MULTIMEDIA PROCESSING

20CYS212

DEPARTNMENT OF COMPUTER SCIENCE

(CYBER SECURITY)

PROJECT PROPOSAL

IMAGE ENCRYPTION USING CHAOTIC MAPS [Inter and Intra Block]

BY

SRIDHARAN	S	CH.EN.U4CYS21080
SRISH	N	CH.EN.U4CYS21081
VIGNESWARAN	S	CH.EN.U4CYS21090

1. Abstract:

The field of cryptography is ever growing due to digitalisation and today data insecurity for large media files like images are a major concern. Many are trying to solve this and chaotic maps are pave the path for further development in secure media encryptions. In this paper, we present an image encryption algorithm using combination of three 2D chaotic maps. The proposed scheme is based on key stream generator for confusion process. The confusion process is initiated by a secret key of 512 bits which is itself generated by 3 maps which we have selected. 'To make the cipher more dynamic against any attack, the secret key is modified after encrypting each block of the image. The experimental results show that the proposed method provides an efficient and secure way for real-time image encryption and transmission.

2. Introduction:

In recent times, with the ever-growing advances in communication technology, illegal data access has become a common passer-by in our lives. Illegal data access and loss have become more prevalent in wireless and general communication networks. Hence, Data security/protection has become very crucial and important issue. Internet, which is widely used by most of Earths' population transmits information in the form of text, media like images, videos etc. The information transmitted are mostly in the form of images these days. Image information is different from text, it has larger scale of data, high redundancy and stronger correlation with pixels. So, the reliable and efficient security method in storage and transmission of digital images is needed at present for many applications, in both public and private sector services like patient data, military information systems, medical imaging systems etc.

Chaotic maps or Chaotic sequences are random -like processes which does neither has a periodic sequence or a convergent sequence. They are more sensitive to the initial conditions using which they were generated. Chaotic secure communication systems have been developed to a certain extent and chaotic security is becoming a hotspot in research areas. The three chaotic maps we chose for this experiment are Henon Chaotic Map, Arnold Cat Map and Tent Map.

Bimolecular computing has emerged as an interdisciplinary field that draws together molecular biology, chemistry, computer science and mathematics. Our knowledge on DNA nanotechnology and bimolecular computing increases exponentially with every passing year.

3. Problem Statement

People send or transfer photos which are sensitive to another person over Internet. Digital Image is more vulnerable and prone to potential attacks. The open nature and medium of security in digital images are the reason for it. That's why many install messaging apps and social media apps have end to end encryption. To prevent unauthorized access to a transmitting image, we hide the information of the original image by using the technique called encryption. In the field like medical treatment, military affairs images need to meet the highest level of confidentiality.

Image encryption technology has become more popular and advanced as an attempt to protect the transmission of images effectively. Conventional encryption algorithms like DES, AES, IDEA etc. These might not be ideal for bulk of data and considerable redundancy among the raw pixels of the digital image. To avoid visual information leaks, a new image encryption algorithm is to be created or formulated.

4. Proposed Solution:

We propose an efficient and complex encryption algorithm based on selective chaotic maps. The proposed encryption algorithm is implemented in MATLAB for computer simulations. We have selected Arnold-cat map, Henon map and tent map as chaotic maps or sequences for the current experiment and we are planning to use Brownian movement calculation to find the initial and final positions of the pixel. We are encoding the image using a 512bit key in parts. So, at first, we will divide and encrypt the image in the form of smaller blocks and then perform henon map chaotic sequence to once again encrypt the map between blocks using boundary pixel values.

5. Literature Review

5.1. Chaotic Maps:

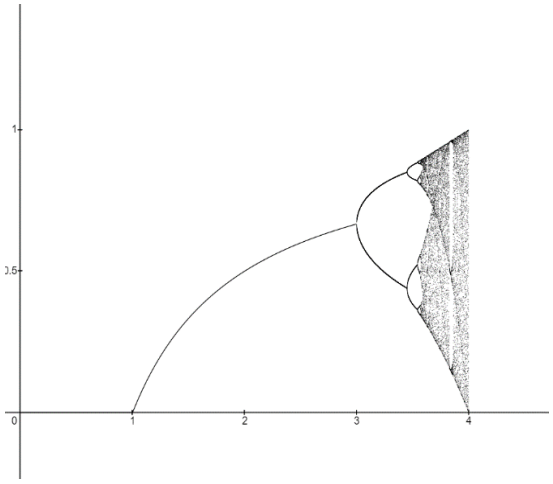
The name Chaotic map is a field of study in mathematics, where the basic dynamic systems to produce sequence of numbers that are random in nature [4]. Chaotic theory explains the relationship between totally appearing random chaotic sequence of outputs and the pattern that generates them. This sequence is used to encrypt messages. For decryption, the sequence of random numbers is highly dependent on the initial condition used for generating this sequence.

$$x_{i+1} = \mu_1 x_i(1 - x_i) + \gamma_1 y_i^2;$$

$$y_{i+1} = \mu_2 y_i(1 - y_i) + \gamma_2(x_i^2 + x_i y_i);$$

$$where\ 2.75 < \mu_1 \leq 3.4, 2.75 < \mu_2 \leq 3.45$$

The above equation is a chaotic sequence and this will generate two chaotic sequences in the region (0,1). Here $\mu_1\mu_2\gamma_1\gamma_2$ are the control parameters. There have been many image encryption algorithms based on chaotic maps like the Logistic map [5-7], the Standard map[8], the Baker map [9], the PWNLCM, the Cat map [4, 5], the Chen map [6, 8], etc. In order to improve the security performance of the image encryption algorithm, the concept of shuffling the positions of pixels in the plain-image.

Fig 5.1: 

Represents Chaotic map sequences

5.1.2. Arnold's cat map

In mathematics, Arnold's cat map is a chaotic map from the torus into itself, named after Vladimir Arnold, who demonstrated its effects in the 1960s using an image of a cat, hence the name. Thinking of the torus T^2 as the quotient space R^2/Z^2, Arnold's cat map is the transformation $\Gamma: T^2 \rightarrow T^2$ given by the formula $\Gamma(x,y) = (2x+y, x+y) \bmod 1$[3,4,5]. Equivalently, in matrix notation, this is

$$r\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ 1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ 1$$

That is, with a unit equal to the width of the square image, the image is sheared one unit up, then two units to the right, and all that lies outside that unit square is shifted back by the unit until it is within the square.

Arnold cat map is a 2d chaotic map which has two keys namely the starting pair of values for the sequence. It just encrypts the image to safeguard it without removing any detail or pixel value from it.

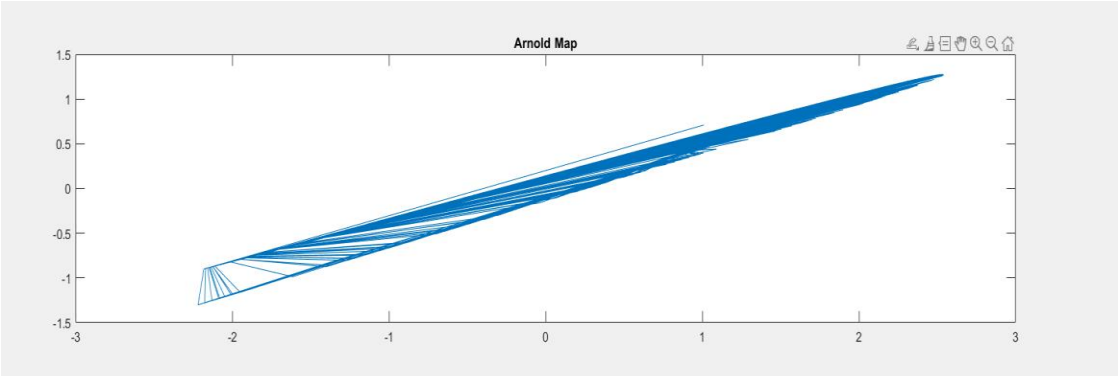


Fig 5.1.2.1: Graph plot of the Arnold cat maps' chaotic sequence.

5.1.3. Tent Maps

Tent Maps are 1d chaotic maps which are used to encrypt images using two main variables, the key (k) and the starting value of the sequence. This is a discrete dynamical system and the graph for this map is like a tent. Logistic map is a special case of tent map. The equation of the tent map is

`z(i) = k*(2*z(i-1) - 1) [4,5],` where k is the key and z(i) is the value to be updated. Initial value z0 will be given with which you can find z1 and so on.

It is bounded between 0 and 1. Any initial value in this range will remain in the same range under iterations. It is symmetric about the line y=x. There are no stable orbits or cycles.

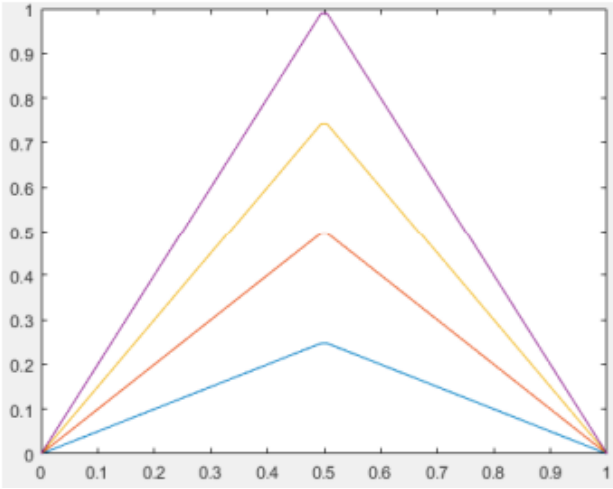


Fig 5.1.3.1: Graph for representation of tent chaotic map

5.1.4. Henon Chaotic maps

The henon chaotic maps are 2d chaotic maps which is based on discrete time dynamical system. The map was introduced as a simplified model of the Poincare section of the Lorenz model by Michel Henon.

Henon maps can be plotted as 1d and 4d plots also, in 1d plots the sequence is defines similarly to Fibonacci sequence.

x(i) = 1-a*x(i-1)^2+y(i-1);
y(i) = b*x(i-1);

This sequence has two secret keys ‘a’ and ‘b’ which will be defined at the start and then the initial values of x and y will also be given. The henon chaotic maps are random and does not remove any details or pixel value off the image. This map is very efficient and secure than logistic map and Lorenz map.

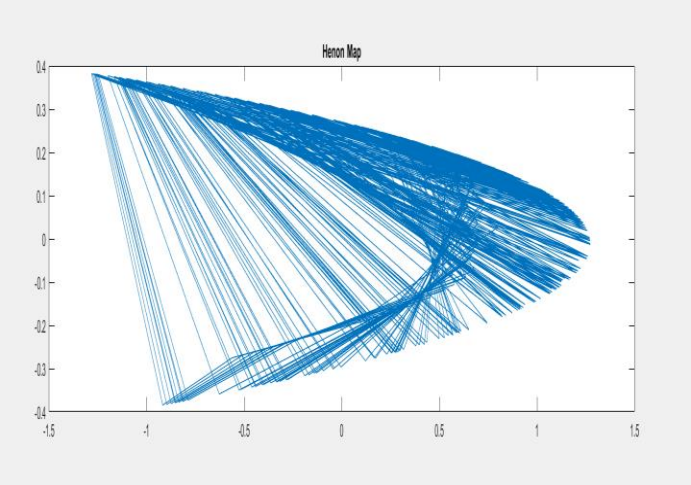


Fig 5.1.4.1: Graphical representation of henon maps

5.1.5. Brownian Movement

It is the random movement of particle i.e. (In our case pixels) from initial position to a final position. The distance between initial and final position of the pixel us calculated by using Euclidian distance formula.

Euclidian Formula:

D(x1,y1) and A(x2,y2) then distance between A and D is

Distance=$\sqrt[2]{(x1^2 - x2^2) + (y1^2 - y2^2)}$, where x and y belong to real number set.

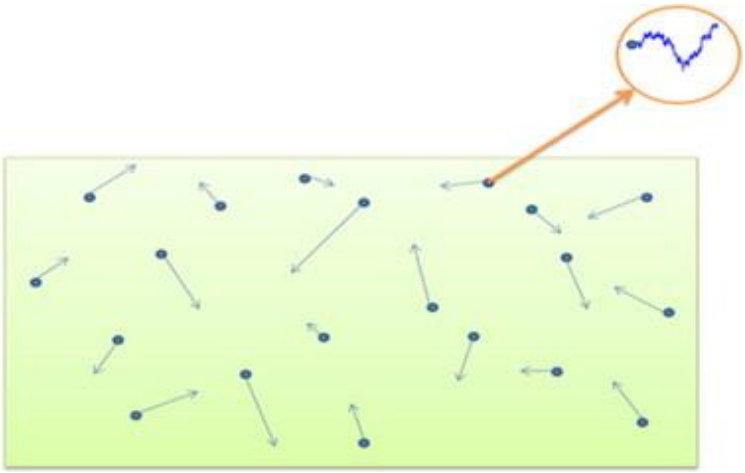


Fig 5.1.5.1: Image showing representation of Brownian movement

In our case we are finding the distance between initial position of pixel and final position of the pixel, to determine the distance the pixel moved while encryption is done.

6. Objective

Develop a MATLAB code to encrypt an Image using chaotic maps and DNA encoding. To make the encryption using chaotic maps more random and efficient for Image encryption. The DNA encoding is used to add more security to the Image and it should be used for secure transmission of images between people as we know that Images are very important data transferred between people and for example: we don't want army intelligence photos to leak or compromise as it is an important piece of information. So, creating a very efficient and secure encryption algorithm is very important and necessary in this digital world.

7. Algorithm

Step 1: Initially the image is imported using imread() function and stores in a variable.

Step 2: Then we are resizing the image to 512 x 512 using the reshape function and the reshaped input image is stored in variable image.

Step3: Another copy of the resized image is done and saved as variable img2.

Step4: Displaying the original image with its histogram plot using imshow() and imhist() functions respectively.

Step 5: Generating the chaotic sequences

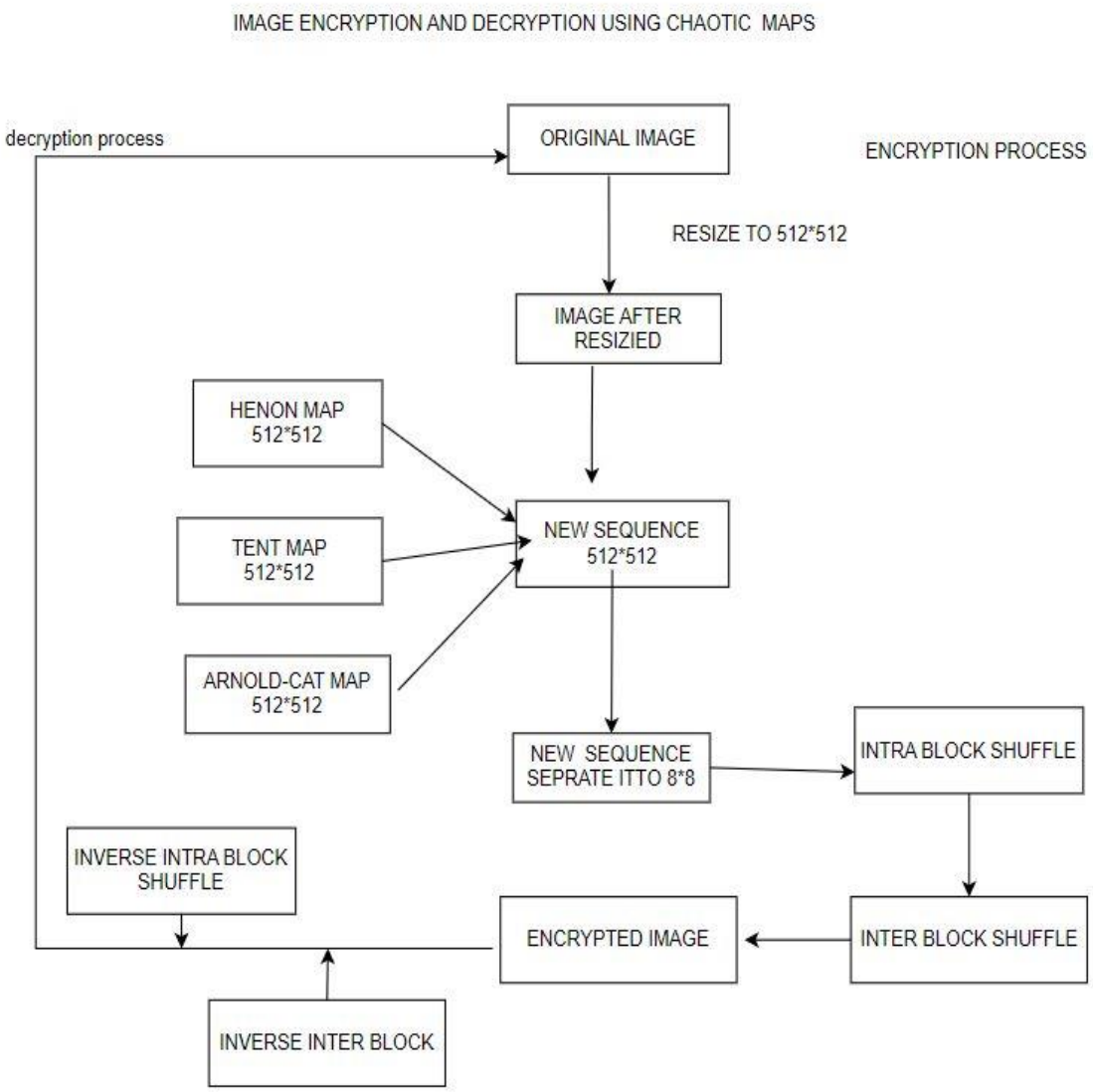
- First henon maps or chaotic sequence is generated. We have used the secret keys a=1.4 and b=0.3, then initial values of x and y are x0=0.0002 and y0=0.27.
    - x(1) = 1-a*x0^2+y0;
    - y(1) = b*x0;
- Iterating 'i' using for loop from 2 to 512 and substituting in the given formulae's:
    - x(i) = 1-a*x(i-1)^2+y(i-1);

    - y(i) = b*x(i-1);
- we get the chaotic sequence for henon maps.
- Arnold-cat maps' chaotic sequence is then generated using the formulae,
    - u(i) = [2*x(i)+y(i)]%1;
    - v(i) = [x(i)+y(i)]%1;
- Tent maps' chaotic sequence is then generated finally using the secret key k=2 and z0=0.3000567
    - z(i) = k*(2*z(i-1) - 1);
- xseq and yseq are generated to create a new chaotic sequence from the generated three chaotic sequences.
- xseq contains cipher indices for x coordinate and yseq contains cipher indices for y coordinate.
    - xseq=[xseq;x(i) u(i) z(i)];
    - yseq=[yseq;v(i) z(i) y(i)];
- first, we encrypt the cipher in blocks of 8x8 using intra shuffling method with new chaotic sequence as key.
- We create indx and indy by sorting xseq and yseq respectively. We will then use four for loops to shuffle the pixels inside an 8x8 block of the image.
- Then second function for inter block shuffling is created with corner_pixel set to [1:8:512].
- The function will check if incoming pixel is matching with corner pixel coordinated or not. If it matches then the newIndx value is swapped with indx and newIndy is swapped with indy.
- Then again four for loops are used to encrypt or shuffle the image pixels.
- Finally, you will get an encrypted image which is then passed for histogram equalisation and then displayed.

Step 7: For decryption we use the inverse of chaotic encryption. i.e., we will switch the 2 inputs and make the swap the indexes inside the encryption function to get the decryption function.

Step 8: Now, we passed the encrypted image into the decryption function. We will get the decrypted image.

8. Flow Chart



---

9. Result

This part summarizes our founding's as you can see from the above given explanation all the encryption algorithms have their advantages and disadvantages. Like that chaotic map also has its own but when comparing its advantages and disadvantages the latter does not stand out so it's used in most of the situations these days. The increase in efficiency and through output is more in chaotic maps where we can integrate two

maps. This suggests that encryption and decryption using multiple chaotic maps is safe and efficient.

9.1. Encrypted Image

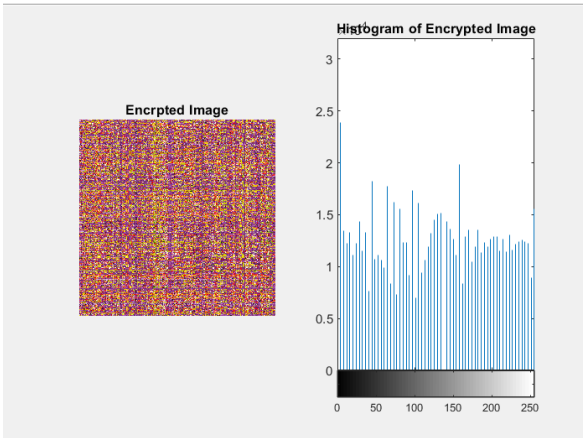


fig 9.1.1 Encrypted image

9.2. Decrypted Image

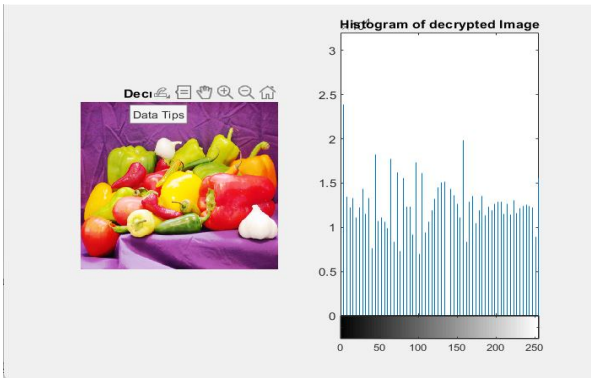


fig 9.2.1 Decrypted image

10. Conclusion

The conclusion of this report is that we are proposing an encryption algorithm using chaotic maps. The pixels are shuffled according to the chaotic character of the map chosen and then it is then complemented according another sequence of the chaotic maps.

11. References

1. [Kuldeep Singh, Komal Preet Kaur], [“Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it”], 2011, 975-8887, Volume 23.

2. Deepshikha Rathore, Anil Suryavanshi, “A proficient Image Encryption using Chaotic Map Approach”, 2016, 975-8887, Volume 23.
3. Narendra K Pareek, Vinod Patidar, Krishan K Sud, “A Random Bit Generator Using Chaotic Maps”, 2010, 32-38, Volume 10.
4. G.A.Sathishkumar, Dr.K.Bhoopathy bagan, Dr.N.Sriraam, “IMAGE ENCRYPTION BASED ON DIFFUSION AND MULTIPLE CHAOTIC MAPS”, Vol.3, No.2, March 2011.
5. Musheer Ahmad, Musheer Ahmad, “A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping”, 2009, 46-50, Volume 2(1).
6. Ashwani Gupta, Ashutosh Gupta, “IMAGE ENCRYPTION USING CHAOTIC MAPS”, 2015, 2348-7550.
7. Somaya Al-Maadeed, Afnan Al-Ali, Turki Abdalla, “A New Chaos-Based Image-Encryption and Compression Algorithm”, 2012, Article ID 179693.
8. Sudeep Nooly B, Ravindra S, “A Survey on Multidimensional Chaotic Maps and Genetic Operator”, 2022, 2321-9653, Volume 10.
9. Ramesh Kumar Yadava, Dr. B. K.Singh, S. K. Sinha and K. K. Pandey, “A New Approach of Colour Image Encryption Based on Henon like Chaotic Map”, Journal of Information Engineering and Applications, vol. 3, no. 6, 2013.
10. Qian Wang, Qiang Zhang, Changjun Zhou, “A Multilevel Image Encryption Algorithm Based on Chaos and DNA Coding”, 2009 IEEE.

11. Stallings W, Cryptography and Network Security: Principles and Practices (London,Pearson Education; 2004)

12. G Chen, Y Mao and C K Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitions & Fractals,21(3),749-761, 2004.

13. chiaraluce F, Ciecarelli L, et al, A new chaotic algorithm for video encryption, IEEE Trans Consum Electron, 48, 838-843, 2002.

14. DingWei, QiDongxu, “Digital image transform, information hiding and camouflage technique”, Journal of Computers, 21, 838-843, 1998.

15. A Shamir, How to share a secret, Communications of ACM, Vol. 22,612-613, 1979.

16. M Noar, Visual cryptography, proceeding of Eurocrypt, 441-449, 1994.

17. C Zhenfu, A threshold key escrow based on public key cryptosystem, Science in China (Series A),44, 441- 448, 2001.

18. C E Shannon, Communication theory of secrecy systems, Bell System Technical Journal, 28,656- 715,1994.

19. Chaos Mathematics, December 2001, Citing Internet sources URL http://library.thinkquest.org/3120/text/math.htm.

20. J Fridrich, Symmetric Ciphers Based on Two-Dimensional Chaotic Maps, International J. Bifurcation and Chaos, 8(6), 1998.

21. J Fridrich, Image Encryption Based on Chaotic Maps, Proceeding IEEE Conference on Systems, Man, and Cybernetics,1105-1110, 1997.

22. M Salleh, S Ibrahim, I F Isnin, Enhanced Chaotic Image Encryption Algorithm Based on Baker's Map, IEEE Conference, 508-511, 2003.

23. A Sinha and Kehar Singh, A technique for image encryption using digital signature, Optical Communications,229-234, 2003.

24. R Blahut, Theory and Practice of Error Control Codes, Addison Wisley, Reading, MA, 1983.

25. Y Li, L Yuanxiang, X Xuewen, Image Encryption Algorithm Based on Self-Adaptive Symmetrical coupled Toggle Cellular Automata, Congress on Image and Signal processing, 32-36, 2008.