Enhanced Two Dimensional Circular Encryption Algorithm

Vikas Mittal

Abstract- In recent years, many multimedia and image encryption techniques based on chaotic maps have been proposed. Recently, a new signal security system called TDCEA (two-dimensional circulation encryption algorithm) was proposed for real-time multimedia data transmission. There exist some essential security defects in TDCEA. This paper gives an analysis on the security of TDCEA and proposed enhanced encryption algorithm. Proposed encryption scheme is based on two digital chaotic maps, which in turn are used to generate two different chaotic sequences. Detail description of the security analysis of TDCEA, proposed encryption technique and performance analysis of enhanced encryption algorithm on various parameters of security is given in later sections of this paper.

Keywords- Multimedia, Encryption, Decryption, Two Dimensional Circular Encryption Algorithm (TDCEA), Piecewise Linear Chaotic Map (PWLCM), Enhanced Two Dimensional Circular Encryption Algorithm (Enhanced TDCEA).

I. INTRODUCTION

With the rapid development of multimedia and network technologies, images are being transmitted over networks more and more frequently. Consequently, reliable security in storage and transmission of digital images is needed in many applications, including both public and private services such as medical imaging systems and military information systems.

Image data have strong correlations among adjacent pixels. Statistical analysis on large amounts of images shows that averagely adjacent 8 to 16 pixels are correlative in horizontal, vertical, and diagonal directions for both natural and computer-graphical images [1]. Moreover, due to some intrinsic features of images, such as bulk data capacity and high redundancy, encryption of images is different from that of texts [2]. Therefore, conventional cipher algorithms such as DES, IDEA etc. are not suitable for image encryption. The chaos-based cryptography has suggested a new and efficient way to develop fast and secure image encryption algorithms. In 1997, chaotic map is first adopted for image encryption by Fridrich [3]. Since then, many chaos-based image encryption algorithms have been designed to realize secure communications [1, 3-8], but it is pointed out that most of them are flawed by lack of robustness and security [9-11].

In this paper, we analyses the security of two dimensional circular encryption algorithm (TDCEA) and also talks about major security defects in the design of TDCEA. We also propose a modified chaotic encryption scheme which addresses the key issues of security of TDCEA and provides enhanced security.

Manuscript received on June, 2014.

Vikas Mittal, Maharaja Agrasen College, University of Delhi, Delhi, India.

Various security analysis of proposed encryption techniques shows that proposed encryption technique is a novel encryption technique, which provides high security to all kinds of multimedia data.

In section 2, design of TDCEA has been explained; Section 3 discussed security defects of TDCEA, followed by description of enhanced encryption scheme in section 4. In section 5, security analysis of the proposed encryption scheme is done using various statistical techniques and comparative analyses with TDCEA are also performed. and last Section concludes the paper.

II. TWO DIMENSIONAL CIRCULAR ENCRYPTION ALGORITHM (TDCEA)

Let us assume an image of *M x N* size where *M* is the height and *N* is the width of the image. TDCEA is a bit circulation algorithm which rotates the bits of 8 consecutive pixels thus 64 bits forming an 8x8 matrix both horizontally and then vertically. The rotations (both horizontal and vertical) in TDCEA are controlled by a chaotic pseudo random binary sequence (PRBS).

TDCEA is composed of two rotation functions: RotateX and RotateY which rotates the bits of 8x8 matrix horizontally and vertically respectively.

$RotateX_i^{p,r}$: This function circularly rotates i^{th} row of the matrix M by r elements in left direction (for p=1) or in right direction (for p=0).

$RotateY_j^{q,s}$: This function circularly rotates j^{th} column of the matrix M by s elements in up direction (for q=1) or in down direction (for q=0).

TDCEA is a block encryption algorithm i.e. it encrypts the plain image in a block of 8 pixels each. It reads 8 consecutive image pixels and forms an 8x8 bit matrix M. First, 8x8 bit matrix is processed by $RotateX_i^{p,r}$ for each row of M and then by $RotateY_j^{q,s}$ for each column of bit matrix M. Values of control parameters (p, r) and (q, s) are obtained from PRBS which uses 1-D chaotic logistics map and secret key. This procedure is repeated for each 8 pixel block of the plain image.

III. SECURITY DEFECTS OF TDCEA

There are some major defects in bit circulation process. First, Pixels of the constant intensity area of the image remains unchanged after encryption. This is also true for any image in which sub regions also contains pixels of constant intensity. Encrypting these sub regions using TDCEA leads the edge of the sub region to appear in the cypher text image. The reason behind above claims is that for constant intensity image pixels we will have 8 x 8 bit matrix, in which all elements either contains a value 0 or 1. Rotating the matrix of the above mentioned nature in any direction and any

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

number of times, doesn't produce the changed matrix. Encrypting the image with sub regions containing constant intensity pixels also not alter the pattern of the sub regions in the cipher text image, resulting edges will appear in the cipher text image. This can be easily seen in figure 2. This clearly shows security defects of TDCEA.

Fig. 1. Encryption result of "house" using TDCEA.

IV. PROPOSED ENCRYPTION ALGORITHM

The proposed modified and enhanced TDCEA is based on 128-bit long shared secret key, which is then divided into sixteen 8-bit session keys represented as:

$$k = k_1 k_2 \ldots\ldots\ldots k_{15} k_{16} \qquad (1)$$

where k_i represents one 8-bit block of session key. One PWLC map of the form

$$F(x) = \begin{cases} x/p, & x \in [0, p) \\ (x-p)/(0.5-p), & x \in [p, 0.5] \\ 1-x, & x \in [0.5, 1). \end{cases} \qquad (2)$$

is used to generate a chaotic sequence, where p is a control parameter, whose value is in the range $0.0 \le p \le 0.7$. To calculate initial condition for chaotic map, we select eight session keys in two groups of four-session keys each. Initial condition X_0 is calculated from four session keys $k_1 k_4 k_7 k_{10}$ as follows:

1. Four session keys are represented as:

$$B_1 = \begin{bmatrix} k_{1,1} k_{1,2} \ldots. k_{1,7} k_{1,8} k_{4,1} k_{4,2} \ldots. \\ k_{4,7} k_{4,8} k_{7,1} k_{7,2} \ldots. k_{7,7} k_{7,8} k_{10,1} \\ k_{10,2} \ldots. k_{10,7} k_{10,8}. \end{bmatrix} \qquad (3)$$

where k_{ij} is the j^{th} binary value of i^{th} block of the session key. Next a real number X_{01} is used which can be computed using the above binary representation as:

$$X_{01} = \begin{pmatrix} k_{11}\times 2^0 + k_{12}\times 2^1 + \ldots. + k_{18}\times 2^7 + k_{41}\times 2^8 + \\ k_{42}\times 2^9 + \ldots. + k_{48}\times 2^{15} + k_{71}\times 2^{16} + k_{72}\times 2^{17} \\ + \ldots. + k_{78}\times 2^{23} + k_{101}\times 2^{24} + k_{102}\times 2^{25} + \ldots. + \\ k_{108}\times 2^{31} \end{pmatrix} \Big/ 2^{32} \qquad (4)$$

is computed. Then $X_0 = (X_{01}) \bmod 1$ is computed. Using initial conditions obtained in equation 4, a sequence of 32 real numbers $f_1 f_2 f_3 \ldots\ldots f_{32.}$ is generated and is converted into an integer using the equation:

$$p_k = (\text{int})(31 \times (f_k - 0.1)/0.8) + 1. \qquad (5)$$

where $k = 1,2,3 \ldots\ldots 32$. After generating a chaotic sequence of 32 numbers, we read a pixel of the plain text image and perform the XOR operation with our first session key. Similarly next seven pixels are XORed with seven other session keys. After XORing is done, we form an 8x8 bit matrix of the XORed pixels, and then applying the $RotateX_i^{p,r}$ for horizontal rotation and $RotateY_j^{q,s}$ for vertical rotation. Value of p, r is taken from two consecutive values from the chaotic sequence i.e. first 16 chaotic numbers will be used by $RotateX_i^{p,r}$ (for r = even circular right, and for r = odd, circular left)function and next 16 numbers will be used by $RotateY_j^{q,s}$ (for s = even, circular up, and s = odd, circular down) function.

The control parameters p and q have same meaning. After encrypting 8 bytes/pixels/samples, we modify the key according to the formula.

$(k_i)_{10} = ((k_i)_{10} + (k_{16})_{10}) \bmod 256$ where $1 \le i \le 15$ and re-calculate the 32 chaotic numbers. In this way entire file is encrypted as shown in Figure 1.

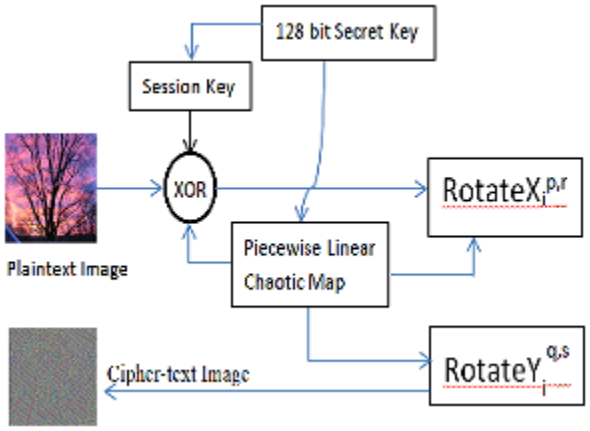


Fig. 2. Proposed Enhanced TDCEA.

V. SECURITY ANALYSIS OF ENHANCED TDCEA

In this section, we will analyze the robustness of proposed encryption technique against statistical and brute-force attacks. Based on amount of security provided by an encryption scheme, we can divide encryption schemes in to two categories: unconditionally secure and conditionally secure schemes. In unconditionally secure schemes, it is impossible for a cryptanalyst to get back the plaintext from the cipher-text generated by the encryption algorithm[12]. Except one- time pad encryption algorithm, no encryption algorithm is unconditionally secure [12]. Whereas, in conditionally secure schemes, either the cost of breaking the cipher is larger than the cost of plaintext itself or time required to decipher the cipher-text by cryptanalyst is larger than the useful time of the plaintext[12]. The security (conditionally secure) of the encryption technique will be analyzed with respect to key and plain text or input image. Any multimedia data (text, image, audio or video) can be transmitted and represented as an image. Thus security of proposed MDEA is analyzed on image.

A. Statistical Analysis

A good encryption technique should be robust against any statistical attack. In 1949 Claude Shannon gave two terminologies called *confusion* and *diffusion*, in order to thwart cryptanalysis based on statistical analysis [9]. Confusion refers to a process of making statistics of cipher text and encryption key as complex as possible so that cipher text should not give any pointer to the cryptanalyst in order to deduce the key. On the other hand, diffusion makes the statistics of plain text and cipher text as complex as possible.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

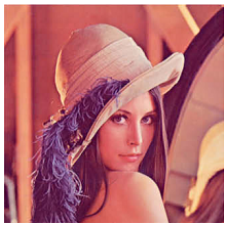
Good amount of diffusion is achieved when statistics of plaintext is dissipated into a long range of cipher text. In this section, we will do histogram analysis, correlation coefficient analysis, which measures amount of confusion created by encryption scheme and key sensitivity analysis which measures the amount of diffusion created by encryption scheme.

1) *Histogram Analysis*: A strongly secure encryption scheme must give similar cipher image for any kind of plain image. For highly secure encryption technique, histogram of encrypted image must be equalized and uniformly distributed over the entire intensity range. We have calculated and analyzed the histograms of both original images of different kinds and their corresponding encrypted images. It is clear from the figures that, histograms of encrypted images are uniformly distributed over the entire range of intensity values. Images used for histogram analyses are 24-bit bitmap color images. Shared secret key used for encryption is "wed9erjk7861knkr". Figure 3 also shows the decrypted image retrieved after applying Enhanced TDCEA in reverse order.

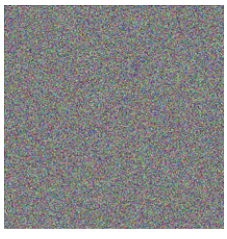
2) *Correlation Coefficient Analysis*: Correlation coefficient shows the linear relationship between two variables. Correlation coefficient between two variable or pixels can be calculated using the formula given by equation 10, where X and Y are the value of two adjacent pixels in the image and N is the total number of pixels selected for the calculation.

$$C_r = \frac{N \times \sum_{j=1}^{N}(X_j \times Y_j) - \sum_{j=1}^{N} X_j \times \sum_{j=1}^{N} Y_j}{\sqrt{\left(N \times \sum_{j=1}^{N} X_j^2 - \left(\sum_{j=1}^{N} X_j\right)^2\right) \times \left(N \times \sum_{j=1}^{N} Y_j^2 - \left(\sum_{j=1}^{N} Y_j\right)^2\right)}} \quad (10)$$

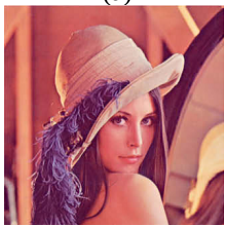
Value of correlation coefficient C_r ranges between $-1 \le C_r \le 1$. $C_r = 0$ shows that there is negligible relationship between two pixel values. The pixels of an image are highly correlated i.e. the value of one pixel can be predicted from its neighbouring pixel. Thus correlation coefficient analysis gives the measure of amount of correlation among the pixels exists in a plaintext image and encrypted image. Table 2 encloses the result of Correlation coefficient analysis of various types of input images and their corresponding encrypted images. It is clear from the table that the value of correlation coefficient between the pixels of encrypted image and original input image is approaching to zero and is uniform which shows that MDEA works well for all kind of images, irrespective of type of input image being processed.



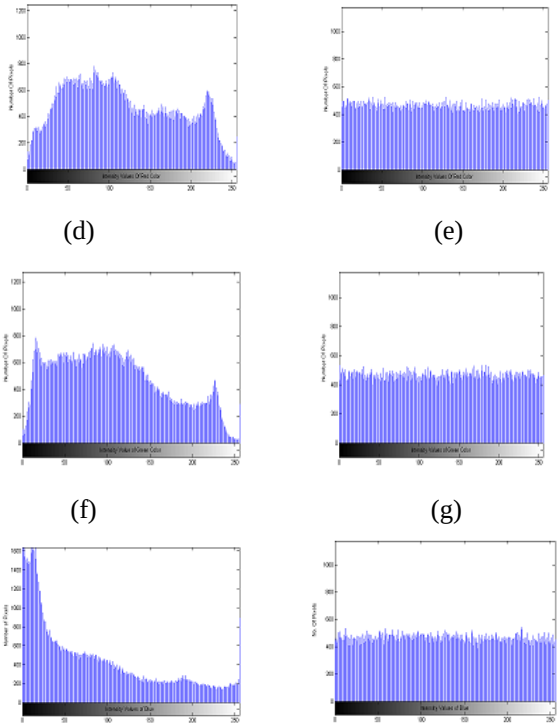
(a)



(b)



(c)



(d) (e) (f) (g) (h) (i)

Fig. 3. In figure 3, images (d), (f), (h) shows the histograms of red, green, blue components of input image lena.bmp (a). Frames (e), (g), (i) shows the histograms of red, green, blue color components of encrypted image (b), whereas image (c) shows the decrypted image.

3)*Key Sensitivity Analysis:*Key sensitivity analysis measures the amount of diffusion created by the encryption scheme. All the images are encrypted using 128-bit key "wed9erjk7861knkr". To evaluate the amount of diffusion created by MDEA, same images are encrypted using the key "wed9erjk7861knks", obtain after single bit change in the original key. Results of Key Sensitivity Analysis are tabulated in table 3. From the last column of table 3 it can be concluded that MDEA creates good amount of diffusion and changing a single bit of the key causes the entire image to be change.

4) *Key Space Analysis*: The key space of an encryption technique consists of all the possible combinations of the shared secret key. There are various approaches to attack an encryption scheme. Brute force attack is the primary attack made on the encryption scheme. Thus for a secure encryption technique, the key space must be large enough in order to make the brute-force attack infeasible. But very large key space increases the computational time of the encryption scheme. Keeping in mind the various issues of security and increasing computing power we used a 128-bit key, which gives 2^{128} possible combinations of the shared secret key and thus brute force attack can not break proposed multimedia data encryption technique using piecewise linear chaotic map with current computing power.

Table I CORRELATION COEFFICIENT ANALYSIS

S. No.	Original Image	Correlation coefficient
1.	House	0.0123
2.	Cameraman	0.0136
3.	Lena	0.0093
4.	Butterfly	0.0210
5.	Flower	0.0073
6.	Sunrise	0.0135
7.	Pepper	0.0124
8.	India	0.0014

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

VI. COMPARATIVE ANALYSIS OF ENHANCED TDCEA WITH TDCEA

Correlation coefficients obtained from Enhanced TDCEA are compared with the correlation coefficients obtained from TDCEA and results are tabulated in table 4. From the table it is clear that correlation coefficient values obtained from MDEA are uniform and thus independent of the type of image being encrypted, whereas C_r values obtained from IES are not uniform and hence it depends upon the type of image being encrypted. Moreover, C_r values of MDEA are closer to zero. Hence, based on correlation coefficients we can say that MDEA creates larger confusion and thus provides high security to all kind of images and multimedia data.

Table II
KEY SENSITIVITY ANALYSIS

S. No.	Original Image	Total number of pixels	Avg. number of pixels changed
1.	House	120000	119402
2.	Cameraman	120000	119588
3.	Lena	120000	119484
4.	Butterfly	120000	119481
5.	Flower	120000	119484
6.	Sunrise	120000	119486
7.	Pepper	120000	119480

VII. CONCLUSIONS

Security analysis of Enhanced TDCEA shows that the proposed algorithm provides very high security to multimedia data. Histogram analysis of Enhanced TDCEA shows that histograms of encrypted images are uniformly distributed throughout the intensity range and are equalized for all kinds of images. Values of correlation coefficients again show that there is less deviation between the output images obtained using the proposed algorithm. Correlation coefficients calculated for encrypted images are closer to zero as compare to the values of correlation coefficient obtained using TDCEA algorithm. Key sensitivity analysis shows that Enhanced TDCEA is very sensitive to initial conditions, which in turn are derived from shared secret key. In last we can conclude that Enhanced TDCEA is a novel approach for encrypting multimedia data.

Table IIIII
CORRELATION COEFFICIENTS OF MDEA AND IES

S. No.	Original Image	Correlation coefficient with E-TDCEA	Correlation coefficient with TDCEA
1.	House	0.0123	0.0237
2.	Cameraman	0.0136	0.0016
3.	Lena	0.0093	0.0455
4.	Butterfly	0.0210	0.0435
5.	Flower	0.0073	0.0425
6.	Sunrise	0.0124	0.0186
7.	Pepper	0.0166	0.0222
8.	India	0.0092	-0.0091

REFERENCES

[1] H. C. Chen, J. I. Guo, L. C. Huang, and J. C. Yen, “Design and realization of a new signal security system for multimedia data transmission,” EURASIP Journal of Applied Signal Processing. vol. 2003, no. 13, pp. 1291–1305, 2003.

[2] N.K. Pareek, Vinod Patidar, “Image encryption using chaotic logistic map”, Image and Vision Computing 24 (2006) 926–934.

[3] J. C. Yen and J. I. Guo, “Design of a new signal security system,” in Proc. IEEE International Symposium on Circuits and Systems (ISCAS ’02), vol. 4, pp. 121–124, Scottsdale, Ariz, USA, May 2002.

[4] J. C. Yen and J. I. Guo, “A new image encryption algorithm and its VLSI architecture,” In Proceedings IEEE Workshop on Signal Processing Systems (SiPS ’99), pages. 430–437, Taipei, Taiwan, October 1999.

[5] K. L. Chung and L. C. Chang, “Large encrypting binary images with Higher security,” Pattern Recognition Letters, vol. 19, no. 5-6, pages 461–468, 1998.

[6] N. Bourbakis and C. Alexopoulos, “Picture data encryption using scan patterns,” Pattern Recognition, vol. 25, no. 6, pp. 567–581, 1992.

[7] C. Alexopoulos, N. Bourbakis, and N. Ioannou, “Image encryption method using a class of fractals,” J. of Electronic Imaging, vol. 4, no. 3, pp. 251–259, 1995. Australia, December 2000.

[8] Li Shujun, “Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems,” IJBC, vol. 16, no. 8, pages 2129-2151, 2006.

[9] Coppersmith, D. “The Data Encryption Standard and Its Strength Against Attacks.” IBM journal Of Research and Development, May 1994.

[10] Rivest, R.; Shamir, A.; and Adleman, L. “A Method for Obtaining Digital Signatures and Public Key Cryptosystems.” Communications of ACM, February 1978.

[11] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard. "Dr. Dobb's Journal, March 2001.

[12] William Stallings, “ Cryptography and Network Security, Principles and Practices”, third edition.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.