing the medical image during transmission over a network. Owing to the huge increase in multimedia information, the need for fast and secure representation, transmission and storage of medical images become more critical since medical details comprises of private and confidential information. These technologies have been used for diagnosing the patients who are isolated from doctors by a distance. Telemedicine is significant, since it enables the on-line consultations through transmission network. When the patient medical information/images have been sent through a network, there is a possibility of hacking/spoofing the medical information. The patient information must be secured from malicious persons since; the medical details are highly sensitive. Therefore, encryption is the only feasible choice for healthcare providers which effectively minimize the threat of information against hacking and random attacks.

Numerous encryption algorithms are available to ensure the security and robustness to a maximum extent. Two standard algorithms are preferred for image encryption namely: Data Encryption Standard (DES) and Advanced Encryption Standard (AES). In Data Encryption Standard (DES) algorithm,
symmetric and asymmetric keys are employed, to encrypt the medical image using different secret keys [1, 2]. AES retain good level of security and the encryption process can be carried out by adjusting the row transformation of the image matrix [4]. Later, Younes et al. [3] exploited a novel technique which includes both permutation and encryption process. In this technique, the image is decomposed into 4 several pixel blocks, and then permutation and encryption process has been carried out successively. The investigational analysis states that, the similarity between the input and encrypted images was dropped off by enhanced entropy functions. Kamali et al. [4], proposed a modified version of AES (MAES) in which the potential of the security is highly maximized when compared with AES. Ismail IA et al. [5], presented a medical image encryption technique using chaotic logistic maps with the key size of 104-bit. In this technique, the plain and the cipher image are being evaluated in order to produce the dissimilarity between the input and encrypted image. In reality, the input image depends on secret keys and the encrypted data depends on the logistic map encryption and hence, there is a less randomness among the input and encrypted image. In [6], the author has proposed an improved encryption algorithm. This algorithm generates nine chaotic sequences using a single secret-key. Later, six sequences are used to shuffle the location of pixels and other three sequences are used to diffuse and confuse the image pixel values. The performance shows that, the algorithm has large secret-key space, high security, fast encryption speed and strong robustness and it uses only a map, but achieves a multi-chaos encryption effect over encryption errors. Consequently, it guarantees a high range of security against certain majority of the attacks. Consequently, Amrane Houas et al. [7] proposed an innovative encryption algorithm to secure binary images to a maximum extent. This algorithm works based on the key generation logic and also, the key-image is obtained from the proposed transformation, which approximately attains the pixel values to be identical. In addition to that, this algorithm encrypts both binary image databases and images having identical size. This algorithm has been verified to be competent in transferring both data and image of huge size with less computational complexity. However, it is not appropriate for all medical images. Considering all the above facts into account, the significance of both reliability and security was felt in real time scenario. Therefore, the major focus of this proposed work is to provide enhanced medical data security without compromising the reliability.

2. Proposed Encryption System

The challenging aspect of any encryption algorithm is to estimate how far the secret data/images can be protected and to what extent the algorithm is secure. The experimental outcome of the proposed work is compared with Elliptic Curve Cryptography (ECC) and Robust chaotic map image encryption algorithm since; these two algorithms are popular in bioinformatics. Mohamed Parvees et al. [8] have proposed a robust chaotic image encryption to protect the medical images during transmission. In this method, a generalized chaotic map has been used, to generate a chaotic sequence in order to ensure high security. Later, diffusion and permutation are employed next to substitution phase.

In addition to that, the algorithm has a larger key space and affords robustness against brute force attack. The experimental analysis has been carried out for all medical images and the performance metrics like key sensitivity, space and correlation are computed and compared with existing techniques which proves that this method is not suitable for all the medical images.

Subsequently, Laiphrakpam Dolendro Singh et al [9] developed an Elliptic Curve Cryptography (ECC) image encryption technique which includes digital signature to provide the authenticity and integrity available at the reconstructed image. The process is generated by adjusting the ECC parameters in the image pixels. It ignores the prior mapping table for encryption and decryption. Moreover, this technique produces a small correlation among the plain and the cipher image at the cost of increased computational complexity.
In addition to that, the algorithm has a larger key space and affords robustness against brute force attack. The experimental analysis has been carried out for all medical images and the performance metrics like key sensitivity, space and correlation are computed and compared with existing techniques which proves that this method is not suitable for all the medical images.

Subsequently, Laiphrakpam Dolendro Singh et al [9] developed an Elliptic Curve Cryptography (ECC) image encryption technique which includes digital signature to provide the authenticity and integrity available at the reconstructed image. The process is generated by adjusting the ECC parameters in the image pixels. It ignores the prior mapping table for encryption and decryption. Moreover,
this technique produces a small correlation among the plain and the cipher image at the cost of increased computational complexity.

The investigational analysis proves that the robustness and computational complexity is limited in the above said methods. Therefore, a novel framework is proposed to resolve the above said shortcomings of the conventional algorithms. In this work, a prediction based encryption framework is presented which comprises of prediction, padding and chaotic map encryption as shown in Figure 1. Prediction based techniques have been used widely in reversible data hiding algorithm for cover image. In this research, a Precise Ramp Selective Prediction (PRSP) is used to identify the exact prediction which is used to accumulate the preprocessing pixels. The PRSP predictor works on 3*3 neighboring pixels (Y1, Y2, Y3, Y4, Y5, Y6, Y7, Y8) of the present pixel Y. The four ways of projected ramps are 45 degree, -45 degree, horizontal and vertical are signified by A1, A2, A3 and A4. The constituent pixel values of these ramps are A1, A2, A3 and A4 are Y6, Y5, Y7 and Y9 correspondingly.

Assume that Amin2 and Amin1 are the two least ramps midst A2, A1, A3 and A4 and the concerned pixels are Bmin1 and Bmin2. The intended prediction of x is as follows

\[ y = \frac{A_{\min 1} \times B_{\min 1} + A_{\min 2} \times B_{\min 1}}{A_{\min 1} + A_{\min 2}} \]

Let I be an 8-bit original image. That original image is segregated into four regions like L1, L2, L3 and L4, where L1 comprises of the pixels used for concealing the medical data, L2 comprises of the used pixels, L3 comprises of pixels for prediction and L4 comprises of pixels for concealing secret medical information. The pixels L1, L2 and L3 does not have any change in this stage. Only L4 are scanned vertically and horizontally.

For the pixel I (d, e) of L4, if it is available in informative section, it leads to poor prediction. The invariance of local smoothness estimator is defined as Ip (d, e) used to find whether I (d, e) is available in texture region or not

\[ I_p (d, e) = F_{\text{max}} - F_{\text{min}} \]

\[ F_{\text{max}} & F_{\text{min}} - \text{Maximum and minimum value of nine adjoining pixels of I (d, e) respectively} \]

If Ip (d, e) is smaller than the value of threshold T ∈ [0 – 255], then I (d, e) and its adjacent pixel values are more correlated and it is stated as smooth region else I (d, e) is deliberated as an informative region. T must be find out in terms of texture region, if the T value is high, it is said to be texture region and if the T value is small it is good and it belongs to smooth region.

Consecutively, Two snail XORing methods have been used in padding process namely: forward and backward, since the entire matrix is upset with one bit change in pixel. The structure of forward and backward snail tours is revealed in Figure 2. For instance, consider 6*6 matrix, a forward snail tour is applied to the medical image in which the pixels in an image is moves towards one bit right. This will be continued until it reaches the last bit of the image. After applying the forward snail tour, the first pixel is XORed with second pixel and the result is shifted to the position of second pixel [10]. Subsequently, a backward snail process has been carried out by XORing the adjacent pixel pairs. After applying the padding, a new resultant matrix will be encrypted using chaotic map encryption. The decryption of the image is done by chaotic map encryption algorithm. For extracting the padding process, again the first pixel is XORed with second pixel and the result is shifted to the first pixel.
The subsequent part of the proposed work is Improved Generalized Chaotic Map (IGCM), which comprises of three sequences namely: permutation, diffusion, and substitution processes. Four iterations have been performed in permutation process by which it scrambles the position of 8-bit image pixels and the corresponding value of the pixels are changed using diffusion process. Later, substitution process takes place and generates the chaotic sequences by processing the IGCM. Finally, the image pixels are encrypted using permutation, diffusion, and substitution processes. In the decryption side, the image pixels are decrypted with necessary parameters. The Generalized Chaotic Map (GCM) encryption has few significant parameters in order to make the system more robust and it is described using:

\[ x_{n+1} = x_n + k \times \left[ a - c - b \times (1 + y) \times x_n^y \right] \quad (1) \]

where \( X_n \) is the ratio of existing population to the maximum possible population, \( y \) represents the total income of the population and \( K \) is the control parameter. \( a \) is the size of the market demand, \( c \) represents a fixed marginal cost, \( b \) signifies the slope of the market price.

The chaotic map has some controlling parameters namely: \( \mu_1, \mu_2, \gamma_1, \gamma_2, X_0, X_1 \). These are initial parameters of chaotic sequences for encryption and decryption. The system exhibits chaotic behavior when it is in the interval of \((0 – 4)\) and \( X_0 \) varies from 0 to 1.

The sequence of action carried out in the chaotic encryption algorithm is detailed under the subsections.
2.1 Permutation of Pixel Sequence (PPS)
Two types of permutation process is performed in chaotic sequence namely: ascending and descending order. By using this sequence, it is feasible to produce an integer-valued permutation sequence. This sequence permits to swap the whole image pixels in a medical image.

2.2 Diffusion of Pixel Sequence (PDS)
The diffusion process can be transformed to an integer valued sequence ‘\(\mu\)’ between the numerals (0-255), since the image pixels are 8-bit in length. This diffusion sequence is used to encrypt the image pixel values.

2.3 Substitution of Pixel Sequence (SPS)
The substitution process is divided into two sorts namely: ascending and descending order to exploit the valid chaotic behavior. By using the sort operations, it is possible to generate a sequence called swapping sequence. In this work, the SPS is employed to substitute the pixel values in order to get the chaotic behavior in the medical image. The steps of the complete algorithm are given as follows:

3. Results and Discussion
The simulation parameters considered for the image encryption study are summarized in Table 1. It shows the parameters relevant to this module of work. The performance metrics are obtained using the formulae’s stated above.

3.1 Correlation Coefficient Analysis
For different image modalities, the consequence of involved parameters in correlation coefficients are Horizontal, vertical and diagonal Correlation which are analyzed and computed for padding based chaotic map encryption (proposed), chaotic map encryption and Elliptical curve cryptography. The correlation coefficient is the measure of similarity between the input and encrypted image. The obtained correlation coefficients of the input and encrypted image indicates that, the proposed work has yield good performance of providing confusion and diffusion which are highly resistive against the differential attacks. Moreover, if the correlation value lies between 0.5 and 1, it indicates a strong correlation between the input and encrypted images and if the value of the correlation is between (0.0 and 0.5) or (-0.1 and -0.5), it infers a weak positive correlation or weak negative correlation between the two images [101]. From the Table 6.2, it is clearly observed that, the proposed algorithm performs better than the conventional schemes unlike chaotic map and ECC algorithm are effective for some of medical images above. Added to it, they are highly complicated. This is accomplished by combining padding and chaotic map encryption.

From the Investigational analysis, it has been observed that, the average value of horizontal, vertical and diagonal correlation for cipher image attained from the proposed encryption logic are 0.0006896, 0.000745, 0.000745 (0.000458, -0.000852, 0.0008196) for MRI (CT) images whereas for chaotic map encryption, the correlation analysis for cipher image is 0.00597, 0.1228, 0.00230 (0.01480, 0.00392, 0.00457) for MRI (CT) images. The obtained result clearly shows that, there is no correlation between two adjacent pixels in cipher image and moreover, the plain image is highly correlated which are highlighted in the Table 1. This fact clearly emphasizes the superiority of the proposed encryption logic and its suitability for both CT and MRI images.
| Image Type | Algorithm | Horizontal Correlation | Vertical Correlation | Diagonal Correlation |
|------------|-----------|------------------------|----------------------|---------------------|
| MRI Image 1 | 0.9663    | 0.0059                 | 0.9756               | 0.1228              |
| MRI Image 2 | Chaotic Encryption M. Y. Mohamed Parveesl et al, Journal of Medical system, 2016 | 0.9872 | 0.0014 | 0.9939 | 0.0010 | 0.982 | 0.002 |
| CT Image 3 | 0.9725 | -0.0002 | 0.9765 | -0.002 | 0.955 | 0.003 |
| CT Image 4 | 0.9368 | 0.0148 | 0.9510 | 0.0039 | 0.958 | 0.004 |
| MRI Image 1 | 0.9467 | -0.006 | 0.9310 | 0.0004 | 0.898 | 0.014 |
| MRI Image 2 | Elliptical curve cryptography Laiphrakpam Dolendo Singh et al, Elsevier, 2015 | 0.9203 | 0.0177 | 0.9120 | 0.0175 | 0.850 | -0.002 |
| CT Image 3 | 0.9686 | -0.0153 | 0.9526 | -0.000 | 0.927 | -0.020 |
| CT Image 4 | 0.9153 | 0.0056 | 0.9562 | 0.0046 | 0.943 | 0.0001 |
| MRI Image 1 | 0.9541 | 0.0024 | 0.9562 | 0.0004 | 0.953 | 0.0005 |
| MRI Image 2 | Padding based chaotic map encryption Method | 0.9472 | 0.00068 | 0.92593 | 0.00074 | 0.9237 | 0.0041 |
| CT Image 3 | 0.9743 | 0.00605 | 0.95403 | 0.00035 | 0.9439 | -0.0034 |
| CT Image 4 | 0.9623 | 0.00045 | 0.94531 | -0.0009 | 0.9546 | 0.0008 |

Images 1 & 2 are MRI images, Images 3 & 4 are CT images.
3.2 Encryption Time

In the proposed work, apart from the security, encryption time is significant consideration for real-time image encryption/decryption algorithm. The performance of the encryption process is based on the processor and memory. These must improve the accuracy of encryption time. In the proposed approach, encryption and decryption time are computed for bio images. On the average, the encryption time of the proposed approach is 0.521 (0.68) and the decryption time is 0.532 (0.62) for MRI (CT) images whereas, the existing approach has the encryption time of 0.4 (0.42) and the decryption time is 0.4 (0.42) for MRI (CT) images.

| S.no | Algorithm | Image Type | Encryption Time (sec) | Decryption Time (sec) | Entropy |
|------|-----------|------------|-----------------------|-----------------------|---------|
| 1    | Chaotic Encryption M. Y. Mohamed Parvees1 et al, Journal of Medical system, 2016 | MRI | 0.4 | 0.4 | 7.0882 |
| 2    | Ellipitical curve cryptotography Laiphrakpam Dolendro Singh et al, Elsevier, 2015 | MRI | 0.29 | 0.3 | 7.9988 |
| 3    | Ellipitical curve cryptotography Laiphrakpam Dolendro Singh et al, Elsevier, 2015 | CT | 0.42 | 0.42 | 7.9981 |
| 4    | Padding based chaotic map Encryption | MRI | 0.521 | 0.532 | 7.9991 |
| 5    | Padding based chaotic map Encryption | CT | 0.68 | 0.62 | 7.9996 |

From the above observation, the existing approach requires minimum time to execute the algorithm when compared to proposed approach. This is owing to the fact that, the proposed approach uses a combination of two encryption algorithms which provides more robustness with least computational complexity.
### 3.3 Number of Pixels Change Rate (NPCR)

To analyze the encryption level of the cipher image, few differential attacks has been applied to the encrypted image. In this attack, hacker attempts to recognize the relationships between the cipher and plain images. To measure the strength of each pixel on the whole encrypted image, the number of pixels change rate (NPCR) has been used to see the influence of changing a single pixel on the encrypted.

Table 3. NPCR Analysis of different encryption algorithms

| S.no | Algorithm                          | Image Type | Images | NCPR % |
|------|------------------------------------|------------|--------|--------|
| 1    | Chaotic Encryption                 | MRI        | Image 1| 99.16  |
| 2    | Chaotic Encryption                 | MRI        | Image 2| 97.55  |
| 3    | Chaotic Encryption                 | MRI        | Image 1| 98.89  |
| 4    | Chaotic Encryption                 | MRI        | Image 2| 99.16  |
| 5    | Elliptical curve cryptography      | MRI        | Image 1| 99.59  |
| 6    | Elliptical curve cryptography      | MRI        | Image 2| 99.60  |
| 7    | Elliptical curve cryptography      | CT         | Image 1| 99.599 |
| 8    | Elliptical curve cryptography      | CT         | Image 2| 99.590 |
| 9    | Padding based chaotic map Encryption| MRI       | Image 1| 99.63  |
| 10   | Padding based chaotic map Encryption| MRI       | Image 2| 99.64  |
| 11   | Padding based chaotic map Encryption| CT         | Image 1| 99.59  |
| 12   | Padding based chaotic map Encryption| CT         | Image 2| 99.62  |

Table 3 illustrates the different NPCR values of the cipher image and also it can be observed that, the NPCR of the proposed work is 99.63, 99.64 (99.59, 99.62) for MRI (CT) images whereas, the existing scheme offers only 99.16, 97.55 (98.89, 99.16) for MRI (CT) images. This implies, the cipher image
pixel of the proposed work is different and it is found to be 99.62 when compared to conventional schemes. A good cipher will have an NPCR value close to 100%.

Figure 3. (a) CT brain input image (b) Histogram plot of CT brain image (c) CT brain encrypted image (d) Histogram plot of CT brain image.
Figure 4. (a) MRI brain input image (b) Histogram plot of MRI brain image (c) MRI brain encrypted image (d) Histogram plot of MRI brain image.
3.4 Histogram Analysis of Input and Encrypted Image

Figure 3. Illustrates the histogram analysis of input and encrypted (CT Abdomen) CT Brain images. An image histogram is the graphical representation of pixel distribution at individual grey levels. A good cipher image has an even frequency distribution of image pixel values. From the observation, it can be concluded that, the frequency distribution of the input image pixel differs a lot whereas the encrypted histogram image is consistently distributed over the image which illustrates the goodness of encrypted image. The performance metrics for evaluating the proposed work are peak signal to noise ratio, Entropy, Encryption/Decryption time and correlation coefficient. The obtained outcomes offers a significant resistant against various attacks.

4. Conclusion

This proposed approach aims to set forth a secure structure for competent telemedicine applications. This approach provides an enhanced security for both patient medical data as well as medical scan images. The Prediction based Encryption approach has been proposed to secure the medical images/data to a great extent. Initially, prediction is applied to the medical image to find out the smooth and texture region. Later, padding is applied which involves two processes in the padding sequence namely: forward and backward snail tour. After the snack tour process, the adjacent pair of pixels in the original image is XORing in order to make it ready for further process using the chaotic map encryption algorithm. Three operations have been carried out in chaotic approach namely: permutation, diffusion and substitution. This encryption method arises, a valid confusion and diffusion in the image pixels such that, the security of the images/data is enhanced. The performance of the proposed approach is assessed and compared with existing schemes such as ECC and Chaotic map encryption on a set of MRI/CT medical images. Both quantitative and visual study has been made for analysis purpose. From the Investigation-al analysis, it has been concluded that, the horizontal, vertical and diagonal correlation attained for the proposed encryption logic are 0.0006896, 0.000745, 0.004168 (0.000458, -0.000852, 0.0008196) for MRI (CT) images and also the entropy attained from the proposed approach are 7.9991 (7.9996) for MRI (CT) images are close to perfect scenario. These facts clearly emphasize the strength of the proposed encryption algorithm in terms of security; reliability and also it provide robustness against differential attacks in real time scenario. On the average, the proposed approach offers good security performance without conceding PSNR and moreover, it has minimal of computational complexity.

References

[1] Mitra A, Subba Rao Y, Prasanna S, 2006 A new image encryption approach using combination al permutation techniques, International Journal of Computer Science, 1, pp.127-31.
[2] D. Socek, Shujun Li, S. S. Magliveras and B. Furht, 2005 “Short Paper: Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption”, First International Conference on Security and Privacy for Emerging Areas in Communications Net-works, Greece, pp.406-407.
[3] Younes MAB, Janatan A, 2008 An image encryption approach using a combination of permutation technique followed by encryption, International Journal of Computer Science and Network Security, 8, pp. 191-97.
[4] Kamali SH, Shankeria R, Hedayati M, Rahmani, 2010 New modified version of advance encryption standard based algo- rithm for image encryption, Proceedings of International Conference on Electronics and Information Engineering (ICEIE), Japan, pp. 141-45.
[5] Ismail IA, Amin M, Diab H, 2010 Digital image encryption algorithm based on composition of two chaotic logistic maps, International Journal on Network Security, 11, pp. 1-10.
[6] J. Peng, S. Jin and Y. Liu, 2010 Design and Analysis of an Image Encryption Scheme Based on Chaotic Maps, Proceed- ings of the International Conference on Intelligent Computation Technology and Automation, Changsha, pp. 1115-8.
[7] Amrane Houas, Zouhir Mokhtari, Kamal Eddine Melkemi, Abdelmalik Boussaad, 2016 A novel binary image encryption algorithm based on diffuse representation, International Journal of Engineering Science and Technology, 19, pp. 1887– 94.
[8] Parvees, M. Y. and Samath, J. Abdul and Bose, B. Parameswaran, 2016 Secured Medical Images - a Chaotic Pixel Scram- bling Approach, Journal of Medical Systems, 40, pp. 1-11.