International Journal of Research in Computer Science
eISSN 2249-8265 Volume 3 Issue 1 (2013) pp. 27- 34
www.ijorcs.org, A Unit of White Globe Publications
doi: 10.7815/ijorcs. 31.2013.058

DESIGN A NEW IMAGE ENCRYPTION USING FUZZY INTEGRAL PERMUTATION WITH COUPLED CHAOTIC MAPS

Yasaman Hashemi

Department of Computer Engineering, Islamic Azad University Varamin-Pishva Branch, IRAN
Email: yasaman.hashemi@iauvaramin.ac.ir

Abstract: *This article introduces a novel image encryption algorithm based on DNA addition combining and coupled two-dimensional piecewise nonlinear chaotic map. This algorithm consists of two parts. In the first part of the algorithm, a DNA sequence matrix is obtained by encoding each color component, and is divided into some equal blocks and then the generated sequence of Sugeno integral fuzzy and the DNA sequence addition operation is used to add these blocks. Next, the DNA sequence matrix from the previous step is decoded and the complement operation to the result of the added matrix is performed by using Sugeno fuzzy integral. In the second part of the algorithm, the three modified color components are encrypted in a coupling fashion in such a way to strengthen the cryptosystem security. It is observed that the histogram, the correlation and avalanche criterion, can satisfy security and performance requirements (Avalanche criterion > 0.49916283). The experimental results obtained for the CVG-UGR image databases reveal the fact that the proposed algorithm is suitable for practical use to protect the security of digital image information over the Internet.*

Keywords: *Fuzzy integral, Chaotic Maps, Image Encryption.*

I. INTRODUCTION

With the rapid development of the networked multimedia, communication and propagation techniques, transmission of a wide range of digital data, from digital images to audio and video files, over the internet or through wireless networks has been increased. One of the major issues considering the digital transmission in this virtual environment is the security of digital images, audio, and video files. Hence, a growing number of researches have been carried out to prevent illegal access to legal data. Encryption is usually one good way to ensure high security. Due to some intrinsic features of image such as bulk data capacity and high correlation among pixels, encryption of images is different from that of texts. Various digital methods have been proposed for image encryption [1-4].

The fundamental ideas for image encryption can be classified into three major types for spatial domain: the value transformation, the position substitution, and their combining form. There already exist several image encryption methods in spatial domain, among which 2D Cellular Automata(CA)-based methods [5, 6], chaos-based methods[7, 8], the tree structure-based methods[9], are most popular.

Cellular automata [5, 6], is applied into encrypting images due to having several strengths. First, large number of CA evolution rules has made many techniques available for producing a sequence of CA data encryption and decrypting images. Second, local interactions have made CA suitable for many physical streams such as those in image processing and data encryption. Third, recursive substitution in CA is computationally simple by the sole use of integer arithmetic and/or logic operations. An image encryption algorithm is recently proposed in [6] using recursive cellular automata substitution. The CA structure in the proposed algorithms allows an infinite number of blocks to be linked together in a chain. There are two potential disadvantages associated with using this chain. First, the entire chain could be garbled by an error anywhere during the transmission, and second, the system security could be weakened by excessive link dilution.

Chaos-based cryptographic scheme [10] is an efficient encryption first presented in 1989. It has many brilliant characteristics different from other algorithms such as the sensitive dependence on initial conditions, non-periodicity, non-convergence and control parameters [11, 12]. The one-dimensional chaos system has the advantages of simplicity and high security [13, 14], and many studies [7, 15-17] were proposed to adopt and improve it. Some of them use high-dimensional dynamical systems [14], other studies use couple maps [18-20]; however, all research is mainly to increase parameters to increase the security. As we know, an ideal image encryption scheme should be sensitive to the secret key and key space should be large enough to make the brute-force attack infeasible [21].

Furthermore, it must have some ability to resist outer attack from statistical analysis. However, too many parameters will influence the implementation and will increase computation; for example, the proposed scheme in [13] uses eight parameters and combines two chaotic maps to shuffle the image pixels . The speed and efficiency will also be low using more than one encryption scheme to an image.

In this paper, we have proposed a novel color image encryption algorithm based on DNA sequence addition combining and coupled two-dimensional piecewise nonlinear chaotic map. The architecture of the algorithm consists of two stages: The permutation stage uses the generated keystream of Sugeno Fuzzy Integral (SFI) to change the position and values of DNA strings. In the diffusion stage, the three components (Red, Green and Blue) of modified image are encrypted in a coupling fashion in such a way to strengthen the cryptosystem security.

The rest of this paper is organized as follows. Section II describes the fuzzy measure and fuzzy integral. In Section III, theory of the DNA sequence operation is explained. The proposed coupled two dimensional piecewise nonlinear chaotic map is discussed in Section IV. In Section V, the proposed encryption and decryption algorithm is introduced. Simulation results and security analysis are provided in Section VI. Finally, the conclusions are drawn in Section VII.

II. FUZZY MEASURE AND FUZZY INTEGRAL

A. Fuzzy Measure

Let $X=\{x_1, x_2,\ldots..,x_n\}$ be a finite set associated with n attributes on information source space, and donate P(X) as the power set X consisting of all subsets of X . A set function [22] $g: P(x)\to[0,1]$ is called a fuzzy measure if the following conditions are satisfied:

1. Boundary conditions: $g(\phi)=0, g(X)=1$;
2. Monotonicity: $g(A)\le g(B)$, if $A\subset B$ and $A,B\in P(X)$;
3. Continuity: $\lim_{i\to\infty} g(A_i)=g(\lim_{i\to\infty} A_i)$, if $\{A_i\}_{i=1}^{\infty}$ is an increasing sequence of measurable sets.

Segeno presented the so-called λ fuzzy measure [22] satisfying the following additional property that for all $A,B\subset X$ with $A\cap B=\phi$:

$$g(A\cup B)=g(A)+g(B)+\lambda g(A)g(B) \quad \lambda>-1 \quad (1)$$

In general, the value of λ can be determined owing to the boundary condition of the g_λ-fuzzy measure. This condition reads as $g(X)=1$, hence, the value of λ can be found by solving the following:

$$\lambda+1=\prod_{i=1}^{n}(1+\lambda g_i) \quad (2)$$

Where $\lambda\in(-1,+\infty), \lambda\neq 0$, and $g_i=g(\{x_i\})$ is the value of the fuzzy density function. Eq. (2) can be calculated by solving the (n-1)th degree polynomial and finding the unique root greater than -1.

Let $A_i=\{x_1,x_2,.....,x_i\}$. The values of $g(A_i)$ by the fuzzy measure over the corresponding subsets of elements can be determined recursively as follows:

$$g(A_1)=g(\{x_1\})=g_1 \quad (3)$$

$$g(A_i)=g_i+g(A_{i-1})+\lambda g_i g(A_{i-1}) \quad 1<i\le n \quad (4)$$

Therefore, in order to obtain λ-fuzzy measure, there are n parameters g_1,g_2,g_3,g_4 needed to be determined in advance.

B. Sugeno Fuzzy Integral

Sugeno fuzzy integral of function h computed over X with respect to a fuzzy measure g is defined in the form:

$$E_g(h)=\max_{i=1}^{n}[\min(h(y_i),g(A_i))] \quad (5)$$

Where $h(x_1)\le h(x_2)\le\ldots\le h(x_n)$, and $h(x_0)=0$. From Eqs. (4) and (5), it is obvious that the calculation of the Sugeno fuzzy integral with respect to λ-fuzzy measure requires the knowledge of the fuzzy density g and the input value h.

III. DNA SEQUENCE DESCRIPTION

In DNA computing, a DNA string is represented by a sequence of four basic nucleotides and is usually described by letters A(Adenine), T(Thymine), G(Guanine), C(Cytosine), where the pairs (A,T) and (G,C) are complementary. In the binary, 0 and 1 are complementary, so 00 and 11 are complementary, 01 and 10 are also complementary. In this paper, we use C, A, T, G to denote 00, 01, 10, 11, respectively. For 8 bit grey images, each pixel can be expressed a DNA sequence whose length is 4. For instance: If the first pixel value of the original image is 220, convert it into a binary stream as [11011100], by using the below DNA encoding rule to encode the stream, we can get a DNA sequence GAGC. Whereas using 00, 01, 10, 11 to denote C, A, T, G, respectively, to decode the above DNA sequence, we can get a binary sequence [11011100].

In recent years, algebraic operations such as the addition operation, based on the DNA sequence have been proposed by researchers [4, 23].For example, 11 + 10 = 01 or G + T=A.

IV. COUPLED 2D PIECEWISE NONLINEAR CHAOTIC MAP

A. Nearest-Neighboring Coupled-Map Lattices

A general nearest-neighboring spatiotemporal chaos system, also called nearest-neighboring coupled-map lattices (NCML) [24], can be described by:

$$z_{n+1}(j) = (1-\varepsilon)f(z_n(j)) + \varepsilon f(z_n(j+1)) \quad (6)$$

Where $n = 1,2,....$, is the time index; $j = 1,2,...,T$ is the lattice state index; f is a chaotic map, and $\varepsilon \in (0,1)$ is a coupling constant. The periodic boundary condition $z_n(j+T) = z_n(j)$ is imposed into this system.

B. Two Dimensional Piecewise Nonlinear Chaotic Map

Two dimensional piecewise nonlinear chaotic map with invariant measure are defined as (see [25, 26], for the detail):

$$\Phi_1(x_n, \alpha) = x_{n+1} = \frac{4\alpha^2 x_n(1-x_n)}{1+4(\alpha^2-1)x_n(1-x_n)} \quad (7)$$

$$\Phi_2(y_n, b_1, b_2) = \begin{cases} y_{n+1} = \dfrac{4b_1^2 y_n(1-y_n)}{1+4(b_1^2-1)y_n(1-y_n)} & x_n \in [0, \frac{1}{2}] \quad (a) \\ y_{n+1} = \dfrac{4b_2^2 y_n(1-y_n)}{1+4(b_2^2-1)y_n(1-y_n)} & x_n \in [\frac{1}{2}, 1] \quad (b) \end{cases} \quad (8)$$

The corresponding invariant measure is (a similar calculation has been presented in [27]):

$$\mu(x,y) = \frac{1}{\pi}\frac{\sqrt{\beta_1}}{\sqrt{x(1-x)}\ (\beta_1 + (1-\beta_1 x))} \times \frac{1}{\pi}\frac{\sqrt{\beta_2}}{\sqrt{y(1-y)}\ (\beta_2 + (1-\beta_2 y))} \quad (9)$$

According to [28], these maps are ergodic in [0, 1].

C. Applying the Coupling Structure to the Two Dimensional Piecewise Nonlinear Chaotic Maps

In the proposed algorithm, we apply the coupling structure to the two dimensional piecewise nonlinear chaotic maps as follows:

$$x_{n+1}(j) = (1-\varepsilon)\Phi_1(x_n(j), \alpha_j) + \varepsilon\Phi_1(x_n(j+1), \alpha_j) \quad (10)$$

$$y_{n+1}(j) = (1-\varepsilon)\Phi_2(y_n(j), b_1^j, b_2^j) + \varepsilon\Phi_2(y_n(j+1), b_1^j, b_2^j) \quad (11)$$

$$n = 1, 2, 3, ..., L; \quad j = 1, 2, ..., T$$

Where ε, α, b_1 and b_2 are the system parameters; $x_0(j)$ and $y_0(j)$ are the initial conditions of the coupled two dimensional piecewise nonlinear chaotic maps. In order to have good chaotic properties, T and ε are chosen as 3 and 0.02 respectively [29, 30].

V. THE PROPOSED CRYPTOSYSTEM

A. Generation of the initial conditions and parameters

The proposed image encryption process utilizes a 256 bit-long external secret key (K) in permutation and diffusion stages. This key is divided into 8-bit blocks (ki) referred to as session keys. The 256-bit external secret-key (K) is given by:

$$K = k_1, k_2, k_3, ..., k_{32} \quad (12)$$

Based on the analysis presented in section II, there are four initial inputs of fuzzy integrals and four membership grades for generating pseudo-random number by the SFI.

For the image of size - $W \times H$, the initial inputs h_1, h_2, h_3, h_4 are derived as follows, respectively:

$$h_m = (((k_{((m-1)\times 8)+1} \oplus .... \oplus k_{((m-1)\times 8)+8}) + \sum_{i=1}^{i=32}(k_i)) \bmod W) / W \quad (13)$$

Where the values h_1, h_2, h_3, h_4 must be rearranged in increasing order [31] and then using these values, this scheme generates four membership grades. These membership grades can be determined in many different ways. Here, we follow the method introduced in [32], namely:

$$g_m = \frac{1}{1+h_m} \quad m=1, 2, 3,4 \quad (14)$$

In diffusion stage, the initial conditions and the parameters (α, b_1, b_2) of the coupled chaotic map are derived as follows:

$$x_0(j) = (((k_{(i-1)\times 4+1} \oplus .... \oplus k_{(i-1)\times 4+4}) + \sum_{i=1}^{i=32}(k_i)) / W) \bmod 1 \quad (15)$$

$$y_0(j) = (((k_{(i+2)\times 4+1} \oplus .... \oplus k_{(i+2)\times 4+4}) + \sum_{i=1}^{i=32}(k_i)) / W) \bmod 1 \quad (16)$$

$$b_{m=1,2} = (((k_{(m-1)\times 4+25} \oplus ... \oplus k_{(m-1)\times 4+28}) + \sum_{i=1}^{i=32}(k_i)) / W) \bmod 1 \quad (17)$$

$$\alpha = (y_0(1) + x_0(2) + y_0(2) + x_0(3) + y_0(3) + b_1 + b_2) \bmod 1 \quad (18)$$

B. Design of the Encryption Algorithm

According to Fig. 1, the proposed encryption algorithm can be divided into the following steps:

Step 1. First of all, convert the image of size $W \times H$ into its RGB components, next, transform each component into binary matrix, and then carry out DNA encoding for the binary matrix according to Section III, to obtain encoding matrices DNAR, DNAG and DNAB. The size of the DNAR, DNAG and DNAB is $(W \times (H \times 4))$.

Step 2. Divide each of matrices DNAR, DNAG and DNAB into blocks $DNA_R(i,j)$, $DNA_G(i,j)$, $DNA_B(i,j)$, $i = 1,2,.....,W$ $j = 1,2,....,H$, where the size of blocks is 1×4.

Step 3. Apply external secret key and produce the initial inputs h_1, h_2, h_3, h_4 and the membership grades g_1, g_2, g_3, g_4 according to section V, then, generate sequences $X_n(i), Y_n(j), M(i,1), N(1,j)$, $n = 1,2,3,4$.

Step 4. Use the new initial data to iterate SFI once using Eqs. (4) and (5):

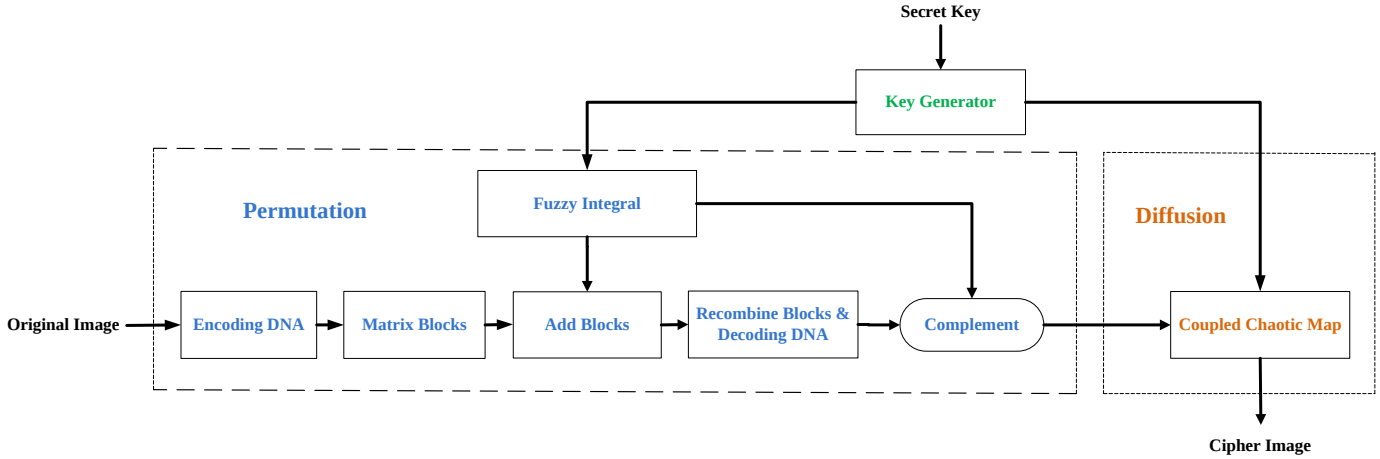

Fig. 1. Architecture of permutation–diffusion type of proposed image cryptosystem

$$M(i,1) = E_i \bmod 1 \quad (19)$$

$$X_{m=1,...,4}(i) = (ARS(Int((E_i \bmod 1) \times 10^{14}),\ (m-1) \times 4)) \bmod W \quad (20)$$

Remark: $ARS(y,x)$ performs the x-bit right-arithmetic-shift operation on the binary sequence y.

Step 5. Update h_1, h_2, h_3, h_4 as follow:

$$h_m = X_m(i) / W, \qquad m = 1,2,3,4 \quad (21)$$

Remark: The values of h_n must be rearranged in increasing order[31].

Step 6. Set $i = i+1$, If $i \le W$, go to step 4, otherwise, Set j=1, and continue the process from step Step 7.

Step 7. Use the new initial data to iterate SFI once using Eqs. (4) and (5):

$$M(1,j) = E_j \bmod 1 \quad (22)$$

$$Y_{m=1,2,3,4}(j) = (ARS(Int((E_j \bmod 1) \times 10^{14}),\ (m-1) \times 4)) \bmod W \quad (23)$$

Step 8. Update h_1, h_2, h_3, h_4 as follow:

$$h_m = Y_m(j) / W, \qquad m = 1,2,3,4 \quad (24)$$

Step 9. Set $j=j+1$, If $j<=H$, go to step 7, otherwise, continue the process from step 10.

Step 10. Sorting X_n and Y_n in descending order, we get two new sequences X'_n and Y'_n.

Step 11. Let the location value of sequences X'_n, Y'_n be row coordinates and column coordinates of $DNA_R(i,j)$, $DNA_G(i,j)$, $DNA_B(i,j)$, in other words, it can be expressed as $DNA_R(x'_p, y'_q)$, $DNA_G(x'_p, y'_q)$, $DNA_B(x'_p, y'_q)$.

Step 12. Add $DNA_R(i,j)$ and $DNA_R(x'_p, y'_q)$, $DNA_G(i,j)$ and $DNA_G(x'_p, y'_q)$, $DNA_B(i,j)$ and $DNA_B(x'_p, y'_q)$, according to the rules in Section III, obtaining the result as blocks BR, BG and BB, respectively.

Step 13. Carry out the inverse process of the step 1 for the decoding matrices BR, BG and BB, we will obtain a real value matrices PR, PG and PB.

Step 14. Two sequences $M_{(W \times 1)}$ and $N_{(1 \times H)}$ are produced by SFI, Performing the multiply operation for $M_{(W \times 1)}$ and $N_{(1 \times H)}$, we obtain the matrix Z whose size is $W \times H$ .Use the following threshold function $f(x)$ to get a binary matrix:

$$f(x)=\begin{cases}0 & ,0<Z(i,j)\le 0.5\\ 1 & ,0.5<Z(i,j)\le 1\end{cases} \quad (25)$$

If $Z(i,j)=1, P_R$, P_G and P_B is complemented, otherwise it is unchanged. After the complementing operation, we get matrices P'_R, P'_G, and P'_B.

Step 15. Matrices P'_R, P'_G, and P'_B are transformed into matrices $R_{(W\times H)\times 1}, G_{(W\times H)\times 1}$ and $B_{(W\times H)\times 1}$, respectively.

Step 16. Set $i=1$, F= false, Bitxor1= 0, Bitxor2= 0, Bitxor3= 0, C0(1)= 0, C0(2)= 0 and C0(3)= 0. Apply external secret key and generate the initial conditions $x_0(1), y_0(1), x_0(2), y_0(2), x_0(3), y_0(3)$ and the parameters α, b_1 and b_2 according to section IV.

Step 17. Step 17: Use the new initial conditions to iterate coupled two dimensional piecewise nonlinear chaotic maps once.

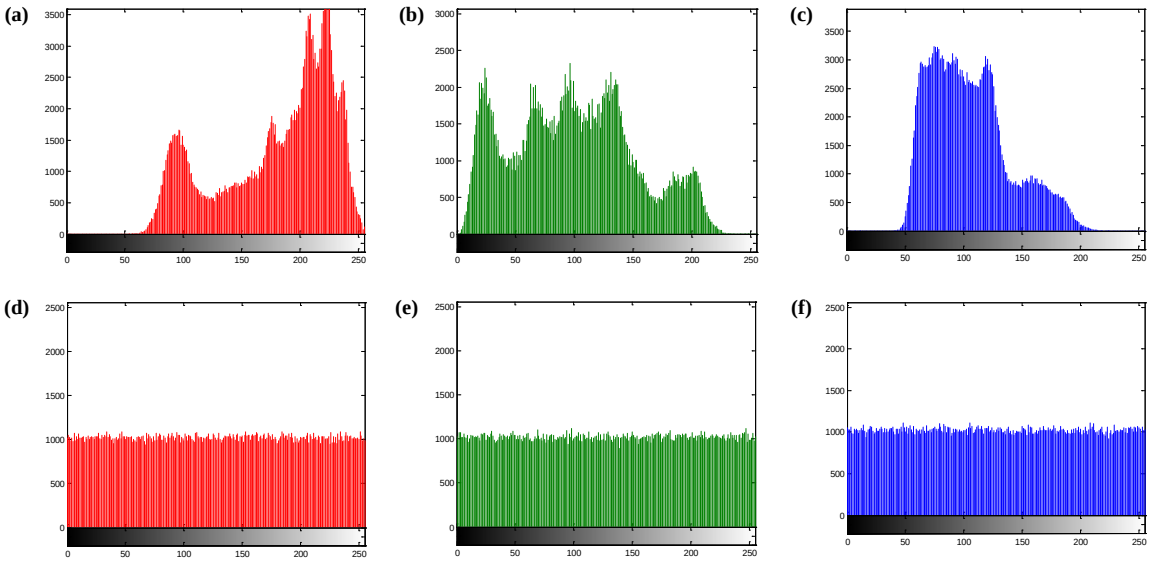

Figure 2: *Histogram of the original image of Lena in the (a) red (b) green (c) blue, components, Histogram of the encrypted image of Lena in the (d) red (e) green (f) blue, components.*

Step 18. In this step, $R_i, R_{i+1}, G_i, G_{i+1}, B_i$ and B_{i+1} are encrypted and the results are stored in the matrices $C_i(1), C_{i+1}(1), C_i(2), C_{i+1}(2), C_i(3)$ and $C_{i+1}(3)$ using equations (11) and (12).

Step 19.

$$C_i(1)=(R_i+\text{int}(x_i(1)\times L)+C_{i-1}(1)+\text{SBox}(\text{Bitxor}_1))\bmod 256 \quad (26)$$

$$C_{i+1}(1)=(R_{i+1}+\text{int}(y_i(1)\times L)+C_i(1)+\text{SBox}(\text{Bitxor}_1))\bmod 256 \quad (27)$$

$$C_i(2)=(G_i+\text{int}(x_i(2)\times L)+C_{i-1}(2)+\text{SBox}(\text{Bitxor}_2))\bmod 256 \quad (28)$$

$$C_{i+1}(2)=(G_{i+1}+\text{int}(y_i(2)\times L)+C_i(2)+\text{SBox}(\text{Bitxor}_2))\bmod 256 \quad (29)$$

$$C_i(3)=(B_i+\text{int}(x_i(3)\times L)+C_{i-1}(3)+\text{SBox}(\text{Bitxor}_3))\bmod 256 \quad (30)$$

$$C_{i+1}(3)=(B_{i+1}+\text{int}(y_i(3)\times L)+C_i(3)+\text{SBox}(\text{Bitxor}_3))\bmod 256 \quad (31)$$

Remark: SBox performs nonlinear transform S-box [33] on variable a.

Step 20. Update $\alpha, b_1, b_2, \text{Bitxor}_1, \text{Bitxor}_2, \text{Bitxor}_3$ and b_2 as follow:

$$\alpha^{new}=(x_i(1)+y_i(1)+\alpha^{old})\bmod 1 \quad (32)$$

$$b_1^{new}=(x_i(2)+y_i(2)+b_1^{old})\bmod 1 \quad (33)$$

$$b_2^{new}=(x_i(3)+y_i(3)+b_2^{old})\bmod 1 \quad (34)$$

$$\text{Bitxor}_{m=1,2,3}=C_m(r)\oplus C_{m+1}(r) \quad (35)$$

Step 21. Set $i=i+2$. Go to step (17) until the elements in the $R_{(W\times H)\times 1}, G_{(W\times H)\times 1}$ and $B_{(W\times H)\times 1}$ exhaust.

Step 22. If value of the variable F=false, it is set equal to true and the operation will start from step 23, otherwise, the process will be continued from step 24.

Step 23. Set $R_{(W\times H)\times 1}, G_{(W\times H)\times 1}, B_{(W\times H)\times 1}$ equal to reverse of matrices $C(1), C(2)$ and $C(3)$ respectively ,next set C0(1)=0, C0(2)=0 and C0(3)=0, Bitxor1= 0, Bitxor2= 0, Bitxor3= 0, and jump to step 17.

Step 24. Transform the elements of the matrices $C_{(W\times H)\times 1}(1), C_{(W\times H)\times 1}(2), C_{(W\times H)\times 1}(3)$ into $C_{W\times H}(1), C_{W\times H}(2), C_{W\times H}(3)$ and output them as color cipher image.

It is obvious that the generation of the keystreams depends on the keys of cryptosystem, the length of the plaintext (L), the width of color image (W) and the plaintext through all the color components (R, G, and B). Besides, since coupled two-dimensional piecewise nonlinear chaotic map has coupling and nonlinear structure, the stream cipher of color components depend on each other. These features will in turn, strengthen the security of cryptosystem. By employing this method, we can strongly claim that our proposed algorithm does not suffer from the cryptosystem weaknesses.

C. Design of the Decryption Algorithm

The decryption procedure is similar to that of the encryption process except that some steps are followed in a reversed order. Therefore, some remarks should be considered in the decryption process as follows:

Remark1: Since the decryption process requires the same keystreams as for decryption of the color image, the same secret key $K = k_1, k_2, k_3, ..., k_{32}$ should be used for decryption. Hence, According to section V, it is possible to set the same initial conditions for SFI and coupled two dimensional piecewise nonlinear chaotic maps.

Remark2: We can rewrite encryption equations to give the pixels' values as follows:

$$R_i = (C_i(1) - \text{int}(x_i(1) \times L) - C_{i-1}(1) - \text{SBox}(\text{Bitxor1})) \bmod 256 \quad (36)$$

$$G_i = (C_i(2) - \text{int}(x_i(2) \times L) - C_{i-1}(2) - \text{SBox}(\text{Bitxor2})) \bmod 256 \quad (37)$$

$$B_i = (C_i(3) - \text{int}(x_i(3) \times L) - C_{i-1}(3) - \text{SBox}(\text{Bitxor3})) \bmod 256 \quad (38)$$

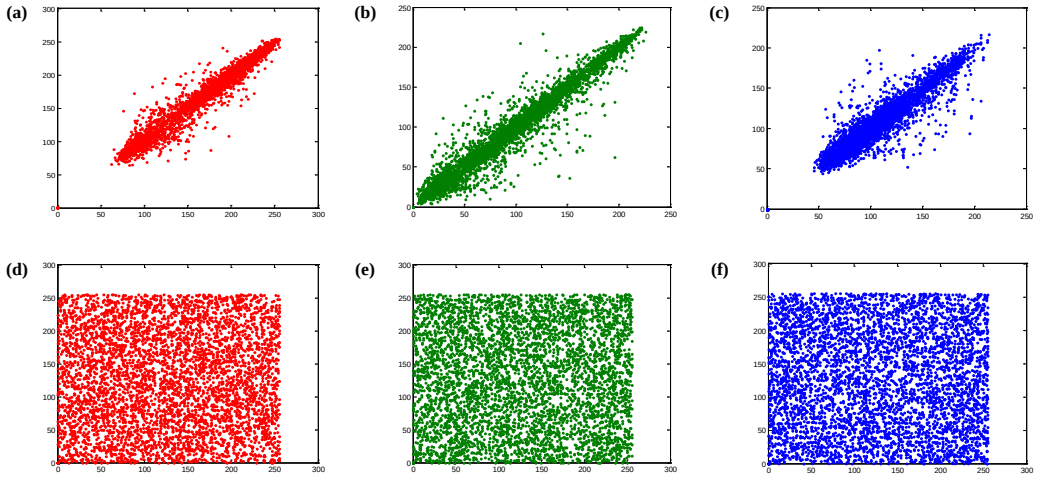

Figure 3: Correlation analysis of two horizontally adjacent pixels: Frames (a), (b) and (c), respectively, show the distribution of two horizontally adjacent pixels in the plain image of Lena in the (a) red (b) green (c) blue, components. Frames (d), (e) and (f) , respectively, show the distribution of two horizontally adjacent pixels in the encrypted image of Lena in the (a) red (b) green (c) blue , components ;obtained using the proposed scheme.

VI. SECURITY ANALYSIS FOR THE PROPOSED ALGORITHM

A. Histogram

Image histogram is a very important feature in image analysis. From Fig. 2, it is obvious that the histograms of the encrypted image are nearly uniform and significantly different from the histograms of the original image. Hence, it does not provide any clue to employ any statistical analysis attack on the encrypted image.

B. Correlation Analysis of Two Adjacent Pixels

We have analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in an image. 5000 pairs of two adjacent (in vertical, horizontal, and diagonal direction) pixels from plain-image and ciphered image were randomly selected and the correlation coefficients were calculated.

Fig. 3 is the horizontal relevance of adjacent elements in image before and after encryption. Fig. 3 shows significant reduction in relevance of adjacent elements.

C. Avalanche Criterion

As we know the change of one bit in the plaintext should result in theoretically 50% difference in the cipher's bits. Hence, for proving the so called sensitivity to plaintext, two plain images are generated with just one-pixel difference. The bits change rate of the cipher obtained by proposed algorithm is 49.916283%. Hence, the avalanche criterion of is very close to the ideal value of 50%. The results of the tests comparing the avalanche criterion of the proposed algorithm and other encryption algorithms are shown in Table I.

Table 1: Avalanche Test

Algorithm	**Avalanche criterion**
Proposed	0.49916283
Ref.[19]	0.49820101
Ref. [20]	0.00000095

VII. CONCLUSION

A novel algorithm based on DNA addition combining and coupled two-dimensional piecewise nonlinear chaotic map has been proposed for the permutation–diffusion architecture. The proposed algorithm combines good permutation and diffusion properties which can be applied to the encryption of color images. Combination of image pixels in permutation stage based on the generated keystreams by Sugeno fuzzy integral is performed. Meanwhile, the keystreams used in the diffusion stage is extracted from a two-dimensional piecewise nonlinear chaotic map.

The generation of the keystreams depends on the keys of cryptosystem, the length of the plaintext (L), the width of color image and the plaintext through all the color components (R, G, and B). Besides, since coupled two-dimensional piecewise nonlinear chaotic map has coupling and nonlinear structure, the stream cipher of color components depend on each other. These features will in turn, strengthen the security of cryptosystem. By employing this method, we can strongly claim that our proposed algorithm does not suffer from the cryptosystem weaknesses.

Simulation results demonstrate that satisfactory performance is achievable in our proposed algorithm. Hence, based on the achieved results, we have come to a conclusion that the new image encryption algorithm with speed and high security can be useful for the real-time secure image and video communication applications.

VIII. REFERENCES

[1] Xiaofeng Liao, Shiyue Lai, Qing Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission," Signal Processing, vol 90, issue 9, pp. 2714-2722, 2010. doi: 10.1016/j.sigpro.2010.03.022

[2] X. Tong, M. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator," Signal Processing, vol. 89, issue 4, 480-91, 2009. doi: 10.1016/j.sigpro.2008.09.011

[3] Guanrong Chen, Yaobin Mao, Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons & Fractals, vol 21, issue 3, pp. 749-761, 2004. doi: 10.1016/j.chaos.2003.12.022

[4] Q. Zhang, Ling Guo, Xianglian Xue, Xiaopeng Wei, "An image encryption algorithm based on DNA sequence addition operation," The Fourth International Conference on Bio-Inspired Computing (BIC-TA '09), pp. 1-5, 2009. doi: 10.1109/BICTA.2009.5338151

[5] O. Lafe, "Data compression and encryption using cellular automata transform," Engineering Applications of Artificial Intelligence, vol 10, issue 6, pp. 581–591, 1997. doi: 10.1016/S0952-1976(97)00040-7

[6] Rong-Jian Chen, Jui-Lin Lai, "Image security system using recursive cellular automata substitution," Pattern Recognition, vol 40, issue 5, pp. 1621-1631, 2007. doi: 10.1016/j.patcog.2006.11.011

[7] Shiguo Lian, Jinsheng Sun, Zhiquan Wang, "A block cipher based on a suitable use of the chaotic standard map," Chaos, Solitons & Fractals, vol 26, issue 1, pp. 117-129, 2005. doi: 10.1016/j.chaos.2004.11.096

[8] H.S. Kwok, Wallace K.S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," Chaos, Solitons & Fractals, vol 32, issue 4, pp. 1518-1529, 2007. doi: 10.1016/j.chaos.2005.11.090.

[9] H. Cheng, Xiaobo Li, "Partial encryption of compressed images and videos," IEEE Transactions on Signal Processive, vol 48, no. 8, pp. 2439-2451, 2000. doi: 10.1109/78.852023

[10] Robert Matthews, "One the derivation of a chaotic encryption algorithm," Cryptologia, vol 13, issue 1, pp. 29-42, 1989. doi: 10.1080/0161-118991863745

[11] M. S. Baptista, "Cryptography with chaos," Physics Letters A, vol 240, issues 1-2, pp. 50-54, 1998. doi: 10.1016/S0375-9601(98)00086-3

[12] Kuo-Liang Chung, Lung-Chun Chang, "Large encrypting binary images with higher security," Pattern Recognition Letters, vol 19, issue 5-6, pp. 461-468, 1998. doi: 10.1016/S0167-8655(98)00017-8

[13] Tiegang Gao, Zengqiang Chen, "Image encryption based on a new total shuffling algorithm," Chaos, Solitons & Fractals, vol 38, issue 1, pp. 213-220, 2008. doi: 10.1016/j.chaos.2006.11.009

[14] Fuyan Sun, Shutang Liu, Zhongqin Li, Zongwang Lü, "A novel image encryption scheme based on spatial chaos map," Chaos, Solitons & Fractals, vol 38, issue 3, pp. 631-640, 2008. doi: 10.1016/j.chaos.2008.01.028

[15] Linhua Zhang, Xiaofeng Liao, Xuebing Wang, "An image encryption approach based on chaotic maps," Chaos, Solitons & Fractals, 24, pp. 759-765, 2005. doi: 10.1016/j.chaos.2004.09.035

[16] Kwok-Wo Wong, Bernie Sin-Hung Kwok, Wing-Shing Law, "A fast image encryption scheme based on chaotic standard map," Physics Letters A, 372(15), pp. 2645-2652, 2008.

[17] Z.-H. Guan, F. Huang, W. Guan, "Chaos-based image encryption algorithm," Physics Letters A, 346, pp. 153-157, 2005.

[18] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos, Solitons & Fractals, vol 35, issue 2, 408-419, 2008. doi: 10.1016/j.chaos. 2006.05.011

[19] Sahar Mazloom, Amir Masud Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," Chaos Solitons and Fractals, vol 42, issue 3, pp. 1745-1754, 2009. doi: 10.1016/j.chaos.2009.03.084

[20] Shubo Liu, Jing Sun, Zhengquan Xu, "An improved image encryption algorithm based on chaotic system," Journal of Computers, vol 4, no. 11, pp. 1091-1100, 2009. doi: 10.4304/jcp.4.11.1091-1100

[21] B. Schneier, "Applied Cryptographic: Protocols, Algorithms, and Source Code in C," Second Edition, New York: Wiley, 1995.

[22] M. Sugeno, "Fuzzy measures and fuzzy integrals—A survey," Fuzzy automata and decision processes, pp. 89-102, Amsterdam, 1977.

[23] Wasiewicz P., Mulawka J.J., Rudnicki W.R., Lesyng, B., "Adding numbers with DNA," International Conference on Systems, Man, and Cybernetics, vol. 1, pp 265-270, 2000. doi: 10.1109/ICSMC.2000.885000

[24] Kunihiko Kaneko, " Pattern dynamics in spatiotemporal chaos: Pattern selection, diffusion of defect and pattern competition intermittency," Physica D: Nonlinear Phenomena, vol 34, issue 2, pp. 1–41, 1989. doi: 10.1016/0167-2789(89)90227-3

[25] A. Akhshani, S. Behnia, A. Akhavan, M.A. Jafarizadeh, H. Abu Hassan, Z. Hassan, "Hash function based on hierarchy of 2D piecewise nonlinear chaotic maps," Chaos, Solitons & Fractals, vol 42, issue 4, pp. 2405-2412, 2009. doi: 10.1016/j.chaos.2009.03.153

[26] A. Akhshani, S. Behnia, A. Akhavan, H. Abu Hassan, Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps," Optics Communications, vol 283, issue 17, pp. 3259-3266, 2010. doi: 10.1016/j.optcom.2010.04.056

[27] M. A. Jafarizadeh, S. Behnia, "Hierarchy of chaotic maps with an invariant and their coupling," Physica D : Nonlinear Phenomena, vol 159, issues 1-2, pp. 1–21, 2001. doi: 10.1016/S0167-2789(01)00325-6

[28] M. A. Jafarizadeh, S. Behnia, S. Khorram, H. Nagshara, "Hierarchy of chaotic maps with an invariant measure," Journal Statistical Physics, vol 104, issue 5-6, pp. 1013–28, 2001. doi: 10.1023/A:1010449627146

[29] Mingzhou Ding, Weiming Yang, "Stability of synchronous chaos and on–off intermittency in coupled map lattices," Physical Review E, vol 56, issue 4, pp. 4009–16, 1997. doi: 10.1103/PhysRevE.56.4009

[30] Yong Wang, Xiaofeng Liao, Di Xiao, Kwok-Wo Wong, "One-way hash function construction based on 2D coupled map lattices," Information Sciences, vol 178, issue 5, pp. 1391-1406, 2008. doi: 10.1016/j.ins.2007.10.008

[31] J.-H. Chiang, "Aggregating membership values by a Choquet-fuzzy-integral based operator," Fuzzy Sets and Systems, vol 114, issue 3, pp. 367-375, 2000. doi: 10.1016/S0165-0114(98)00145-6

[32] Swarup Medasani, Jaeseok Kim, Raghu Krishnapuram, "An overview of membership function generation techniques for pattern recognition," International Journal of Approximate Reasoning, vol 19, issue 3-4, pp. 391–417, 1999. doi: 10.1016/S0888-613X(98)10017-8

[33] "Announcing the advanced encryption standard (AES)," ed: Federal Information Processing Standards Publication, 2001.

How to cite

Yasaman Hashemi, " Design a New Image Encryption using Fuzzy Integral Permutation with Coupled Chaotic Maps". *International Journal of Research in Computer Science*, 3 (1): pp. 27-34, January 2013. doi: 10.7815/ijorcs. 31.2013.058