A Novel Choas-Based Partial Image Encryption Scheme Using Lifting Wavelet Transform

Fadia Ali Khan[*,**], Jameel Ahmed[**], Jawad Ahmad[***], Jan Sher Khan[****], Fawad Ahmed[*****], Vladimir Stankovic[*], and Hadi Larijani[***]

[*]*Department of Electronics and Electrical Engineering, University of Strathclyde, Glasgow, UK*
[**] *Department of Electrical Engineering, Riphah International University, Islamabad, Pakistan*
[***]*School of Engineering and Built Environment, Glasgow Caledonian University, Glasgow, UK*
[****] *Department of Electrical Engineering, University of Gaziantep, Turkey*
[*****] *Department of Electrical Engineering, HITEC University Taxila, Pakistan*

Abstract. Depending on applications and specific security requirements, digital images can either be fully or partially encrypted. Partial encryption is one of the methods that reduces computational and processing cost. To achieve partial encryption, chaotic maps in combination with different transforms, like the Wavelet Transform (WT), Discrete Cosine Transform (DCT) and Lifting Wavelet Transform (LWT) are often used. Due to higher efficiency and fast processing, LWT is preferred over wavelet transform. In this paper, a novel partial image encryption scheme based on LWT, Secure Hash Algorithm (SHA-512), Logistic-sine chaotic map, TD-ERCS chaotic map and Substitution Box (S-Box) is presented. In comparison to other schemes, the proposed encryption technique is computationally efficient, secure and sensitive to initial key conditions.

Introduction

Transmission of multimedia data such as image, video and audio has dramatically increased over the last decade. Many of this data is sensitive and can be easily intercepted especially over a wireless channel. Encryption is one way of protecting text or multimedia data from intruders by hiding sensitive private information. Due to the bandwidth limitation or data storage capacity, image or video encryption is generally divided into two main areas: (i) full encryption, and (ii) partial encryption. In full encryption each pixel or block of an image is encrypted. In this type of encryption, the image data is fully encrypted and the intruders have no or very little information about original data. Full encryption is considered to be a secured method, however due to extensive computational requirement, this type of encryption causes significant real-time latency. Advanced data Encryption (AES), Data Encryption Standard (DES), and Triple DES (3DES) are examples of full encryption which are not suited for real-time image encryption. In partial or selective encryption, only the most meaningful part of an image or some data bit-stream called Region of Interest (ROI) is encrypted.

In partial encryption, an image is generally converted to frequency domain and then only selected frequency domain coefficients are encrypted. As a result, partial encryption is time efficient and also reduces computational cost. Partial encryption has become an active research area which can play a vital role in real-time image encryption applications. Some of the practical applications of partial encryptions are pay TV and social networks where users are restricted to access only TV channels or social network services they are subscribed to. Moreover, partial encryption has application in medical image processing where only a part of the image is needed to be encrypted. In medical imaging, a small portion of image contains valuable information which needs encryption. In a good cryptosystem, a minor change in key must generate a complete different cipher. Chaotic maps are sensitive to initial conditions and a slight change can cause a drastic change in the output. Thus chaotic map(s) can play a vital role in secure and efficient cryptography. Logistic map has smaller key space and has some limitations which are outlined in [1]. Thus other chaotic maps such as Tent map, Logistic-sine map and Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS) etc., can be used in higher secure cryptographic algorithms. In Logistic-sine and TD-ERCS, tangent function and power law are incorporated which makes the output more random and the key space is also higher when compared to other maps.

TD-ERCS and Logistic-sine Maps

In 2004, researchers reported the pseudo-randomness of a two-dimensional chaotic system on a physical model of ellipse reflecting cavity, known as Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS) [3]. TD-ERCS [2] is two dimensional map and it can be used in the image permutation process i.e., row and column permutation respectively. Td-ERCS chaotic map fulfills certain criteria such as zero correlation in total field and equi-probability. As a result, chaotic random number generated through TD-ERCS exhibits higher security such as Sensitive to Initial Conditions (SDIC), ergodicity, deterministic Pseudo-randomness, and structural complexity. Due to aforementioned reasons, TD-ERCS will be used in the proposed scheme. The mathematical equation of TD-ERCS chaotic map is written as:

$$\begin{cases} x_n = -\frac{2k_{n-1}y_{n-1}+x_{n-1}(\mu^2-k_{n-1}^2)}{\mu^2+k_{n-1}^2} \\ y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1}, \quad n = 1, 2, 3... \end{cases} \tag{1}$$

where

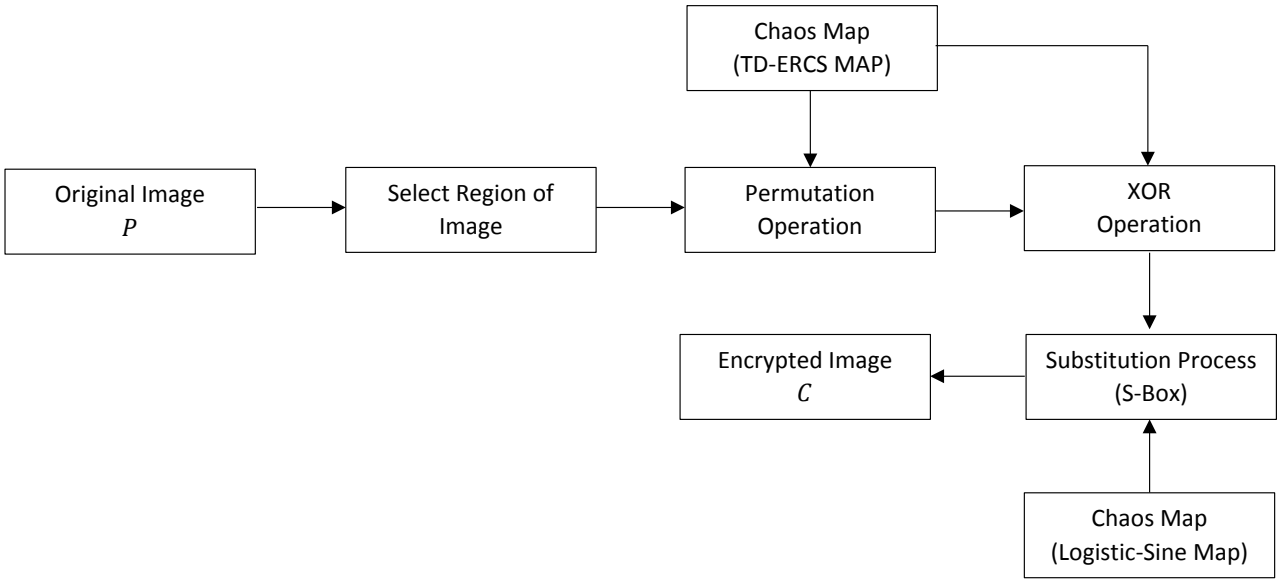

Figure 1: Flow chart of the proposed chaos-based encryption.

$$k_n = \frac{2k'_{n-m} - k_{n-1} + k_{n-1}(k'_{n-m})^2}{1 + 2k_{n-1}k'_{n-m} - k(k'_{n-m})^2} \tag{2}$$

where x_o is initial condition and α and μ, m are the control parameters. These control parameters are also called seed or initial parameters. In permutation and diffusion processes, these control parameters have a key role. In our proposed cryptosystem, TD-ERCS map is used in permutation stage.

A novel map known as Logistic-sine map was proposed in [4]. It overcomes the drawbacks of simple Logistic map. Two maps i.e., Logistic map and Sine map were combined together for a larger key space. The mathematical equation of a Logistic-sine map is:

$$z_{n+1} = (rz_n(1 - z_n) + (4 - r)\frac{sin(\pi z_n)}{4})mod(1), \tag{3}$$

where $n >= 0$, $z_n \in (0, 1)$ is the initial condition which produces z_{n+1} and $r \in (0, 4)$ is the control parameter. In our proposed algorithm, we used Logistic-sine map in the diffusion process.

The Proposed Image Encryption Scheme

Detail steps of chaos-based image encryption are shown in Fig. 1. The well-known Baboon image is encrypted through the proposed scheme and the resultant ciphertext C is tested against differential and statistical attacks. Values of contrast, correlation, energy, homogeneity, NPCR and UACI defined in [1] are 10.6165, -0.0088, 0.0157, 0.3873, 99%, and 33%, respectively. Due to page limit, we will show the detail experimental tables in the extend version of paper.

Conclusion

A novel Logistic-sine and TD-ERCP map-based partial image encryption scheme is reported in this article. The applications of LWT and SHA-512 are exploited in the proposed image encryption. Due to the sensitive initial conditions, equi-probability, ergodicity and higher key space, the proposed chaos-based image encryption is highly secure different type of attacks. In LWT only a part of an image is selected and hence the proposed is faster and suitable for real-time application when compared to the traditional schemes.

References

[1] Jawad Ahmad and Seong Oun Hwang. A secure image encryption scheme based on chaotic maps and affine transformation. *Multimedia Tools and Applications*, 75(21):13951–13976, 2016.

[2] Jan Sher Khan, Jawad Ahmad, and Muazzam A Khan. Td-ercs map-based confusion and diffusion of autocorrelated data. *Nonlinear Dynamics*, 87(1):93–107, 2017.

[3] Sheng Li-Yuan Cao Li-Ling and Sun Ke-Hui Wen Jiang. Pseudo-random number generator based on td-ercs chaos and its statistic characteristics analysis [j]. *Acta Physica Sinica*, 9:013, 2005.

[4] Yicong Zhou, Long Bao, and CL Philip Chen. A new 1d chaotic system for image encryption. *Signal processing*, 97:172–182, 2014.