IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018(CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

Image Encryption Using Chaos Theory

Krishna Yadav[1] , Dipesh Chawda[2] , Arti Prajapati[3]

Electronics & Telecommunication, Thakur College of Engineering & Technology, Mumbai, India[1,2,3]

Abstract:Encryption basically follow two different approaches, the first being encrypting the images through encryption algorithms using keys, the other approach involves dividing the image into random shares to maintain the images secrecy**.** Chaotic encryption of images is the better approach for cryptography**.** The chaotic encryption algorithms have several advantages over the traditional encryption algorithms like high security, speed, sensible computational overheads and computational power**.** The Chaos theory that aims to disadvantage of existing algorithm In recent years, a large type of cryptanalytic algorithms supported chaos are argue and most of them are verified to achieve success by adopting the normal permutation-diffusion design**.** However, one downside these strategies largely hold is that they need very little reference to the plaintext or, to be precise, the link between them is quite less**.** The downside makes the encoding algorithms prone to the known-plaintext and chosen-plaintext attack**.** In addition, the secret keys are unit stationary at the most times, and that they can't be elite dynamically by the corresponding plain image pixels**.** So as to beat these disadvantages mentioned higher than, we have a tendency to introduce a new chaos-based image encoding rule with dynamic key choice mechanisms**.** During this we have a tendency to gift a dynamic keystream sequence cluster choice mechanism **(**DKSGSM**)** and a dynamic keystream choice mechanism **(**DKSM**).** They powerfully enhance the connection between the plaintext and also the encryption scheme**.** Especially, the DKSGSM and DKSM expand the choice vary of the keys and permit us to pick out the keys dynamically by the corresponding plaintext pixels**.** What's a lot of, by adopting the bidirectional encryption, we are able to unfold the influence to the complete image once a little modification in plain image and this could greatly increase the protection level of our encryption technique**.**

KEYWORDS: Dynamic keystream sequence group selection mechanism(DKSGSM),Dynamic keystream selection mechanism(DKSM),ImageEncryption,Chaos,Permutatio, Diffusion.

I. INTRODUCTION

Nowadays, in conjunction with the dramatic development of intelligent devices, web of things (IOT) and high definition (HD) multimedia system, the transmission of most of knowledge in our life, like document, audio, video, particularly image info seriously rely on the network. On the one hand, the pc has brought convenience to our way of life, however, on the opposite hand, the network will be used by the criminals to get the lead, leading to potential risk to people's privacy extraordinarily. So the issue of whether the data is safe in transmission has aroused wide concern in the public. Generally speaking, digital image is characterized with some intrinsic features such as bulk data, high pixel correlation and redundancy. The commonly used encryption methods, such as DES, AES, Blowfish and other algorithms are mainly designed for the textual information rather than the digital image information. Chaotic system is a nonlinear system, having the complex pseudo randomness and outstanding confusion rules. It is very sensitive to the initial conditions and management parameters, therefore any little initial deviation are exponential amplified. At identical time, it is determined by scheme equation, system parameters and initial conditions. Owing to the characteristics of chaotic system with uncertainty, randomness, randomness and extremely sensitivity of initial values, a series of fantastic coding algorithms supported chaotic systems are projected. Indeed, these new ways mentioned higher than strengthen the connection between the secret writing methodology and therefore the plaintext and improve the safety level, however, some issues area unit still unresolved: (1) In some algorithms, the swapped positions of the permutation stage lack of the reference to the plain image. Though elements of them take into account the connection with the plaintext, it still cannot unfold the secret writing impact to the complete image once one element is modified. And at it slow, the dynamical vary is merely restricted to the following elements of the modified picture element. (2) Whether or not within the scrambling stage or within the diffusion stage, as long because the initial values and management parameters square measure a similar, the encoding secret's additionally a similar. The key couldn't be chosen dynamically by the plain image. And this makes the cryptography ways ineffective to known-plaintext and chosen-plaintext attack. (3) Most of algorithms tend to require the low dimensional chaotic systems to code the image, however, tiny key house and weak resistance to the brute force cannot make sure the security of cryptography. In addition, an excellent deal of chaotic encoding ways employs quite one chaotic system to come up with the key streams, what's additional, the chaotic state variables generated with high computation quality aren't used sufficiently and these cause the wasting of system resources and time. supported the on top of analyses, during this paper, we have

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018(CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

a tendency to introduce a brand new chaos-based image encoding rule with dynamic key choice mechanisms. This new algorithmic rule will satisfy the protection needs we have a tendency too expected and well overcome the failings existing in most cracked algorithms by up them in three elements. Firstly, we have a tendency to use the hyperchaotic system to get the key streams, therefore it not solely overcomes the flaw of low dimensional chaotic system mentioned however conjointly improves the key space greatly. Secondly, so as to beat the failings we tend to adopt constant hyperchaotic system instead of two or more chaotic systems to get secret keys, downgrading the quality of hardware implementation. What's a lot of, we tend to gift a dynamic keystream sequence cluster choice mechanism (DKSGSM) and a dynamic keystream choice mechanism (DKSM), so the rule incorporates a robust reference to the plaintext pixel and therefore the key may be chosen dynamically by DKSGSM and DKSM, and these improve the use of chaotic state variables and enhance the flexibility of the strategy to resist the known-plaintext and chosen-plaintext attack. Lastly, so as to beat the limitation of traditional scrambling encoding methodology, we tend to adopt the twoway encoding, namely, forward encoding and backward encoding. Within the forward encoding stage, it contains the forward confusion and forward diffusion whereas within the backward encoding stage, it's created of backward confusion and backward diffusion. The forward cryptography operates the constituent from the primary one to the last one whereas the backward cryptography is beginning with the last one and ending with the primary one. The yank scholar Fridrich hints the classical image cryptography schemes in 1998 . This design consists of two stages, alleged the permutation and diffusion. In the permutation stage, we modify the placement of every picture element within the original image to destroy the special distribution and native correlation, creating the image unable to be knownwithin the second stage, the plain image picture element is cloaked consecutive by the pseudo random sequence that is generated by the chaotic system to switch the picture element price. Most of chaos-based ways eventually reach satisfactory results per the 2 stages, like novel pixel-level scrambling approaches [2,3,4], bit-level confusion ways [5,6,7], increased diffusion schemes [8], improved key stream generator ways [9]. However, we have a tendency to should notice that typically encrypting a picture solely with the chaotic systems cannot guarantee the enough security, particularly adopting the low dimensional chaotic systems. Most of algorithms are evidenced insecure [10, 11, 12, 13]. The analysis found that one in every of the foremost deadly reasons is that the cryptography method has very little reference to the plaintext. Zhang et al. [13] conferred a completely unique image cryptography technique mistreatment permutation-diffusion design and skew tent chaotic map, Eslami et al. [11] gave Associate in Nursing improved technique supported referee. [13], and recently Akhavan et al. [10] cryptanalyzed this improved algorithmic program mistreatment differential attack and located it absolutely was not sensitive enough to the plain image. The disadvantage makes the cryptography algorithms susceptible to the known-plaintext and chosen-plaintext attack. Recently, a series of algorithms looking on plaintext are conferred [14, 15, 16]. In Ref. [15], Ye et al. presented a block chaotic image secret writing technique with a self-adaptive model. By introducing a blunder idea, the initial values are often combined with the plaintext in each spherical. In Ref. [14], Chen et al. incontestable a nonlinear scrambling approach and a dynamic state variable choice mechanism, and each secret key employed in permutation and diffusion stages are often determined dynamically by the corresponding plaintext constituent. In Ref. [16], Zhang et al. put forward a brand new secret writing theme with a temp-value feedback AND an expand XOR operation. The keys used were generated from the supplying map whereas the initial values were calculated by the plain image.

II. OBJECTIVE

Objective of this project is to securing the communication method whereas transmission or delivering the information. Also the aim of this technique is to produce the replacement for existing formula that area unit less Secured as compared to current method that we tend to area unit approaching during this project. This can even be used as replacement for wellliked formula like DES, AES, RSA, BLOWFISHBlock digram of the proposed system

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018(CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

III.FLOW DIAGRAM

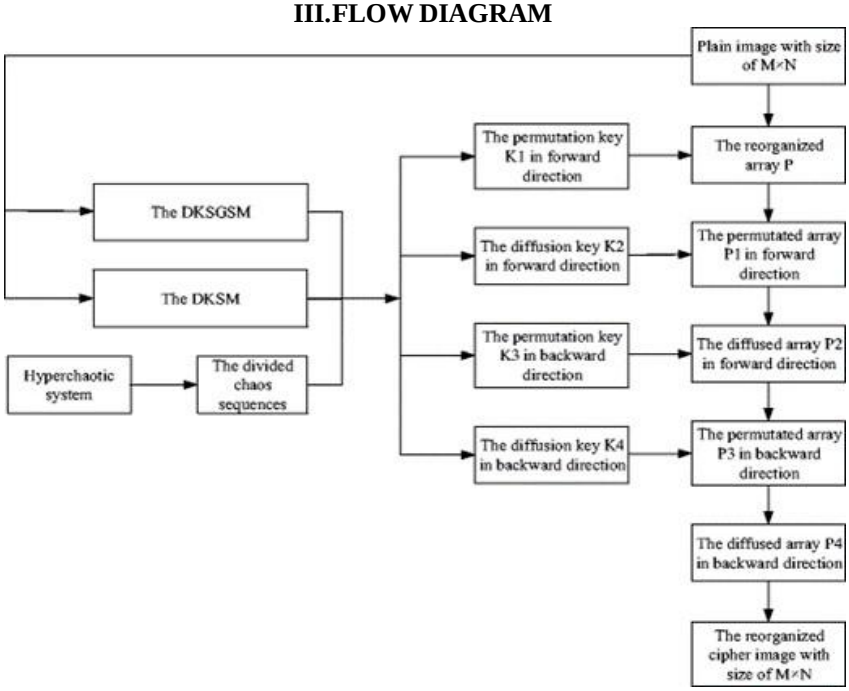

Figure 1: Image Encryption Process [17]

IV.METHODOLOGY

This new algorithm can satisfy the security requirements we expected and well overcome the flaws existing in most cracked algorithms by improving them in different parts.

1. **Key Generation Module**:

i) Hyperchaotic system:

The hyper chaotic system to come up with the key and key streams and conjointly improves the key space. In this same hyper chaotic system are going to be used instead of two or additional chaotic systems to come up with secret keys. Low dimensional chaotic systems have the benefits of easy structure and straightforward operations, however, weak resistance to brute-force attack and tiny key house cannot guarantee the enough security of the steer. Therefore, using the high dimensional hyperchaotic system may be a more sensible choice. A four-dimensional hyperchaotic system with four system parameters and four initial conditions can be modeled by Equation (1).

$$\begin{aligned} \dot{x} &= a(y - x) \\ \dot{y} &= -xz + dx + cy \\ \dot{w} &= xy - bz \\ \dot{z} &= yz + kw \end{aligned} \qquad (1)$$

In addition, the chaotic sequences also perform better randomness. Therefore, the security of confidential data can be improved extremely by employing it.

ii) The DKGSM:

It is a dynamic keystream sequence group selection mechanism, and it's an advance to boost the link of the coding technique and plaintext and increase the use quantitative relation of chaotic state variables.We regard the plain image with size M × N as P0 and it has been resized to a one dimensional array P from the upper-left corner to the lower-right corner. These pixels are defined by P = {P(1), P(2),….., P(n)}, where n = M × N. Firstly, we need to divide the chaotic state values calculated from Eq. (1) into groups. The detailed steps are as follows: firstly, in order to avoid the harmful effect of transitional procedure, we iterate the hyperchaotic system (1) for N_o ($N_o \geq 500$) times from (x_o , y_o , z_o , w_o) by Runge–Kutta algorithm with step length h = 0.001, where N is a constant. Next, we continue to iterate the

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018(CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

hyperchaotic system for M × N times to obtain four block realnumber sequences with size of M × N, Namely, X = [x_1 , x_2 , …,x_n], Y = [y_1 , y_2 , …, y_n], Z = [z_1 , z_2 , …, z_n], W = [w_1 , w_2 , …, w_n], where n = M × N. Then,we set:

$$Ao = \begin{bmatrix} X \\ Y \end{bmatrix}, A1 = \begin{bmatrix} X \\ Z \end{bmatrix}, A2 = \begin{bmatrix} X \\ W \end{bmatrix}, A3 = \begin{bmatrix} Y \\ Z \end{bmatrix}, A4 = \begin{bmatrix} Y \\ W \end{bmatrix}$$
$$A5 = \begin{bmatrix} Z \\ W \end{bmatrix} \qquad (2)$$

Then, we provide a variable, denoted by index1, index1 = T1%6. T1 is a nonnegative integer, which is calculated from the plaintext pixels. We assume that if index1 = i, selecting the A to generate the key stream, i∈[0, 5]. We calculate the T1 value by the following formulas (3) and (4),

$$yo = \begin{cases} 0; & if \max(ai = 0), \\ \dfrac{\sum_1^{MXN} ai}{M\ X\ N\ X\ max(ai)} & otherwise. \end{cases} \qquad (3)$$

$$T1 = \text{mod}\ (\text{floor}\ (y_0 \times 10^8)\ , M \times N) \qquad (4)$$

Where $a_i$is the ith element value of the array P,max(a_i)represents the maximum value of P, floor(x) returns the value nearest integers less than or equal to x, mod(x, y) returns the remainder after division.

iii) The DKSM:

The DKSM is to demonstrate the way to assign the chaotic
state variables from the keystream sequence cluster designated by DKSGSM to inscribe every constituent dynamically. Confusion Strategy: Permutation of pixels of
pictures is finished by some chaotic maps and treated as confusion method Diffusion Strategy: whereas in diffusion method, the conversion of constituents in an exceedingly distinctive manner such even a tiny low variance in an exceedingly pixel of the authentic input image stimulate the corresponding encrypted image to be assessed otherwise.

2. The confusion strategy by nonlinear operations

In the permutation method, the swapped array P1 is obtained by nonlinear pixel scrambling operations. What's more, it should be pointed out that the permutated array is directly grown on the array P, and it does not allocate new space to store the confused element. For any pixel in plaintext, it will be swapped with another one located after it, as shown in Figure 2. The concrete nonlinear pixel swapping operations are conducted by Eqs (5) – (8), and the creation of P1(X) is illustrated as follows.

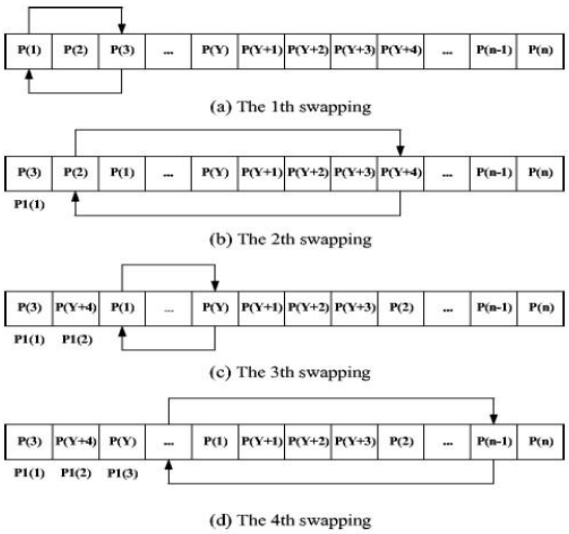

Figure 2:Confusion Strategy by non linear operations[17]

Step 1:

For the current element in location X, the corresponding swapped position X' is firstly calculated by Eq. (5). Where, K1(X) is the Xth secret key chosen by the DKSM. P1(X-1) is the value of the previous swapped element. Especially, P1(0) is a initial value given in advance, X∈[1, M × N], X'∈[1, M × N].

Step 2:

Compute P1(X) and the updated pixel value at X' with Eqs. (6) – (8), where P(X) represents the Xth element in array P, the exchange(a, b) means exchanging the value of a and b.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018(CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

$$X' = X + \mathrm{mod}\left(\left(K1(X) + P1(X-1)\right), (MXN - X + 1)\right) \quad (5)$$

$$P(X') = P[X + \mathrm{mod}((K1(X) + P1(X-1), (MXN - X + 1) \quad (6)$$

$$\mathrm{exchange}\left(P(X), P(X')\right) \quad (7)$$

$$P1(X) = P(X) \quad (8)$$

Encryption Process: The plain image P0 (M × N) is resized to a one-dimensional array P from the upper-left corner to the lower-right corner.
Step 1: Perform one round permutation operation in forward direction
Step 2: Perform one round diffusion operation in forward direction
Step 3: Perform one round permutation operation in backward direction from the last pixel to the first one.
Step 4: Perform one round diffusion operation in backward direction from the last pixel to the first one. Then, resize the diffused array to a two dimensional matrix with the size of M × N, and the cipher image is gotten.

Encryption steps:
Firstly, the plain image P0 (M × N) is resized to a onedimensional array P from the upper-left corner to the lowerright corner. The detailed encryption process will be illustrated as follows:
Step 1: Perform one round permutation operation in forwarddirection.
1.1) Employ the hyperchaotic system (1) to obtain foursequences with size of M × N, namely, X = [x1 , x2 , , x_{MXN}], Y = [y 1, y ,2 …, y_{MXN}], Z = [z1 , z2 , …, z_{MXN}], W = [w1 , w2 , …, w_{MXN}].
1.2) Divide the X, Y, Z, W into blocks, as shown in methodology.
1.3) Compute the permutation key K1 by DKSGSM and DKSM, and in the forward permutation stage, T2 is denoted as T20 .
1.4) Calculate the exchanging location of the plain image corresponding pixel and scramble the pixel according to Eqs. (5) – (9) with secret key P1(0).
1.5) Return to 1.3) until all elements are confused, then get the permutation array P1.

V. RESULTS

Simulation results will be demonstrated to test the performance of the algorithm. We will be using Matlab to run the encryption and decryption programs. To test the robustness of the algorithm, security analysis will be performed with respect to key.
A four-dimensional hyperchaotic system with four parameter and four initial conditions has been modelled.

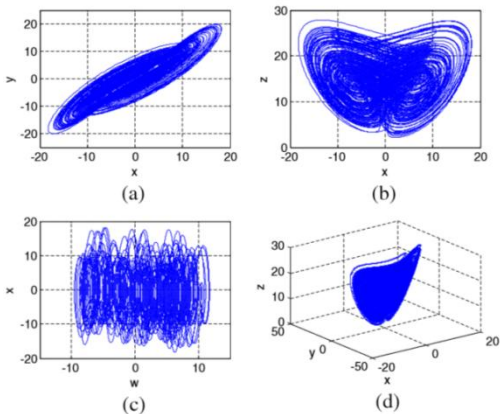

Figure 3: Hyperchaotic attractor **a** (x-y) plane**b** (x-z)plane **c** (w-x) plane **d** (x-y-z) plane [17]

The figure presents the system attractor curves for the hyperchaotic system, when a=36, b=3, c=28, d= -16 ,k=0.5. The hyperchaotic system has more complex phase space and dynamic property.Also in this algorithm the size of key space we are excepting around 10^{70} which will make the brute-force ineffective. Also different parameter such as key sensitivity histogram analysis and differential attackshould be carried out to test the efficiency of the algorithm.

VI. CONCLUSION

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018(CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

A new chaos-based image encryption algorithm with dynamic key selection mechanism is put forward. By employing the DKSGSM and DKSM, the secret keys which are used in permutation stage and diffusion stage are generated with the same hyper chaotic system and these keys can be selected dynamically by the corresponding plain pixels. Thus, a tiny change in the plain image will bring about totally different key stream sequences and cipher image, "one plain image, one key" can be achieved. In addition, we encrypt the image in bidirectional, contributing a lot to spreading the encryption effect to the whole image. The algorithm possesses a larger key space, a stronger anti-attack ability, a higher security level and efficiency. It will have widely application in secure communication.

REFERENCES

[1] Fridrich J Symmetric ciphers based on two- dimensional chaotic maps. Int J Bifur Chaos 8:1259– 1284..
[2] Hung-I H, Junghsi L ,Color image encryption using chaotic nonlinear adaptive fiter. Signal Process 117:281–309.
[3] Wu Y, Zhou YC, Sos A, Noonan Joseph P A symmetric image cipher using wave perturbations. Signal Process 102:122–131.
[4] Mirzaei O, Yaghoobi M, Irani H A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dyn 67(1):557–566.
[5] Chai XL An image encryption algorithm based on bit level Brownian motion and new chaotic systems. Multimed Tools Appl. doi:10.1007/s11042015-3088-1.
[6] Fu C, Lin BB, Miao YS, Liu X, Chen JJ A novel chaos-based bit-level permutation scheme for digital image encryption. Opt Commun 284(23):5415–5423.
[7] Zhang W, Wong KW, Yu H, Zhu ZL A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Commun Nonlinear Sci Numer Simul 18(3):584–600.
[8] Patidar V, Pareek N, Purohit G, Sud K Modified substitution–diffusion image cipher using chaotic standard and logistic maps. Commun Nonlinear Sci Numer Simul 15(10):2755–2765.
[9] Zhu CX A novel image encryption scheme based on improved hyperchaotic sequences. Opt Commun 285:29–37.
[10] Akhavan A, Samsudin A, Akhshani A Cryptanalysis of Ban improvement over an image encryption method based on total shuffling. Opt Commun 350:77–82.
[11] Eslami Z, Bakhshandeh A ,An improvement over an image encryption method based on total shuffling. Opt Commun 286:51–55.
[12] Li CQ, Liu YS, Zhang LY ,Breaking a chaotic image encryption algorithm based on modulo addition and xor operation. Int J Bifur Chaos 23:1350075.
[13] Zhang G, Liu Q ,A novel image encryption method based on total shuffling scheme. Opt Commun 284:2775–2780.
[14] Chen JX, Zhu ZL, Fu C, Yu H, Zhang LB. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Commun Nonlinear Sci Numer Simul 20:846–860.
[15] Ye GD, Zhou J A block chaotic image encryption scheme based on self-adaptive modelling. Appl Soft Comput 22:351–357.
[16] Hang L, Hu X, Liu Y, Wong K A chaotic image encryption scheme owning temp-value feedback. Commun Nonlinear Sci Numer Simul 19(10):3653–3659.
[17] https://link.springer.com/article/10.1007/s11042-016-%203585-x