International Journal of Computer Applications (0975 – 8887)
International Conference on Futuristic Innovations and Challenges to Diversity Management Emerging Technologies and Sustainability for Inclusive Industrial Growth (ICFIDM 2014)

Enhancing Image Security using Chaotic Map and Block Cipher

Irene Getzi S.
Asst. Professor, Dept. of MCA
Jyoti Nivas College Autonomous
Bangalore,India.

Minu Prabhakaran E.K.
V Semester MCA
Jyoti Nivas College Autonomous
Bangalore,India.

Niviya C.N.
V Semester MCA
Jyoti Nivas College Autonomous
Bangalore,India.

ABSTRACT
We live in the era of information explosion and have witnessed the trend of leveraging cloud-based services for large scale content storage, processing, and distribution. Data security and privacy are among top concerns for any business environments. As more and more security breaches happening all over the world in different forms as a threat to the information industry, the end user should have the protection and privilege of secured access. Chaos possesses many interesting properties, such as deterministic but random like complex behavior, high sensitivity to initial conditions and system parameters and long term unpredictability. This paper introduces a cellular automata based chaotic encryption scheme and the results are comparable with well-known AES block cipher algorithm.

Keywords
Chaotic encryption, Cellular automata, AES Block Cipher, image encryption, symmetric key cryptography

1. INTRODUCTION
Cryptography deals with protection of data. It can be acquired by Public Key Cryptography or Secret key Cryptography. One of the challenges in cryptography is to generate random number key or nonce for use each use. Many crypto system uses pseudo-random numbers that are generated by recursively solving a mathematical equation from a given 'seed or initial value' thus it is vulnerable for any attacker that the seed value can be easily traced.

In Chaos based system, even very simple rules can lead to extremely complex and unpredictable behaviour. In recent years many chaos-based image cryptosystems are proposed. Pankesh Bamotra developed an algorithm for grayscale images which consisted of shuffling of sub-matrices of the grayscale images based on the depth of the encryption technique. It is based on conversion of grayscale images to sub matrices of grayscale values which are of random order. The random order is retained and determined as the secret key which then passes over the network to the receiver. The level of security is very much less [1]. Rakesh S, Ajitkumar A Kaller, Shadakshari B C and Annappa B proposed a multilevel encryption algorithm where concept of uniform scrambling, row, column and block based image shuffling is used to reduce correlation. On the shuffled image, the encryption algorithm based on chaotic maps is performed. Although this paper has better level of security, it consumes more time to shuffle the pixel positions and then generate chaotic maps [2]. Yunpeng ZHANG, Wenquan LV, Renjie ZHAO, Ding YUdeveloped an algorithm for image scrambling and gray change; this is based on the chaotic system and two encryption schemes are combined organically, making the effect of encryption better, which meets the higher standard in security[3]. Somaya Al-Maadeed, Afnan Al-Ali, and Turki Abdalla proposed a method for the selective encryption of an image combined with a compression method [4]. When encryption process is applied to the whole image, it was difficult to improve the efficiency.

John Conway proposed a theory 'Game of Life' based on simple set of rules that forms the basis for the new field cellular automata. The game of life is played on a grid, divided into cells. Each cell can be "alive" or "dead" and a set of four rules determine whether any given cell will live, die, or be born in each iteration. The game's simple set of rules brought rise to surprisingly complex and compelling behavior. Even a complex cellular-automata simulation can be determined from the starting state of cells on the grid and if the initial cells are arranged the same way, the results will always be the same after a set number of generations. If one single cell was different in the starting configuration, after sufficient generations, the state of every cell would eventually be different. Though deterministic, the information represented by the cells of a cellular-automata simulation is not generated through reversible, logical mathematical algorithms and this truly random nature can be used to encrypt data and can be decrypted if we know the initial configuration.

This paper presents a chaotic based encryption scheme based on cellular automata and the results are compared with popular AES algorithm. The work is implemented in .net frame work and analyzing the images created with the PSNR value.

2. ENCRYPTION METHODS USED
The cellular automata theory is used to build a chaotic based cryptographic scheme, by choosing an arrangement of cells on a grid, a set of rules, and an agreed number of generations. The initial arrangement of cells and the number of generations forms key for the encryption. The rid of cells forms the sequence of binary digits by choosing "alive" for true, and "dead" for false. The result is then XORed with the data to encrypt; since the pattern of data does not repeat, nor follow logical mathematical progressions this procedure produces a secure cryptographic system.

Chaotic Encryption Algorithm using Cellular Automata
Step 1: Input the image and select encryption seed value

Step 2: Design a cellular automata simulation by creating a basic cellular grid (CA)

Step 3: Add two sets of rules ; the Conway's original set of four rules for game of life and Fredkin rule which is based on whether the number of living neighbour cells is odd or even

Step 4: Initializing the Grid ; The grid width and height are set to the same dimensions asthe original image, and the selected seed value is passed to a random number generator to create a dynamic bitmap by randomly setting each cell to be 'alive' or 'dead'.

Step 5: The resultant key is XORed with image to produce the encryption

AES Algorithm

Step 1: Do the following one-time initialization processes

- Expand the 16 byte key to get the actual key block to be used.
- Perform one time initialization of the 16 byte plain text block
- XOR the states with the key block

Step 2: For each round perform the following:

- Apply S-box to each of the plain text bytes.
- Rotate row k of the plain text block by k bytes.
- Perform a mix column operation where four bytes of every column are mixed in linear fashion. This step involves shifting left and XOR with the round result. These provide both confusion and diffusion.

The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. The PSNR is calculated based on the original image and decrypted images obtained from the chaotic algorithm and the AES algorithm.

3. IMPLEMENTATION AND RESULTS

In this work we have used the C# windows application for the analysis and visualization of the experimental data. The standard dimension of image of size 256*256 is used for the result analysis been selected for the encryption and decryption of the image. The application followed a thread approach and progress notification which will be useful for the images having much higher size.

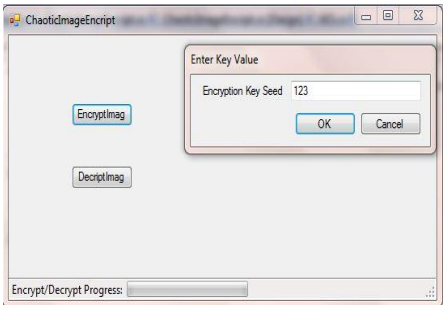

Figure 1: Implementation of Chaotic Algorithm

Chaotic algorithm is basically done by an XOR with the stream byte of the input image. To generate the unique key we follow the cellular automatic pattern as described earlier. For the implementation concept we are creating the grid which is having the 8 cells in one rows and each cell have 1bit of data. Using the seed value entered we are creating a random number between 0 and 1 the we are checking if the random number generated is greater than 0.5 then the active state is modified as 1.After the execution we have done the FredKin Rule which described as below. Looping through each cell 100 times, to find out the living neighbors' and calculating the mode by 2, based on the remainder if 0 then set the next set of the cell as 0. In each iteration do a commit, and swap the bits in active state with the next state.

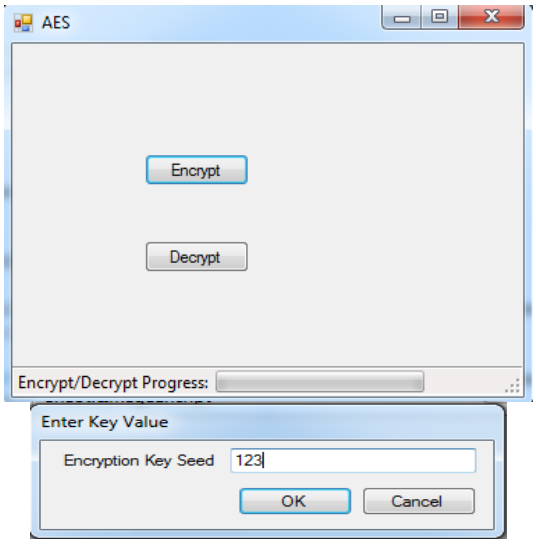

Figure 2: Implementation of AES Algorithm

The AES algorithm is implemented through the built-in function available in the .net package and the PSNR value is calculated. The implementation and the results obtained in chaotic and AES encryption is given below. Both the algorithms provide high PSNR value and are almost equal and the difference is less than 1%. The result shows that the performance of cellular automata is almost equivalent to AES encryption procedure in terms of the quality of the image but a bit slower than AES. Steps can be taken to further improve the speed of cellular automata based chaotic encryption.

Figure 4 (a) : Original Image

4 (b) : AES_decrypted **4 (c) : Chaos _decrypted**

4. CONCLUSION

The prevalence of multimedia technology in the society has promoted digital images and videos to play a more significant role than the traditional texts, which demands a serious protection of users' privacy. Currently the chaos based scheme was designed for still images. The chaos based image encryption scheme can be applied to moving images and

video as well. This paper can be extended to create a secure channel to transfer the images from the client to the server by the software itself.

In this paper, two different techniques are applied on images among these techniques and cellular automata based chaotic encryption algorithm performs close to the well-studied AES algorithm and thus can be considered for better security since it provides better random behavior. Efforts can be taken to improve its speed by using parallel approach. Variations to cellular automation can be considered such as having an interactive seed to have better security.

5. REFERENCES

[1] Pankesh et al., Image Encryption Using Pixel Shuffling, International Journal of Advanced Research in Computer Science and Software Engineering 2(12),December - 2012, pp. 279-282

[2] Rakesh S, Ajitkumar A Kaller, Shadakshari B C and Annappa B, Multilevel Image Encryption, cryptography and security Journal, Cornell University, 2012.

[3] Yunpeng ZHANG, Wenquan LV, Renjie ZHAO, Ding YU, Research On Image Encryption Algorithm Based on Wavelet Transform, International Journal of latest research in science and technology, *2013.*

[4] Somaya Al-Maadeed, Afnan Al-Ali, Turki Abdalla, A New Chaos-Based Image-Encryption and Compression Algorithm, Journal of Electrical and Computer Engineering, Volume 2012 (2012), Article ID 179693.

[5] Dr. Vivek Sharma, Hariom C. Agnihotri, Chetan H. Patil An Image Encryption and Decryption Techniques Using Two Chaotic Schemes, International Journal of Research in Advent Technology, Vol.2, No.2, February 2014 .

[6] Monisha Sharma et. al., Image Encryption Techniques Using Chaotic Schemes: A Review , International Journal of Engineering Science and Technology, Vol. 2(6), 2010, 2359-2363 2010.

[7] Xiaopeng Wei — Bin Wang — Qiang Zhang — Chao Che, Image Encryption Based On Chaotic Map And Reversible Integer Wavelet Transform, Journal of ELECTRICAL ENGINEERING, VOL. 65, NO. 2, 2014, 90–96.

[8] Nidhi Sethi et.al, Novel Method of Image Encryption Using Logistic Mapping, International Journal of Computer Science Engineering (IJCSE), 2012.

[9] Shuiping Zhang, Huijune Luo, Journal of Multimedia, Vol 7, No 1 (2012), 66-73, Feb 2012, doi:10.4304/jmm.7.1.66-73

[10] Abir Awad, Abdelhakim Saadane, The Research of Image Encryption Algorithm Based on Chaos Cellular Automata, Proceedings of the World Congress on Engineering 2010 Vol IWCE 2010, June 30 - July 2, 2010, London, U.K.

[11] Alireza Jolfaei, Abdolrasoul Mirghadri, An Image Encryption Approach Using Chaos And Stream Cipher, Journal of Theoretical and Applied Information Technology, © 2005 - 2010 JATIT & LLS.

[12] Marina Jeaneth Machicao, Anderson G. Marco, Odemir M. Bruno, Chaotic Encryption Method Based on Life-Like Cellular Automata, Mathematics (Symmetric key) and Number Theory (AsymarXiv:1112.6326v1, [math.DS] , Dec 2011.