IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 4, April 2016.
www.ijiset.com
ISSN 2348 – 7968

Gaussian pyramid Image and Choas based Logistic Map Techniques Using Encryption and Decryption

Dr.B. Indrani[1] **R. Bahirathy**[2]

[1]Assitant professor, Department of computer science, Directorate of Distance Education
Madurai Kamaraj university, India

[2] Lecturer, Department of Computer Applications,
Madurai Kamaraj university, India,

[1] indrani.phd@gmail.com [2] bahirathyphd@gmail.com

Abstract: This paper described for improving the level of security and secrecy provided by the digital colour and digital-based image encryption techniques. The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmit of the image based data as well as in storage. This new proposed encryption algorithm can ensure the lossless of transmissions of image using Gaussian pyramid method the proposed Encryption alogorithm in this study has been tested on some image and showed good results.

Keywords: *Encryption, Decryption, Image, Digital Image, Gaussian Pyramid, chaos, Lyapunov exponent, Key space, Logistic map, Statistical analysis, Histogram.*

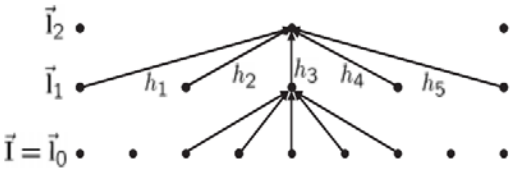
1.Introduction

In the past deanery, the security of secret digital images or video objects through a transference channel contrary anonymous attacks get again and Again care in the domain of intelligence security. The encryption algorithms such as (i) private key encryption methods- DES or Blowfish [1], (ii) public key encryption methods- RSA or El-Gamal [2] are generally not suitable in view of the slow speed of operation, complexity and disability to handle distinct data formatting. Now a day , the technique of using chaos in cryptosystems [3-16] have been examined by many researchers, because the chaotic map content the requirements of a fine cryptosystem like simplicity in implementation, sensitivity to initial conditions and parameters, high encryption rate, good security, etc. Basically, chaotic series are used to puzzle the relation between original image and encrypted image by means of modifying the pixel values and pixel position. In this paragraph we will agitate in concise some chaos based image encryption techniques informed in the literature in the recent years. In reference [3] Chenetal. proposed to convert a two-dimensional chaotic map to a three-dimensional chaotic map for image encryption by using pixel shuffling and confusing the pixel value from the original image. Two logistic maps with different initial conditions are used in image encryption in [4]. They used 80-bit secret key for the generation of starting conditions of logistic maps and eight variant types of operation for the encryption of plane image. A fast image encryption system is proposed in [5] by using chaotic sequences generated by the cascade of chaotic maps. In references [6,7] Gao et al. proposed a scheme of total shuffling of the image pixel position and then they used a hyper chaotic system to confuse the pixel value with respect to the original image. Four different third order chaotic systems are used for chaotic sequences generation and pixel shuffling for color image encryption in [8]. In reference [9] Wang and Yu proposed a block encryption technique using dynamic sequences generated by one dimensional multiple chaotic system. Recently, a chaotic block cipher scheme for image encryption based on chaotic tent map is proposed in [10]. In reference [11] Lin and Wang described image encryption algorithm based on chaos with the piecewise linear memristor in Chua’s circuit. An image encryption scheme based on chaotic discrete quadratic map and parameter perturbation technique is also described recently in [12]. However, some reported encryption algorithms [13-17] are either inefficient or weak in view of computational Complexity and strength of security. In this paper, we have proposed a novel pyramid resize scheme for image encryption based on chaotic logistic map. The proposed scheme uses logistic map with suitable starting condition for different pixel values randomly with corresponding to its initial values of the original image. Next we resize the original image using the pyramid techniques then chaotic sequences of the logistic map are applied for pixel shuffling. The proposed algorithm uses a secret key of 32 characters (256-bits) to generate the initial conditions of the logistic map. The rest of the paper is organized as follows: In section 2 to describe the Gaussian pyramid resize techniques. Section three the reality of the chaotic logistic map is described. Section 3 characteristic behavior of the logistic map encryption and decryption algorithms done step by step in section 4. Experimental results are presented in the section 5. And section 6 represented the security analysis of the proposed encryption scheme such as key space analysis, key and plane image sensitivity analysis, statistical analysis, differential analysis, bias test, quality of assurance etc. The conclusion is described in the section 7.

2.Gaussian pyramid type images

Goal of the techniques in Develop filter-based representations to decompose images into information at multiple scales, to extract features/structures of interest, and to attenuate noise. The main motivation of the image using to extract image features such as edges at multiple scales then redundancy reduction and image modelling for efficient coding, image enhancement/restoration and image analysis/synthesis

Gaussian Pyramid
Sequence of low-pass, down-sampled images $[\vec{I}_0, \vec{I}_1, \ldots, \vec{I}_N]$.



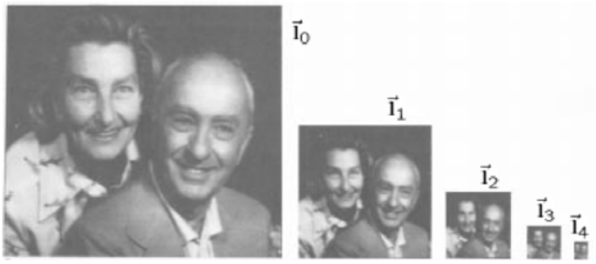
Usually constructed with a separable 1D kernel $\mathbf{h} = [h_1, h_2, h_3, h_4, h_5]$, sampling factor of 2 (in each direction): In matrix notation (for 1D) the mapping from one level to the next has the form:

$$\vec{I}_{k+1} = \mathrm{R}\,\vec{I}_k = \underbrace{\begin{bmatrix}1&0&0&0&0&\\0&0&1&0&0&\cdots\\0&0&0&0&1&\\&&\vdots&&&\ddots\end{bmatrix}}_{\text{down-sampling}}\underbrace{\begin{bmatrix}\ddots&&&\\&-\mathrm{h}-&&\\&&-\mathrm{h}-&\\&&&-\mathrm{h}-\\&&&&\ddots\end{bmatrix}}_{\text{convolution}}\vec{I}_k$$

Typical weights for the impulse response from binomial weights:

$$\mathbf{h} = \frac{1}{16}[1,\ 4,\ 6,\ 4,\ 1]$$

digital image and next four pyramid levels:



First three levels scaled to be the same size:

Properties of Gaussian pyramid _ used for multi-scale edge estimation,_ efficient to compute coarse scale images. Only 5-tap 1D filter kernels are used, _ highly redundant, coarse scales provide much of the information in the finer scales.

3.Characteristics and Behavior of the Logistic map

In novel, one actual simple chaotic map has been studied and analyzed for cryptography applications is logistic map [4,18]. Mathematically, the logistic map is written as Where x_n denote the chaotic sequence which lies between zero and one as shown in the Figure 1. The initial condition of the map is x_{n-1} x

$$f(x) = rx(1-x)$$
$$x_{n+1} = f(x_n) \qquad (1)$$

n= [0,1] .

The parameter r is a positive number in the range 0 to 4. Relying on the value of r the Eq. (1) has different properties as mention below. When r between 0 and 1 the value of $x_n = 0$ substantively of the initial conditions X_0 . When r between 1 and 3 the value of x_n steady on the value $(r-1)/r$ substantively of the initial conditions x_0. When r between 3 and 1+ 6 (approximately 3.45) the value of x_n wavering between two values forever relying on r . When r between 3.45 and 3.54 (approximately) the value of x_n wavering between four values forever. With r slendering bigger than r the value of x_n wavering between 8 values, then 16, 32, etc. This method theatrically is an example of a period-doubling cascade. At r approximately 3.57 is the onset of chaos, at the end of the period-doubling cascade. In this domain substantively variations in the initial condition yield theatrically different results over time, a prime characteristic of chaos. The values beyond 3.57 exhibit chaotic behavior, but there are still certain insulated values of r that appear to show non-chaotic behavior; these are sometimes called islands of stability. For instance, beginning at [1+√8] (approximately 3.83) there is a region of parameters r which show wavering between three values, and for differently higher values of r wavering between 6 values, then 12 etc. There are other ranges which yield wavering between 5 values etc. In this way all wavering periods do occur but over $r = 4$, the value of x_n eventually leave the interval [0,1] and x_n diverge for almost all initial values of $x0$. These variance phenomena are illustrated in Figure 2. The various region of chaos for r between 3.57 and 4 are shown in Figure 3 by plotting the Lyapunov exponents (^) with r. The phrase of the Lyapunov exponent for the origin starting at x_0 is given by

$$\Lambda = \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'(x_i)\right|\right\}. \qquad (2)$$

In this paper, we have taken the parameter r = 3.999 of the logistic map in the chaotic region having positive Lyapunov exponents as shown in Figure 3.

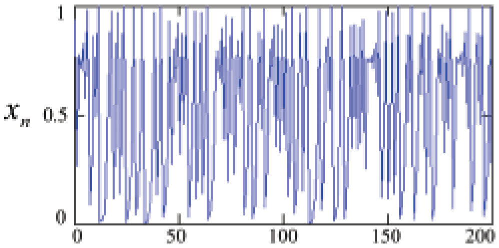


Figure 1: Variation of chaotic logistic map with iteration values.

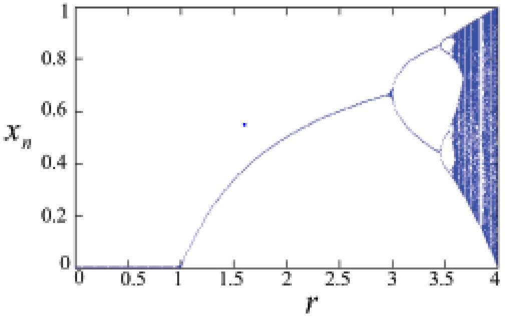


Figure 2: Bifurcation diagram of the logistic map.

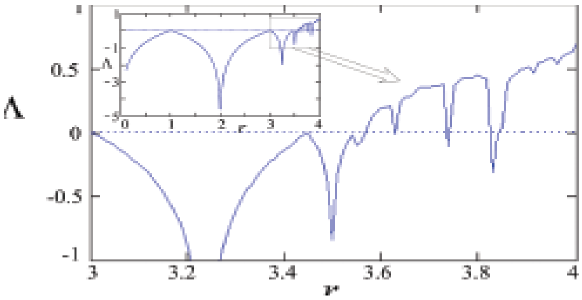


Figure 3: Lyapunov exponents of the logistic map.

4.The Proposed Image Encryption and Decryption Algorithm

The encryption algorithm includes four main steps. The first step is used to generate the original image into resizing the image using Gaussian pyramid techniques then second step we calculate chaotic sequences. Third step confused the pixel values and fourth step shuffled the pixel position to produce the required encrypted image. Let f be an image of size$M\times N$. The pixel of *f* is denoted by $f(i, j)$, where i and j is in the range of $1\leq i\leq M$ and $1\leq j\leq N$. Now, $f(i, j)$ denotes the gray value at the pixel position (i, j) of the image f. The initial condition for the logistic map is extracted from the secret key of 256 bits (32 characters) taken in ASCII form denoted as $K = K_1\ K_2\ K_3\ K_4$ ......K_{32} (K_i denotes the 8-bit key character in the i-th key position). The value of the starting condition for the logistic map is given by.

$$x_0 = \sum_{i=1}^{32} \mathrm{mod}\left(K_i \times 10^i\ ,1\right)$$

The step by step procedure of the algorithm is described below.

Step 1: Transmitting the resize image of $M\times N$ pixels into an array of $P_{i=}\{P_1\ P_2\ P_3\ P_{4\ldots}P_n\}$, where i = 1, 2, 3,……..,n and $n = M\times N$. Next convert the pixel values to unsigned integer in the range of 0 to 255 using mod operation.

Step 2: Generate n number of chaotic sequence $x_{i=\{}\ x_1\ x_2 x_{3\ldots\ldots}\ X_n$ } where i=1 2 3 ,…..n in the range 0 to 1 using the logistic
map mention in Eq. (1) with initial condition $x0$ and taking the parameter $r = 3.999$. Next convert x_i into unsigned integer in the range of 0 to 255 using mod operation.

Step 3: Generate the sequence $C_i = P_i \oplus x_i$ _ for confusing the pixel value. The sign $\ominus$ indicates bitwise XOR operation.

Step 4: Transform $C_{\ i=}\{C_{\ 1}C_2\ C_{3\ldots\ldots\ldots}\ C$ n} where i=1 2 3 , , ,n, to an array of
size $M\times N$ to get the image f' . Next add one to the unsigned integer sequence $x\ x_{i=\{}\ x_1\ x_2 x_{3\ldots\ldots}\ X_n$ } where i=1 2 3 ,…..n and transform it into an array of size $M\times N$ to get X .

Step 5: Atlast execute the following two steps for pixel shuffling to get the required encrypted image f. Here j and k varies from 1 to 255. The symbol ⇔
indicates the interchange the values between two pixel position of f'.

$$f'\left(X(j,j),k\right) \Leftrightarrow f'\left(X(j+1,j+1),k\right)$$

$$f'\left(k,X(j,j)\right) \Leftrightarrow f'\left(k,X(j+1,j+1)\right). \qquad (4)$$

Now f is the final encrypted image. The decryption of the image is the inverse process of encryption.

5.Experimental Results

5.1Experiments Stage

Experiments are done using various original images (plain images) to prove the validity of the proposed algorithm.Figures 4a–7a show four different plain images and Figures 4b–7b show their encrypted images (cipher images) using key zxcvbnmlkjhgfdsa1 234567890!@#$%x. All the encrypted images look similarly and they will carry no visual information about their plain-images. The decrypted images using the same key xcvbnmlkjhgfdsa1234567890!@#$%x are shown in Figures 4c–7c, whereas decrypted images using slender different key zxcvbnmlkjhgfdsa123456
7890!@#$%**y** are also shown in Figures 4d–7d. From

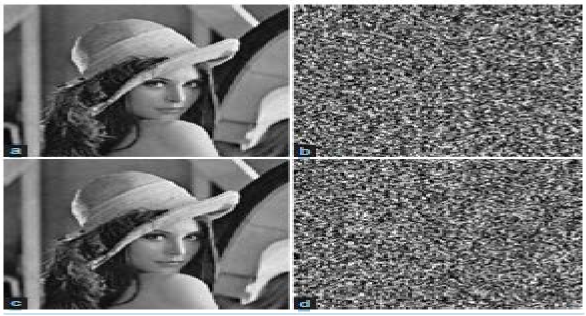


Figure 4: Application of the encryption/decryption algorithm to the image Lena: (a) Plane image; (b) Encrypted image using key zxcvbnmlkjhgfdsa1234567890!@#$%**x**; (c) Decrypted image using same key of encryption; (d) Decrypted image using wrong key xcvbnmlkjhgfdsa1234567890!@#$%**y**.

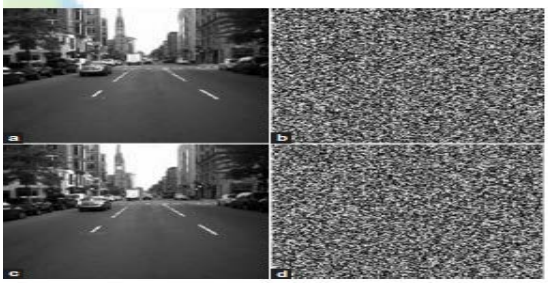


Figure 5: Application of the encryption/decryption algorithm to the image Road: (a) Plane image; (b) Encrypted image using key zxcvbnmlkjhgfdsa1234567890!@#$%**x**; (c) Decrypted image using same key of encryption; (d) Decrypted image using wrong key zxcvbnmlkjhgfdsa1234567890!@#$%**y**.

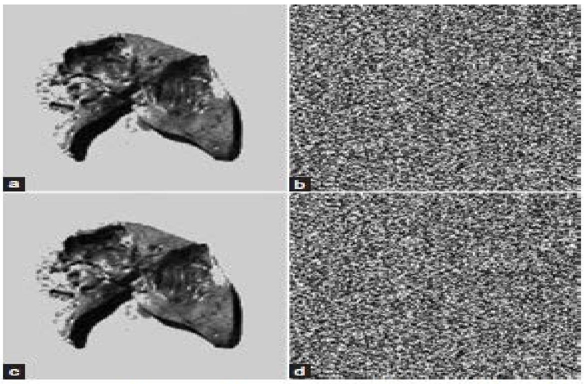


Figure 6: Application of the encryption/decryption algorithm to the image Liver: (a) Plane image; (b) Encrypted image using key zxcvbnmlkjhgfdsa1234567890!@#$%**x**; (c) Decrypted image using same key of encryption; (d) Decrypted image using wrong key zxcvbnmlkjhgfdsa1234567890!@#$%**y**.

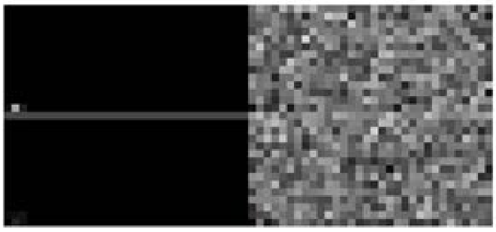


Figure 7: Application of the encryption/decryption algorithm to the image Black: (a) Plane image; (b) Encrypted image using key zxcvbnmlkjhgfdsa1234567890!@#$%**x**; (c) Decrypted image using same key of encryption; (d) Decrypted image using wrong key zxcvbnmlkjhgfdsa1234567890!@#$%**y**.

This figure it is clear that decrypted images using the wrong key will carry no information of the original images.

6. Analysis

6.1 Security Analysis

An use chaotic encryption system should be robust contrary all types of attacks such as cryptanalytic, statistical and brute-force attacks. In this section, we will discuss the security analysis of the proposed algorithm by addressing key space and key sensitivity analysis, statistical analysis, and Differential analysis. The resistance contrary various types of attacks is a available measure of the performance of a cryptosystem. Therefore some security analysis results are included in the following subsection to prove the validity of the proposed cryptosystem.

6.2 Key Space Analysis and Key Sensitivity Analysis

A good cryptosystem should have satisfactory large key space to produce the brute-force attack infeasible [19,20]. Key space simply the total number of various keys which can be applied for the purpose of encryption and decryption. The algorithm proposed in the paper uses a 32 character, i.e., 32×8=256 bits key, so that the key space is 2256, which is large satisfactory to avoid brute-force attack thus to the present compilation speed. On the other method the encryption and decryption algorithm is highly sensitive to the secret key. The transform of a single bit in the secret key should produce a completely different encrypted/decrypted image. Two encrypted images using two different keys zxcv bnmlkjhgfdsa1234567890!@#$%**x** and zxcvbnmlkjhgf dsa1234567890!@#$%**y** (these two key have only one bit different) are more than 99% different in terms of pixel values. The encrypted image cannot be decrypted correctly with a slightly different key as shown in Figures 4d–7d. This analysis examined that the algorithm of the cryptosystem is highly sensitive to the secrete key and it guarantees the security against known plain-text attacks.

6.3 Statistical Analysis

Statistical analysis is crucial importance for a cryptosystem. An ideal cryptosystem should be resistive against any statistical attack. To prove the robustness of the proposed algorithm, we have performed the following statistical test such as histogram analysis.

6.4 Histogram Analysis

Image histogram describes how the image pixels are allocated by plotting the number of pixels (along the y-axis) at each intensity level (along the x-axis). A right image encryption system should provide uniform image histogram for all encrypted images Independent the nature of the original plane image. The histogram of four different plane images like- Lena,

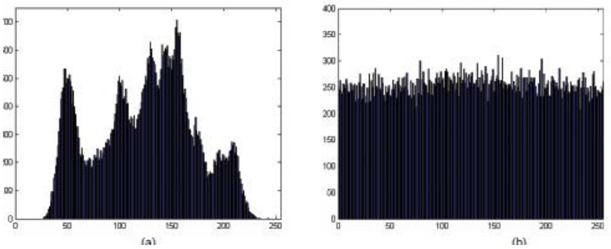


Figure 8: Histogram of the (a) Plane image and (b) Encrypted image of Lena.

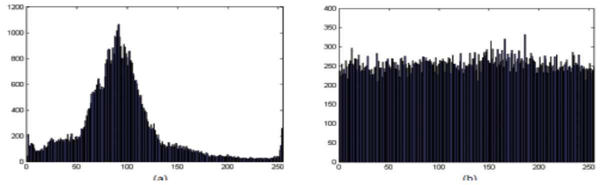


Figure 9: Histogram of the (a) Plane image and (b) Encrypted image of road.

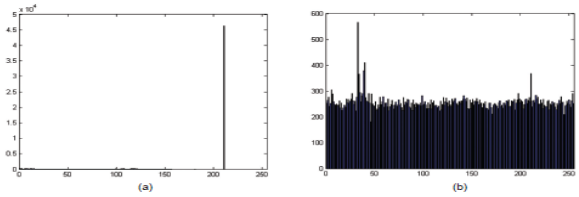


Figure 10: Histogram of the (a) Plane image and (b) Encrypted image of liver.

Road, Liver and Black are shown in Figures 8(a)–11(a). These histograms show not uniform and large spikes, which relatively to the gray values that seem more often in the plain-images. The histograms of their encrypted images are shown in Figures 8(b)–11(b) severely. Here all the spikes are almost equally allocated and important different from those of the original images. A histogram of the encrypted image suffer no statistical similarity to the plain image and hence do not give any clue to use anystatistical attack on the proposed image encryption technique.

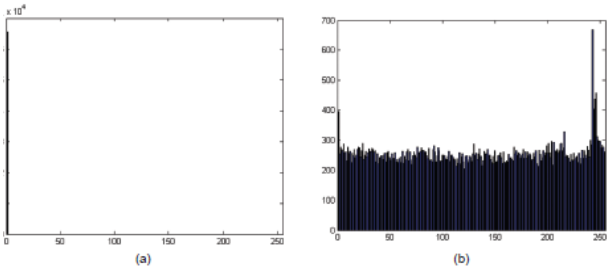


Figure 11: Histogram of the (a) Plane image and (b) Encrypted image of black.

7.Conclusions

The paper described a novel chaos based image encryption technique using Gaussian image resize method. The XOR operations and pixel shuffling of the image are provide to confuse and defuse the pixel value and pixel position. The key in the chaotic system produces the initial condition, so the security of the chaotic sequences totally rely on the secrete key. The key of the proposed cryptosystem is very large and totally secure so it can stand brute-force attack also. Moreover, key sensitivity analysis, statistical analysis, are discussed to prove the well performance of the proposed algorithm. The future enhancement we analysis the Intensity Tempering analysis, image Quality assurance test etc.,

References

[1]. B. Schneier. “Applied cryptography- protocols, algorithms and source code in C”. John Wiley & Sons, New York, 1996.

[2]. W. Stallings. “Cryptography and network security: Principles and practice”. Prentice-Hall, New Jersey, 1999.

[3]. G. R. Chen, Y. B. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat map,” Chaos, Solitons and Fractals, Vol. 21, pp. 749-61, Mar. 2004.

[4]. N. K. Pareek, V. Patidar, and K. K. Sud, “Image encryption using chaotic logistic map,” Image Vision Comput, Vol. 24, pp. 926-34, Sept. 2006.

[5]. H. S. Kwok, K. Wallace, and S. Tang, “A fast image encryption system based on chaotic maps with finite precision representation,” Chaos, Solitons and Fractals, Vol. 32, pp. 1518-29, Apr. 2007.

[6]. T. Gao, Q. Gu, and Z. Chen, “A new image encryption algorithm based on hyper-chaos,” Phys. Lett. A, Vol. 372, pp. 394-400, Apr.2008.

[7]. T. Gao, and Z. Chen, “Image encryption based on a new total shuffling algorithm,” Chaos, Solitons and Fractals, Vol. 38, pp. 213- 20, Jan. 2008.

[8]. C. K. Huang, and H. H. Nien, “Multi chaotic systems based pixel shuffle for image encryption,” Optical communications, Vol. 282, pp. 2123-7, Feb. 2009.

[9]. X. Y. Wang, and Q. Yu, “A block encryption algorithm based on dynamic sequences of multiple chaotic systems,” Commun Nonlinear Sci Numer Simulat, Vol. 14, pp. 574-81, 2009.

[10]. M. Amin, O. S. Faragallah, and A. A. El-Latif, “A chaotic block cipher algorithm for image cryptosystems” Commun Nonlinear Sci Numer Simulat, Vol. 15, pp. 3484-97, 2010.

[11]. Z. Lin, and H. Wang, “Efficient image encryption using a chaosbased PWL meristor,” IETE Technical Review, Vol. 27, pp. 318-25, Jul-Aug 2010.

[12]. D. Chattopadhyay, M. K. Mandal, and D. Nandi, “Robust chaotic image encryption based on perturbation technique,” ICGST- GVIP, Vol. 11, pp. 41-50, Apr. 2011

[13]. H. Cheng, and X. Li, “Partial encryption of compressed images and videos,” IEEE Trans. Signal processing, Vol. 48, pp. 2439-51, Aug. 2000.

[14]. Y. Mao, G. Chen, and S. Lian, “A novel fast image encryption scheme based on 3D chaotic baker maps,” Int J Bifurcation & chaos, Vol. 14, pp. 3613-24, Oct. 2004.

[15]. K. Wang, W. Pei, L. Zou, A. Song, and Z. He, “On the security of 3D cat map based symmetric image encryption scheme,” Phys Lett A, Vol. 343, pp. 432-9, June. 2005.

[16]. R. Rhouma, and S. Belghith, “Cryptanalysis of a new image encryption algorithm based on hyper chaos,” Phys Lett A, Vol. 372, pp. 5973-8, 2008.17. G. Alvarez, and S. Li, “Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption,” Commun Nonlinear Sci Numer Simulat, Vol. 14, pp. 3743-9, Nov. 2009.

[18]. A. Kanso, and N. Smaoui, “Logistic chaotic maps for binary numbers generations,” Chaos, Solitons and Fractals, Vol. 40, pp. 2557-68, 2009.

[19]. L. Zhang, X. Liao, and X. Wang, “An Image Encryption Approach Based on Chaotic Maps,” Chaos, Solitons & Fractals, Vol. 24, pp. 759-65, 2005.

[20]. G. Alvarez, and S. Li, “Some basic cryptographic requirements for chaos based cryptosystems,” Int. J Bifurcation Chaos, Vol. 16,
pp. 1-8, 2006.

[21]. Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay and Debashis Nandi1Department of Physics, 1Information Technology, National Institute of Technology, Durgapur, West Bengal, India **“**An image encryption and decryption based on chaotic logistic map”