Pacific Science Review A: Natural Science and Engineering xxx (2016)

HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Pacific Science Review A: Natural Science and Engineering

journal homepage: www.journals.elsevier.com/pacific-science-review-a-natural-science-and-engineering/

Hyperchaotic dynamical system based image encryption scheme with time-varying delays

Zia Bashir [a], Tabasam Rashid [b,*], Sohail Zafar [b]

[a] Quaid-i-Azam University, Islamabad, Pakistan
[b] University of Management and Technology, Lahore, Pakistan

ARTICLE INFO

Article history:
Received 26 March 2016
Received in revised form
5 November 2016
Accepted 18 November 2016
Available online xxx

Keywords:
Chaotic maps
Chaotic dynamical systems
Dynamic state variables selection mechanism
Pixel-swapping
Time-varying delays

ABSTRACT

In this paper, we propose a 4D chaotic image encryption technique based on a dynamic state variables selection mechanism to improve the effectiveness and security of chaos-based image cryptosystems. Experimental outcomes of our scheme demonstrate better security against many known attacks, as well as high efficiency.

1. Introduction

Conventional encryption schemes are classically intended for the exchange of text-based information. These schemes are not appropriate for image encryption because of various intrinsic properties of images such as redundancy and high pixel correlation. In view of the features of image data, many different image encryption schemes have been considered based on different methodologies; examples include elliptic curve ElGamal [14], *p*-Fibonacci transform [33], greycode [32], SCAN [4], circular random grids [5], quantum [1,2,8,12,27] and chaos [9,10]. Among these schemes, chaos-based image encryption has become an efficient and exceptional encryption method. The main reason for this is that chaotic maps have high initial value sensitivity, chaotic properties and non-convergence.

Chaotic systems/maps in image encryption algorithms can be categorized into two classes: one-dimension (1D) and multi-dimension (MD). 1D chaotic maps have a simple structure and are straightforward to execute [22,24,29,31]. However, they also have three problems, which are outlined below.

- Limited or/and discontinuous range of chaotic behaviours.
- Vulnerability to low computation-cost analysis using iteration and correlation functions.
- Nonuniform data distribution of output chaotic sequences.

Conversely, MD chaotic systems have many applications in image security [3,7,9,11,16] but are not without their own complications related to their difficult structures and multiple parameters, which increase hardware.

A perfect cryptosystem must have two essential properties: confusion and diffusion. Some cryptosystems with properties of substitution and diffusion have been considered in recent years [6,13,15,17,26,30,31]. In [9], Fridrich recommended a substitution-diffusion architecture for chaotic encryption. This architecture became the foundation of various chaos-based image cryptosystems designed in [7,11,28,29,34,35]. The substitution stage changes the location of image pixels but does not modify their values. In the diffusion stage, the pixel values are modified sequentially so that a tiny change in one pixel is spread out to almost all pixels in the whole image. The permutation-diffusion round repeats for a number of times to attain an acceptable level of security.

* Corresponding author.
E-mail addresses: ziabashir@gmail.com (Z. Bashir), tabasam.rashid@gmail.com (T. Rashid), sohailahmad04@gmail.com (S. Zafar).

Peer review under responsibility of Far Eastern Federal University, Kangnam University, Dalian University of Technology, Kokushikan University.

http://dx.doi.org/10.1016/j.psra.2016.11.003

Some chaos-based image encryption algorithms with a permutation-diffusion structure have severe problems [21,25]. The common defects of these algorithms are outlined below.

- Control parameters for permutation are permanent in all permutation-diffusion rounds.
- In the diffusion stage, the key stream extracted from the chaotic orbit only depends on the key (the initial values or parameters of the chaotic map).

Based on the first defect, an attacker could easily divide the permutation-diffusion process into two unrelated stages by using a plain-image with identical pixels. The permutation process has no effect on this kind of image, and the security of these algorithms relies only on the diffusion process. In the diffusion process, the key stream is solely determined by the key. Decrypting the cipher-image is accomplished by computing the key stream. According to the second defect mentioned above, the same key stream is used to encrypt different plain-images if the key remains unchanged. The attacker can obtain the key stream by known-plaintext and chosen-plaintext attacks, i.e., by encrypting some special plaintext sequences and then comparing them with the corresponding ciphertext sequences [20,23]. Therefore, in order to further enhance the security the control parameters used in the permutation stage and the key stream employed for diffusion should be distinct for different rounds and related to the plain-image [3,22]. In [3], Chen et al. suggested a chaos-based image encryption scheme with a dynamic state variables selection mechanism (DSVSM) for the case of a 3D chaotic system. This cryptosystem can assure the security necessities and properly address all the imperfections in the defective mechanism. It is well known that time-varying delays [19] can cause complex dynamics such as periodic or quasi-periodic motion, Hopf bifurcation and higher-dimensional chaos [19].

In this paper, we extended the work of [3]. We propose a dynamic state variables selection mechanism (DSVSM) for a 4D chaotic system and in the diffusion stage we use time-varying delays to improve security. This paper is structured as follows. In Section 2, the dynamic state variable selection mechanism with Lü's hyperchaotic system is described. In Section 3, the proposed image encryption scheme is explained in detail. In Section 4, experimental outcomes, the effectiveness, efficiency and security analysis of the proposed scheme are presented. The study's conclusions are presented in the last section.

2. DSVSM

In this paper, we used Lü's hyperchaotic system for the illustration of a DSVSM, as described by the following system of equations:

$$\begin{cases} \dot{x} = 15(y - x) \\ \dot{y} = -xz + 10y + w \\ \dot{z} = xy - 5z \\ \dot{w} = z - w \end{cases} \quad (1)$$

The starting values x_0, y_0, z_0 and w_0 in system (1) act as the secret key. For each iteration of the hyperchaotic system, we obtain four state variables, denoted as X, Y, Z and W. In a DSVSM, the chaotic state variables that will be utilized for key stream production are chosen according to the earlier processed pixel. The present processing image with $M \times N$ pixels is observed as a one-dimensional array, pixels are symbolized by $P = \{P(0), P(1),\ldots, P(M \times N - 1)\}$ from the higher-left corner to the bottom-right corner. To effectively explain the DSVSM, we provide the following definitions.

1. For every pixel's encryption, the state variable will be chosen from a set of state values X, Y, Z and W. Suppose that $\{X_i,Y_j,Z_k,W_l\}$ is the present set of state variables, where X_i, Y_j, Z_k and W_l are the states of X, Y, Z and W in ith, jth, kth and lth iteration, respectively. Note that, i, j, k and l are not required to be equal to each other and without loss we assume that $i \le j \le k \le l$.
2. Let $P(L)$ represent the present processing pixel, which indicates the state variable sequence $\{X_0, X_1,\ldots, X_{i-1}\}$, $\{Y_0, Y_1,\ldots, Y_{j-1}\}$, $\{Z_0, Z_1,\ldots, Z_{k-1}\}$ and $\{W_0, W_1,\ldots, W_{l-1}\}$ chosen for encrypting the pixels $\{P(0), P(1),\ldots,P(L-1)\}$. Thus, $i + j + k + l = L$.
3. We define $slt(L)$ as the chosen variable from $\{X_i, Y_j, Z_k, W_l\}$, and it will be utilized to create the key stream element for $P(L)$. The choice will be made according to an indicator $index(L)$, defined below:

$$index(L) = P(L-1)\%4.$$

The state values X_i, Y_j, Z_k and W_l will be chosen according to the values of $index(L) = 0, 1, 2, 3$, respectively. For the first pixel, we assign an integer to $P(-1)$ as a starting value.

The actions of the DSVSM are described as follows.

Without loss, we suppose that $index(L) = 0$. In this case, the state value X_i is selected for $P(L)$, and the set of state variables is reorganized as $\{X_{i+1}, Y_j, Z_k, W_l\}$. Likewise, suppose that $index(L+1) = 1$. The state value Y_j is chosen for $P(L+1)$, and the set of state variables transforms to $\{X_{i+1}, Y_{j+1}, Z_k, W_l\}$. Now let $index(L+2) = 2$. The state value Z_k will be chosen for $P(L+2)$ and the set of state variables changes to $\{X_{i+1}, Y_{j+1}, Z_{k+1}, W_l\}$. Now let $index(L+3) = 3$. The state value W_l will be selected for $P(L+3)$. As W_l is the final element of the chaotic state W, Lü's system will iterate one more time to create enough state variables to construct the set of state variables for the consequent encryption. Next, the set of state variables will renew to $\{X_{i+1}, Y_{j+1}, Z_{k+1}, W_{l+1}\}$.

3. Proposed chaotic cryptosystem

This section describes our proposed chaotic encryption scheme which is associated with the plain-image.

3.1. Confusion algorithm

In the confusion stage, first we produce the key stream $k_c(x)$ by using the following formula

$$k_c(x) = mod\left[(abs(slt(x)) - floor(abs(slt(x)))) \times 10^{15}, M \times N - x\right] \quad (2)$$

where $floor(x)$ gives the nearest integers less than or equal to x, $abs(x)$ represents absolute value of x and $mod(x,y)$ is the remainder when y divides x.

The confused image with size of $M \times N$ is viewed as a one-dimensional array, $C = \{C(0), C(1),\ldots, C(M \times N - 1)\}$. In the confusion strategy we perform a nonlinear pixel swapping process. Every pixel of the plain-image will be exchanged with a different one positioned after it. Let x be the position of the current pixel and x' be the location of the corresponding swapping pixel, x' is determined by the formula

$$x' = x + k_c(x) \quad (3)$$

where $k_c(x)$ is the current confusion key stream element. The pixel swapping process will be performed as described by the following equations:

$$C(x) = P(x') = P(x + k_c(x)); \quad (4)$$

Please cite this article in press as: Z. Bashir, et al., Hyperchaotic dynamical system based image encryption scheme with time-varying delays, Pacific Science Review A: Natural Science and Engineering (2016), http://dx.doi.org/10.1016/j.psra.2016.11.003