Chaotic Image Encryption via Convex Sinusoidal Map

F. ABU-AMARA[1*], I. ABDEL-QADER[2]
[1]Department of Computer Engineering
Al-Hussein Bin Talal University
P.O.Box: 20, Ma'an
Jordan
fadiabuamara@ahu.edu.jo

[2]Department of Electrical and Computer Engineering
Western Michigan University
1903 W. Michigan Ave., Kalamazoo, MI 49008
USA
ikhlas.abdelqader@wmich.edu

Abstract: - A new image encryption scheme is proposed based on one-dimensional Convex-Sinusoidal Map (CSM). The dynamics of this chaotic map are analyzed and used to develop a two-phase image encryption framework. In the first phase, the image-permutation, a pseudorandom number generator is proposed to shuffle pixel locations while in the second phase, the image-substitution, CSM is utilized to modify pixel intensity values. Experimental results indicate that the Convex-Sinusoidal Map exhibits robust chaos with wide range chaotic behavior. Results also show that the proposed image encryption framework has a large-key space with complexity of order $O(2^{129})$ making it immune against Brute-Force Attack methods. It only requires $845ms$ to encrypt 200×200 pixels images using Intel Core i3 with 4GB memory machine. Moreover, this algorithm provides complete obscure for plain-text images and high encryption performance.

Key-Words: - Image encryption, Chaotic maps, Pseudorandom number, Image substitution, Image permutation

1 Introduction

Image encryption algorithms can be classified into analog-based and digital-based algorithms. In analog-based algorithms, a continuous-time transmitter circuit is built where its output is digitized and used to encrypt an image. The encrypted image along with the secret key are then transmitted. At the receiver end, the received secret key is used to synchronize a continuous-time receiver circuit with the transmitter circuit in order to recover the original transmitted image [1-2]. On the other hand, digital-based image encryption algorithms can be classified into non-chaos, such as advanced encryption standard (AES) [3] and data encryption standard DES [4], and chaos-based. Chaos-based image encryption algorithms utilize chaotic maps to change pixel intensity values [5-12]. Other chaos-based algorithms consist of two stages of encryption; one stage changes pixel intensity values based on chaotic maps while the other stage shuffles pixel locations based on pseudorandom number generators [13-14]. Different pseudorandom number generators were used to shuffle pixel locations such as Henon Map [14,15], Arnold Cat Map [13,16], and Chebyshev Map [13]. Chaotic maps are used in encryption since they have been found to hold attractive characteristics such as high sensitivity to their control parameters and initial conditions, the instability of system orbit, and the ease of implementation. Therefore, chaos-based encryption algorithms meet the demand for fast and reliable image transmission.

Several one-dimensional chaotic maps were proposed in the literature [5-6, 8-14]. However, encryption methods based on the Logistic Map offer low-level security, do not satisfy the uniform distribution property, and have small key space [14]. To increase encryption security based on Logistic Map, nonlinear functions were adopted to Logistic Map [14]. In [17], the Logistic Map was generalized to obtain B-Exponential Map (BEM). The BEM exhibited robust chaos for the selected range of the control parameter. Then based on BEM, a pseudorandom number generator was proposed to shuffle pixel locations. Also, in [18], the encryption security of the Logistic Map, Madelbrot Map, and Symmetric Tent Map were investigated. It was concluded that the investigated maps possess a large set of vulnerabilities. In [19], the encryption security of the Domino Signal Encryption Algorithm (DSEA) framework was analyzed and they found that DSEA is insecure against Brute-Force Attack methods and chosen-plaintext attacks.

In this paper we propose a novel chaotic map, referred to as convex-sinusoidal map (CSM) and investigate its properties and its suitability for image encryption. Our image encryption framework is developed based on the convex-sinusoidal map and it consists of two phases, a pseudorandom number generator is proposed to shuffle pixel locations in the image-permutation phase while in the image-substitution phase, the CSM is utilized to modify pixel intensity values.

The outline of the paper is as follows: in section 2, the convex-sinusoidal map is presented. In section 3, properties of CSM are explored while a detailed description of the proposed CSM-based image encryption framework is provided in section 4. The experimental results along with detailed analysis of CSM-based image encryption framework are presented in section 5 and section 6 concludes the paper.

2 Convex-Sinusoidal Map (CSM)

The proposed convex-sinusoidal chaotic map can be presented per Equation 1.

$$x_{n+1} = \begin{cases} 0.75\lambda x_n + 0.25\sin\left(\frac{\pi}{2}\lambda x_n\right), & 0 \le x_n \le 0.5 \\ 0.75\lambda(1-x_n) + 0.25\sin\left(\frac{\pi}{2}\lambda(1-x_n)\right), & 0.5 < x_n \le 1 \end{cases} \tag{1}$$

where the sequence of real values $\{x_0, x_1, \cdots, x_n, \cdots\}$ forms the system orbit, x_0 is the initial condition, the iteration function $x_{n+1} = CSM(x_n, \lambda)$ satisfies the condition $CSM:[0,1] \to [0,1]$, and the control parameter λ has the range of $[0.95, 2.71]$ and within this range, the dynamical behavior of CSM ranges from chaotic to predictable as will be explored next.

3 CSM Properties and Significance

This section investigates properties of the proposed convex-sinusoidal map. The investigated properties are S-unimodality, dynamical behavior, bifurcation diagram, and sensitivity to control parameters and initial conditions.

Figure 1 shows a graph of CSM per Equation 1 for $\forall x_0 \in [0,1]$ with $\lambda = 2$. As the figure shows, CSM has a single critical point at $x = 0.5$, starting from zero, monotonically increasing to one, and then monotonically decreasing to zero. Therefore, CSM satisfies the unimodality property.

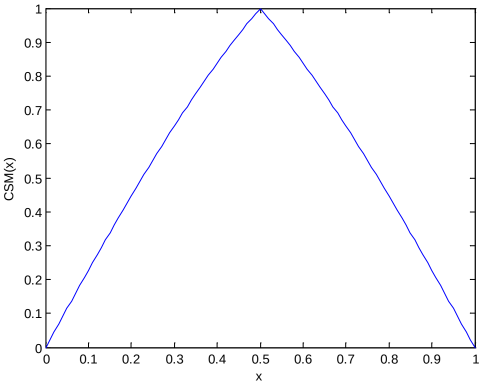


Fig.1: The iteration function associated with the CSM for $\forall x_0 \in [0,1]$ and for $\lambda = 2$

The bifurcation diagram is used to qualitatively analyze convex-sinusoidal map since it is a great tool to show all possible ranges of $CSM(x_n, \lambda)$ against λ. The bifurcation diagram of CSM is shown in Figure 2. The range of λ that makes CSM satisfy the unimodality property is extracted from the figure as $[1.95, 2.1091]$.

The Schwarzian derivative can be used to analyze the dynamical behavior of CSM as shown in Equation 2 [7]. The Schwarzian derivative of CSM for 100 iterations obtained for $x_0 = 0.301$ is shown in Figure 3. From Figure 3, we observe that the Schwarzian derivative is negative. This result along with that of Figure 1 show that CSM satisfies the S-unimodality property and provides a robust chaos within the previous range.

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

The high sensitivity of the convex-sinusoidal map to its initial conditions is illustrated in Figure 4, which shows two sequences of 100 iterations each obtained using Equation 1 with $\lambda = 2$ and for two initial values; $x_0 = 0.662$ and $x_0 = 0.662001$. As shown in this figure, the two sequences become different after a few iterations.

Range of λ that achieves chaotic behavior for CSM can be found using the Lyapunov exponent [7] as defined by Equation 3.

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

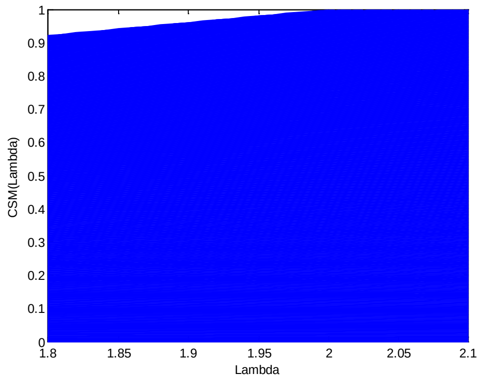


Fig.2: The Bifurcation diagram of CSM for $\lambda \in [1.8, 2.11]$

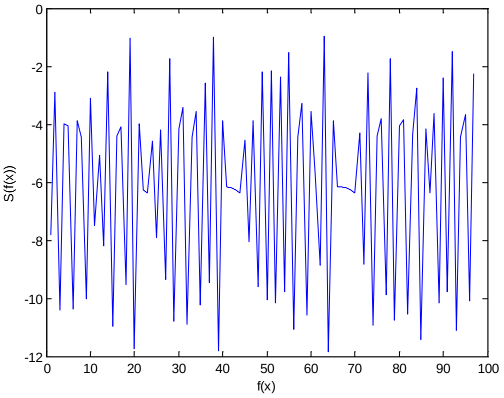


Fig.3: Schwarzian derivative of the Convex-Sinusoidal Map

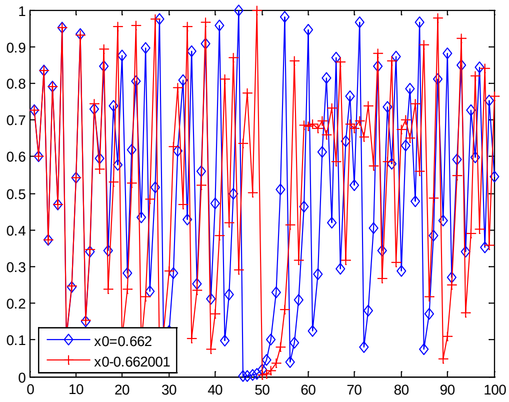


Fig. 4: Two sequences obtained for $(x_0, \lambda) = (0.662, 2)$ shown in blue and for $(0.662001, 2)$ shown in red

and the derivative of Equation 1 is shown in Equation 4,

$$f'(x_n,\lambda)=\begin{cases}0.75\lambda+\frac{\pi}{8}\lambda\cos\left(\frac{\pi}{2}\lambda x\right), \ 0\le x<0.5\\ -0.75\lambda-\frac{\pi}{8}\lambda\cos\left(\frac{\pi}{2}\lambda(1-x)\right), 0.5<x\le 1\end{cases} \qquad (4)$$

where $f'(0.5,\lambda)$ is undefined. The Lyapunov exponent of convex-sinusoidal map is graphed in Figure 5. As reported in [7], a chaotic behavior is obtained for $0 < \lambda_{LE} \le 0.69$ which is extracted from Figure 5 for $\lambda \in [0.96, 2.71]$. We also observe a large variation in the Lyapunov exponent indicating a robust chaos for convex-sinusoidal map within the previous range.

Combining the result from Bifurcation diagram with result of Lyapunov exponent, we can conclude that convex-sinusoidal map exhibits S-unimodality property with chaotic behavior for $\lambda \in [1.95, 2.1091]$. This indicates a wide chaotic range can be used in comparison with range of other maps. For example, the Tent and Logistic Maps achieve S-unimodality with chaotic behavior for $\lambda \in [1.999, 2)$ and $\lambda \in [3.96, 4]$, respectively [8].

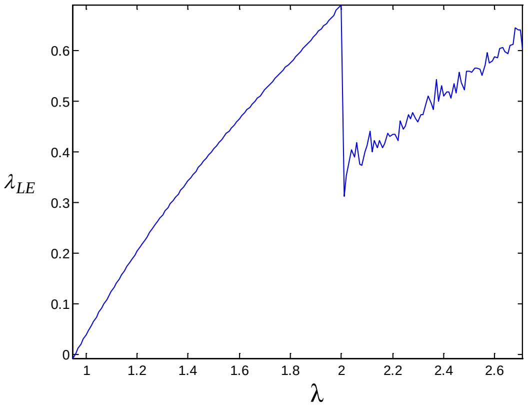


Fig.5: The Lyapunov exponent of the CSM for $\lambda \in [0.95, 2.71]$

4 CSM-Based Encryption Framework

In this section, the CSM-based image encryption framework is explored which consists of two phases, pixel locations are shuffled in the image-permutation phase and pixel intensity values are modified in the image-substitution phase using the proposed mapping algorithm.

4.1 Image Permutation Phase

To decrease correlation between adjacent pixels of raw image, the permutation phase consists of two steps, which are described as follows.

1. In Equation 5, we show the proposed pseudorandom number generator (PRNG) used to shuffle original pixel locations in the raw image,

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 2\alpha x_n + 3y_n \\ x_n + (1+\alpha)y_n \end{bmatrix} \bmod \begin{bmatrix} M \\ N \end{bmatrix} \qquad (5)$$

where M and N are the dimensions of the raw image, (x_n, y_n) represents original location of a pixel, (x_{n+1}, y_{n+1}) represents its new location after shuffling, and α is a part of the secret key which should take on different values in the range $\alpha \in [0.9988, 1.0012]$. This range ensures that PRNG achieves the uniformity and consistency properties.

2. The image obtained from previous step is divided into a number of blocks with each block of size $N_b \times N_b$ pixels according to Equation 6. Let the block indices be a vector denoted as $b = \{0, 1, ..., m-1\}$. The block indices vector is rotated left *nr* times resulting in a new vector that represents the new block indices. The shuffled image I_s is reconstructed according to the new block indices vector.

$$N_b = \left\lfloor \frac{\sqrt{MN + nr}}{nr - 1} \right\rfloor \qquad (6)$$

where *nr* is a part of the secret key, *nr* is set to 6 resulting in a block size of 40x40 pixels with 25 blocks per 200x200 pixels image.

4.2 Image Substitution Phase

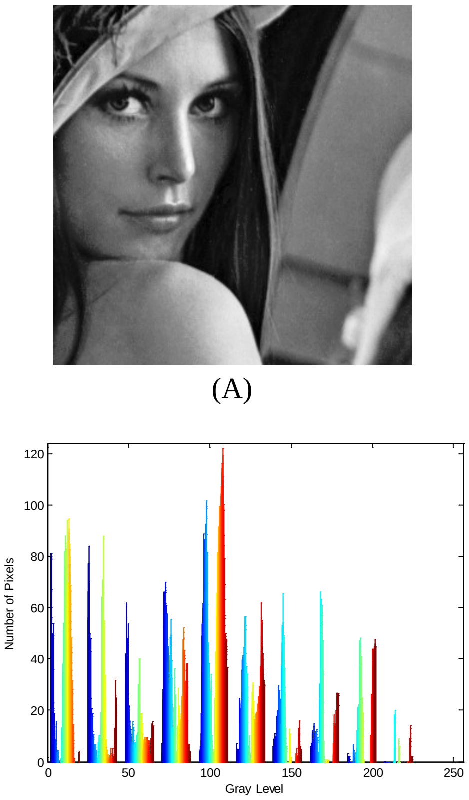
Image substitution is intended to change the intensity value of shuffled pixels to achieve higher security with this method of encryption. We propose equation 7 for the substitution process,

$$I_f = \left| W^{-0.5} \right| (I_s \oplus K) \qquad (7)$$

where K represents the key image obtained using Equation 1, I_s represents the shuffled image obtained from the permutation phase, I_f represents the resulting substituted image, and W is the identity matrix of same size as the original image.

5 Experimental Results and Discussion

Two different images are used to evaluate the encryption performance of the proposed CSM-based image encryption framework. The first image is the well-known Lena image as shown in Fig. 6. The shuffled image as shown in Fig.7-A is obtained for α=1.0004. The shuffled image shows no useful visual information. However, we observe that there is not much of a difference between its histogram and that of the original image as shown in Fig. 7-B which indicates that the original image can be revealed by histogram attacking methods up to this point of the encryption process [20]. The reconstructed shuffled image is shown in Fig.7-C where the correlation between adjacent pixels of the shuffled image is expected to decrease after the block shuffling process.



(A)

(B)

Fig. 6: (A) Original image and (B) its histogram

The substituted image, as shown in Fig. 8-A, is obtained for initial condition x_0 and control parameter λ values of 0.662 and 2, respectively. We note that the original image is 100% obscured. A statistical test on the histogram of substituted image is performed and we note: 1) the histogram of substituted image is fairly uniform and significantly different from that of original image, 2) the correlation between two adjacent pixels in horizontal, vertical and diagonal orientations is found by using Equation 8.

$$r = \frac{N_p \sum_{i=1}^{N_p} (x_i y_i) - \sum_{i=1}^{N_p} x_i \sum_{i=1}^{N_p} y_i}{\sqrt{\left(N_p \sum_{i=1}^{N_p} x_i^2 - \left(\sum_{i=1}^{N_p} x_i \right)^2 \right) \left(N_p \sum_{i=1}^{N_p} y_i^2 - \left(\sum_{i=1}^{N_p} y_i \right)^2 \right)}} \qquad (8)$$

where N_p represents number of adjacent pixels taking into account, (x,y) represents intensity values of the two selected adjacent pixels. We used 1000 randomly selected adjacent pixels to calculate the vertical, horizontal, and diagonal correlation of the original and substituted images. The substituted images are obtained using proposed CSM-based, Tent Map-based, and Logistic Map-based image encryption algorithms for control parameter λ values of 2, 1.9999, and 3.97, respectively. The correlation results are summarized in table 1. As table 1 show, the neighboring pixels in the original image are highly correlated while they are poorly correlated in the substituted images. The correlation results of the substituted images are very close. However, best average correlation result is obtained using Logistic Map-based encryption algorithm. Entropy is a statistical measure of randomness. The ideal value of Entropy of an encrypted image is 8. Entropy of the substituted images is summarized in table 1. Entropy of the substituted images is close to the ideal value with best result obtained using the proposed CSM-based and Tent Map-based image encryption algorithms indicating that the substituted image is highly secured against entropy attack methods [17]. The obtained correlation and entropy results are indicative of the superior permutation and substitution properties of the CSM-based encryption framework.

Since most of the reported encryption algorithms do not provide high encryption efficiency for plain text images [21], we decided to test robustness of this proposed encryption framework for text images. A plain text image is used, shown in Fig.9-A and its shuffled image is shown in Fig.10-A. The resultant image shows no visual useful information. However, as with the previous results, not much difference in the histogram of the original image, Fig. 9-B, is observed when compared to those of the shuffled image, Fig. 10-A, or reconstructed image, Fig. 10-C, per their histograms shown in Figs. 10-B and 10-D, respectively.

Using the same experimental setup for this shuffled text image as we used in the image of Fig. 6-A, that is the same initial condition and control parameter values are used, we generate the substituted text image shown in Fig.11-A. The original image is 100% obscured. Also, histogram of the substituted image is fairly uniform and significantly different from that of original image. We would like to note that we propose to use Equation 9 for the anti-substitution phase. The anti-permutation phase is done through reversing the steps involved in section 4.1. The decryption process exactly recovered the original encrypted image without loss of information.

$$I_s = \left(|W|^{0.5} I_f\right) \oplus K \tag{9}$$

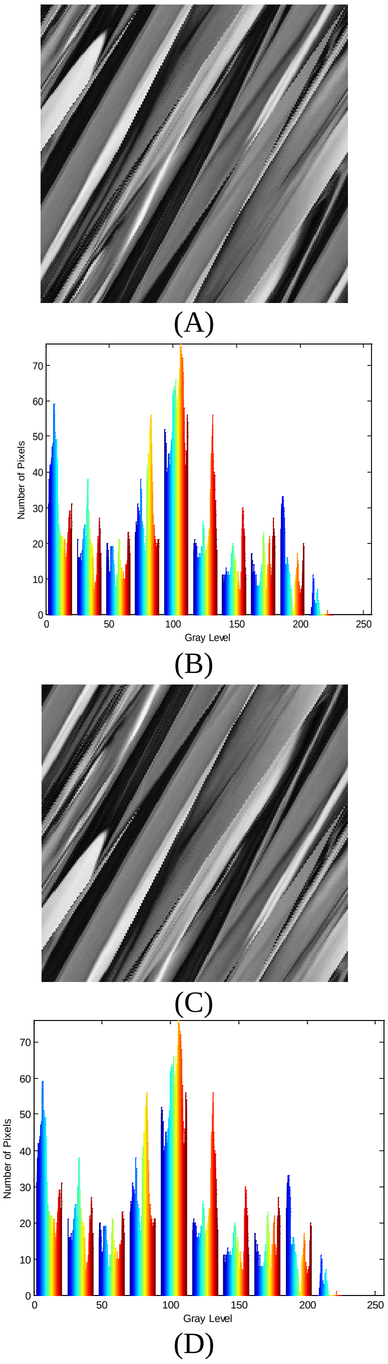
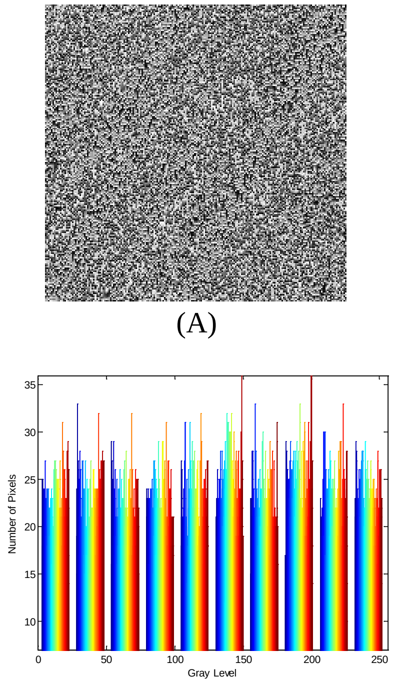


Fig. 7: (A) Shuffled image, (B) histogram of A, (C) Reconstructed shuffled image, (D) histogram of C

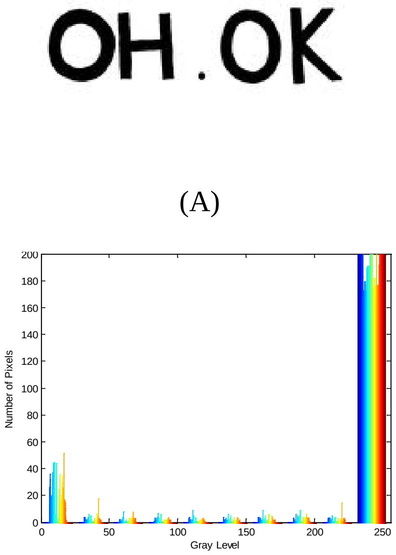
We also tested the proposed framework for sensitivity to small changes in initial conditions and/or the control parameter. For example, we implemented a very small change to one parameter of the received secret key while the rest are kept constant. We found completely different images from the original encrypted image are recovered in the decryption phase for each one of the secret keys $(x_0,\lambda)=(0.662,2.000000000000001)$ and $(x_0,\lambda)=(0.6620000000000001,2)$. Also, changing value of *nr* and/or α recovers a completely different image from the original image.



(A)

(B)

Fig. 8: (A) Substituted image and (B) its histogram



(A)

(B)

Fig. 9: (A) Text Image and (B) histogram of A

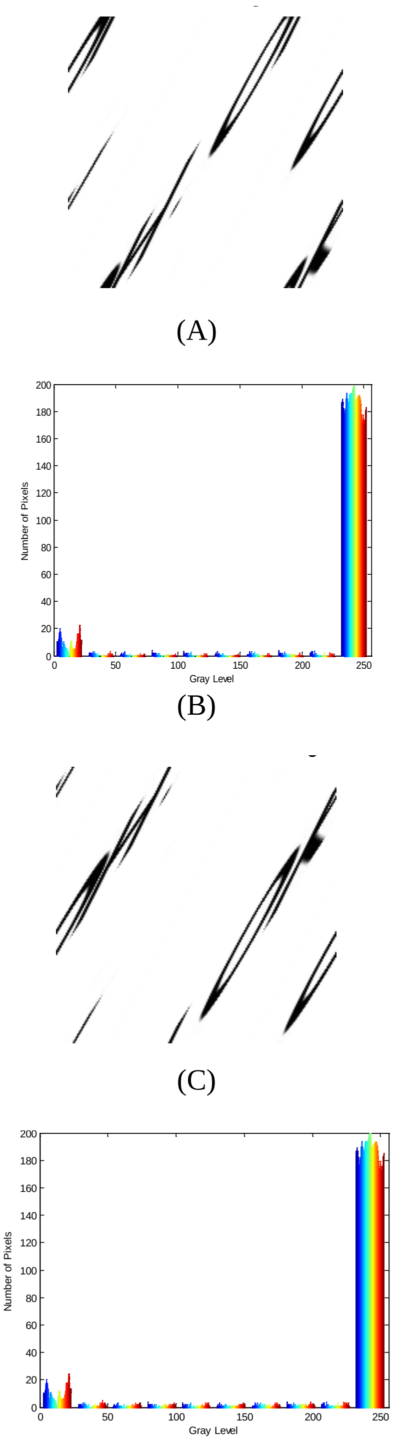
One of the well-known methods of recovery from an encrypted image is Brute-Force Attack [22]. Brute-force attack estimates secret key parameters through exhaustive search of all possible value of parameters in the secret key. The secret key of CSM-based encryption framework consists of three parameters and one initial condition. The parameters x_0, *nr*, α, and λ have be adjusted to an accuracy of one part in 10^{16}, 10^{4}, 10^{3}, and 10^{16} to correctly recover the original reconstructed image. This indicates 10^{39} mathematical operations are needed to conduct an extensive search of all possible value of parameters in the secret key to exactly recover the original image. In other words, the proposed CSM-based image encryption framework has a complexity of order $O(2^{129})$. In comparison, the 56-bit DES algorithm requires 2^{56} mathematical operations [13]. Also, Li et. al. [24] analyzed the security of the proposed image encryption scheme by [23] and found that is has a complexity of order $O(2^{72})$. Any encryption scheme to be secure enough against brute-force crypto-analysis must at least have a complexity of order $O(2^{128})$ [16].

Speed of the CSM-based encryption framework is an important factor and needed to be addressed. The proposed CSM-based framework requires 845ms to encrypt a 200x200 pixels image using Intel Core i3 with 4GB memory machine using MATLAB. In comparison, the nonlinear chaotic algorithm proposed by [14] and the encryption scheme proposed by [25] take 0.5s and 1.125s to encrypt a 256x256 pixels Lena image.

6 Conclusions

In this paper, a one-dimensional convex sinusoidal chaotic map is proposed for grayscale image encryption. The dynamics of this chaotic map are analyzed and found to have interesting properties such as S-unimodality and a wide chaotic range. Our proposed digital image encryption CSM-based framework consists of two phases, 1) the image-permutation phase-in which a pseudorandom number generator is proposed to shuffle locations of image pixels and 2) the CSM-phase or the image-substitution phase, which is utilized to modify pixel intensity values.

Experimental results indicate that the proposed image encryption framework has a large-key space with complexity of order $O(2^{129})$ making it immune against Brute-Force Attack methods while providing complete obscured image content and high encryption performance. Finally, the proposed encryption framework provides high encryption efficiency for plain text images.



(A)

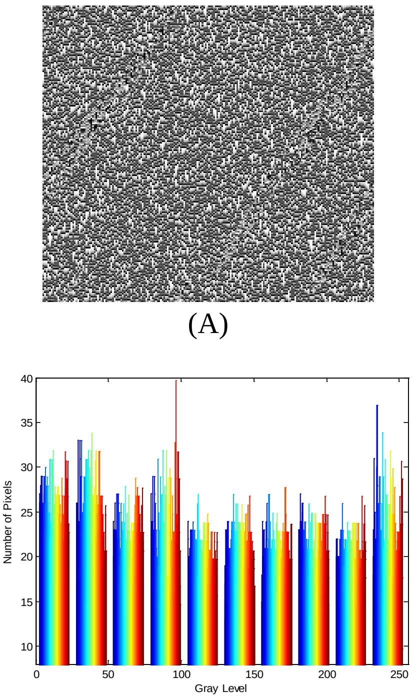
(B)

(C)

(D)

Fig. 10: (A) Shuffled image, (B) histogram of A, (C) Reconstructed shuffled image, (D) histogram of C

The proposed framework consists of different steps intended to provide high encryption performance, resulting in a relatively high computational complexity which decreases the encryption speed. Future work should be focused on reducing the computational complexity without compromising the encryption performance.



(A)

(B)

Fig. 11: (A) Substituted image and (B) its histogram

Acknowledgement

The authors thank the anonymous referees for their helpful comments on the initial version of this manuscript.

References

[1] L.M. Pecora, T.L. Carroll, Synchronization in chaotic systems, *Physical review letters*, 64, 1990, pp. 821-4.

[2] G. Alvarez, F. Monotoya, G. Pastor, M. Romera, Chaotic cryptosystems, *Proceedings of IEEE international carnahan conference on security technology*, 1999, pp. 332-8.

[3] Announcing the advanced encryption standard, *Federal information processing standards publication*, 197, Oct. 2, 2012.

[4] Cryptographic algorithms for protection of computer data during transmission and dormant storage, Federal register 38 (93), May 15, 1973.

[5] G. Jakimoski, L. Kocarev, Chaos and cryptography: block encryption ciphers based on chaotic maps, *IEEE transactions in circuit*

systems-I: fundamental theory applied, 48 (2), 2001, pp. 163-9.

[6] A. Kanso, N. Smaoui, Irregularly decimated chaotic map(s) for binary digits generations, *International journal of bifurcation and chaos*, 19 (4), 2009, pp. 1169-83.

[7] J.M. Aguirregabiria, Robust chaos with variable lyapunov exponent in smooth one-dimensional maps, *Chaos, solitons and fractals*, 42 (4), 2009, 2531-2539.

[8] A. Kanso, Self-shrinking chaotic stream ciphers, *Communications in nonlinear science and numerical simulation*, 16, 2011, pp. 822-836.

[9] K. S. Ntalianis, An object adaptive chaotic cipher: increasing the security of multimedia encryption schemes, *WSEAS transactions on systems*, 3 (10), 2004, pp. 3059-3064.

[10] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos, Solitons & Fractals*, 21 (3) 2004, pp. 749-C761.

[11] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *International journal of bifurcation and chaos,* 8 (6), 1998, pp. 1259-C1284.

[12] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic baker maps, *International journal of bifurcation and chaos*, 14 (10), 2004, pp. 3613-C3624.

[13] X. Ma, C. Fu, W. Lei, S. Li, A novel chaos-based image encryption scheme with an improved permutation process, *International journal of advanced computer technology*, 3(5), 2011, pp. 223-233.

[14] H. Gao, Y. Zhang, S. Liang, D. Li, A new chaotic algorithm for image encryption, *Chaos, solitons, and fractals*, 29 (2), 2006, pp. 393-399.

[15] A. Jolfaei, A. Mirghadri, An image encryption approach using chaos and stream cipher, *Journal of theoretical applied information technology*, 19(2), 2010, pp. 117-125.

[16] Z.H. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm, *Physical review letters*, 346, 2005, pp. 153-157.

[17] M. Shastry, N. Nagaraj, P. Vaidya, The b-exponential map: a generalization of the logistic map, and its applications in generating pseudo-random numbers, cs.CR/0607069, 14 Jul 2006.

[18] D. Arroyo, J. Amig´o, S. Li, G. Alvarez, On the inadequacy of unimodal maps for cryptographic applications, *In proceedings of 11th spanish meeting on cryptology and information security* (*RECSI* 2010), 2010, pp. 37-42.

[19] C. Li, S. Li, D.C. Lou, D. Zhang, On the security of the yen–guos domino signal encryption algorithm (DSEA), *Journal of systems and software*, 79 (2), 2006, pp. 253-8.

[20] H. Cheng, Partial encryption of compressed images and videos, *IEEE transactions on signal processing*, 48(8), 2000, pp. 2439-2451.

[21] C.Q. Li, S.J. Li, G. Alvarez, G.R. Chen, K.T. Lo, Cryptanalysis of two chaotic encryption schemes based on circular bit shift and xor operations, *Physical letters A*, 369(1-2), 2007, pp. 23-30.

[22] L.M. Adleman, P.W.K. Rothemund, S. Roweis, E. Winfree, On applying molecular computation to the data encryption standard, *Journal of computational biology*, 6(1), 1999, pp. 53-63.

[23] N. Pareek, V. Patidar, K. Sud, Image encryption using chaotic logistic map, *Image and vision computing*, 24 (9), 2006, pp. 926–934.

[24] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, *Image and vision computing*, 27 (9), 2009, pp. 1371-1381.

[25] J. Giesl, L. Behal, K. Vlcek, Improving chaos image encryption speed, *International journal of future generation communication and networking*, 2(2), 2009, pp. 23-36.

Table 1: Vertical, horizontal, and diagonal correlation of two adjacent pixels for encryption based on CSM, Tent map, and Logistic map

	Original Image	**Substituted Image (CSM)**	**Substituted Image (Tent map)**	**Substituted Image (Logistic map)**
Entropy	7.3893	7.995	7.995	7.9851
Horizontal Correlation	0.9874	0.04	0.0406	0.0404
Vertical Correlation	0.9934	0.0395	0.0404	0.0365
Diagonal Correlation	0.9815	0.0402	0.0403	0.0398
Average Correlation	**0.9874**	**0.0399**	**0.0404**	**0.0389**