Multistage Encryption of Mammogram Images Using Fractional Fourier Transform and 3D Chaotic Map

Banhi (Dutta Choudhuri) Das[1*], Arijit Saha[2], Somali Sikder (Sanyal)[1]

[1]B. P. Poddar Institute of Management and Technology, Department of Electronics and Communication Engineering, Kolkata, West Bengal, India
[2]Principal, Dum Dum Motijheel Rabindra Mahavidyalaya, Kolkata, West Bengal, India

banhidass@gmail.com

Abstract. Transmission of biomedical images over long distance is very important for various applications like telemedicine and distant consultation with health experts. Many of these images carry confidential information and need to be highly secured before transmission. For the purpose of secured transmission, images must be encrypted. Hence, an efficient technique for secured communication of biomedical images is proposed in this communication, which is applicable equally for all types of images. In this communication, the algorithm is applied on mammogram images for detection of breast cancer. Security of transmitted images is enhanced by application of Fractional Fourier Transform (FRFT) and 3D Rabinovich Chaotic map. The algorithm shows satisfactory result for applications where image data are to be transmitted in highly secured way.

Keywords: Chaotic encryption, FRFT, Information entropy, Correlation coefficients, Cyberattack.

1 Introduction

Breast cancer is one of the leading reasons of female death due to cancer. Survival rate can only be increased with proper diagnosis and commencement of treatment as early as possible. Mammogram images are used to detect early signs of breast cancer. In the era of communication, where internet is playing the key role, remote diagnosis and treatment of patients by means of telemedicine can effectively help a large section of ailing patients. These types of applications require transmission of images over a long distance over digital medium. Containing highly confidential patient data, these images must be secured with robust encryption schemes before transmission.

Since image security is a major concern, as already mentioned, several researchers are working in the domain of image encryption techniques. Image encryption using chaotic maps are robust enough as encrypted image cannot be deciphered without exact keys [1-4]. Chaotic encryption in higher dimension is proved to be more robust than lower dimensional chaotic maps [5-7]. Fractional Fourier transform, which is a special

C. Kiran Mai et al. (eds.), *Proceedings of the Fourth International Conference on Advances in Computer Engineering and Communication Systems (ICACECS 2023)*, Atlantis Highlights in Computer Sciences 18,
https://doi.org/10.2991/978-94-6463-314-6_24

application of Fourier transform is also used by researchers for the purpose of encryption. [8-9]

In this paper we have developed an encryption algorithm to enhance security of transmitted images by using Fractional Fourier Transform (FRFT) and 3D Rabinovich chaotic map. This in turn will improve the robustness of the encryption model in terms of key space. To assess the robustness of the encryption algorithm, we have performed the histogram analysis, correlation analysis, key-sensitivity analysis, and also calculated the information entropy and key space.

2 Methodology

2.1 Selection of Images and Separating red, green and blue plane:

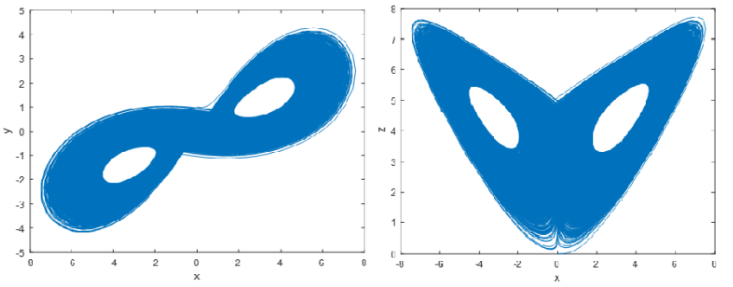
We have chosen mammogram images for encryption. In this communication we have chosen a mammogram image of 1024×1024-pixel size. Red, green and blue planes of the image are separated. Each of these three image planes are separately encrypted with different encryption keys. At the receiving end the corresponding keys are required to decrypt each image plane. Any variation in keys will result in erroneous decryption. So, recovery of original image is possible only if all the three image planes are properly recovered with correct keys.

2.2 Encryption using 3D Rabinovich system

The 3D Rabinovich system is given in equation 1.

$$\left.\begin{aligned} \dot{x} &= ky - \alpha x + yz \\ \dot{y} &= kx - \beta y - xz \\ \dot{z} &= -\delta z + xy \end{aligned}\right\} \tag{1}$$

System parameters are $k \geq 4.92,\ \alpha = 4,\ \beta = \delta = 1$ and initial conditions are $x_0 = 0,\ y_0 = 1$ and $z_0 = 0$. Three Lyapunov exponents are $L_1 = 0.2825$, $L_2 = 0$ and $L_3 = -6.2829$. One positive value of Lyapunov exponent proves that the system executes chaotic behaviour. Fig 1 shows 2D graph of chaotic attractor in x-y and x-z planes, while Fig 2 shows 3D plot in x-y-z space. Lyapunov exponent graph is displayed in Fig 3.



(a) (b)

Fig. 1. Rabinovich Attractor in (a) x-y plane (b) x-z plane

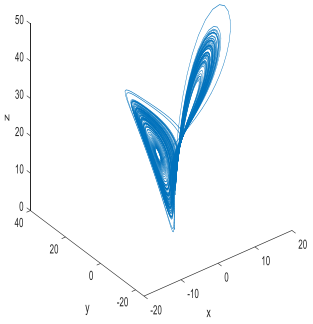


Fig. 2. Rabinovich Attractor in x-y-z space

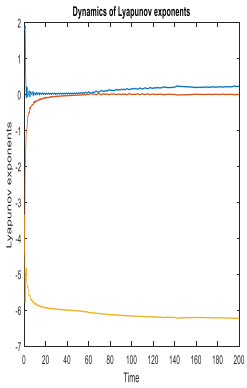


Fig. 3. Lyapunov Exponent Graph

2.3 Encryption using FRFT

2.3.1 Defining FRFT

FRFT is a general form of Fourier transform which transforms the input signal from time domain to some intermediate domain between time and frequency depending upon the fractional order of transform (a).
Conventionally, the nth order FRFT is given by $f_n\,(x_n)$ of function $f\,(x)$. It is calculated using integral transform kernel $K_n\,(x, x_n)$.

$$K_n(x, x_n) = \begin{cases} \xi_\phi \; exp\{j\pi(x^2 \cot\phi - 2xx_n + x_n^2 \cot\phi)\} & 0 < |n| < 2 \\ \delta(x - x_n) & n = 0 \\ \delta(x + x_n) & n = \pm 2 \end{cases} \quad (2)$$

Where

$$\xi_\phi = exp\left[-j\pi \frac{sgn(\sin\phi)}{4} + j\phi/2\right] \qquad \phi = a\pi/2$$

$x =$ coordinate system of the input domain. (0th order)

$x_n =$ coordinate system of the output domain. (nth order)

For any real ϕ , the FRFT of a function f with angle ϕ is denoted by $\mathcal{F}_\phi(u)$, where

$$\mathcal{F}_\phi[f](u) = \sqrt{1 - i\cot\phi}\; e^{i\pi\cot(\phi)u^2} \int_{-\infty}^{\infty} e^{-2\pi i\left((\csc\phi)ux - x^2\frac{\cot\phi}{2}\right)} f(x)dx \quad (3)$$

$\phi = a\pi/2$ Where ϕ be the angle of rotation and a be the order of transform.

The fractional order a can be used as a key of encryption as by any minute alteration of the fractional order a the input signal will be transformed to distinct intermediate domains.

Encryption steps are given as follows:

A mammogram image of size 1024×1024 pixels is chosen for the experiment. The R, G and B components of the image are separated and are encrypted separately with different set of keys.

From the chaotic system represented by equation (1), we can generate 3 different keys. These keys are $key1, key2\ and\ key3$ generated from three arrays of numbers generated from chaotic sequence generator (x, y, z) respectively. The initial values are selected as $x_0 = 0$, $y_0 = 1$, $z_0 = 0$, which acts as secret keys. We have discarded the first 1000 values for true chaos onset. In the first stage of encryption, the red plane is encrypted by $key1$, the green plane is encrypted by $key2$ and the blue plane is encrypted by $key3$.

In the second stage of encryption, the encrypted outputs from first stage undergoes encryption using FRFT. The fractional orders of FRFT (a) acts as secret keys. $key4$ is generated with $a = 0.5$, which is used to encrypt the red plane. $key5$ is generated with $a = 0.4$ for encryption of the green plane, whereas $key6$ generated with $a = 0.25$ is to encrypt the blue plane.

In the third stage of encryption, all the three encrypted image planes from previous two stages of encryption are again ciphered with a random phase matrix generated with specific initial condition, which acts as an additional key for the cryptosystem ($key\ 7$). This is given by equation (4).

$$key\ 7 = [abs\ k(i) \times 255] \quad (4)$$

These successive three stages of encryption make the cryptosystem truly robust to be used for encryption of images those contain confidential information and require high security.

2.4 Decryption of Received Signals

At the receiving end encrypted image planes are received. Different set of encryption keys are used for these three planes. So, three planes are needed to be decrypted with equivalent set of keys for retrieval of the image planes.

2.5 Reconstruction of Mammogram Image by Combining Red, Green and Blue planes

The mammogram image is reconstructed by combining recovered red, green and blue planes after decryption with proper set of keys at the receiving end.

3 Results and Discussion

We have used a mammogram image of size 1024×1024 pixels. Original image is shown in Figs. 4. Figs. 5(a-c) depicts R, G and B components of the image. Figs. 6(a-c) shows ciphered image planes. Decrypted R, G, B images are illustrated in Figs. 7(a-c) respectively. The reconstructed mammogram image is shown in Fig 8.

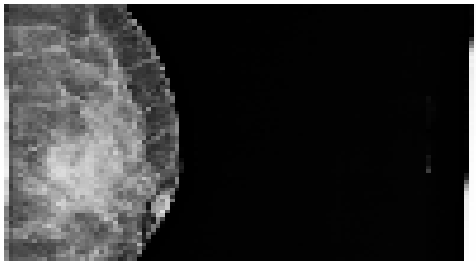
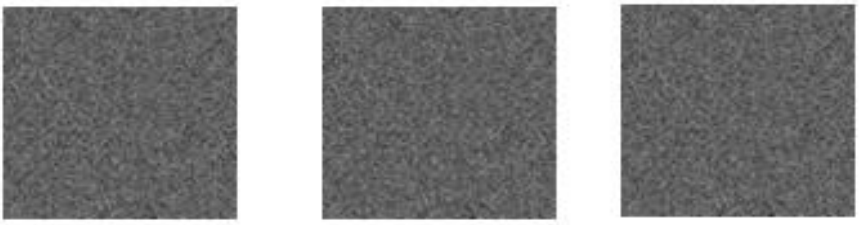


Fig. 4. Original mammogram image

(a) (b) (c)

Fig. 5. (a)-(c). Red, Green and Blue planes of mammogram image



(a) (b) (c)

Fig. 6. (a)-(c). Encrypted Red, Green and Blue plane images

(a) (b) (c)

Fig. 7.(a)-(c) Decrypted images

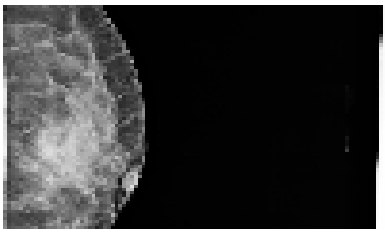


Fig. 8. Reconstructed mammogram image

3.1 Performance analysis of the Cryptosystem

The proposed cryptosystem algorithm was developed using matlab_R2021b_win64.exe. Standard biomedical image dataset is used for testing performance of the proposed cryptosystem.

3.1.1 Key space analysis

.

Key space of an encryption scheme is an important feature to assess its ability to protect the image from unauthorized attack. A cryptosystem with key space lower than 2128 is not robust enough [10]. For the proposed algorithm it is calculated to be 2375.

Performance of the cryptosystem compared in terms of key space with standard algorithms is given in Table 1.

Table 1. Key space analysis

Algorithms	**Proposed One**	**[11]**	**[12]**	**[13]**	**[14]**
Key space	2^{375}	2^{279}	2^{273}	2^{300}	2^{280}

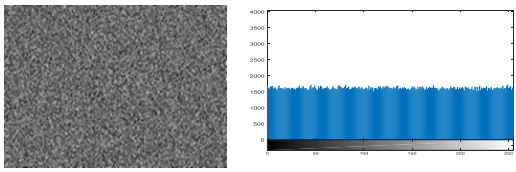
3.1.2 Key sensitivity analysis

.

A robust encryption scheme must be highly sensitive to any minor change in initial condition of key generation. A minute alteration in initial condition at the time of decryption will result in complete erroneous recovery. For testing the robustness of the scheme in terms of key sensitivity, we have used the initial condition of x for generating $key1$ as $x = 0.001$ at the time of decryption of the red plane which was originally encrypted with $x = 0$.This results in complete erroneous decryption with the correlation coefficient value of 0.013 between original and decrypted image. This prove the system to be robust enough in terms of key sensitivity.

3.1.3 Histogram Analysis

Fig 9 shows the histogram of the encrypted image obtained after multiple stages of encryption. The image histograms become uniform enough, which helps to avoid the possible histogram exploitation.



(a) (b)

Fig. 9. Histogram analysis (a) diffused red plane (b) histogram of diffused red plane

3.1.4 Correlation Analysis

Table 2 shows the calculated values corelation coefficient and SSIM.

Table 2. Performance of Cryptosystem

Sl. No.	Image	Correlation Coefficient (Original and Ciphered Image)	Correlation Coefficient (Original and deciphered Image)	SSIM
1	Image (Red plane)	0.0301	1	1
2	Image (Green plane)	0.0213	1	1
3	Image (Blue plane)	0.0134	1	1

3.1.5 Information Entropy Analysis

Information entropy is calculated by following expression (5).

$$H(m) = \sum_{i=0}^{M-1} P(m_i) \log_2 \frac{1}{P(m_i)} \tag{5}$$

The information entropy ideally should be 8 [15]. The proposed algorithm achieves Information Entropy as 7.9997 which is quite satisfactory. Comparison of our proposed method with some recently developed encryption algorithm in terms of information entropy is given in Table 3.

Table 3. Information entropy

Encipher algo-rithm	Proposed model	[11]	[12]	[13]	[14]
Infor-mation entropy	7.9997	7.9993	7.9972	7.9993	7.9976

4 Conclusion

Image security, an important feature of image processing, is addressed in this communication. As, we have designed our model for highly sensitive images like biomedical images, where privacy of patient's data is very important, robust encryption scheme must be applied for security enhancement. With the advancement in the field of telemedicine, patients' data need to be transferred in a secured way across the world for remote consultation with health experts. Security of transmitted images is ensured by our newly developed multistage encryption scheme using 3D chaotic map and fractional Fourier transform. Hence, the proposed algorithm has a broad scope of application in health care industry. It assures perfect recovery of images and has the potential

to be used for various applications where confidential images need to be transmitted with robust encryption technique.

References

1. Erick Armando Hernández Díaz; Héctor Manuel Pérez Meana; Víctor Manuel Silva García, "Encryption of RGB Images by Means of a Novel Cryptosystem using Elliptic Curves and Chaos", *IEEE Latin America Transactions*, Volume: **18**, Issue: 08 ,2020.
2. Rongjun Ge;Guanyu Yang; Jiasong Wu; Yang Chen; Gouenou Coatrieux; Limin Luo, "A Novel Chaos-Based Symmetric image encryption using Bit-Pair Level Process", *IEEE Access*, Volume: **7** ,2019.
3. Akram Belazi; Muhammad Talha; Sofiane Kharbech, Wei Xiang, "Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding", *IEEE Access*, Volume: **7** ,2019.
4. Robert Matthews, "On the derivation of a "chaotic" encryption algorithm", *Cryptologia,* Volume:**13**, 2010.
5. Bin Ge;Xu Chen;Gang Chen;Zhihua Shen ,"Secure and Fast Image Encryption Algorithm Using Hyper-Chaos-Based Key Generator and Vector Operation", *IEEE Access*, Volume: **9** ,2021.
6. Gao, T., Chen, Z., "A new image encryption algorithm based on hyper-chaos". *Phys. Lett. A* 2008;372(4):394–400
7. Jeng, F.G, Huang, W.L, Chen, T.H., "Cryptanalysis and improvement of two hyperchaos-based image encryption schemes". *Signal Process. Image Communication*, 2015;34:45–51.
8. H.M. Ozaktas, Z. Zalevsky, M.A. Kutay, "The Fractional Fourier Transform with Applications In Optics And Signal Processing", *Wiley*, Chichester, 2001.
9. G. Unnikrishnan, J. Joseph, K. Singh, *Appl. Opt*. 40 (2001) 299
10. W. Janke, *Pseudo random numbers: Generation and quality checks.*
11. Ghebleh, M., Kanso, A.: A novel efficient image encryption scheme based on chained skew tent maps. Neural Comput. Appl. 2019;31(7):2415–30.
12. Li Y, Wang C, Chen H. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt. Lasers Eng., 2017;90:238–46.
13. Chai, X.L., Gan, Z.H., Zhang, M.H.: A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. Multimedia Tools Appl. 2017;76:15561–85
14. Chai, X., et al., Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption. Signal Processing, 2021. 183: p. 108041
15. B.Stoyanov, K. Kordov, "Image encryption using chebyshev map and rotation equation". *Entropy* 2015; Volume **17**:2117–39.