A Novel Medical Image Encryption using Cyclic Coding in Covid-19 Pandemic Situation

Barsha Bose, Diptana Dey, Anupam Sengupta, Nikita Mulchandani, Anirban Patra*

Student, Dept. of ECE; JIS College of Engineering; Kalyani; West Bengal
* Asst. Professor; Dept. of ECE; JIS College of Engineering; Kalyani; West Bengal

anitublu@gmail.com

Abstract. During this Covid - 19 pandemic situation, encryption of medical images takes a major role in medical information systems as well as in telemedicine. However according to government rule, it is essential to hide the information of the patients. Recent development in computer network enhances a lot of facilities in communication area. Unfortunately, hackers are misusing this facility and always try to attack on the transmitted information in insecure network. For secure transmission of medical images, it is essential to encrypt the information before transmitting. In this communication, we are going to present a novel approach of medical image encryption using cyclic coding. We have proved that it is quite difficult to decrypt the original information from encoded data in one common mode of attacking- chosen ciphertext attack. Moreover, we have proved the effectiveness of the encryption using correlation coefficients. Our proposed scheme is suitable for efficient encoding of multiple medical images.

Keywords: Medical Image, Encryption, Cyclic Coding, Cyber Attack, Correlation Coefficient

1. Introduction:

In general, images used in medical field are treated as sensitive information in the bio information systems. To transmit these types of images through network, a secure encryption algorithm is required. Researchers have proposed a lot of image encryption algorithm for the last few decades. Data Encryption Standard algorithm is oldest algorithm used for encryption which requires minimum time for cost computations [1, 2]. By applying either symmetric or asymmetric algorithm, a secure image encryption can be done in very effective way. [3-5]. Image encryption is considered very effective while it can provide better result against common attacks- known-plaintext as well as ciphertext attack [6]. In medical image encryption, to enhance security, Cipher Feedback Mode is used to encrypt the image [7]. Shamir described a secret sharing encryption scheme based on (k, n) method and polynomial
interpolation [9]. In this method, with the proper value of \(k\) and \(n\), the selected images can be reconstructed using the retrieval process.

In 2008, Hill explained an encryption method at both grayscale and color images [11] with a drawback of same level of color attributes on background. Nag described a method of rearranging the pixel position within the specified target images with digital function, XORing [12]. This method shows an excellent correlation information. Sokouti and his associates [13, 14], proposed a one time password based encryption system by splitting the image bits into block of rows for encryption purpose. With the help of pixels block and permutation, encryption has been performed by Rijn Dael algorithm process [15]. Ismail described [17] an algorithm based large key space to make more different pixels. Kamali SH [18] has been proposed modified version of AES where the security are highly increased in comparison to normal system of AES. A Patra, A Saha and K Bhattacharya proposed an effective image encryption algorithm using phase grating along with random phase matrix. They have analysed their values with plaintext and ciphertext attacks. [19]. A lot of different methods are successfully used in to hide images, in both spatial and frequency domain [20-22]. LSB bit replacement technique, a well-known method, widely used for its embedding property which is really useful for changing information of a bit in each pixel [23]. A Patra proposed a method of using sinusoidal phase grating and random phase masking for multiplexing, compression and encryption of digital images [24-27]

In this present research work, medical images are encrypted using well known cyclic coding and convolution coding. In general, there two types of cyclic coding- non-systematic and systematic cyclic coding. We have used non-systematic cyclic coding. A well-known generator polynomial is selected encoding as well as decryption process. Initially the selected images are multiplied by generator polynomial for encryption and at the receiving end they are decrypted using inverse process. Our work is mainly in frequency domain; therefore, some spatial-domain cyber-attacks are not effective. In our proposed method, decryption of a particular image is dependent on proper generator polynomial selection. To check the security of our method, we have applied this in very well-known cyber-attack technique- chosen ciphertext attack. Correlation coefficient is one effective tool to measure the effectiveness in image encoding process. In every case, correlation coefficient provides satisfactory results.

2. Methodology:

The selected image is represented by \(f(x, y)\). We have used non-systematic cyclic coding. In non-systematic cyclic coding system, generator polynomial
\[ g(x) = x^3 + x^2 + 1 \]  
\[ s(x, y) = f(x, y) \ast g(x) \]  

The entire encoded image is transformed into frequency domain.

It should be mentioned that Mod 2 arithmetic is applied here.

\[ F(u, v) = \iint s(x, y) e^{-j2\pi(ux+vy)} \, dx \, dy \]  

Let us assume that, retrieved image is represented as \((x, y)\). So

\[ m(x, y) = \iint_{-\infty}^{\infty} F(u, v) e^{j2\pi(ux+vy)} \, du \, dv \]  

To retrieve the images, we have followed the inverse process.

\[ m(x, y) = s(x, y)/g(x) \]  

To check quality of output image, PSNR calculation is used with Mean Square Error

\[ \text{MSE} = \frac{1}{mn} \sum_{x=1}^{m} \sum_{y=1}^{n} [f(x, y) - m(x, y)]^2 \]

Where \(f(x, y)\) and \(m(x, y)\) represent original image and retrieved image respectively.

\( m, n \) denotes size of images

3. Result:

In this section we have showed our results. We have worked with MATLAB software. Correlation coefficient of the output images is also shown in the table.

Selected images are displayed in Fig 1 (a-c). Pixel resolution of each medical image is 512 x 512.

![Figure : 1(a-c) Three Selected Images](image-url)
With the help of generator polynomial, the images are encoded and then transformed into frequency domain (shown in the Fig 2 (a-c))

![Encoded Images](image1)

**Figure: 2 (a-c) Encoded Images**

The encoded images have been decrypted using the reverse process. Decrypted images are displayed in the Fig 3 (a-c)

![Decrypted Images](image2)

**Figure: 3 (a-c) Decrypted Images**

### 3.1 Chosen Ciphertext Attack :

We have decrypted the encrypted images using different keys. In each case, correlation coefficients have been calculated of the original and decrypted plaintexts for all images. Though we have applied this process on every image using different keys, only three cipher texts have been displayed in the Fig. 4 (a-c) and correlation coefficient test is mentioned in Table 2.
Figure: 4 (a-c) Different Cipher texts

Table 1:
PSNR Calculation

| Selected Image | Output Image | PSNR |
|----------------|--------------|------|
| \( f_1(x, y) \) | \( m_1(x, y) \) | 30.7 |
| \( f_2(x, y) \) | \( m_2(x, y) \) | 31.3 |
| \( f_3(x, y) \) | \( m_3(x, y) \) | 30.6 |

Table 2:
Correlation Coefficient

| Selected Image | Correlation Coefficient |
|----------------|-------------------------|
| \( f_1(x, y) \) | 0.712                   |
| \( f_2(x, y) \) | 0.538                   |
| \( f_3(x, y) \) | 0.486                   |

Conclusion:
We have proposed a new method to effectively encrypt and retrieve multiple medical images using cyclic code. Three independent images are separately encoded with same generator polynomial. PSNR values of all decrypted images are greater than 30 which indicate the better quality of the decoded images. Our proposed system is quite different from conventional encryption techniques used in the frequency domain. To decode the image, attacker should know proper key as well as proper algorithm.
In absence of anyone parameter, it is quite impossible to decode the original image. The proposed method is very fast and it is suitable for encryption of multiple medical images in telemedicine area. In preventing piracy of digital images, this method also can be effectively used.

Reference:

[1] Öztürk I., Sogukpınar I.; 2004; “Analysis and comparison of image encryption algorithms”; Transactions on engineering. Comput. Tech.; 3:1305–1313.

[2] Potdar V., Chang E.; 2004; “Disguising text cryptography using image cryptography”; 4th International Network Conference INC; July 6-9, University of Plymouth, UK.

[3] Mitra A., S Rao Y, Prasanna S.; 2006; “A new image encryption approach using combinational permutation techniques”; International Journal of Computer. Science. ;1(2):1306–4428.

[4] Socek D., Li S., Magliveras S., Furht B.; 2005; “Enhanced 1-D chaotic key-based algorithm for image encryption”. IEEE/CreateNet Secure Comm; 2005, pp. 406-408.

[5] Shuangyuan Y., Zhengding L., Shuihua H.; 2004, “An asymmetric image encryption based on matrix transformation. Communications and Information Technology”, IEEE International Symposium on, ISCT 2004. vol. 1, pp. 66-69.

[6] Mao Y., Chen G., Lian S.; 2004; “A novel fast image encryption scheme based on 3D chaotic baker maps”. International Journal of Bifurcation. Chaos. ; 14(10):3613–3624.

[7] Alsultanny Y.; 2007; “Image encryption by cipher feedback mode”; Innovative. Computation. Inf. Control.; 3: pp 589–596.

[8] Cagnoni S., Dobrzeniecki A., Poli R., Yanch J.; 1999 ;“Genetic algorithm-based interactive segmentation of 3D medical images”; Image Vision. Computation.;17: pp 881–895.

[9] Shamir A.; “How to share a secret. In: Communications of ACM” doi: 10.1145/359168.359176.

[10] Zhao R., Zhao J-J., Dai F., Zhao F-Q.; 2009; “A new secret image sharing scheme to identity characters”; Comput. Stand. Interfaces.; 31: 252–257.

[11] Panigrahy S., Acharya B., Jen D.; 2008; “Image encryption using self-invertible key matrix of hill cipher algorithm”; 1st International Conference on Advances in Computing, Chikhli, India, pp: 1-4.

[12] Nag A., Singh J., Khan S., Biswas S., Sarkar D., Sarkar P.; 2011; “Image Encryption Using Affine Transform and XOR Operation”; International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSSCCN 2011).; pp. 309–12.

[13] Sokouti M., Pashazadeh S., Sokouti B.; 2013 ;“Medical image encryption using genetic-based random key generator (GRKG)”; National Joint Conference on Computer and Mechanical Eng. (NJCCCM2013); Mianooab, Iran.. pp. 1–6.

[14] Sokouti M., Sokouti B., Pashazadeh S., F Derakhshi M-R., Haghipour S.; 2013 ;“Genetic-based random key generator (GRKG): a new method for generating more-random keys for one-time pad cryptosystem”. Neural Computation. Appl. 22(7-8):1667–1675.
[15]. Younes M, Janatan A; 2008; “An image encryption approach using a combination of permutation technique followed by encryption”; IJCSNS. 8(4):191–197.

[16]. Seyedzade S.M., Atani R.E., Mirzakuchaki S.; 2010; “Novel image encryption algorithm based on hash function”; 6th Iranian Conference on Machine Vision and Image Processing; pp. 1–6.

[17] Ismail I.A., Amin M., Diab H; 2010; “Digital image encryption algorithm based on composition of two chaotic logistic maps”; International Journal of Networking Security; 11(1):1–5.

[18]. Kamali SH, Shankeria R, Hedayati M, Rahmani M.; 2010; “New modified version of advance encryption standard based algorithm for image encryption”. International Conference on Electronics and Information Engineering (ICEIE); pp. v1-141–v1-5

[19]. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, 1996; “Techniques for data hiding,” IBM Systems Journal, Vol. 35, No. 3.4, pp. 313–336,

[20]. B. Li, J. He, J. Huang, and Y. Q. Shi; 2011; “A survey on image steganography and steganalysis,” Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No. 2, pp. 142–172

[21]. A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt; 2010; “Digital image steganography: Survey and analysis of current methods” Signal Processing, vol. 90, no. 3, pp. 727–752

[22]. Y.J. Chanu, T. Tuithung, and K. M. Singh; 2012; “A short survey on image steganography and steganalysis techniques,” in Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on, IEEE, pp. 52–55.

[23]. A. Westfeld and A. Pfitzmann, 1999; “Attacks on steganographic systems,” in International workshop on information hiding, pp. 61–76, Springer,

[24]. A Patra, A Saha, K Bhattacharya; 2020; “Multiplexing and encryption of images using phase grating and random phase mask”; Optical Engineering; Vol – 59, Issues – 3; pp- 033105-111;

[25]. A Patra, A Saha, K Bhattacharya ; 2020; “Multiplexing and encryption of images using phase grating and random phase mask”; Computational Intelligence and Its Applications in Healthcare; Chapter- 5; pp- 63-71;

[26]. A Patra, D Chakraborty, A Saha, K Bhattacharya ; 2019 ; “Compression of Satellite Images using Sinusoidal Amplitude Grating”; IJEE; Vol – 11(1); pp- 664-667

[27]. A Patra, A K Chakraborty, A Saha, K Bhattacharya ; 2018 ; “A New Approach to Invisible Watermarking of Color Images using Alpha Blending”; IEEE Emerging Trends in Electronic