Locally Applied Mixed Chaotic Maps based Encryption for High Crypto Secrecy

S. Arivazhagan, Professor
W. Sylvia Lilly Jebarani, Associate Professor,
S.Veera Kalyani, A. Deiva Abinaya
Department of Electronics and Communication Engineering,
Mepco Schlenk Engineering College,
Sivakasi, India.

***Abstract*— In recent years, the chaos based cryptographic algorithms have enabled some new and efficient ways to develop secure image encryption techniques. In this paper, we propose a new approach for image encryption based on chaotic maps in order to meet the requirements of secure image encryption. The chaos based image encryption technique uses simple chaotic maps which are very sensitive to original conditions. Using many chaotic maps which works based on simple substitution and transposition techniques to encrypt the original image yields better performance with less computation complexity which in turn gives high crypto-secrecy. The initial conditions for the chaotic maps are assigned and using that seed only the receiver can decrypt the message. The results of the experimental, statistical analysis and quantitative tests show that the proposed image encryption scheme provides an efficient and secure way for image encryption.**

***Keywords*— Mixed Chaotic Maps, initial conditions, Substitution, Transposition, secure image encryption.**

I.INTRODUCTION

Chaos-based cryptography receives broad recognition and continues to prosper. Especially, encrypting the image information using chaos has become a particularly hotspot in recent years. A great many digital image encryption schemes were created in the past few years. One of those image encryption systems is Elliptic Curve Cryptography. Elliptic curve cryptography is a way of encoding data files so that only specific individuals can decode them. ECC is based on the mathematics of elliptic curves and uses the position of points on an elliptic curve to encrypt and decrypt information. ECC employs a relatively small encryption key, a value that must be fed into the encryption algorithm to decode an encrypted message. One of the main disadvantages of ECC is that it increases the size of the encrypted message. Furthermore, the ECC algorithm is more complex and more difficult to implement which increases the likelihood of implementation errors, thereby reducing the security of the algorithm.

To overcome complexity issue of ECC, we propose a better encryption technique using chaotic maps alone. Applying one Chaotic Map after the other yields better results. We classified the chaotic maps as substitution based chaotic maps and transposition based chaotic maps. All possible combinations of mixing two kinds of chaotic maps are experimentally analyzed and the NPCR and UACI are used as performance measures. Various simple chaotic maps like Arnolds Cat Map, Logistic Map, Tent Map, Standard Chaotic Map etc., are used. The algorithm is implemented on MATLAB 2014a to evaluate performance and the results show improved security.

II. RELATED WORK

There are numerous papers which make use of chaos for image encryption. Wang and Yu, 2016 [1], introduced chaos by random sequences. Vasundhara.S, 2017 [2] has explained the recent developments and different algorithms in Elliptic Curve cryptography. Jia et al, 2016 [3] combines the advantages of ECC and chaos. To provide security, the text / image is first encrypted using one dimensional logistic map and it is encrypted using ECC that avoids resource consumption by increasing the length of the key in ECC encryption system. Kumar et al, 2016 [4] explained the multiple encryption using ECC. The algorithm used in Saha et al, 2013 [5] is DES followed by ECC. Here, Chaotic Key Generator is used to generate key for DES. The Chaotic Logistic Maps are used for image encryption in Taleb, 2014 [6]. The algorithm is used to encrypt color images where pixel is encoded on 24 bits using chaotic sequences (based on the principle of confusion and diffusion) generated by one dimensional chaotic applications called logistic maps. The swapping based Confusion Approach for introducing chaos is cited in Ye et al, 2016 [7]. Xu et al, 2012 [8] used fast image encryption schemes. Henon map is adopted in Wei-bin and Xin, 2012 [9] to encrypt the shuffled the image, while Som and Kotal, 2012 [10] use 1D logistic map for generation of keys for encryption of pixels. Yun-peng et al, 2009 [11] combine the advantages of DES and chaos. To reduce the computational time of DES, 4 rounds are used instead of 16. It has been shown that 4 iterations balance the security and speed. Logistic maps are used to create round keys for the DES algorithm. The chaotic map used in Assad et al, 2014 [12] is a tent map for production of S-box and Arnold’s map for permutation of pixels.

III. PROPOSED METHOD

Chaos has been widely investigated since the 1990s for Encryption. It shows resemblance to Claude Shannon’s work on secrecy systems in his paper of 1949 [13]. Fridrich, 1998 [14] suggests transformations and mapping functions which depend on initial conditions. It is cleared that Chaos is highly sensitive to initial conditions. “Chaos” refers to “Confusion”.

In chaotic Image Encryption, we can introduce the confusion either to the pixel value or to the pixel position of the image. Based on that, we classified the chaotic maps as substitution based chaotic maps and Transposition based chaotic maps. In Substitution based Chaotic Maps, each and every pixel of the original image is substituted by some new pixel value in the encrypted image depending on the chaotic function used. In Transposition based chaotic maps, only the position of the pixel in the original image is changed in the encrypted image based on the chaotic map used.

A. *Chaotic Encryption*

The original image to be encrypted is converted to a one dimensional binary string of length l .The binary sequence 'w' is formed using the different chaotic maps. The length of the binary sequence 'w' must be same as that of the original plain text string. The binary stream 'w' is extracted using chaotic map, which means the value of 'x' is derived from the chaotic map.

$$w_n = \begin{cases} 0, x_i > c \\ 1, x_i \leq c \end{cases}$$
$$where\ c = 0.505 \qquad \ldots (1)$$

By XOR ing the original plain text string and the binary sequence 'w', we can get the cipher text string. Converting this string to the image again, we can get the encrypted image.

B. *Types of Chaotic Maps*

We classified two kinds of chaotic maps.

- Substitution based chaotic map
- Transposition based chaotic map

(i)*Substitution based Chaotic Map*:

Each and every pixel value of the original image is substituted by the new value which is obtained based on the application of the chaotic maps. Logistic map, Tent map, Gauss map, Henon map, Gingerbread Map and Duffing Map are the substitution based chaotic map used.

(ii*)Transposition based Chaotic Map*:

The position of each and every pixel of the original image

is changed based on the conditions of the chaotic maps. Arnolds Cat Map and Standard Chaotic Map are the transposition based Chaotic maps used. The procedure of applying chaotic maps can be understood with the help of Fig.1

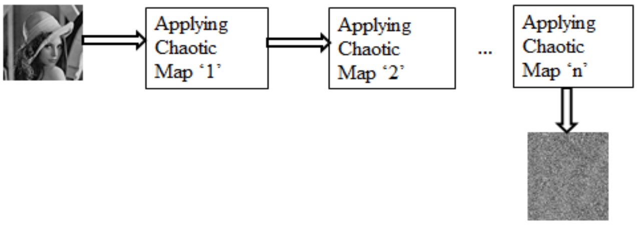


Fig.1 Schematic of Mixed Chaotic Maps based Encryption

First, the original image is encrypted individually. To get better encryption results, the original image is encrypted using multiple chaotic maps. In this paper, up to seven chaotic maps are used to get better NPCR and UACI value. This kind of applying multiple chaotic maps to the original can be referred as 'Mixed Chaotic Maps'. Mixed Chaotic maps add Cryptographic significance since the order of applying simple chaotic maps and what maps have been employed are additionally required for decryption and this increases the work of the hacker manifold thereby improving the secrecy of the system. The different chaotic maps used can be explained as follows:

Logistic map can be explained by the equation

$$x_{i+1} = \mu x_i(1 - x_i)x_i$$
$$where\ x_i \in [0, 1], \mu \in [0,4] and\ x_0 = 3.58 \quad \ldots (2)$$

Tent map can be explained by

$$x_{n+1} = \mu(1 - 2|x_n - 0.5|)$$
$$where\ \mu = 0.1, x_0 = 3.58 \quad \ldots (3)$$

Gauss map can be given by

$$x_{n+1} = \exp(-\alpha x_n^2)+\beta$$
$$where\ \alpha = 4.90, \beta = 0.58\ and\ x_0 = 3.58 \quad \ldots (4)$$

Henon Map can be explained by

$$x_{n+1} = 1 - ax_n^2 + y_n$$
$$y_{n+1} = bx_n$$
$$where\ a = 1.4, b = -0.3, x_0 = 0.98\ and\ y_0 = 0.5 \ldots (5)$$

Ginger bread Map can be given by

$$x_{n+1} = 1 - y_n + |x_n|$$
$$y_{n+1} = x_n$$
$$where\ x_0 = 3.58\ and\ y_0 = 0.5 \quad \ldots (6)$$

Duffing Map can be explained by

$$x_{n+1} = y_n$$
$$y_{n+1} = -bx_n + ay_n - y_n^3 \quad \ldots (7)$$
$$where\ a = 2.75, b = -0.2, x_0 = 3.58, y_0 = 0.5$$

x_0 is the initial condition due to which all the maps exhibit chaotic behavior. The value of x obtained from these chaotic maps is the key to form the binary sequence 'w'.

Considering the transposition based chaotic map, Arnolds Cat Map is one of the unique maps because applying the Arnolds cat map again and again to the encrypted image we can get back the original image. The Arnolds Cat Map (ACM) is given by

$$x' = (x + y) mod\ N$$
$$y' = (2x + y) mod\ N \quad \ldots (8)$$

where x and y are pixel position of the original image. x' and y' are the pixel position of the encrypted image.

The Standard Chaotic Map can be explained as

$$\theta_{n+1} = \theta_n + p_n\ modulo\ 2\pi$$
$$p_{n+1} = p_n + K sin(\theta_{n+1}) modulo\ 2\pi \quad \ldots (9)$$

C. *Mixed Chaotic Encryption*

The chaotic encrypted image is again encrypted using another chaotic map. To improve the randomness between plain and cipher image the idea of mixed chaotic maps based encryption is proposed. In general, key for chaotic based encryption is its initial condition value alone. But, the highlight of the mixed chaotic based encryption is that along with the initial condition value, the type of chaotic maps, the number of the chaotic maps used and the order of the chaotic maps also serves as the key. Hence this increases the work of the hacker manifold thereby improving the secrecy of the system

This can be explained with the help of the Fig.2

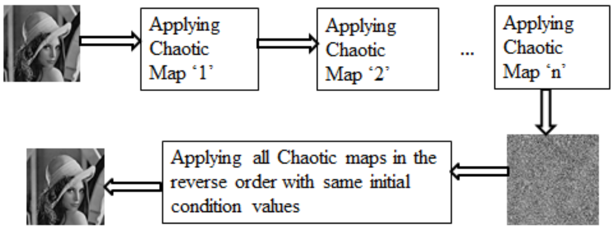

Applying Chaotic Map '1'
Applying Chaotic Map '2'
...
Applying Chaotic Map 'n'
Applying all Chaotic maps in the reverse order with same initial condition values

Fig.2 *Schematic Diagram of Mixed Chaotic Maps based Decryption*

The original image can be retrieved by the step by step decryption in the reverse process.

D.Locally Applied Chaotic Maps

In the second proposed approach, the input image is divided into 'n' blocks. First, for each block, same chaotic map is applied. To improve the secrecy, a different combination of mixed chaotic maps is applied to all blocks. This proposed method is less computationally complex compared to Elliptic Curve Cryptography. The schematic diagram of locally applied chaotic maps is shown in Fig.3.

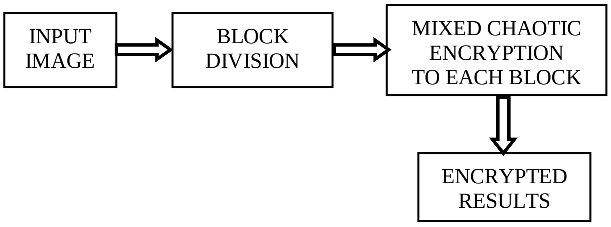


Fig. 3 Schematic Diagram of Locally applied Chaotic Maps

E.Chaotic Decryption

The Chaotic Decryption can be done in the similar way by using same initial condition values. The initial condition is known to the sender and receiver alone. The hacker needs to find out that encryption has been performed locally and will have to work with all blocks with varying degrees of complexity to decipher the image. The encrypted image is converted to one dimensional binary string 'b'. The key binary sequence 'w' which uses chaotic map is available for decryption. XOR ing 'b' and 'w' one can get the decrypted output.

IV. EXPERIMENTAL RESULTS

For the experimentation, we used four standard test images to observe the encryption results. Each standard test image is subjected to mixed chaotic encryption. The selection of specific maps and applying them in order is chosen by exhaustive experimentation. Out of exhaustive experimentation, the sequence of chaotic maps that yielded the best results are tabulated in every case.

The Mixed chaotic maps can be categorized as four types.

- Substitution based chaotic map followed by Substitution based chaotic map.(SCMSCM)
- Transposition based chaotic map followed by Transposition based chaotic map.(TCMTCM)
- Substitution based chaotic map followed by transposition based chaotic map.(SCMTCM)
- Transposition based chaotic map followed by substitution based chaotic map.(TCMSCM)

The Standard Test Images are shown in Fig.4.

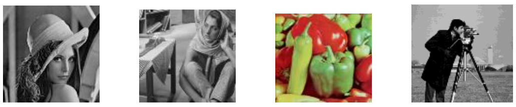

(a) (b) (c) (d)

Fig.4 Standard Test Images
(a) Lena.jpg (b) Barbara.jpg,(c) Peppers.png (d) Cameraman.tif

The Performance Analysis is done by measuring NPCR and UACI value. The Net Pixel Change rate and Unified Average Changing Intensity can be explained as follows:

$$NPCR = \frac{\sum i,j\, D(i,j)\ X\ 100}{M_1\ X\ M_2} \qquad \ldots (10)$$

$$UACI = \frac{\sum i,j\, |C_1(i,j) - C_2(i,j)|\ X\ 100}{M_1\ X\ M_2\ X\ 255} \qquad \ldots (11)$$

$$D(i,j) = \begin{cases} 0\ , if\ C_1(i,j) = C_2(i,j) \\ 1, if\ C_1(i,j) \neq C_2(i,j) \end{cases} \qquad \ldots (12)$$

where C_1 and C_2 are the plain image and cipher image respectively. M_1 and M_2 are the width and height of the image respectively. The experimental analysis is done by performing each and every combination of chaotic map. The performance analysis is done by NPCR (Net Pixel Change Rate) and UACI (Unified Average Changing Intensity). It is clear that NPCR (Net Pixel Change Rate) is a measure of the average number of pixels being affected (quantitative). UACI is a measure of the average change in pixel values (qualitative) between the images. The NPCR and UACI are in the range [0, 1]. The NPCR and UACI can also be represented in percentage and they are the two most common quantities used to evaluate the strength of image encryption algorithm with respect to different attacks. High NPCR and UACI values are usually interpreted as high resistance to differential attacks.

A. Substitution based chaotic map followed by Substitution based chaotic map

Here, the output is shown for applying Duffing Map followed by Logistic Map.The results ensure that the NPCR of the individual Duffing map is highly improved byapplying mixed chaotic maps. The NPCR and UACI values are tabulated in Table I.

TABLE I NPCR and UACI analysis for SCMSCM

IMAGES	NPCR	UACI
Lena.jpg	1	0.408122881721048
Barbara.jpg	1	0.311043354109222
Peppers.png	0.626847654321463	0.310031042108418
Cameraman.tif	0.526168823242188	0.200310441559436

The encrypted results for SCMSCM are given in Fig.5.

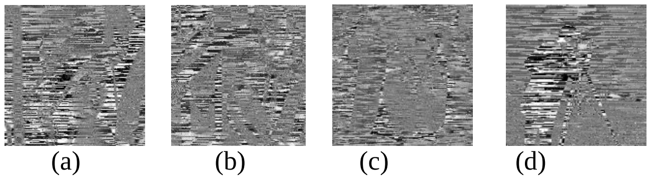


Fig.5 Encryption results for SCMSCM
(a)Lena.jpg (b) Barbara.jpg (c) Peppers.png (d) Cameraman.tif

B.Substitution based chaotic map followed by transposition based Chaotic Map

In this category, better results are obtained in the case of Henon map being selected as the substitution based chaotic map and ACM as the transposition based chaotic map and the results are shown in Table II.

TABLE II NPCR and UACI Analysis for SCMTCM

IMAGES	NPCR	UACI
Lena.jpg	0.996429443359375	0.315652465820312
Barbara.jpg	0.995346069335938	0.256516280828738
Peppers.png	0.995971679687500	0.282401888978248
Cameraman.tif	0.997741699218750	0.293565637925092

The encrypted results for SCMTCM are given in Fig.6.

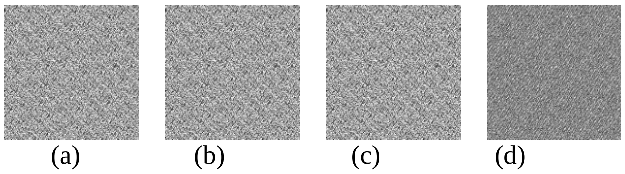


Fig.6 Encryption results for SCMTCM
(a)Lena.jpg (b) Barbara.jpg (c) Peppers.png (d) Cameraman.tif

C. Transposition based chaotic maps followed by Transposition based Chaotic Maps

The example for this kind of mixed chaotic map is Standard Chaotic Map followed by ACM (Arnolds Cat Map) and the results are tabulated in table III. From the Table III, it can be seen that the UACI value has not much improved but it reaches maximum of 31.5%.

TABLE III NPCR and UACI analysis for TCMTCM

IMAGES	NPCR	UACI
Lena.jpg	0.994598388671875	0.239754231770833
Barbara.jpg	0.994486543212354	0.226897532146897
Peppers.png	0.994568752312364	0.244986542323584
Cameraman.tif	0.990310668945313	0.266217938591452

The encrypted results for TCMTCM are given in Fig.7.

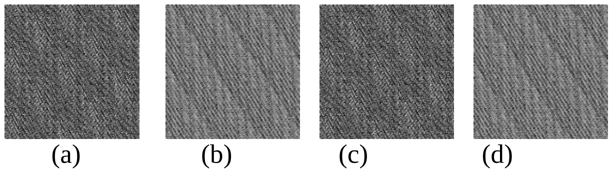


Fig.7 Encryption results for TCMTCM
(a)Lena.jpg (b) Barbara.jpg (c) Peppers.png (d) Cameraman.tif

D. Transposition based chaotic maps followed by Substitution based Chaotic Maps

Comparing all the techniques, Transposition based chaotic Map followed by Substitution based chaotic map yields better results. So, further combination of chaotic map starts with ACM being applied as the first map. Combining three chaotic maps, four Chaotic Maps up to seven Chaotic Maps are tried.

I.ACM followed by Tent Map.

Applying Combinations of two chaotic maps, ACM followed by Tent Map yields better results by experimental analysis. The results are tabulated in Table IV.

TABLE IV NPCR and UACI analysis for TCMSCM-1

IMAGES	NPCR	UACI
Lena.jpg	0.997161865234375	0.31686796300515
Barbara.jpg	0.994537353515625	0.247371718462776
Peppers.png	0.994567871093750	0.243716909371170
Cameraman.tif	0.997741699218750	0.293565637925092

Compared to TCMTCM, TCMSCM-1 (ACM followed by Tent Map) provides better UACI value still having good NPCR value. In this scheme with ACM followed by Tent Map, the UACI value reaches even 36 %.The encryption of the original image using combination of two chaotic maps is compared with the encryption of the original image with individual chaotic maps. The experimental results proved that the encryption of original image using two chaotic maps yield better results. Trying various combinations, ACM followed by any other combination gives high crypto secrecy. The encrypted results are shown in Fig.8.

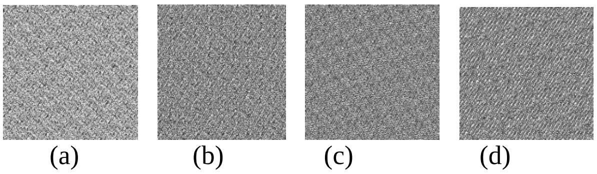


Fig.8 Encryption results for TCMSCM-1
(a)Lena.jpg (b) Barbara.jpg (c) Peppers.png (d) Cameraman.tif

II.ACM followed by Tent followed by Duffing Map

In this combination of three chaotic maps, ACM alone transposition based chaotic map and other two are substitution based chaotic maps. The NPCR and UACI values are tabulated in Table V.

TABLE V NPCR and UACI analysis for TCMSCM-2

IMAGES	NPCR	UACI
Lena.jpg	0.996666503906250	0.281285843194700
Barbara.jpg	0.9947973632813	0.246779976639093
Peppers.png	0.994369506835938	0.244651525160846
Cameraman.tif	0.994140625000000	0.280865239162071

From the Table V, the UACI value is reduced to the average of 26% and also the NPCR value for the ACM-Tent-Duffing is also minimized to 99.6% for the image lena.jpg and for the other images, the NPCR value is around 99.4% only. The encrypted results for SCMTCM are given in Fig.9.

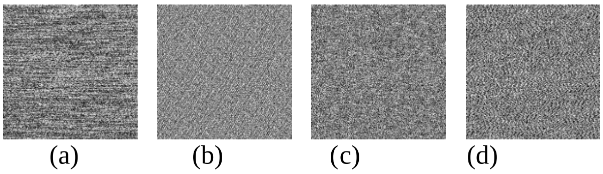


Fig.9 Encryption results for TCMSCM-2
(a)Lena.jpg (b) Barbara.jpg (c) Peppers.png (d) Cameraman.tif

III.ACM followed by Tent followed by Duffing followed by Henon Map

Since the experimental results shows that the ACM followed by Tent Map combination yields better results compared to other combinations of two chaotic maps, that sequence follows. This is the reason to choose the combination, ACM followed by Tent followed by Duffing followed by Henon Map. The NPCR and UACI values are tabulated in Table VI.

TABLE VI NPCR and UACI analysis for TCMSCM-3

IMAGES	NPCR	UACI
Lena.jpg	0.99729114257813	0.298004030713848
Barbara.jpg	0.997643066406250	0.320985622032016
Peppers.png	0.997683935546875	0.343801760206036
Cameraman.tif	0.998941268736542	0.368174055510876

Table VI shows that UACI value for lena.jpg alone very less. Also, UACI values for other images are around 35%. The NPCR value is obtained around 99%.The encrypted results are shown in the Fig. 10.

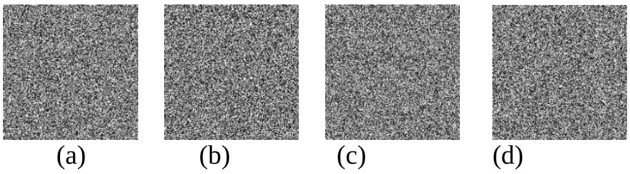


Fig.10 Encryption results for TCMSCM-3
(a)Lena.jpg (b) Barbara.jpg (c) Peppers.png (d) Cameraman.tif

IV.ACM followed by Tent followed by Duffing followed by Henon followed by Logistic Map

The original image is first encrypted using ACM. Because, observing NPCR and UACI performance yields better results only if the starting encryption is ACM. The encrypted output of the ACM followed by Tent Map followed by Duffing Map followed by Henon Map is again encrypted using Logistic map. This yields very high crypto-secrecy since NPCR and UACI values are very high and they are tabulated in Table VII.

TABLE VII *NPCR and UACI Analysis for TCMSCM-4*

IMAGES	NPCR	UACI
Lena.jpg	1	0.505622175628064
Barbara.jpg	1	0.508264878216912
Peppers.png	1	0.502437337239583
Cameraman.tif	1	0.510193110447304

From the Table VII, it is observed that NPCR value has reached its maximum value 1 and UACI value is also comparatively better because, the UACI value is obtained as 51% for combining ACM followed by four substitution based chaotic maps. The encrypted results for TCMSCM are given in Fig.11.

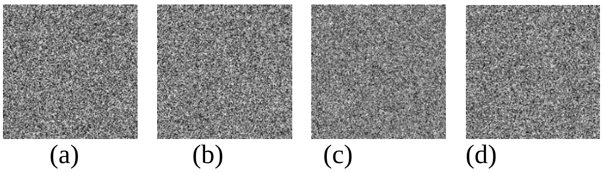


Fig.11 Encryption results for TCMSCM-4
(a)Lena.jpg (b) Barbara.jpg (c) Peppers.png (d) Cameraman.tif

V. ACM followed by Ginger followed by Tent followed by Duffing followed by Logistic followed by Henon Map

The encrypted output of the ACM followed by Ginger followed by Tent Map followed by Duffing followed by Logistic Map is again encrypted using Henon map. This yields high crypto-secrecy since NPCR and UACI values are very high and they are tabulated in Table VIII.

TABLE VIII NPCR and UACI Analysis for TCMSCM-5

IMAGES	NPCR	UACI
Lena.jpg	1	0.509381761737898
Barbara.jpg	1	0.51309868307646
Peppers.png	1	0.500568811753217
Cameraman.tif	1	0.495318495806526

Table VIII gives the NPCR and UACI value for combining six chaotic maps based encryption. The result of NPCR values is 1 for all the four test images and UACI value reaches around 50%. This assures that the randomicity of the plain image and secrecy of the cipher image has been enhanced well. The encrypted results are shown in the Fig. 12.

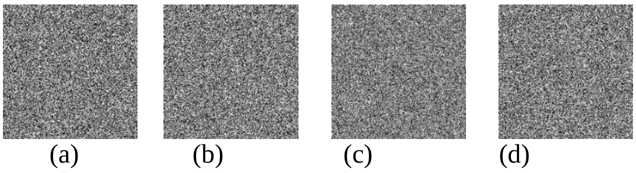


Fig.12 Encryption results for TCMSCM-5
(a)Lena.jpg (b) Barbara.jpg (c) Peppers.png (d) Cameraman.tif

VI. ACM followed by Tent followed by Logistic followed by Duffing followed by Henon followed by Ginger followed by Gauss Map

To enhance the secrecy of the system, the number of substitution based chaotic maps has been increased to six maps .Applying seven chaotic maps to the original image, the performance metrics are improved efficiently. The NPCR and UACI values for encryption using ACM followed by Tent followed by Logistic followed by Duffing followed by Henon followed by Ginger followed by Gauss Map is tabulated in Table IX.

IMAGES	NPCR	UACI
Lena.jpg	1	0.512412456437653
Barbara.jpg	1	0.51525801116345
Peppers.png	1	0.541038543102788
Cameraman.tif	1	0.505318495806526

TABLE IX NPCR and UACI Analysis for TCMSCM-6

Table IX gives the values of NPCR and UACI for combining seven chaotic maps (ACM-Tent-Logistic-Duffing-Henon-Ginger-Gauss Map). The result shows that NPCR value is 1 for all the images taken for experimentation. The UACI value is obtained as 51%. This technique of combining seven mixed chaotic maps yields better results comparatively. The encrypted results are shown in the Fig. 13.

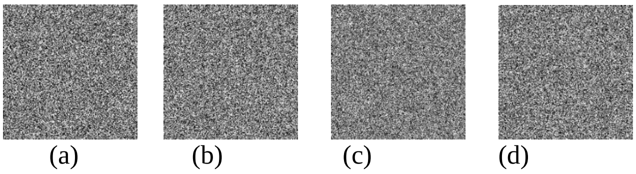


Fig.13 Encryption results for TCMSCM-6
(a)Lena.jpg (b) Barbara.jpg (c) Peppers.png (d) Cameraman.tif

E. Locally Applied Chaotic Maps based Encryption

Using mixed chaotic maps which works based on simple substitution and transposition techniques to encrypt the original image yields better performance with less computation complexity still giving high crypto-secrecy. The initial conditions for the chaotic maps are assigned and using that seed only the receiver can decrypt the message. These kinds of mixed chaotic maps can be applied locally to a single image. That is, a single image is divided into parts and different kind of mixed chaotic maps can be applied to each part. The results of the experimental, statistical analysis and key sensitivity tests show that the proposed image encryption scheme provides an efficient and secure way for image encryption. Fig.14 shows the division of original image into blocks.

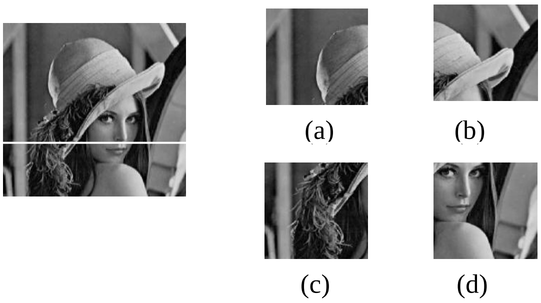
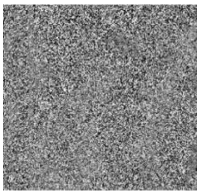


Fig.14 Block Separation of Lena.jpg

I. Applying the same chaotic map to all blocks

The same chaotic map is applied to all the blocks of the original image. The output for applying Henon Map alone for all the four blocks is shown in Fig.15.

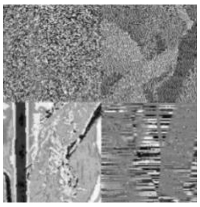


NPCR : 0.9979095458984338
UACI : 0.354040946212469

Fig.15 Encryption results for locally applied same chaotic maps for lena.jpg

II. Applying different chaotic maps to each block

A different chaotic map is applied to each block of the original image. Though the NPCR and UACI values are not high as mixed chaotic maps, the strength of the key has been increased here. Block ‘A’ is encrypted with Henon Map. Block ‘B’ is exposed to Gingerbread map. Block ‘C’ is encrypted using Logistic Map and Block ‘D’ is subjected to Duffing Map.The encrypted results are shown in Fig.16.

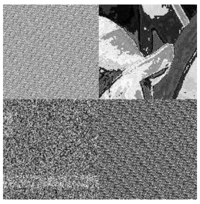


NPCR : 0.885833740234375
UACI : 0.317970305798100

Fig.16 Encryption results for locally applied different chaotic maps to each block for lena.jpg

III. Applying Mixed Chaotic Maps to all blocks

The mixed chaotic map is applied to each block of the original image. The strength of the key has still strengthened here, because the number of chaotic maps used in each block is also different. Block ‘A’ is encrypted with Henon followed by ACM. Block ‘B’ is exposed to Tent-Henon-Logistic followed by ACM. Block ‘C’ is encrypted using Tent followed by Henon and Block ‘D’ is subjected to ACM.The result for this encryption is shown in Fig.16.



NPCR: 0.9967346191406250
UACI: 0.330232567880688

Fig.17 Encryption results for locally applied mixed chaotic maps to each block for lena.jpg

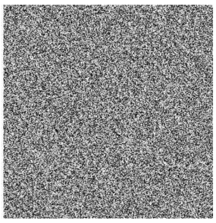
F. Locally Applied Chaotic Maps followed by Transposition based Chaotic Map

In the locally applied chaotic maps, there are chances to guess that encryption has been performed locally due to the visible blocking artifacts.

To overcome this, the Arnolds Cat Map (a Transposition Based Chaotic Map) is used to encrypt the output of the locally applied chaotic maps. From the experimentation, it is observed that the UACI value is improved than locally applied chaotic maps based encryption alone.

I. Locally applied different chaotic maps followed by Transposition based Chaotic Map

The outputs of the locally applied different chaotic maps are applied to all the blocks of the original image are further encrypted using Arnolds Cat Map. The encrypted results are shown in Fig.18.

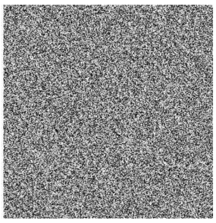


NPCR: 0.995513916015625
UACI: 0.316875502642463

Fig.18 Encryption results for locally applied different chaotic maps to each block followed by ACM for lena.jpg

II. Locally applied mixed chaotic maps followed by Transposition based Chaotic Map

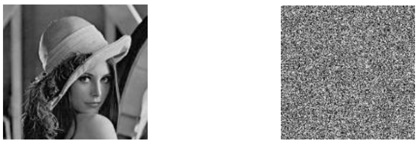
The outputs of the locally applied mixed chaotic maps are applied to all the blocks of the original image are further encrypted using Arnolds Cat Map. The encrypted results are shown in Fig.19.



NPCR: 0.995635986328125
UACI: 0.352954340916054

Fig.19 Encryption results for locally applied mixed chaotic maps to each block followed by ACM for lena.jpg

The decryption results are shown in Fig.20.



(a)With same initial conditions values

(b)With different Initial condition values

Fig.20 Decrypted Results for Lena.jpg

This chaotic encryption technique improves security because the order of applying chaotic maps also serves as the key for decrypting the image along with the initial condition values (seed). The hacker needs to predict the order of chaotic maps applied and the initial condition values to recover the image. In the decryption phase, if the sequences of chaotic maps are not in the strictly reverse order then, the image cannot be decrypted. Fig.21 shows the difference between decrypting the image in sequence of chaotic maps and decrypting the image without following the order of the chaotic maps.

(a)Applying the Chaotic maps in order while decryption

(b)Applying the chaotic maps not in order during decryption

Fig.21 Decrypted Results

In Elliptic Curve Cryptography, there is a need to map image pixels to the message point P_m. The selection of the elliptic curve system E_p(a, b) is needed. The Cipher text can be obtained by

$$\text{Cipher text, } C_m = \{k\,G, P_m + kP_B\} \qquad \ldots (13)$$

where k is the shared secret key and G is the point on the Elliptic Curve E_p(a, b). Each and every pixel of the image should be encoded as point P_m and that P_m should be in the elliptic curve. To address this problem, 'p' should be assigned with the larger value. But, In this proposed mixed chaos based image encryption, there are no such restrictions and it is very simple to encrypt the image and it gives high crypto secrecy too.

V.CONCLUSION

This paper proposed a novel image cryptosystem based on locally applied mixed chaotic system. This proposed approach is better than Elliptic Curve encryption because, Complexity is less than ECC encryption. The high crypto secrecy can be achieved easily with these mixed chaotic maps. Since this encryption technique is optimized to operate on images, it is faster and simpler than any other methods. We can extend this by trying encryption of the original image by increasing the number of chaotic maps used for further optimization and proceedings.

REFERENCES

[1] Qianxue Wang, Simin Yu, "Theoretical Design and FPGA Based Implementation of Higher Dimensional Digital Chaotic Systems" , IEEE Transactions on Circuits and Systems, Vol. 63, No.3, March 2016.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] Vasundhara.S,"Elliptic Curves and Cryptography", International Journal of Information Research and Review, January, 2017.

[3] Nan Jia, Songyan Liu, Qun Ding, Shangru Wu, Xuming Pan, "A New method of Encryption Algorithm Based on Chaos and ECC", Journal of Information Hiding and Multimedia Signal Processing, Vol. 7, No.3, May 2016.

[4] Vishal Kumar, Ratnesh Kumar, Mashud A. Barbhuiya and Monjul Saikia, "Multiple Encryption using ECC and Its Time Complexity Analysis" , International Journal of Computer Engineering In Research Trends, Vol. 3, Issue 11, November-2016.

[5] Bidyut Jyoti Saha, Kunal Kumar Kabi, Arun, "Digital Image Encryption using ECC and DES with Chaotic key generator", International Journal of Engineering and Research & Technology, Vol. 2 , Issue 11, Nov. 2013.

[6] Fadia TALEB, "A New Chaos based Image Encryption scheme using Chaotic Logistic Maps", IEEE International Conference on Multimedia Computing and Systems, April 2014.

[7] Ruisong Ye, Yuting Xi, Yuanlin Ma, "A Chaotic Image Encryption Scheme using Swapping based Confusion Approach", IEEE International Conference on Computer Communication and the Internet, 2016.

[8] Shujiang Xu, Yinglong Wang, Jizhi Wang, Yucui Guo , "A Fast Image Encryption Scheme Based on a Nonlinear Chaotic Map", IEEE International Conference on Signal Processing Systems, 2012.

[9] Chen Wei-bin, Zhang Xin, "Image Encryption Algorithm Based on Henon Chaotic System," in International Conference on Image Analysis Images using Multiple Chaotic Maps," in 2012 National Conference Computing and Communication Systems, West Bengal, India.

[10] Sukalyan Som and Atanu Kotal, "Confusion and diffusion of GrayscaleImages using Multiple Chaotic Maps," in 2012 National Conference on Computing and Communication Systems, West Bengal, India.

[11] Z. Yun-peng, Z. Zheng-jun, L. Wei, N. Xuan, C. Shui-ping, D. Wei-di, "Digital Image Encryption Algorithm Based on Chaos and Improved DES," Proceedings of the 2009 IEEE International Conference on Systems, Man and Cybernetics, San Antonio, TX, USA.

[12] S. El Assad, M. Farajallah, C. Vladeanu, "Chaos-based Block Ciphers: An Overview," in 10th International Conference on Communications, 29-31 May, 2014.

[13] Claude. E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, Vol. 28-4, Page 656-715, October 1949.

[14] Jiri Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps," in International Journal of Bifurcation and Chaos, Vol 8, No. 6 (1998) 1259-1284.