INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

More Secure Color Image Encryption Scheme Based on 3D Chaotic Maps

Chinchu Thampi[1], Dona Jose[2]

[1]MTech Student (CSE)
Viswajyothi College of Engg.& Tech.,Vazhakulam
chinchumary7@gmail.com

[2]Asst. Professor – Dept. of Computer Science
Viswajyothi College of Engg. & Tech.Vazhakulam
donanjose@gmail.com

Abstract-*Different chaos based encryption schemes exist now a day. As image encryption is comparatively difficult to handle by traditional encryption schemes chaos based schemes are more efficient. The major problem in image encryption algorithms is it's difficult to shuffle and diffuse such image data by traditional schemes. Chaotic theory is about the behavior of dynamical systems which are very sensitive to initial conditions and that effect is commonly known as butterfly effect. Small differences in initial conditions produce widely diverging outcomes for such dynamical systems, making prediction almost impossible. This paper proposes a color image encryption based on three dimensional chaotic maps. A three dimensional chebyshev map and logistic map is used for key generation. Initial conditions for three dimensional maps are generated using triple key method. The random keys generated will be used in turn for encryption. Three dimensional maps provide more security and randomness compared to one dimensional and two dimensional maps.*

1. INTRODUCTION

Security of images is a critical issue and it's a major research area. Image encryption is difficult compared to text image encryption due to some properties of images such as bulky data capacity and high redundancy .The major problem in image encryption algorithms is its difficult to shuffle and diffuse such image data by traditional schemes. Also, these algorithms require more computation time and power while performing image encryption.

A chaotic map exhibits some chaotic behavior. Since chaotic has pseudo- randomness, ergodicity, high sensitivity to initial conditions and parameters, the chaotic maps have demonstrated high potential for information especially image encryption. Various image encryption techniques have been proposed during the last years based on multiple one-dimensional, two-dimensional or higher-dimensional chaotic systems, coupled chaotic maps.

2. RELATED WORKS

In [1] Seyed Mohammad Seyedzadeh & Sattar Mirzakuchaki demonstrated a color image encryption based on coupled two dimensional piecewise non –linear chaotic map. In this scheme an external 256 bit key is used to generate the initial conditions and parameters required for chaotic map. Then the random key streams required in encryption is generated using coupled two dimensional piece-wise nonlinear chaotic map. To add the security in addition to forward encryption, inverse encryption, substitution and masking phases are incorporated in the scheme. Although coupled maps improve the security compared to usual chaotic maps, it has less security compared to three dimensional ones. In [4] Yaobin Mao and Guanrong Chen generalized the advantages of chaos based image encryption. Chaotic equations are very much sensitive to initial conditions. Because of that it has high security compared to prior non chaotic schemes. In [5] Wong & Kwok explained a fast color image encryption based on standard chaotic map. In this paper, certain diffusion effect is introduced in the confusion stage by simple sequential add-and-shift operations. The purpose is to reduce the workload of the time consuming diffusion part so that fewer overall rounds and hence a shorter encryption time is needed. The authors in [6&7] also has mentioned a novel image encryption based on spatial chaotic maps. In

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

[7], certain diffusion effect is introduced in the confusion stage by simple sequential add-and-shift operations. The purpose is to reduce the workload of the time consuming diffusion part so that fewer overall rounds and hence a shorter encryption time is needed. But the problem with above mentioned schemes is that chaotic maps used in the schemes are less sensitive to initial conditions & parameters compared many other chaotic equations & are more complicated. Authors in [8] has also proposed a chaotic encryption scheme one of the three dynamic chaotic systems (Lorenz or Chen or LU chaotic system selected based on 16-byte key) is used to shuffle the position of the image pixels (pixel position permutation) and uses another one of the same three chaotic maps to confuse the relationship between the cipher image and the plain-image (pixel value diffusion), thereby significantly increasing the resistance to attacks..In [9] Yaobin mao, Guanrong Chen & Shiguo Lian demonstrated a chaotic encryption based on 3 dimensional baker map. Here the two-dimensional baker map is extended to three-dimensional and is then used to compose a fast and secure image encryption scheme. Although it has the advantages of 3 dimensional maps its very complex since 2D is extended to 3D.Authors in [10&11] introduced encryption schemes based on piecewise & coupled non-linear chaotic maps. It has its own advantages but it's less secure compared to 3 dimensional schemes.

3. 3D CHAOTIC FUNCTIONS

3D Chebyshev map [2]: Chebyshev polynomial is used to generate the keys required for encryption. Chebyshev polynomial $F_n(x)$ of the first kind is a polynomial in x of degree n, defined as follows:

$F_n(x) = \cos n\theta$ where $x=\cos\theta$.

Putting n=0,1,2,3,4 we get $\cos 0\theta = 1, \cos 1\theta = \cos\theta, \cos 2\theta = 2\cos^2\theta - 1, \cos 3\theta = 4\cos^3\theta - 3\cos\theta, \cos 4\theta = 8\cos^4\theta - 8\cos^2\theta + 1$.

By putting $\cos\theta = x$ we get

$F_0(x) = 1,$

$F_1(x) = x,$

$F_2(x) = 2x^2 - 1,$

$F_3(x) = 4x^3 - 3x,$

$F_4(x) = 8x^4 - 8x^2 + 1.$

Here its transformed as

$F_2(x) = 2x^2 - 1$ (1)

$F_3(y) = 4y^3 - 3y$ (2)

$F_4(z) = 8z^4 - 8z^2 + 1$ (3)

and so on polynomials exhibit the chaotic behavior hence we can use them to generate the random values for generating random keys.

3D Logistic Map [2]: Logistic map is the most simplest chaotic function and is defined by the equation $X_{n+1}=\lambda X_n(1-X_n)$.The equation exhibit chaotic behavior when $0<X_n<1$ and $\lambda=4$.Here a 3 dimensional logistic map is used.

The equations are as follows:

$x_{i+1} = \lambda x_i (1- x_i) + \beta y_i^2 x_i + \alpha z_i^3$ (4)

$y_{i+1} = \lambda y_i (1-y_i) + \beta z_i^2 y_i + \alpha x_i^3$ (5)

$z_{i+1} = \lambda z_i (1- z_i) + \beta x_i^2 z_i + \alpha y_i^3$ (6)

The above shown equations have good chaotic characteristics when $3.53<\lambda<3.81$, $0<\beta<0.022$, $0<\alpha<0.015$ and it takes the values between [0, 1].

4. PROPOSED SYSTEM

The proposed scheme as shown in figure 1 consists of key stream generation process, diffusion-substitution and masking process. A set of three hexadecimal values & floating point values are used for generation of initial conditions of chaotic maps. The first stage consists of key stream generation using three dimensional chebyshev map and a three dimensional logistic map.

First a set of random keys are generated using three dimensional chebyshev maps and that keys in turn are used as initial conditions for three dimensional logistic maps. Chebyshev map is iterated 80 times. Then these random values generated using these maps are used for forward encryption which is detailed in next section. Then an inverse encryption is performed. Additionally to improve security and to have proper substitution S-box of AES is used. S-box transformation makes attacks difficult as it results in diffusion and substitution of information. The masking process in last phase will make use of the information of one part of the image for shuffling the other part.

Vol. 1, Issue IX, Oct.2013
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

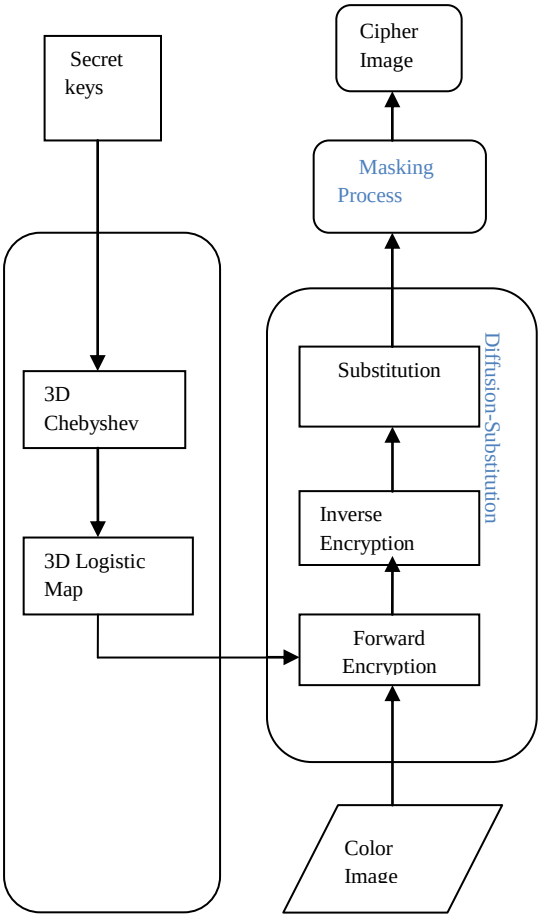

Figure1: Architecture of proposed cryptosystem

4.1Keystream and initial condition generation:

In the proposed scheme for key generation a hexadecimal key and a floating point value is used for each dimension of 3D chebyshev map to generate initial condition. Its generated as in [3].As shown in figure 2 P_n is

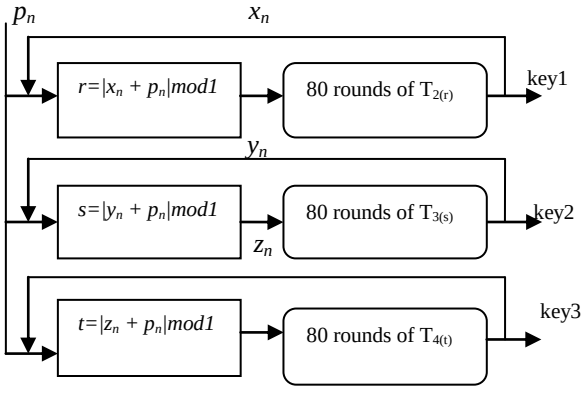

Figure 2: Key Generation using 3D Chebyshev map [3].

a 128 bit random number generated. And the output of 3D chebyshev map is given to the 3D logistic map and its iterated L=W×H times so that L random values are generated for encryption.

4.2Masking Process:

On each encrypted image component masking process is done [1].If the image component is not a multiple of 256,it is padded by replication of the right-most column and the bottom row. Image array of size 256×256 is segmented into four sections. and each section is denoted by a label in the form of $Se._{x,}$where x= 1,2,3,4.Masking process is done as follows.

4.3 Encryption Algorithm:

Step 1.Apply the set of external secret keys and set n =0, L=W×H.

Key stream generation process: Based on the 3D chebysehev map and 3D logistic map described in Section 3 this process produces pseudo-random key streams for encryption of the color image. 6×L pseudo- random numbers are produced for each color image of size W× H such that2 × L pseudo- random numbers are used for encryption of each component (Red,Green and Blue).

Step 2.Initial conditions are generated according to section 3.1.

Step3.Initial conditions are used to iterate eqs. (1),(2)and (3) 80 times. That is 80 rounds of chebyshev map is iterated. The output is given to 3D logistic map. It is iterated L=W×H times so that L random values are obtained for encryption of L pixels of the color image. And store output equations in matrices $X_{n\times1}(1),Y_{n\times1}(1),Z_{n\times1}(1),X_{n\times1}(2),Y_{n\times1}(2),Z_{n\times1}(2),$ $X_{n\times1}(3),Y_{n\times1}(3),Z_{n\times1}(3)$.

Step4.Setn=1,k=1,$Ciph_{0\times1}(1)=0,Ciph_{0\times1}(2)=0,$ $Ciph_{0\times1}(3)$ = 0 and transform the plain-image $P_{W\times H}$ into matrices $R_{L\times1},G_{L\times1}$ and $B_{L\times1}$.

Diffusion and substitution process: Here the pixels of the image are encrypted using the encryption transformation as given starting from the first pixel to the last one, i.e, (Forward Encryption).This process is done in reverse i.e inverse Encryption after the last pixel is encrypted. Finally, according to the S-box of AES [4], the elements of the encrypted matrices are substituted.

Step5.The encryption transformation is applied as the follows

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

$Ciph_{k\times1}(1)=R_{k\times1}+int(X_{n\times1}(1)\times L)$
$+Ciph_{(k-1)\times1}(1))mod256$ (7)

$Ciph_{(k+1)\times1}(1) = R_{(k+1)\times1}+int(Y_{n\times1}(1)\times L)$
$+Ciph_{k\times1}(1))mod256$ (8)

$Ciph_{(k+2)\times1}(1) = R_{(k+2)\times1}+int(Z_{n\times1}(1)\times L)$
$+Ciph_{(k+1)\times1}(1))mod256$ (9)

$Ciph_{k\times1}(2) = G_{k\times1}+int(X_{n\times1}(2)\times L)$
$+Ciph_{(k-1)\times1}(2))mod256$ (10)

$Ciph_{(k+1)\times1}(2) = G_{(k+1)\times1}+int(Y_{n\times1}(2)\times L)$
$+Ciph_{k\times1}(2))mod256$ (11)

$Ciph_{(k+2)\times1}(2) = G_{(k+2)\times1}+int(Z_{n\times1}(2)\times L)$
$+Ciph_{(k+1)\times1}(2))mod256$ (12)

$Ciph_{k\times1}(3) = B_{k\times1}+int(X_{n\times1}(3)\times L)$
$+Ciph_{(k-1)\times1}(3))mod256$ (13)

$Ciph_{(k+1)\times1}(3) = B_{(k+1)\times1}+int(Y_{n\times1}(3)\times L)$
$+Ciph_{k\times1}(3))mod256$ (14)

$Ciph_{(k+2)\times1}(3) = B_{(k+2)\times1}+int(Z_{n\times1}(3)\times L)$
$+Ciph_{(k+1)\times1}(3))mod256$ (15)

Set n=n+1,k=k+3 and iterate step 5 until $k\leq L$.

Step 6.Set n = (L/2), k=k+3 and $R_{L\times1},G_{L\times1},B_{L\times1}$ equal to reverse of matrices $Ciph_{L\times1}(1),Ciph_{L\times1}(2),Ciph_{L\times1}(3)$, respectively, and then iterate step 6 until $k\leq L$.

Step 7.Substitute the elements of matrices according to S-box of AES and then transform them to $C_{W\times H}(1),C_{W\times H}(2), C_{W\times H}(3)$.

Step 8.Masking process is performed on matrices as equations in [1].

4.4 Decryption Algorithm:

Decryption process is similar to that of encryption except that certain steps are performed in reverse order. Masking process is done as in [1].Inverse S-box is used. Equations from 7 to 15 are replaced as follows:

$R_{k\times1}(1)=Ciph_{k\times1}-int(X_{n\times1}(1)\times L)$
$-Ciph_{(k-1)\times1}(1))mod256$ (16)

$R_{(k+1)\times1}(1) = Ciph_{(k+1)\times1}-int(Y_{n\times1}(1)\times L)$
$-Ciph_{k\times1}(1))mod256$ (17)

$R_{(k+2)\times1}(1) = R_{(k+2)\times1}-int(Z_{n\times1}(1)\times L)$
$-Ciph_{(k+1)\times1}(1))mod256$ (18)

$G_{k\times1}(2) = Ciph_{k\times1}-int(X_{n\times1}(2)\times L)$
$-Ciph_{(k-1)\times1}(2))mod256$ (19)

$G_{(k+1)\times1}(2) = Ciph_{(k+1)\times1}-int(Y_{n\times1}(2)\times L)$
$-Ciph_{k\times1}(1))mod256$ (20)

$G_{(k+2)\times1}(2) = Ciph_{(k+2)\times1}-int(Z_{n\times1}(2)\times L)$
$-Ciph_{(k+1)\times1}(2))mod256$ (21)

$B_{k\times1}(3) = Ciph_{k\times1}-int(X_{n\times1}(3)\times L)$
$-Ciph_{(k-1)\times1}(3))mod256$ (22)

$B_{(k+1)\times1}(3) = Ciph_{(k+1)\times1}-int(Y_{n\times1}(3)\times L)$
$-Ciph_{k\times1}(3))mod256$ (23)

$B_{(k+2)\times1}(3) = Ciph_{(k+2)\times1}-int(Z_{n\times1}(3)\times L)$
$-Ciph_{(k+1)\times1}(3))mod256$ (24)

Decryption process requires the same key as encryption.

5. CONCLUSION

In this paper, a color image encryption based on 3D chebyshev map and 3D logistic map is proposed. The proposed scheme is designed to overcome the drawbacks of usually used one dimensional and two dimensional chaotic system. The proposed scheme provides more randomness than the one dimensional and two dimensional schemes. Additionally to add security a triple key [3] is used and resistance against plaintext attack is obtained using masking process.

REFERENCES

[1] Seyed Mohammad Seyedzadeh , Sattar Mirzakuchaki "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map" Signal Processing 92 (2012) Elsevier.

[2] Pawan N.Khade and Prof.Manish Narnaware"3D Chaotic Functions for image encryption"IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.

[3] Srividya.G and Nandakumar.P "A Triple-Key Chaotic Image Encryption Method"IEEE,2011.

[4] Announcing the advanced encryption standard (AES), Federal Information Processing Standards Publication 197, 2001. Yaobin Mao and Guanrong Chen" Chaos-based image encryption"Handbook of Geometric Computing 2005 Springer

[5] K.-W. Wong, B.S.-H. Kwok, W.-S. "A Fast Image Encryption Scheme based on Chaotic Standard Map" Law Physics Letters (2008).

[6] Fuyan Sun , Shutang Liu , Zhongqin Li , Zongwang Lu "A novel image encryption scheme based on spatial chaos map" 2008 Elsevier Ltd.

[7] G.A.Sathish Kumar,Dr.K.Boopathy Bagan and Dr.N.Sriram "Image encryption based on diffusion and multiple chaotic maps", International Journal of Network Security and its Applications(IJNSA),Vol .3,No.2,March 2011.

[8] Huaqian Yang , Kwok-Wo Wong, Xiaofeng Liao , Wei Zhang , Pengcheng Wei 2010 "A fast image

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

encryption and authentication scheme based on chaotic maps" Elsevier

[9] Yaobin mao , Guanrong Chen, Shiguo Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps"International Journal of Bifurcation and Chaos, Vol. 14, No. 10 (2004)

[10] S. Mazloom, A.M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map "Solitons & Fractals 42 2009

[11] S. Behnia , A. Akhshani , S. Ahadpour , H. Mahmodi , A. Akhavan, "A fast chaotic encryption scheme based on piecewise non-linear chaotic maps" Physics Letters A 366 (2007) Elsevier