Robust Chaos via Smooth Exponential Map

Fadi Abu-Amara and Ahmed Musa

Abstract—**This paper proposes a robust image encryption algorithm via Smooth Exponential Map (SEM) to meet the demand for fast and highly secure image transmission. The proposed algorithm consists of two phases; image-diffusion and image-fusion. In the image diffusion phase, pixel locations of the original image are shuffled in the spatial domain while pixel values are modified in the image fusion phase. Investigating the chaotic map characteristics of proposed SEM indicates a full chaotic behavior. Results of testing the proposed algorithm show that the proposed algorithm has a large key space with complete obscuring of the original image, secured against brute-force attack as it is achieved a large complexity of order $O\left(2^{90}\right)$, and requires 343ms to encrypt 200x200 pixels image.**

Index Terms—**Chaotic map, image encryption, lyapunov exponent, image fusion, image diffusion.**

I. Introduction

Different digital image encryption algorithms have been proposed in the literature [1-4]. The main concern of such algorithms is to meet the demand for fast and highly secure image transmission. There are two major groups of digital image encryption algorithms: non-chaos selective methods (i.e., traditional algorithms) and Chaos-based selective or non-selective methods [5]. Unfortunately, traditional image encryption algorithms were reported with low-level efficiency [2]. On the other hand, the chaos-based image encryption scheme provides an efficient encryption solution [6].

In this paper, a robust image encryption algorithm based on Smooth-Exponential-Map (SEM) is proposed to meet the demand for fast and highly secure image transmission. The proposed algorithm consists of two phases; image-diffusion and image-fusion. In the image diffusion phase, pixel locations of the original image are shuffled in the spatial domain while pixel values are modified in the image fusion phase.

The rest of this paper is organized as follows. Section 2 presents the proposed SEM. Section 3 discusses and analyzes the chaotic map characteristics of proposed SEM. The two implementation phases; diffusion and fusion, of the proposed SEM-based image encryption algorithm are explored in Section 4. Experimental results and evaluation of the proposed algorithm are illustrated in Section 5 while Section 6 concludes the paper.

II. Smooth-Exponential Map (SEM)

The proposed Smooth-Exponential-Map is characterized by

$$SEM(x,\lambda)=\begin{cases}\dfrac{e^{1.67x}-0.31}{\lambda}-0.51, & 0\le x\le 0.5\\[2ex] \dfrac{e^{-1.67x}-0.31}{\lambda-1.1}+0.51, & 0.5<x\le 1\end{cases} \quad (1)$$

where $x_{n+1}=SEM(x_n,\lambda)$ is the iteration function such that $SEM:[0,1]\rightarrow[0,1]$. The initial value x_0 and the parameter λ compromise the initial condition and the control parameter of the SEM, respectively. The parameter λ has the range of $\lambda\in[1.3324,1.468]$ while the sequence of real values $\{x_0,x_1,\cdots,x_n,\cdots\}$ forms the system orbit.

III. SEM Characteristics Investigation

The following chaotic-map characteristics of the SEM algorithm are investigated in this section: return maps, bifurcation diagram within an interval, high sensitivity to initial conditions and control parameters, and Lyapunov exponents.

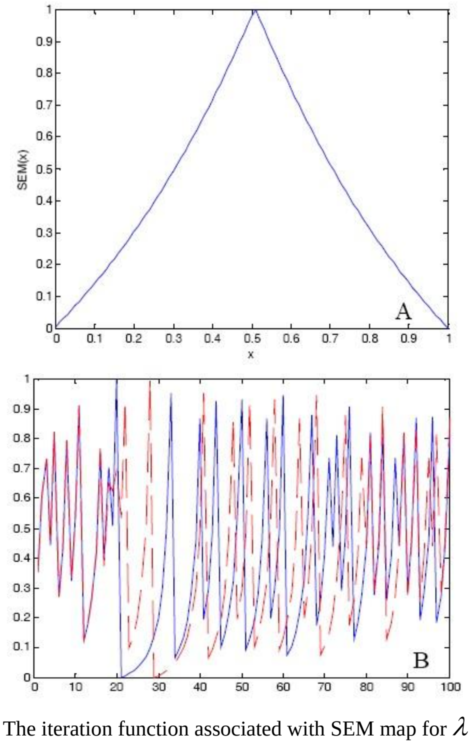

Fig. 1. (A) The iteration function associated with SEM map for $\lambda=1.338$. (B) time series plot for two sequences of 100 iterates generated by the SEM. The solid-blue and red-dashed lines stand for 0.2287 and 0.2287001, respectively.

Manuscript received April 05, 2012; revised May 5, 2012

The authors are with the Department of Computer Engineering, Al-Hussein Bin Talal University, Ma'an, Tel: +962799128884 (e-mail: Jordan, fadiabuamara@ahu.edu.jo, shorman@ahu.edu.jo).

Fig. 1-A shows a plot of $SEM(x,\lambda)$ for $\lambda = 1.338$ and for $\forall\, x_0 \in [0,1]$. As the figure indicates, SEM is S-unimodal function satisfies the conditions: (i) $SEM(0) = SEM(1) \approx 0$; (ii) has a single critical point at $c \in (0,1)$; (iii) increases from its null value at $x = 0$ until it reaches its maximum value of 1 at $x = c$ and then decreases until it reaches its null value again at $x = 1$.

The second characteristic a chaotic map should hold is bifurcation within an interval. The Schwarzian derivative can be used to investigate SEM against this characteristic [4]:

$$S_{f(x)} \equiv \frac{f'''(x)}{f'(x)} - 1.5\left(\frac{f''(x)}{f'(x)}\right)^2 \qquad (2)$$

The Schwarzian derivative of the SEM for 100 iterates generated with $\lambda = 1.338$ and $x_0 = 0.228723$ is negative along the entire interval. This indicates that the proposed SEM has a robust chaos for these values of λ and x_0.

The qualitative analysis of the proposed SEM can be performed via analyzing its bifurcation diagram. This graph displays all possible range of $SEM(x,\lambda)$ values against λ. The ranges of the parameter λ that ensure SEM is S-unimodal function are listed in Table 1.

TABLE I: THE RANGES OF Λ THAT ENSURE THE SEM IS S-UNIMODAL FUNCTION.

[1.3324,1.3336	[1.3337,1.335]	[1.3352,1.3365	[1.3367,1.338
[1.3381,1.3395	[1.3396,1.3401	[1.3452,1.3544	

The high sensitivity of the SEM to its initial conditions is illustrated in Fig.1-B. This figure shows time series plot of two different sequences of 100 iterations generated according to Eq.1 with $\lambda = 1.338$ and two initial values $x_0 = 0.2287$ and $x_0 = 0.2287001$. As Fig.1-B indicates, after a small number of iterations the two sequences become completely far apart.

The Lyapunov exponent can be used to determine whether the chaotic system has chaotic behavior (all orbits are unstable) or non-chaotic (periodic) behavior [4]. The Lyapunov exponent is defined by

$$\lambda_{LE}\ \ x_0\ = \lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1}\ln\left|f'\ \ \lambda, x_n\ \right| \qquad (3)$$

The derivative of the SEM algorithm of Eq. 1 is found as shown in Eq. 4

$$f'(x_n,\lambda) = \begin{cases} \dfrac{1.67e^{1.67x}}{\lambda}, 0 \le x < 0.5 \\ \dfrac{1.67e^{-1.67x}}{1.1-\lambda}, 0.5 < x \le 1 \end{cases} \qquad (4)$$

where $f'(0.5,\lambda)$ is undefined. The values of λ that result in a chaotic behavior are the ones that have $0 < \lambda_{LE} \le \ln 2$ which are $\lambda \in \left\{\begin{matrix} [1.157\ ,\ 1.162]\ ,\ [1.17\ ,\ 1.178]\ ,\ [1.183\ ,\ 1.302] \\ ,[1.337\ ,\ 1.338]\ ,[1.34\ ,\ 1.563] \end{matrix}\right\}$.

In summary, S-unimodal function with a robust chaotic behavior can be achieved for $\lambda \in \{[1.337, 1.338], [1.34, 1.3401], [1.3452, 1.3544]\}$. These ranges of λ are obtained by combining the ranges obtained based on Lyapunov exponent with those listed in Table 1. These ranges reveal that the SEM has a wide chaotic range in comparison with other maps such as the Tent map which has a full chaotic behavior for $\lambda \in [1.999, 2)$, [3].

IV. PROPOSED SEM-BASED IMAGE ENCRYPTION ALGORITHM

The proposed SEM-based image encryption algorithm consists of two phases. In the image diffusion phase, pixel locations of the original image are shuffled in the spatial domain while in the image fusion phase, pixel values are modified.

A. Image Diffusion Phase

The proposed image diffusion algorithm can be summarized in the following steps. Without loss of generality, we assume the dimension of the original grayscale image I is M × N.

1) Pixels of the original image are shuffled in the spatial-domain. The following two-dimensional Map is proposed as a pseudorandom number generator to shuffle the pixel locations.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} \alpha x_n + 2\alpha y_n \\ \alpha x_n + y_n \end{bmatrix} \operatorname{mod} \begin{bmatrix} M \\ N \end{bmatrix}$$

where the parameter α represents the control parameter. There are different values of α that result in a pseudorandom numbers such as $\alpha = 0.9992$. The point (x_{n+1}, y_{n+1}) is the new location of the original pixel location (x_n, y_n).

2) The shuffled image is divided into a number of blocks N_b. For better transformation the block size should be small in order to reduce the correlation between adjacent pixels. Each block is then reconstructed using the Zigzag method [7]; resulting in the shuffled image I_s

B. Image Fusion Phase

Image fusion is done between the shuffled image I_s and the key image K. The proposed image fusion algorithm can be performed as follows.

3) Eq. 6 is used for the image fusion.

$$I_f = w(K - I_s) + I_s \qquad (6)$$

where I_f is the fusion-image, I_s is the shuffled image obtained from the image diffusion phase, and the parameter $w \in (0,1)$ is a part of the secret key.

4) The key image K is constructed according to Eq. 1.

V. Experimental Results and Analysis

The well-know $200x200$ pixels 8-bit Lena image is used as shown in Fig.2-A. Fig. 2-B shows the shuffled image according to Eq. 5 where the correlation among the adjacent pixels is completely disturbed. Fig. 2-C shows the reconstructed shuffled image with block size of $10x10$ pixels. Fig. 2-D shows the obtained fusion image using the secret key $(x_0, \lambda, w) = (0.228723,\ 1.338,\ 0.8147)$. As Fig.2-D shows, the encrypted image is rough-and-tumble and unknowable.

The proposed SEM algorithm is very sensitive to a small change in the secret key parameters. For example, the secret key $(\mathrm{x}_0, \lambda) = (0.22872300001,\ 1.338)$ recovers a completely different image. Also, the secret key $(\mathrm{x}_0, \lambda) = (0.228723,\ 1.338000000000001)$ recovers a completely different image.

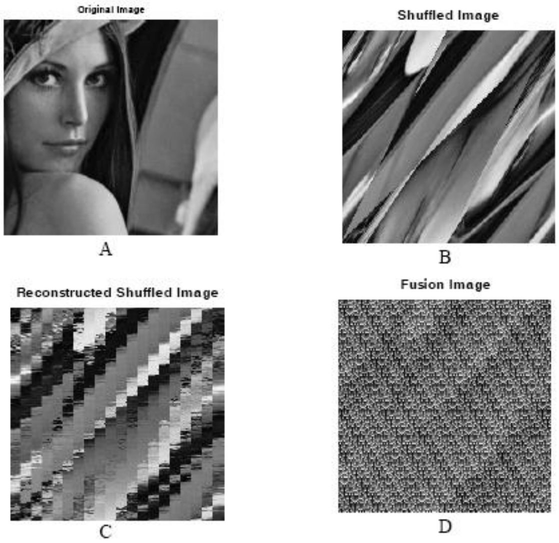

Fig. 2. (a) 200x200 pixels 8-bit Lena image, (b) Shuffled image, (c) Reconstructed shuffled image, (d) Fusion image.

The proposed SEM algorithm must be secure against the brute-force attack which estimates the secret key through exhaustive search of the set of all possible keys. The SEM algorithm has two constants and one initial condition. The parameters x_0, λ, and w have to be adjusted to an accuracy of one part in 10^{11},10^{15}, and 10^{1}, respectively to correctly recover the original image. Therefore, the SEM algorithm has a complexity of order $O(2^{90})$ which means 10^{27} mathematical steps are required for brute-force crypto analysis in order to recover the original image.

Speed of the encryption algorithm is also a major aspect. A time analysis has been performed on a Pentium 4 Core 2 Duo with 2GB RAM machine. With the $200x200$ pixels Lena image, the SEM requires 343ms for the encryption phase.

VI. Conclusions

In this paper, an image encryption algorithm via Smooth Exponential Map (SEM) is proposed to meet the increasing demand for fast and highly secure image transmission. Results indicate that the proposed SEM is S-unimodal function, has robust chaos, highly sensitive to initial conditions, and poses a full chaotic behaviour. Results also indicate that the proposed SEM-based image encryption algorithm has a large key space, complete obscuring of the original image, modifies every pixel in the original image without leaving shadows, and secure against brute-force attack.

Any proposed image encryption algorithm should compromise between high encryption rate and secure transmission. The proposed SEM-based encryption algorithm consists of two phases with different steps in each phase. This result in a highly secure transmission but increases the computational complexity with slight decrease the encryption speed. Future work should reduce steps used in the encryption phase to increase encryption rate without affecting algorithm's security.

References

[1] C. Fu, Z. Zhang, and Y. Cao, "An Improved Image Encryption Algorithm Based on Chaotic Maps," *Proceedings of the Third International Conference on Natural Computation*. 2007, August vol. 3, pp. 189- 193.

[2] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," *Chaos, Solitons and Fractals.*2006, 29: 393-399.

[3] A. Kanso. Self-shrinking chaotic stream ciphers. *Commun Nonlinear Sci Numer Simulat*. 2011, vol. 16, pp. 822–836.

[4] J. M. Aguirregabiria, "Robust chaos with variable Lyapunov exponent in smooth one-dimensional maps," *Chaos, Solitons and Fractals*. 2009, vol. 42, pp. 2531–2539.

[5] A. Acharya, "Image encryption using a new chaos based encryption algorithm," *Proceedings of the 2011 International Conference on Communication, Computing and Security*. 2011, doi: 10.1145/1947940.1948060.

[6] X. Ma, C. Fu, W. Lei, and S. Li, "A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process," *International Journal of Advancements in Computing Technology*. 2011, vol. 5, no. 3.

[7] R. Gonzalez and R. Woods, "Digital Image Processing," *Prentice Hall*, third Edition, 2008.