International Journal of Security and Its Applications
Vol.8, No.4 (2014), pp.89-100
http://dx.doi.org/10.14257/ijsia.2014.8.4.09

A Block Encryption Scheme for Secure Still Visual Data based on One-Way Coupled Map Lattice

Alaa Zaghloul[1,2], Tiejun Zhang[3], Handan Hou[4], Mohamed Amin[1], Ahmed A. Abd El-Latif[1,*] and Mohamed S. Abd El-Wahab[2]

[1]Menoufia University, Egypt
[2]Misr University for Science and Technology, Egypt
[3]Harbin University of Science and Technology, China
[4]Harbin Finance University, China
alaa_zaghloul@yahoo.com, tiejun.zhang@hrbust.edu.cn, hou.handan@gmail.com, ahmed_rahiem@yahoo.com

Abstract

How to protect the secret digital images is an important issue in commercial or military application. In this paper, we propose a new scheme for secure still visual data with a block cipher structure, which is composed of three parts: encryption, decryption and key generator. The encryption process based on cryptographic primitive operations and Boolean functions is proposed. A key generator based on one-way coupled map lattice (OCML) is derived. Experimental results have demonstrated that the proposed cipher has satisfactory security with a low cost, which makes it a potential candidate for encryption of multimedia data such as images, audios and even videos.

Keywords: *Encryption, block cipher, spatiotemporal chaotic system, Boolean functions*

1. Introduction

In recent years, various cryptosystems have been proposed and widely used, such as DES, IDEA or AES. However, these encryption schemes have been invented to text or bit encryption and appear not to be ideal for image applications due to some intrinsic features of images such as the high correlation between neighbour pixels and the high redundancy. Conventional encryption algorithms may not be sufficient to hide these features which can still be visually and statistically apparent even after encryption.

Recently, the challenges of conventional cryptography such as the complexity of their internal structure have been solved by physics (*e.g.,* chaos theory) instead of mathematics (*e.g.,* number theory). Inspired by the subtle similarity between chaos and cryptography [1], various encryption techniques based on chaos have been proposed in the literature [2-8]. However, most of the proposed schemes flawed by some security and performance problems [9-12] such as the way of generating the keystream, small key space, the required round encryption time (the trade off between security and the over all performance), *etc.*

Spatiotemporal chaotic systems have attracted more interests among researchers in many fields. The spatiotemporal chaos possesses inherent features can be useful in cryptography means. The orbit of spatiotemporal chaos has a long period and is found much longer than that of temporal chaotic system even with dynamical degradation of digital chaos [13]. Moreover, the spatiotemporal chaos is high dimentional, having a large number of positive

[*] Corresponding author: ahmed_rahiem@yahoo.com, TEL: +2 01285851184

ISSN: 1738-9976 IJSIA

Lyaponov exponents that guarntee the randomness of the orbit. In addition, spatiotemporal chaos has multiple sites that can generate independent keystreams simultaneously.

Here we aim to use a spatiotemporal chaotic system incorporating with cryptographic primitives operations for designing a new cipher. This provides the opportunity for great flexibility in both security level and performance characteristics. In this paper, we introduce a new image encryption scheme based on a spatiotemporal chaotic system. The proposed scheme consists of three parts: encryption, decryption and key generator. The encryption process based on cryptographic primitive operations and Boolean functions is proposed. A key generator based on one-way coupled map lattice (OCML) is derived. Finally, the performance and security of the proposed scheme will both be analyzed and tested.

The rest of this paper is organized as follows. The proposed algorithm is introduced in Section 2. Section 3 is devoted to performance analysis. Finally, Section 4 gives the conclusion.

2. A Block Cipher based on One-Way Coupled Map Lattice

A block cipher based on a spatiotemporal chaotic system, adopting here an OCML, is constructed in the following section.

2.1. One-Way Coupled Map Lattice

Eq. (1) defines the chaotic logistic map as

$$f(x,r) = rx(1-x), \tag{1}$$

where x∈[0,1], $0 \le r \le 4$. When $3.57 \le r \le 4$, the map in the chaotic region as shown in Fig.1. Fig. 1 shows the Lyapunov exponent curve of logistic and generalized logistic maps. Generally, the positive value of Lyapunov exponent, a measure for sensitive dependence on initial conditions, is a sign of chaos. It is noted that the logistic map has some drawbacks such as non-uniform behaviour and blank windows in the chaotic region as can be seen in Figure 1, there are some areas where the Lyapunov exponent is either zero or negative.

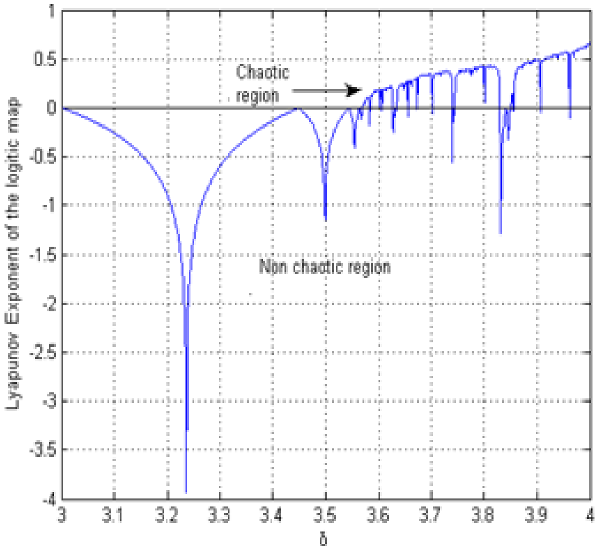


Figure 1. Lyapunov Exponent Curve of Logistic Map

To overcome the issue of the logistic map, we introduce a One-way coupled map lattice (OCML). OCML is a chaotic system that can exhibit spatiotemporal chaos [13]. It has its evident advantages in media security, as it possesses a large number of positive Lyapunov exponents.

The reasons for chosen the spatiotemporal chaotic system in this paper is as follows:

- The orbit of spatiotemporal chaos has a long period and is found much longer than that of temporal chaotic system even with dynamical degradation of digital chaos [13, 14].
- The spatiotemporal chaos is high-dimensional, having a number of positive Lyapunov exponents that guarantee high randomness. It is therefore difficult to predict the time series generated by this kind of chaotic systems [14].
- In addition, spatiotemporal chaos has multiple sites that can generate independent keystreams simultaneously [13].

By adopting different local maps and coupling methods, different coupled map lattices can be constructed. Herein, an OCML based on chaotic logistic map is given by

$$v_{m+1}(t) = (1-\tau)\, f(v_m(t)) + \tau\ f(v_m(t+1)) \tag{2}$$

where m=0,1,…,T-1 is the time index; t =1,2,…,L is the lattice state index; f is a chaotic logistic function Eq.(1); $\tau \in (0,1)$ is a coupling constant; T is the length of the plainimage; and L is maximum value of lattice state index. Here, L is chosen as 1, while the other parameter is selected as $\tau = 0.02$ in order to have good chaotic properties [15].

2.2. Cryptosystem Key Generation

We propose a new secret key generation for encryption/decryption by initializing array of random sequences through adopting the OCML to generate random sequences XORed with an array of subkeys mixed with the adapted user's secret key. The key schedule algorithm consists of three algorithmic steps: conversion, initialization, and mixing respectively. For conversion, copy user secret key K [$0...b-1$] into an array L[$0....c$-1] of words c= [b/u], where u=w/8 is the number of bytes/word. This operation is done in a natural manner, using u consecutive key bytes of K to fill up each successive word in L, low-order byte to high-order byte, as in the identical RC6. For initialization, we initialize the array S to a particular fixed pseudorandom bit pattern using a spatiotemporal chaotic map. Finally, the user's secret key is mixed over the array S and L.

Algorithm: Cryptosystem Key Generation

```
INPUT: user secret key (key b byte), number of rounds r, initial value $x_1(0)$ , control parameter
       $\eta$
OUTPUT: w-bit round keys S[0,...,2r+4]
Step 1: $for\ (i = b-1, L[c-1] = 0; i\,! = -1; i--)$
            $L[i/u] \leftarrow (L[i/u] <<< 8) + K[i];$
Step 2: $for(IV\ [0] = init\_pad, i = 1; i < t; i++)$
            $IV[i] \leftarrow OCML\ (chop\ (Map1\ (K[subkey] + pad), K\ [next\_subkey\ (Subkey)])$
            $+ IV\ [i-1];$
            $subkey \leftarrow next\_subkey\ (subkey);$
        $for(i = 0; i < t; i++)$
        $C[i] \leftarrow Map2\ (IV[i]);$
        $S[i] \leftarrow C[i];$
Step 3: $for(X = Y = i = j = k = 0; k < t; k++, i = (i+1) \bmod t,\ j = (j+1) \bmod c)$
        $X \leftarrow S[i] \leftarrow (S[i] + X + Y) <<< \lg w;$
        $X \leftarrow L[j] \leftarrow (L[j] + X + Y) <<< (X + Y);$
```

COMMENT:

1. The function *Map*1 (*x*) denotes maps a byte to [0, 1] interval
2. The function *Map*2 (*x*) denotes maps the [0, 1] interval to an integer into [0, 255]
3. The function chop (*x*) denotes return *x* with the integer part
4. init_pad (*K*[*b*]) denotes the initial pad from the user supplied secret key
5. The function OCML (*x*, iterations) means to evaluate the spatiotemporal chaotic map starting from *x*, iteration times

2.3. Encryption Scheme

The following algorithmic steps give the proposed encryption process.

Algorithm: Encryption Scheme

INPUT: The scrambled image *P*, number of rounds *r*, *w*-bit round keys *S*[0,...,2r+4]
OUTPUT: 128-bit cipherimage *C* stored in $P_i\ (i=1,2,3,4)$

```
Step 1: Initial key addition
    $k \leftarrow (S[0] \oplus S[1]) <<< \lg w;$   $l \leftarrow (S[0] \vee S[1]) <<< \lg w;$
    $P_2 \leftarrow P_2 + (S[0] * k);$   $P4 \leftarrow P4 + (S[1] * l);$
Step 2: One round mixer
    $for\ (i = 1; i <= r; i++)$
        $a \leftarrow (P_2\ (2P_2 + 1)\ ) <<< \lg w;$   $b \leftarrow (P_4(2P_4 + 1)) <<< \lg w;$
        $c \leftarrow \mathrm{a} \oplus \mathrm{b};$
        $P1 \leftarrow (P_1 \oplus c) <<< (a \wedge b) + S[2i];$   $P_3 \leftarrow ((P_3 \oplus c) <<< (a \wedge b)) + S[2i+1];$
Step 3: Swapper
    $temp \leftarrow P_1;\ P_1 \leftarrow P_2;\ P_2 \leftarrow P_3;\ P_3 \leftarrow P_4;\ P_4 \leftarrow temp;$
Step 4: Final key addition
    $P_1 \leftarrow P_1 + S[2r+2];\ P3 \leftarrow P3 + S[2r+3];$
```

2.4. Decryption Scheme

Decryption is the inverse of encryption. At the receiver side, using the same round transformations and the same secret key, the decryption can easily derive from the encryption routine through the following steps.

Algorithm: Decryption Scheme

INPUT: the cipherimage C, number of rounds r, w-bit round keys S[0,...,2r+4]
OUTPUT: 128-bit plainimage P stored in $\mathrm{P}_i\ (i = 1, 2, 3, 4)$

```
Step 1: Initial key subtraction
    $P_1 \leftarrow P_1 - S[2r+2];\ P_3 \leftarrow P_3 - S[2r+3];$
Step 2: Inverse swapper
    $temp \leftarrow P_4;\ P_4 \leftarrow P_3;\ P_3 \leftarrow P_2;\ P_2 \leftarrow P_1;\ P_1 \leftarrow temp\ ;$
```

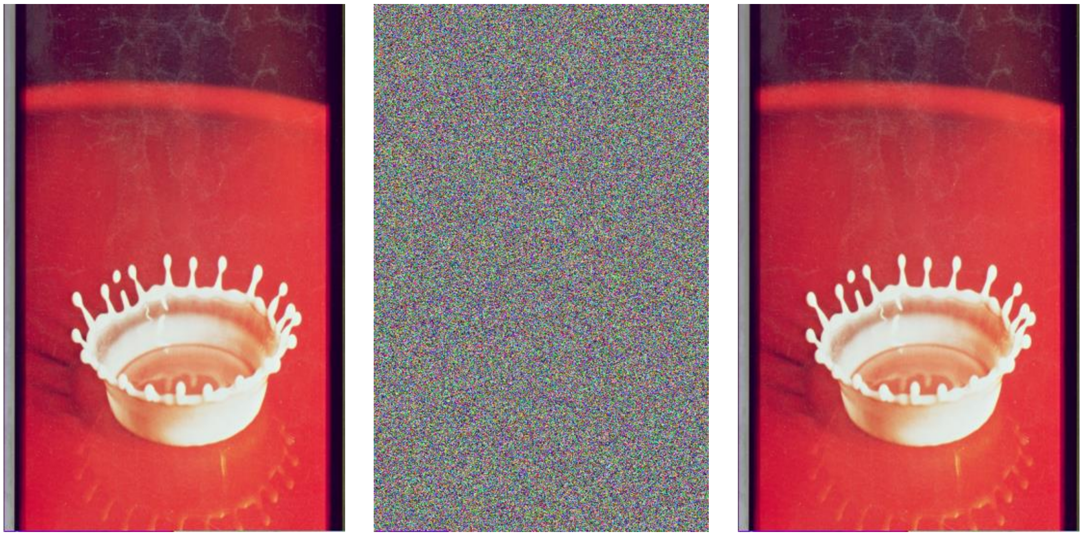
Step 3: Inverse the round mixer

```
$for\ (i = r; i > 0; i--)$
    $a \leftarrow (P_2\ (2\ P_2 + 1)\ ) <<< \lg\ w;$    $b \leftarrow (P_4(2\ P_4 + 1)) <<< \lg\ w;$
    $c \leftarrow a \oplus b;$
    $P_3 \leftarrow ((P_3 - S[2i+1]) >>> (\ a \wedge b)) \oplus c; P_1 \leftarrow ((P_1 - S[2i])\ >>> (a \wedge b)) \oplus c;$
```

Step 4: Final key subtraction

```
$k \leftarrow (S[0] \oplus S[1]) <<< \lg\ w;\ l \leftarrow (S[0] \vee S[1]) <<< \lg\ w;$
$P_2 \leftarrow (P_2 - (S[0] \times k);\ \ P_4 \leftarrow P_4 - (S[1] \times l);$
```

Figure 2 shows the encryption and decryption of Splash image.



a) Original image b) Encrypted image c) Decrypted image

Figure 2. Application of the Proposed Cipher to Splash Image

2.5. Remarks

Remark 1: Incorporation of a spatiotemporal chaotic system (OCML) as well as the cryptographic primitive operations, which strengthen the round keys for encryption and enlarge the key space required to resist the brute force attack.

Remark 2: The inner loop of the encryption and decryption is based on data-dependent rotations as well as integer multiplication, which is very effective primitive “diffusion”. The diffusion effect is increased due to the heavy dependence on rotations, the quadratic function that speed up the avalanche of change between rounds, and fixed bit shifting by five bits, which complicates advanced cryptanalytic attacks. This allows the proposed algorithm to run with fewer rounds of encryption and decryption at increased security.

Remark 3: Several simple steps in the round increase the rate of diffusion: integer multiplication, the quadratic equation, and fixed bit shifting by five bits, which is a secure way against both linear and differential attacks.

Remark 4: Like RC5 and RC6 algorithms, the proposed algorithm provides a great amount of flexibility with regards to the number of rounds r, the size of the encryption key b and the word size of the basic computational unit w.

3. Performance and Security Analysis

Here, the performance of the proposed cipher is analyzed in detail. We have made several experiments and tests to check the performance and security of the proposed scheme: differential attack tests including calculus of NPCR and UACI, information entropy analysis, statistical tests including calculus of the correlation coefficient of adjacent pixels and histogram analysis, and tests of key and plainimage sensitivity.

3.1. Differential Attack

As a requirement for image encryption algorithm to resist the differential attack, a minor change in the plainimage should cause a significant change in the cipherimage. To test the influence of a one-pixel change in cipher image, two common measures [16] are used, *i.e.,* number of pixels change rate (NPCR) and unified average changing intensity (UACI), they can be defined as:

$$NPCR = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\theta(i,j)}{m \times n} \times 100\%, \tag{3}$$

$$UACI = \frac{[\sum_{i=1}^{m}\sum_{j=1}^{n}|\theta'(i,j) - \theta''(i,j)|]/255}{m \times n} \times 100\%, \tag{4}$$

where θ' and θ'' are two images with the same size $m \times n$. m and n are width and height of the image. Define a bipolar array, θ, with the same size as images θ' and θ''. Then, $\theta(i,j)$ is determined by $\theta'(i,j)$ and $\theta''(i,j)$, namely, if $\theta'(i,j) \neq \theta''(i,j)$ then $\theta(i,j) = 1$; otherwise, $\theta(i,j) = 0$.

We have tested the NPCR and UACI with the proposed scheme to assess the influence of changing a single pixel in the original image on the encrypted image. We have performed the analysis of both NPCR and UACI for different images. From the results, we have found that the percentage of pixels changed in encrypted image is grater than 99.57 % for NPCR and is grater than 33.31 % for UACI even with one-bit difference in the plain images, indicating that the scheme is very sensitive with respect to small changes in the plain image.

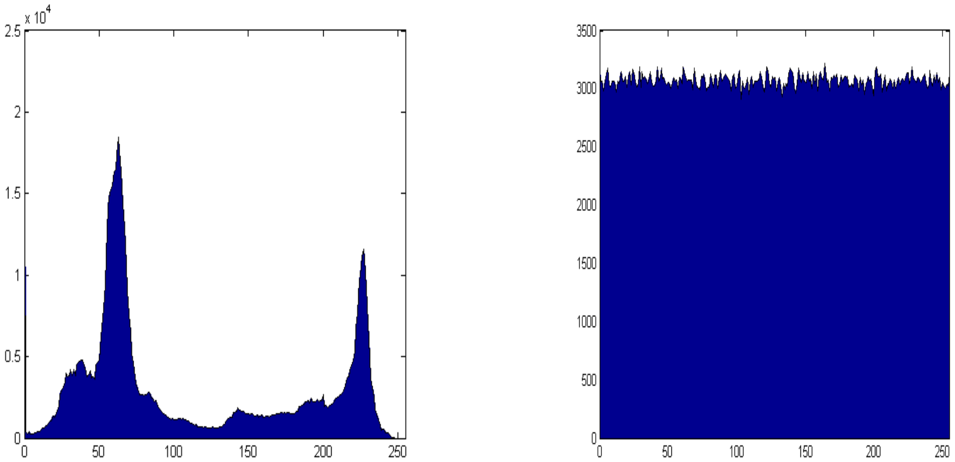
3.2. Statistical Analysis

Statistical analysis on cipher image is of crucial importance for any encryption algorithm. Actually, an ideal cipher should frustrate the powerful attacks based on statistical analysis.

Statistical analysis has been performed to show the resistance of the proposed encryption scheme against the statistical attacks. This is shown by a test on the histograms of the cipher images and on the correlations of adjacent pixels in the ciphered image.

- Histogram: Figure 3 shows the histogram analysis for the original (Figure 2a) and encrypted (Figure 2b) separately. The histogram of the encrypted image, approximate by a uniform distribution, is significantly different from the original image histogram.
- Correlation of adjacent pixels: An ideal encryption technique should produce the cipher images with no such correlation in the adjacent pixels (correlation coefficient

≈ 0) [17, 18]. The correlation coefficients of the adjacent pixels are calculated and listed in Table 1. The corresponding distribution for the vertical, horizontal and diagonal directions are shown in Figure 4. These figures demonstrate that the encryption algorithm has covered up all the plainimage characters image and shows good performance with a balanced 0–1 ratio.

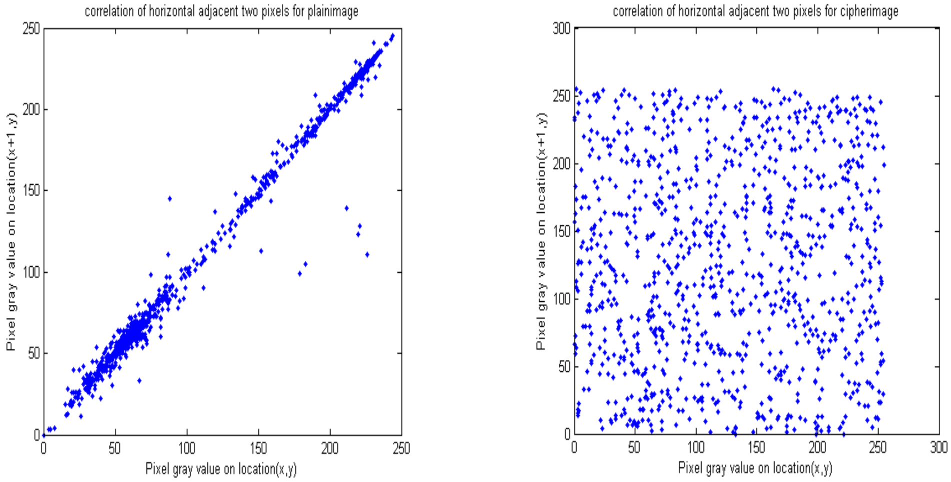


a) Histogram of original image of Figure 2a b) Histogram of original image of Figure 2b

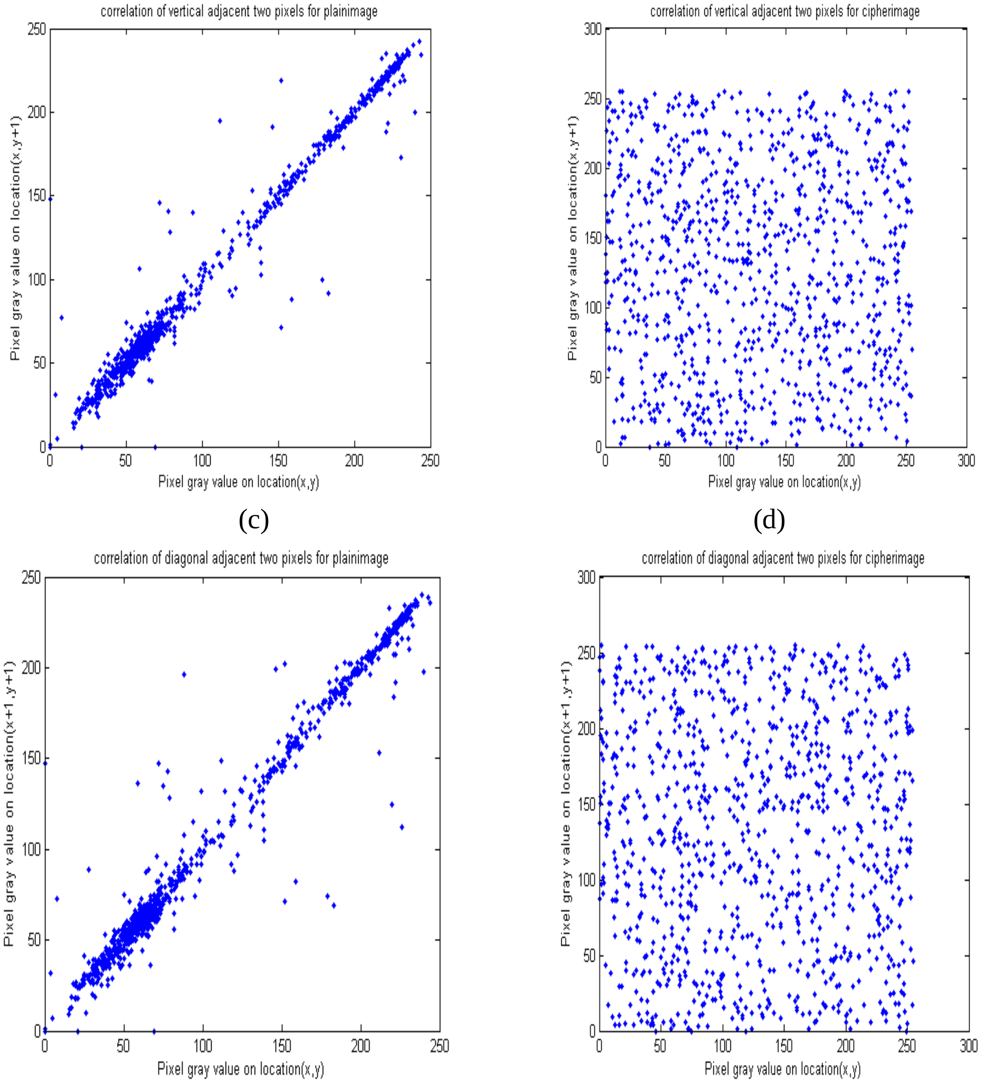
Figure 3. Histogram Analysis of Original and Encrypted Images

Table 1. Correlation Coefficient of Two Adjacent Pixels in Plainimages and Cipherimages on Splash Image of Size 512×512

Test images	Horizontal	Vertical	Diagonal
Original image	0.997325	0.992321	0.991393
Encrypted image	0.002541	0.004150	0.003421



(a) (b)



(c)

(d)

(e)

(f)

Figure 4. Correlations of Two Adjacent Pixels for Splash Image of Size 512×512

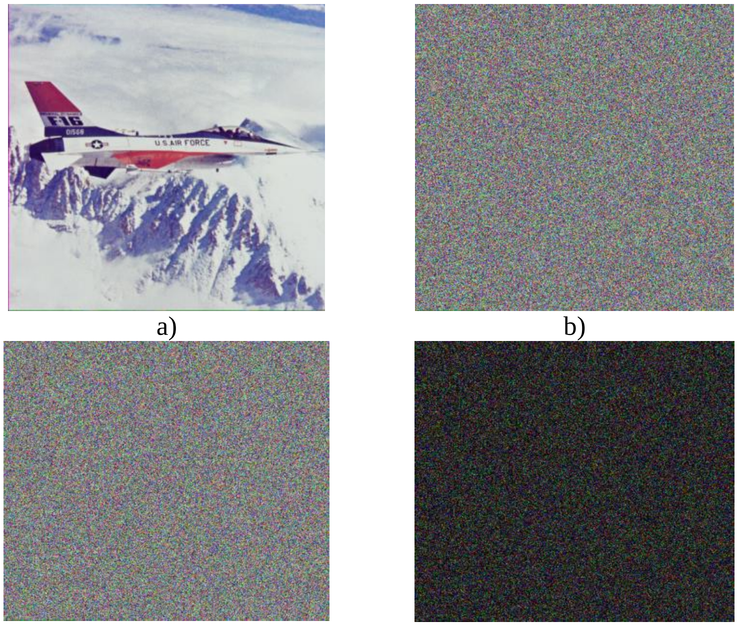
(a) horizontal direction of the plainimage, (b) horizontal direction of the cipher image, (c) vertical direction of the plainimage, (d)vertical direction of the cipher image, (e) diagonal direction of the plainimage, and (f) diagonal direction of the cipher image.

3.3. Security Key Analysis

An efficient image cryptosystem scheme must have large key space to tackle the brute-force attack [17]. In our proposed scheme, a 256-bit key is used, which satisfies the general requirement of resisting the brute-force attack. The cryptosystem has also to be key-sensitive that is an incremental change in key; even of the order of (Δ =) 10^{-10}, result in a completely unrecognizable decrypted image. Figure 6 shows an example of two ciphered images generated from two secret keys, key 1 and key 2, with only character difference. In addition, the average pixel differences of several images, adapted from USC-SIPI Image Database [18], over different random keys are calculated, some of it is tabulated in Table 2. We can see that the values are close to the expected value of pixel difference on two randomly generated images.

Table 2. Pixel Difference between the Encrypted Images when a Slight Change in the Key

Test images	Average NPCR (%)	Average UACI (%)
Jet	99.55	33.43
Splash	99.60	33.44
Lena	99.58	33.38
Sailboat	99.57	33.40



a) b)

c) d)

Figure 5. Results of Key-sensitivity

(a) is the original 'Jet' image, (b) is the encrypted image of (a) with *k1* (c) is the encrypted image of (a) with *k2*, (d) difference image between the two cipher images (Figures 5(b) and 5(c)).

3.4. Information Entropy Analysis

To calculate the entropy *H*(*s*) of a source *s*, we have:

$$H(s) = \sum_{i=0}^{M} P(s_i)\log_2 \frac{1}{P(s_i)} \, bits \tag{5}$$

where M is the total number of symbols $s_i \in s$; $p(s_i)$ represents the probability of occurrence of symbol s_i and log denote the base 2 logarithm so that the entropy is expressed in bits. For a random source emitting 256 symbols, its entropy is $H(s) = 8$ bits. The entropy values for different images and corresponding cipherimages are tested. The average entropy value for different 100 images is $7.9996 \approx 8$. This implies that the information leakage in the proposed encryption process is negligible and the encryption scheme is secure against the entropy-based attack.

3.5. Speed Performance

Apart from security considerations, some other issues for image cryptosystem algorithm are also important. This includes the encryption/decryption speed, particularly for real time Internet multimedia applications. The simulator for the proposed scheme is implemented using Visual C++ compiler on a computer of Dual-Core CPU 2.7 GHz and 1.99 GB of RAM. The operating system used is Windows XP SP2. Each set of the timing tests was executed ten times to improve the accuracy of the timing measurements, and we calculated the average of the times thereby obtained. The results show that the average encryption/decryption speed is 46.532 MB/s for encryption and 46.184 MB/s for decryption.

4. Conclusion

This paper presented a new cryptosystem scheme for secure still visual data based on a spatiotemporal chaotic system. The presented work shows effective confusion and diffusion mechanism based on simple encryption operations such as rotations, integer multiplication, addition, subtraction, the quadratic function, and fixed bit shifting by five bits, which made the encryption more secure with less computation overhead. Moreover, the hybrid compound of chaotic system and cryptographic primitive operations strengthen the encryption performance and enlarge the key space required to resist the brute force attacks. Thorough encryption performance and security analysis ascertains efficacy of the proposed encryption scheme.

Acknowledgments

This work is supported by the Ministry of Scientific Research (Egypt-Tunisia Cooperation Program). Heilongjiang Province Science and Technology research: GZ11A302, and Natural Science Foundation of Heilongjiang Province: QC2014C076.

References

[1] G. Alvarez and S. Li, “Some basic cryptographic requirements for chaos-based cryptosystems”, Int J Bifurcat Chaos, vol. 16, no. 8, **(2006)**, pp. 2129-51.

[2] G. Chen, Y. Mao and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps”, Chaos, Solitions and Fractals, vol. 21, **(2004)**, pp. 749-761.

[3] Y. Mao, G. Chen and S. Lian, “A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps”, Int. J. Bifurcation and Chaos, vol. 14, **(2004)**, pp. 10.

[4] Z-H. Guan, F. Huang and W.Guan, “Chaos based image encryption algorithm”, Phys Lett A, vol. 346, **(2005)**.

[5] T. Gao and Z. Chen, “A new image encryption algorithm based on hyper-chaos”, Physics Letters A, no. 372, **(2008),** pp. 394-400.

[6] A. N. Pisarchik and M. Zanin, “Image encryption with chaotically coupled chaotic maps”, Physica D, no. 237, **(2008),** pp. 2638-2648.

[7] S. Lian, “Efficient image or video encryption based on spatiotemporal chaos system”, Chaos, Solitons & Fractals, no. 40, **(2009),** pp. 2509-2519.

[8] V. Patidar, N. K. Pareek and K. K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps", Communications in Nonlinear Science and Numerical Simulation, no. 14, **(2009),** pp. 3056-3075.

[9] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos", Physics Letters A, no. 372, **(2008),** pp. 5973-5978.

[10] R. Rhouma and S. Belghith, "Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem", Physics Letters A, no. 372, **(2008),** pp. 5790-5794.

[11] R. Rhouma, E. Solak and S. Belghith, Cryptanalysis of a new substitution–diffusion based image cipher", Communications in Nonlinear Science and Numerical Simulation, no. 15, **(2010),** pp. 1887-1892.

[12] H. Hermassi, R. Rhouma and S. Belghith, "Security analysis of image cryptosystems only or partially based on a chaotic permutation", The Journal of Systems & Software **(2012)**.

[13] P. Li, Z. Li, W. A. Halang and G. Chen, "A stream cipher based on a spatiotemporal chaotic system Chaos", Solitons & Fractals, no. 32, **(2007),** pp. 1867-1876.

[14] P. Li, Z. Li, W. A. Halang and G. Chen, "A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map", Physics Letters A, no. 349, **(2006),** pp. 467-473.

[15] Y. Wang, X. Liao, D. Xiao and K.-W. Wong, "One-way hash function construction based on 2D coupled map lattices", Information Sciences, no. 178, **(2008),** pp. 1391-1406.

[16] M. Amin, O. S. Faragallah, A. Ahmed and A. El-Latif, "A Chaotic Block Cipher Algorithm for Image Cryptosystems Communications", In Nonlinear Science and Numerical Simulation, no. 15, **(2010),** pp. 3484-3497.

[17] M. Amin, A. Ahmed and A. El-Latif, "Efficient Modified RC5 Based on Chaos Adapted to Image Encryption", Journal of Electronic Imaging, vol. 19, no. 1, **(2010)**.

[18] L. Li, A. Ahmed, A. El-Latif and X. Niu, "Elliptic Curve ElGamal based Homomorphic Image Encryption Scheme for Sharing Secret Images", Signal Processing, vol. 92, **(2012),** pp. 1069-1078.

[19] "The USC-SIPI Image Database", http://sipi.usc.edu/database/database.php.