NVEO
Natural Volatiles & Essential Oils

Efficient Pattern Generation In Cryptography Supporting Edge Computing

Kusuma S M [1] , Ananya K [2] , Meghana S [3] , Rashmi Harish [4] , Sameeksha Kamath [5]

1,2,3,4,5 Dept. of Electronics and Telecommunication Engineering, Ramaiah Institute of Technology Bangalore, India

Abstract - Technology usage for communication and its applications that requires security, mainly focusing in the field of image encryption is abundantly embedded and used. Such methods with secured and low cost information transfer in different domain areas, where information sharing and distribution through edge based mobile computing communication is in demand and to be increased. Hence secured and highly protected ways of computing techniques need to be addressed in future communication systems. In this research work, an image based encryption technique is proposed to ensure a highly secure transmission. The method uses hybrid fractal based encryption technique with low computing cost to support the edge based embedded computing devices. The procedure involves image fractal generation, encryption and decryption to maintain secure information flow through images. Implementation of the proposed methodology is carried out to evaluate the performance of the technique. The results are compared with respect to computational cost and found to be more effective for mobile edge based computing scenarios.

Keywords - Image Encryption, Cryptography, L-shaped tromino, decryption, histogram

I. INTRODUCTION

A pattern is a series of lines or shapes that repeat the same shape across a surface at regular intervals. Mathematics, economics, statistics, art, biology, architecture, and even language studies all use the concept of pattern. Cryptography is one that belongs to such category and helps to handle certain patterns for secured and privacy information. Nature's information's like sound, activities, odor and visual patterns are frequently chaotic, sometimes deterministic and rarely exactly repeating, and frequently include fractals. Tree branches, growth of different bushes, snake and other reptiles sleeping patterns, bird flying patterns, are some of the natural patterns that follow certain geometric structures. Such patterns have mathematical regularities and justifiable by some equations and predictions can be made, and also functions of different activities can be explained. All the above patterns experience the real world scenario with augmentation and are virtually created for simulation purposes.

Pattern generation has been an evident part in all of these fields for a long time. Patterns in math can be generated using certain rules. They can be numeric or geometric. One such highly math-dependent pattern system are fractals. In 1975, mathematician Benoit M proposed the term "fractal." Benoit M utilised the fractal to describe the concept of theoretical fractional dimensions to geometric patterns, that are broken or fractured based on the Latin fructus.

Solid cryptography is hidden and encoded correspondence that is all around secured against cryptographic investigation and unscrambling, guaranteeing that only the planned beneficiaries can understand it. Patterns abound in cryptography. Patterns can be found in code creation, decoding.

Image encryption is undeniably more testing contrasted with printed information encryption. Usually any picture normally have adjacency relation and some patterns are followed to continue with the neighboring group of entities and have some correlation. Such concepts are used in many ways for crypto analysis. Also, symmetric encryption may not work smoothly with the images, however few novel techniques are proposed to adjust with standard encryption technique to match the distributive nature of images. Even a simple encryption with plain image will leads to a large change in the enciphered image.

Image encryption has hence drawn in the consideration of numerous specialists, who endeavor to foster new plans addressing various tradeoffs between the intricacy of the calculation and its dependability. Henceforth fractals are utilized to scramble pictures. Fractal pictures can be effectively created and they are utilized as a wellspring of arbitrariness for developing a solid key.

First, an introduction to the domain is done in brief, then related work is discussed in section II . Proposed methodology and implementation platforms are described in section III. Finally, the experimental results with advantages of the proposed methods are discussed in section IV and concluding remarks in section V.

II. Related work

Some of the recent works in the areas of image encryption and their performance evaluation methods are briefly described in this section.

In [1] a hybrid (fractal and chaos) encryption is proposed in order to provide high secure transmission. Karrar et. al in [2] came up with a strategy in which the public key cryptosystem called RSA Cryptosystem is presented to be applied over gray and color images for improved security..

Salwa Kamal et. al., [3] suggested a fractal based technique for image with is encrypted using fractals with sensitivity analysis, entropy, and many more. Swati Gupta et.al [4] have comparative study on the algorithm for image encryption using fractal geometry. A two phase image encryption scheme is proposed based on FFCT and fractals for image encryption by Mervat et. al., [5]. Encryption through the use of fractals with neumaricals model and its analysis is done in Santiago et. al [6]. Yongjin Xian et. al [7] introduced another technique for worldwide image dispersion with two turbulent arrangements that offer extraordinary security and high encryption productivity by providing fractal sorting matrix for chaotic image encryption in real time scenario.

In Shafali Agarwal [8] summed up the different ongoing picture encryption strategies in which a fractal key is utilized in encryption and decoding measures. Comparison of various chaos-based image encryption schemes is considered by Jai Ganesh et. al [9]. They have studied the important properties of the system that a chaotic map should possess and describes a brief overview of various chaotic maps available in the literature. Secured image transmission using fractal and 2D chaotic mapping techniques are proposed by Shafi Agarwal [10].

In Shiguo Lian [11] proposed a secure fractal image coding scheme and evaluated it. In this research, parameters with large space and high sensitivity are encrypted during fractal image encoding and decrypted during fractal image decoding.

III. Proposed Algorithm and Implementation

The input image is encrypted to produce the encrypted image, which is transferred to the receiver where it is decrypted to produce the original image. The process of encryption shows that the original image being combined with the fractal image generated, through bitwise XOR to produce the fractal encrypted image. Decryption is exactly the opposite of the process of encryption, where the encrypted image undergoes bitwise XOR with the same fractal key to give the output as the original image.

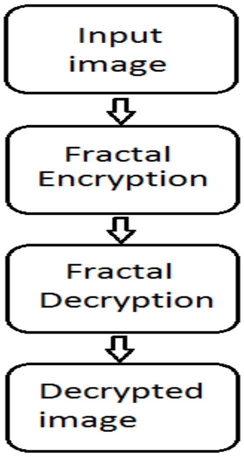

Fig. 1. Block diagram of encryption and decryption

We have used MATLAB version R2021a for the implementation of this block diagram and simulation of results. Measurements and show parameters in MATLAB. The advantage of using MATLAB is that we are able to reduce code density. It is a popular platform for image processing and hence we opted the same for image encryption as well.

Encryption evaluation techniques - There are several ways to evaluate the encryption technique. Some of them are statistical while some are sensitivity measures. Some statistical measures are Histogram analysis, entropy and Correlation coefficient (CC). Histogram analysis with encrypted images leads to a normalized distribution of different entitiesmeasured with respect to different colors, as that of normal image, where in the defiant colors will have certain outliers specific to the distribution of dominant colors present in the images. This will help in measuring the potentiality of the encryption technique.

In order to increase the randomness and avoid leakage of the information from encrypted image, **entropy** is one of the evaluation parameters for image encryption.
Correlation coefficient is one of the statistical methods to measure the similarity and gradient distribution across the image with pixel-by-pixel intensity between two images with and with our encryption. Other common statistical measures relating to sensitivity analysis includes Peak signal to Noise ratio, mean square error, pixel change rate, mean absolute error.

IV. Results and Discussions

The output of the program for different image templates shown in figure 2 and and the histogram for the image with and without encryption is shown figure 3.

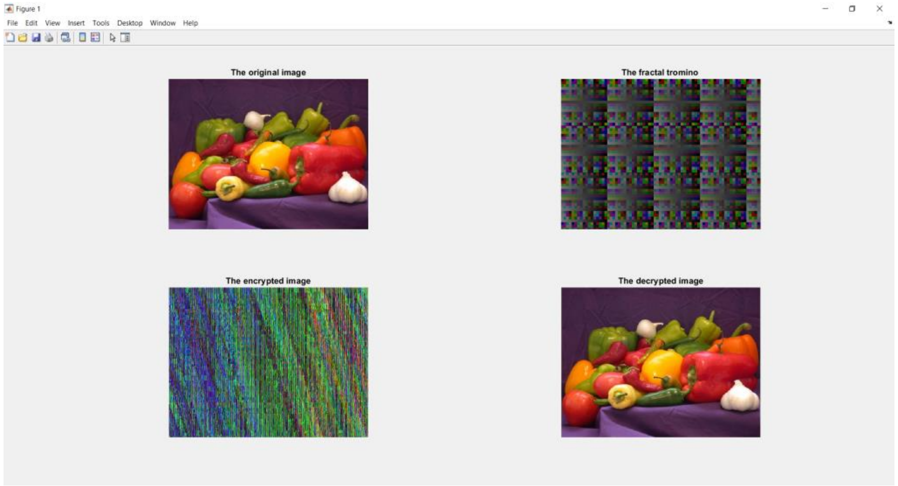

Fig. 2 Images used for encryption
(Courtesy: wikipedia and Internet resources)

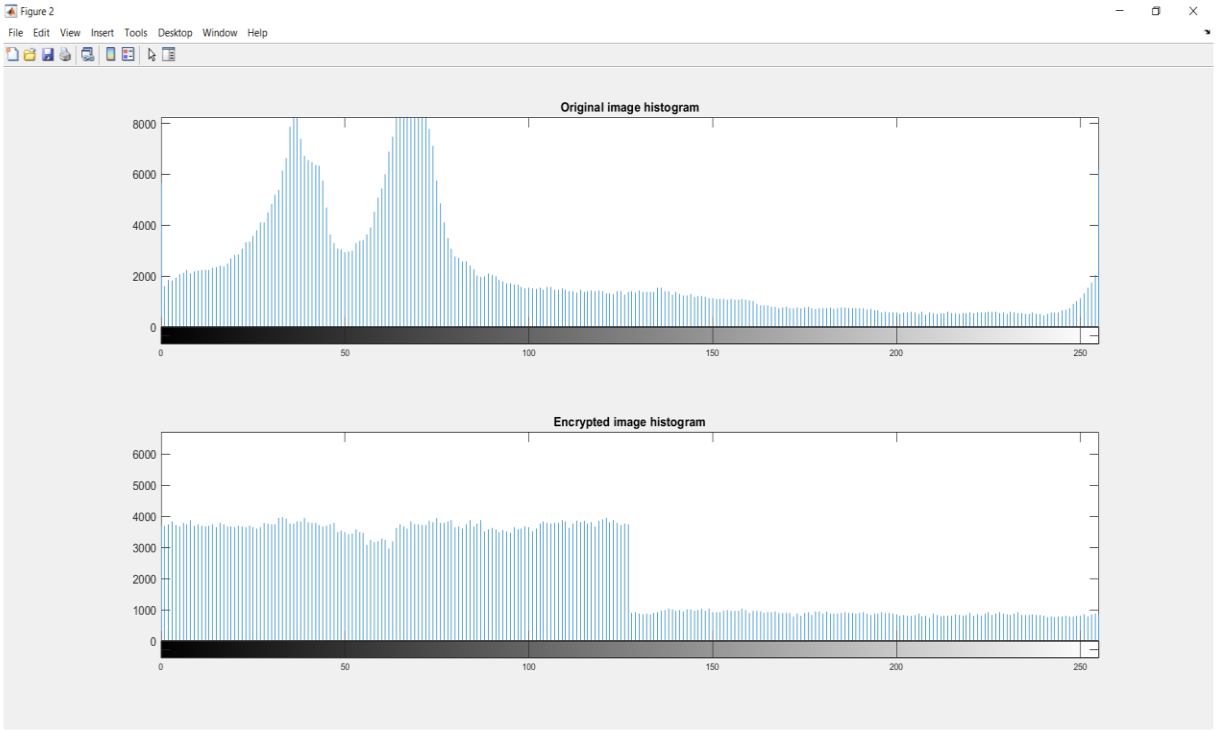

Fig. 2.Histogram of original and encrypted image

Tabular column of parameters measured for different images

Table I

Image	Size of image	Entropy (orig) < Entropy (enc)	CC	PSNR	NPCR	MSE	MAE	Time taken in seconds
Monalisa	447x300	7.2683 < 7.3960	0.0698	11.0639	60.0522%	5.1004e+03	32.7596	3.520490
Taj Mahal	358x636	7.0466< 7.0712	0.0033	9.5893	63.9183%	9.3671e+03	28.3783	2.269960
Peppers	381x512	6.9920< 7.4411	-0.0131	9.5556	64.8154%	8.1205e+03	37.7900	2.370966
Lena	225x225	6.9978< 7.7525	0.2361	8.4259	65.1830%	5.3962e+03	29.1248	3.564761
Parrot	1024x1024	6.8659< 7.1313	0.0074	10.8003	61.4379%	2.4743e+04	34.3620	6.179800

From the table I we can see that the measured values of the parameters are aligned with the parameters discussed in the previous section. Some extra parameters measured are size of the image and time taken. The time taken is directly proportional to the size of the image and hence it is seen that the parrot image with the largest dimension takes upto 6 secs to go through encryption and decryption. Here the entropies of source images are lesser than that of their corresponding encrypted images. The correlation coefficient is measured between the source image and encrypted image and found very low correlation between them, which means that the encryption quality is good. The peak signal to noise ratio (PSNR) is relatively low meaning that the noise is higher in the encrypted image than the source image, whereas the PSNR between source image and decrypted image is higher because the quality of reconstruction is good. Here the number of pixel change rate is around 60% implies that a one pixel difference in the source image will lead to a completely different encrypted image.

This means that our model of chaos based fractal encryption is consistent with the result. Mean Square Error is in the range of 10^3 for smaller images and 10^4 for 1024 x 1024 images which lies in the ideal range for mean square error expected from good encryption models. Lastly the mean absolute error between the source and encrypted images lies in the range of 25 to 40. This Means that the pixels are scrambled to a higher order in the encrypted image than in the source image.

Table II. Comparison between RSA and Fractal encryption

Technique	Lines of Code	Avg. Encryption Speed	Time Complexity
RSA	142	9.327819 seconds	$O(n^2)$
Fractal	50	4.064684 seconds	O(n)

The **time complexity of RSA** is $O(n^2)$. It is observed that as the size of private key length increases, the increase in **time** becomes nonlinear and exponential. RSA is computationally Intensive and slower when compared to its counterpart Algorithms [12].

Because of this, it is not commonly used to directly encrypt user data. More often, RSA is used to transmit shared keys for symmetric key cryptography, which are then used for bulk encryption-decryption. Since we are working on Image Cryptography, with the help of our concept "Pattern Generation used as key" , we can build some kind of system for dynamically updating the key to make the system more secure". All the above techniques are more suitable for mobile edge based computing used in most of the application areas with portable devices used with secured transmission.

Based on the above works done, some of the conclusions regarding the advantages of using fractals for Image cryptography can be mentioned as follows. i. Butterfly effect and randomness property - makes the key extremely secure. Reduces chances of hackers trying to guess the key. ii. Complex number mathematics rather than prime numbers - fractal dimensions are dependent on complex number mathematics whereas the RSA algorithm uses prime number arithmetic. iii. Normally the fractals leads to the sensitivity of the key due its Chaotic nature. iv. From table II it is evident that the method used consumes less time and memory, an ideal condition in case of mobile edge computing devices and is evident that fractal encryption is better. v. Small footprint of fractal, so less memory is consumed - hardly any memory is consumed in storing the fractal image, approximately around 800 kilobytes in our experimentation. This is important when system scaling comes into picture in an edge based embedded mobile computing and distributed systems.

V. CONCLUSION

With the quick progression of correspondence and data transmission advancements, there is a need for secured transmission with less computing resources like in edge computing portable devices, normally used in most of the applications. One of several secured information transmission methods includes image encryption technique. In this work an approach towards hybrid fractal based image encryption technique with lower resource requirements for computing is proposed. Implementation of the technique for different image scenarios and key generations were carried out and compared the performance. It is observed that an increase in the average encryption speed and reduction in the usage of memory space from the results. Comparisons are made to verify the results, and obtained an improved performance that supports edge computing with resource constrained environments.

ACKNOWLEDGEMENT

We acknowledge our department faculty and college, MSRIT for providing the opportunity to carry out this research work and implementation.

REFERENCES

[1] Sandhya Rani Malligere Halagowda, Sudha Kanakatti Lakshminarayana, “Image Encryption Method Based on Hybrid Fractal-Chaos Algorithm”, International Journal of Intelligent Engineering and Systems, Vol 10, No.6, 2017.

[2] Karrar Dheiaa Mohammed Al Sabti and Hayder Raheem Hashim, “A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB”, Global Journal of Pure and Applied Mathematics”, Volume 12, 2016.

[3] Salwa Kamal Abd-El-Hafiz, Ahmed G Radwan, Sherif H Abdel Haleem, Mohammed L Barakat, “A fractal-based image encryption system” , IET Image Process, Vol.8 , 2014.

[4] Swati Gupta, Nisha Bansal, “Image Encryption Technique using Fractal Geometry: A Comparative Study”, IOSR Journal of Computer Engineering, Volume 16, Sep-Oct 2014.

[5]Mervat Mikhail, Yasmine Abouelseoud, Galal ElKobrosy, "Two-Phase Image Encryption Scheme Based on FFCT and Fractals", Security and Communication Networks, vol. 2017.

[6] Santiago Marquez Ortiz, Octavio Jose Salcedo Parra, Miguel J Espitia R, “Encryption through the Use of Fractals”, International Journal of Mathematical Analysis, Vol.11, 2017.

[7]Yongjin Xian, Xingyuan Wang, “Fractal sorting matrix and its application on chaotic image encryption”, Information Sciences, Volume 547,2021.

[8] Shafali Agarwal, “Image Encryption Techniques using Fractal Function: A Review”, International Journal of Computer Science & Information Technology, Vol 9, No.2, April 2017.

[9] Jai Ganesh Sekar, C.Arun, “Comparative Performance Analysis of Chaos Based Image Encryption Techniques”, Journal of critical reviews, , 2020, 7(9).

[10] Agarwal, S. “Secure Image Transmission Using Fractal and 2D-Chaotic Map”. Journal of Imaging 4(1):17, 2018

[11] Shiguo Lian France Telecom R&D Beijing,’ Secure Fractal Image Coding’, 2011.

[12]Nadia M.G. AL-Saidi, 1 Mohamad Rushdan Md. Said and 2 Adil Mahmood Ahmed , Efficiency Analysis for Public Key Systems Based on Fractal Functions, Journal of Computer Science 7 (4): 526-532, 2011

[13]Cryptography and network security -Principles and Practice by William Stallings - Sixth edition - Pearson Publications

.