A Novel Encryption Scheme based on Piecewise Linear Chaotic Maps for Multimedia Data

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

ABSTRACT
In recent years, many multimedia and image encryption techniques based on chaotic maps have been proposed. In this paper, we propose a novel multimedia data encryption technique called MDEA (Multimedia Data 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 proposed encryption technique and performance analysis of MDEA on various parameters of security is given in later sections of this paper.

Keywords
Multimedia, Encryption, Decryption, Multimedia Data Encryption Algorithm (MDEA), Piecewise Linear Chaotic Map (PWLCM), Image Encryption Scheme (IES).

1. INTRODUCTION
In recent years, Internet is widely used as a means to share multimedia data across the world. Almost all business activities share or transmit their multimedia data over internet. This enables the requirement of a fast and simple encryption technique, so that various illegal activities such as theft can be stopped and thus a successful secret transmission of multimedia data can be achieved. There are number of data encryption techniques available but most of them are used for encrypting text data. Another reason for need of multimedia data encryption scheme is that the size of multimedia data is very large as compared to text data and multimedia data is highly correlated. In other words large amount of data is used for very little information. Moreover, none of the existing traditional encryption schemes such as DES [9], RSA [10], and AES [11] provides very high security at high encryption speed [2] because of their complex structure and large number of iterations. Thus there is a need of an encryption algorithm for multimedia data with simple structure but should provide high security.

Basically design of all cryptographic techniques can be classified into 3-categories out of which, first two categories are, Value Transformation, and Position Permutation [1]. Third category can be derived by combining above mention two categories and hence is called combination form. Value transformation form uses transformation schemes to change the value of original data and have low computational complexity. Position permutation form changes the position of original data to generate encrypted data using some kind of permutation, but they provide low security. Whereas, combination form applies both forms, but they provides high security at low computational complexity.

Since 1992, many researchers are trying to get a new cryptosystem to remove the problems in the existing encryption techniques mentioned above. They found that properties of chaotic systems have their analogous in Cryptosystems. The chaotic maps have properties like Ergodicity, Sensitivity to initial conditions/control parameters and Deterministic Dynamics etc, whose analogous in cryptosystems are Confusion, Diffusion, Deterministic Dynamics etc. [8].

In mathematics, a function that possesses some kind of chaotic behaviour is defined as a chaotic function or map. Chaotic behaviour of the function ensures that it is highly sensitive to initial conditions or parameters. This ensures that even an infinitesimal small change in the initial conditions could result a very large or dramatic change in the behaviour of the chaotic map. As a result of this sensitivity to initial conditions or parameters, the behaviour of chaotic systems "appears to be random". Here the phrase "appears to be random" signifies that being random, the future dynamics of the chaotic system are fully defined and determined by the initial conditions or parameters, without involvement of any random element. Because of the above-mentioned property, the behaviour of the system is called Deterministic Chaos or simply "Chaos".

All chaotic systems must have following properties:

1. Sensitivity to initial conditions.
2. Topological mixing/ Ergodicity.
3. Dense periodic orbits.

In this paper, we propose a new chaotic encryption scheme based on combination form. Proposed encryption technique uses two different chaotic sequences generated by two piecewise linear chaotic maps (PWLCM). Two PWLCM are use in cascade form i.e. output from first PWLCM is an input to second PWLCM. Initial conditions for both PWLC maps are derived from 128-bit shared secret key. The process of calculating initial conditions is similar as used by pareek *et al.* [2], except for some modifications. 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, the proposed multimedia encryption technique has been discussed in detail. In section 3, security analysis of MDEA has been done. Section 4, covers the comparative analysis of proposed algorithm with other algorithm and last section concludes this paper.

2. PROPOSED MULTIMEDIA DATA ENCRYPTION ALGORITHM (MDEA)
The proposed MDEA is based on 128-bit long shared secret key, which is then divided into sixteen 8-bit session keys represented as:

$$k = k_1 k_2 .....k_{15} k_{16} \quad (1)$$

where k_i represents one 8-bit block of session key. Two PWLC maps of the form

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

(2)

are used to generate two different chaotic sequences, where p is a control parameter, whose value is in the range $0.0 \le p \le 0.7$. To calculate initial conditions for both the chaotic maps, we select eight session keys in two groups of four-session keys each. Initial condition X_0 is calculated from four session keys $k_1k_4k_7k_{10}$ as follows: Four session keys are represented as:

$$B_1=\begin{bmatrix} k_{1,1}k_{1,2}....k_{1,7}k_{1,8}k_{4,1}k_{4,2}.... \\ k_{4,7}k_{4,8}k_{7,1}k_{7,2}....k_{7,7}k_{7,8}k_{10,1} \\ k_{10,2}....k_{10,7}k_{10,8}. \end{bmatrix}$$

(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:

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

(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 $f_1f_2f_3.....f_{32}$ is generated and is converted into an integer using the equation:

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

(5)

where $k=1,2,3.....32.$

We use another four blocks of session keys i.e. $k_5k_8k_{11}k_{14}$ to calculate the initial condition Y_0 of the second PWLC map. We than calculate Y_{01} as we calculated X_{01} i.e.

$$Y_{01}=(B_2)_{10}/2^{32}.$$

(6)

where B_2 is calculated as B_1 is calculated as shown in eq. 3.

Another real number Y_{02} is calculated as:

$$Y_{02}=\left(\sum_{k=1}^{32}B_2[p_k]\times 2^{k-1}\right)\Big/2^{32}$$

(7)

where $B_2[p_k]$ denotes the value of p_k^{th} bit in binary sequence B_2. On the basis of Y_{01} and Y_{02} the initial parameter of second PWLC map is calculated as follows:

$$Y_0=(Y_{01}+Y_{02})\bmod 1.$$

(8)

Using second initial condition Y_0, we get 32 real chaotic values. Then we divide the range [0.0 to 1.0] obtained from second PWLC map, into 32 non-overlapping intervals and these intervals are grouped together in 3 different groups. Then different types of operations shown in table 1, are assigned to these groups.

We read one byte/pixel/sample from a multimedia file and then processed the byte/pixel/sample by value transformation function as shown in table1.

After encrypting 32 bytes/pixels/ or samples, we then processed them by position permutation function. Position permutation function permutes the position of byte/pixel/sample within 32 bytes/pixels/samples block with the value of byte/pixel/sample at the index in the block obtained by converting the 32 real numbers into integer values using the equation:

$$y(k)=(\text{int})(100\times y(k)) \quad (9)$$

Block diagram of MDEA is given in figure 1. After encrypting 32 bytes/pixels/samples, we modify the key according to the formula.

$$(k_i)_{10}=((k_i)_{10}+(k_{16})_{10})\bmod 256 \text{ where } 1\le i\le 15$$ and re-calculate the 32-real chaotic numbers. In this way entire file is encrypted. Entire process is repeated five times or we can say that MDEA is iterated five times on multimedia file. On further iterations of MDEA, security is not increasing as compared to increasing computational cost. Decryption algorithm of proposed encryption technique is just reverse process of the encryption algorithm i.e. first 32 bytes/pixels/sample block is reverse permuted by position permutation function and then individual byte/pixel is processed by value transformation function.

3. SECURITY ANALYSIS OF MDEA

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 ciphertext 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 ciphertext 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.

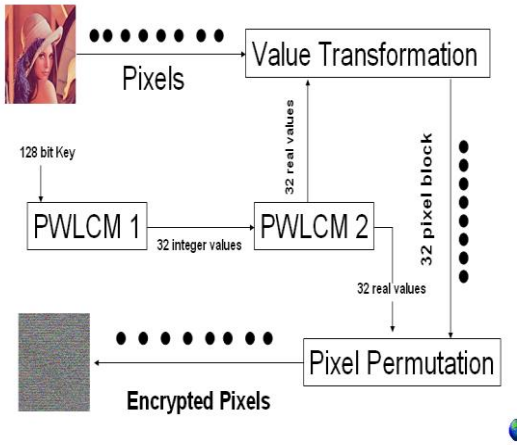


Fig. 1. Proposed Multimedia Encryption Algorithm (MDEA)

Table 1. Operations Performed in Value Transformation Function

S. No.	Value of y (k)	Encryption/ Decryption Operation
1.	(0.0-0.030), (0.10-0.13), (0.20-0.23), (0.30-0.33), (0.40-0.43), (0.50-0.53), (0.60-0.63), (0.70-0.73), (0.80-0.83), (0.90-0.93)	Encryption $C_i = P_i \oplus Key[p(k) \bmod 16]$ Decryption $P_i = C_i \oplus Key[p(k) \bmod 16]$
2.	(0.03-0.06), (0.13-0.16), (0.23-0.26), (0.33-0.36), (0.43-0.46), (0.53-0.56), (0.63-0.66), (0.73-0.76), (0.83-0.86), (0.93-0.96)	Encryption $C_i = NOT(P_i) \oplus Key[p(k) \bmod 16]$ Decryption $P_i = NOT(C_i \oplus Key[p(k) \bmod 16])$
3.	(0.06-0.10), (0.16-0.20), (0.26-0.30), (0.36-0.40), (0.46-0.50), (0.56-0.60), (0.66-0.70), (0.76-0.80), (0.86-0.90), (0.96-1.0).	Encryption $C_i = NOT(P_i)$. Decryption $P_i = NOT(C_i)$.

A. Statistical Analysis

A good encryption technique should change the statistical properties of plaintext completely. That's why many encryption techniques have successfully analyzed with statistical analysis of their ciphers. So a good encryption technique should be robust against any statistical attack. Statistical analysis of encryption scheme, which takes human readable language as the plain text, is done using frequency analysis of all individual characters and their pairs with other characters used in that language. But when input to the encryption scheme is an image, the histograms of the image and correlation coefficient between the corresponding pixels of input image and encrypted image provides the required statistics. 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. Good amount of diffusion is achieved when statistics of plaintext is dissipated into a long range of cipher text. In other words, a small change in the plain text causes a large change in the 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.

3.1 Histogram Analysis

Histogram shows the distribution of pixels in an image at particular intensity level. In image based cryptography, histograms measure the amount of confusion created by encryption scheme. Thus 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. Figure 2-6 show the examples of original input images and their encrypted images after five iterations of MDEA along with their red, green, blue color histograms. 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. Size of all images used for analyses is 400 by 300 pixels. Shared secret key used for encryption is "hjd9erjk7863knjd". Figure 2 also shows the decrypted image retrieved after applying MDEA in reverse order.

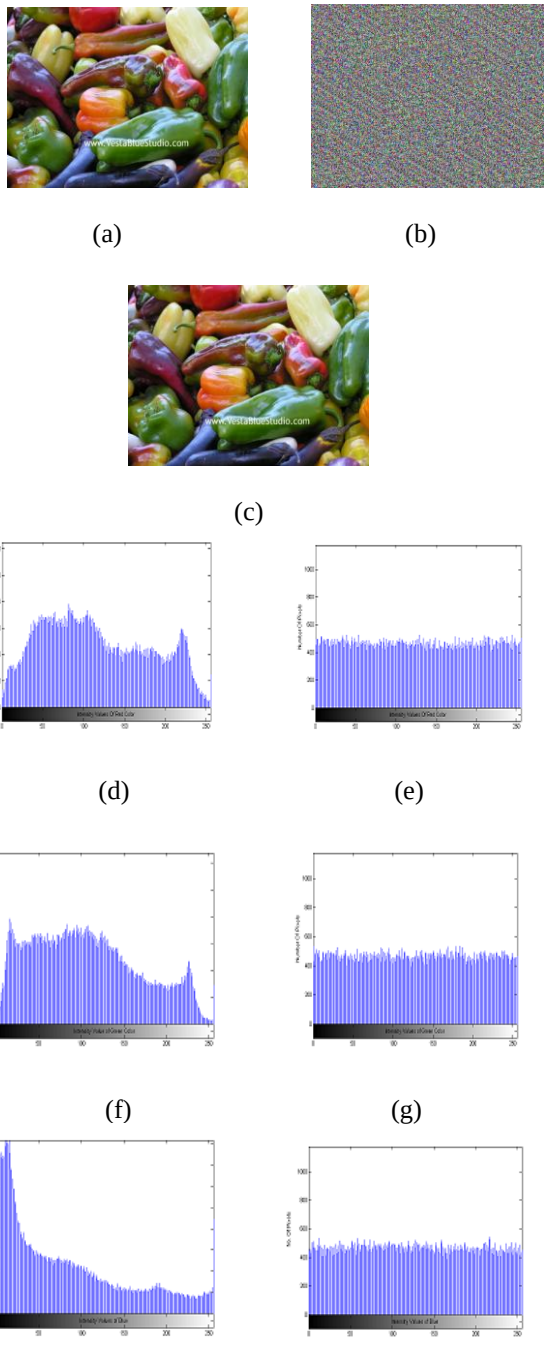
3.2 Correlation Coefficient Analysis

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.

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

(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)

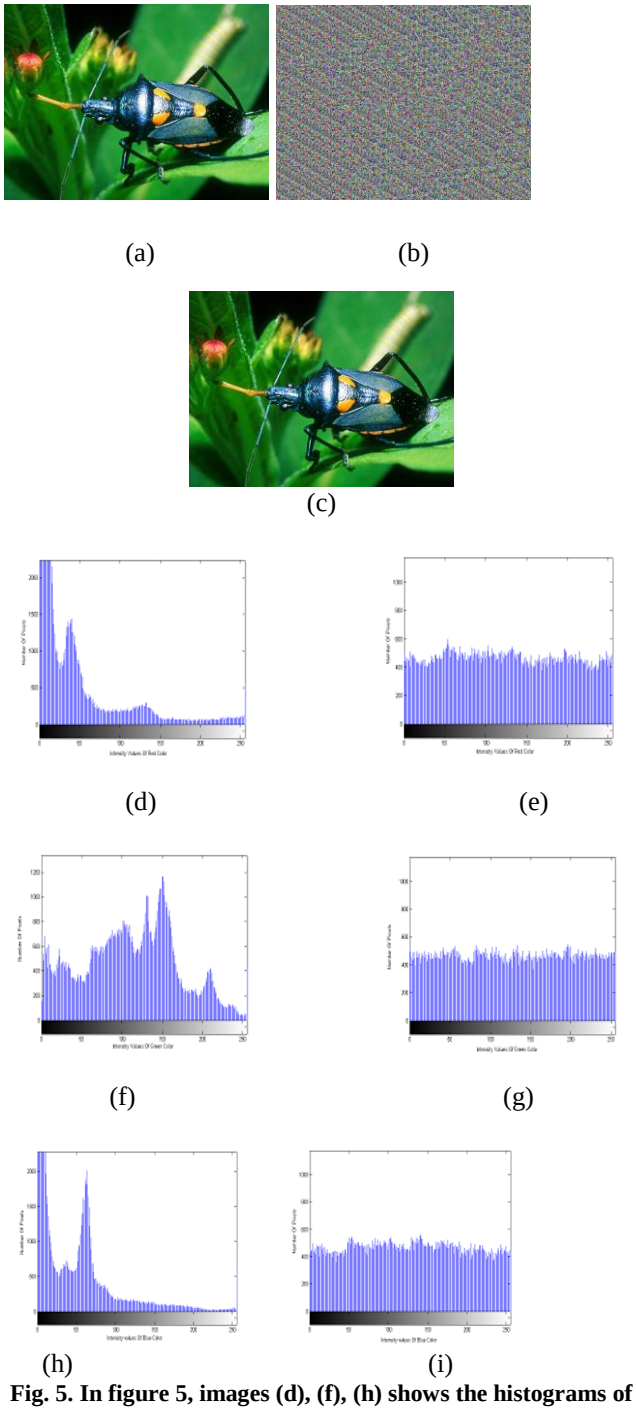
(c)

(d) (e)

(f) (g)

(h) (i)

Fig. 2. In figure 2, images (d), (f), (h) shows the histograms of red, green, blue components of input image pepper.bmp (a). Frames (e), (g), (i) shows the histograms of red, green, blue color components of encrypted image (b) after 5 iterations of MDEA, whereas image (c) shows the decrypted image



(a) (b)

(c)

(d) (e)

(f) (g)

(h) (i)

Fig. 5. In figure 5, images (d), (f), (h) shows the histograms of red, green, blue components of input image beetle.bmp (a). Frames (e), (g), (i) shows the histograms of red, green, blue color components of encrypted image (b) after 5 iterations of MDEA, whereas image (c) shows the decrypted image

3.3 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 "hjd9erjk7863knjd". To evaluate the amount of diffusion created by MDEA, same images are encrypted using the key "hjd9erjk7863knje", 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.

3.4 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 2 Correlation Coefficient Analysis

S. No.	Original Image	Correlation coefficient
1.	Aurora	0.0123
2.	Beetle	0.0136
3.	Bird	0.0093
4.	Butterfly	0.0210
5.	Peacock	0.0073
6.	Sunrise	0.0135
7.	Pepper	0.0124
8.	Flower	0.0166
9.	India	0.0092

4. COMPARATIVE ANALYSIS OF MDEA WITH IES

Correlation coefficients obtained from Multimedia Data Encryption Algorithm (MDEA) are compared with the correlation coefficients obtained from Image Encryption Scheme (IES) proposed by Pareek and Patidar 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 3 Key Sensitivity Analysis

S. No.	Original Image	Total number of pixels	Avg. number of pixels changed
1.	Aurora	120000	119452
2.	Beetle	120000	119488
3.	Bird	120000	119484
4.	Butterfly	120000	119481
5.	Flower	120000	119484
6.	Sunrise	120000	119486
7.	Pepper	120000	119480

5. CONCLUSIONS

Security analysis of Multimedia Data Encryption Algorithm (MDEA) shows that the proposed algorithm provides very high security to multimedia data. Histogram analysis of MDEA shows that histograms of encrypted images are uniformly distributed throughout the intensity range and are equalized for all kinds of images which in turn shows that output of MDEA is similar for experimented 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 after 5 iterations of MDEA are closer to zero as compare to the values of correlation coefficient obtained using IES algorithm except one or two exceptions. The reasons for this exception are not known. For less than 5 iterations, C_r values are high and for more than 5 iterations, changes in C_r values are not significant as compared to increase computation time. The proposed algorithm can further be studied to identify the reasons for the exception. Key sensitivity analysis shows that MDEA is very sensitive to initial conditions, which in turn are derived from shared secret key. Key space of MDEA is very large and thus can't be broken with brute force attack with current computing cost. In last we can conclude that MDEA is a novel approach for encrypting multimedia data.

Table 4 Correlation Coefficients of MDEA and IES

S. No.	Original Image	Correlation coefficient with MDEA	Correlation coefficient with IES
1.	Aurora	0.0123	0.0237
2.	Beetle	0.0136	0.0016
3.	Bird	0.0093	0.0455
4.	Butterfly	0.0210	0.0435
5.	Peacock	0.0073	0.0425
6.	Pepper	0.0124	0.0186
7.	Flower	0.0166	0.0222
8.	India	0.0092	-0.0091

6. 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.