Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Image Encryption using Cellular Automata

Akshay Chamoli, Jawed Ahmed, Mohammad Afshar Alam, Bhavya Alankar

Department of Computer Science, Jamia Hamdard, New Delhi
Email: akachamoli@gmail.com

An optimal image encryption model has been suggested using a diffusion model based on cellular automata. First the test or original image pixels are mixed with randomly generated sequences based on intertwining logistic map. Then a shuffling engine is used to permute the pixel positions. Further, Cellular Automata based diffusion models are carried out. The main advantage of using cellular automata is that it is impossible to decode the original data without having information about cellular automata, its procedures and the set of rules used in the model. The test results obtained from the proposed model are efficient in numerous test scenarios. Resistivity against differential and statistical attacks, broader key space and brute force attack resistance makes the proposed model a better scheme.

Keywords: Encryption; Decryption; Cellular Automata; Shuffling; Intertwining Logistic Map; Confusion and Diffusion.

1. Introduction

Due to increased dependency in digital technology, huge data is produced, stored and relocated over the communication channel. So, there is a need for the security of data. Recently, more trusted, robust and secure platforms have emerged. Newly several image encryption models have been suggested. Due to low sensitivity, high correlation between neighboring pixels and huge capacity of data, many data encryption models have not been used. There are some other limitations like higher complexity, type of data, computing power and speed of operation. On the other hand, chaos-based encryption models have good randomness properties, are more sensitive to initial conditions, faster implementation, good confusion and diffusion and various control parameters are relevant for encryption of image. Recently various image encryption models have been used like Chen's system, Logistic map, 2-D cellular automata, Intertwining logistic map and others. One can generate encryption keys using any of the symmetric encryption models based on a chaotic dynamical system. Other keys and sub keys were deduced using the same chaotic dynamical systems. In literature, various chaotic dynamical systems and their advantages have been discussed. Logistic map-based encryption algorithms have been proposed in various models. Various issues like blank windows, uneven sequence distribution and stable windows have been found in logistic maps. It may lead to the origin of

the Intertwining logistic map which disables the strengths of logistic map [1]. An efficient image encryption model has been suggested using the techniques of cellular automata with intertwining logistic map. For the security enhancement, the model proposed uses both confusion and diffusion models. To make the system more sensitive with reference to initial condition, random numbers are being generated with the help of intertwining logistic map.

2. Cellular Automata

Von Neumann proposed the self-replication theory in relation with cellular automata. It is used for different robots. Cellular automata manifest dynamical behavior due to the presence of few discrete parameters like space and time. Some set of conditions have been used as rules to govern the behavior of CA. Rule consists of logical conditions which derive the next state of a particular cell while taking into consideration the neighborhood of the current cell. In literature, various rules were discussed and defined to allocate the neighborhood of a cell. Von Neumann, 3-neighbourhood and Moore's neighborhood are some rules to define the neighborhood. The following set of equations were used to define the cellular automata.

3. SECRET KEY GENERATION

The secret key (K), 128 bit long is randomly generated and involved with proposed encryption model. The secret key is utilised in various processes like matrix generation, shuffling and diffusion and also being used in the model. The key used is distributed into various sub keys i.e., sixteen that are further used to derive various parameters to be used in encryption processes. The range of sub keys are between 0-255. The following algebraic relation is used to generate various parameters and sub keys [3].

$K = KEY\ (8 \times i + 1)\ to\ KEY\ (8 \times (i + 1))\ i$

Here, $i \in (0 - 15)$,initial condition and various control parameters are computed in the following manner.

$$x_1 = \frac{K_1 + K_2}{K_3 + K_4} \bmod 1$$

$$x_2 = \frac{K_5 + K_6}{K_7 + K_8} \bmod 1$$

$$y_1 = \frac{K_9 + K_{10}}{K_{11} + K_{12}} \bmod 1$$

$$y_2 = \frac{K_{13} + K_{14}}{K_{15} + K_{16}} \bmod 1$$

$$z_1 = \frac{K_1 + K_5}{K_{11} + K_8} \bmod 1$$

$$z_2 = \frac{K_{10} + K_{15}}{K_2 + K_7} \bmod 1$$

$$S_1 = \frac{K_2 + K_6}{K_{12} + K_9} + 112 \mod 255$$

$$S_2 = \frac{K_3 + K_7}{K_{13} + K_1} + 123 \mod 255$$

$$S_3 = \frac{K_4 + K_8}{K_{14} + K_5} + 139 \mod 255$$

$$S_4 = \frac{K_{14} + K_9}{K_{11} + K_4} + 159 \mod 255$$

In the above equations (3-8), the values of the parameters generated between 0 and 1. Then in equations (9-12), scaling factors were computed and calibrated to be used in other processes [4].

SHUFFLING ENGINE

To permute the pixels, shuffling engine is used in a way that it hides any statistical information about the test image. Shuffling of each array was carried out multiple times. In each run, the last value becomes the initial condition for the next iteration. In each run, all the values are generated between 0 and 1 which are further updated using scaling factors s1 and s2.

The Logistic Map is shown as below:

$x_{n+1} = r\ x_n\ (1- x_n)$

Here, variable r represents control parameters and xn indicates the initial value generated from the secret key. Shuffling engine shuffles the array in the following ways.

Step 1: First, two arrays (q1 and q2) of equal lengths are generated in the range 1 to 256.

data about a secret key [6].

Step 2: Then, ith value of q1(i) is indexed and the corresponding value of q(q1(i)) is noted.

Step 3: Elements of q(q1(i)) are exchanged with q(q2(i)). Therefore, every element of q gets shuffled as q1(i) = q2(i).

Step 4: Repetition of steps 2 and 3 for the complex array.

Step 5: To achieve two tier shuffling steps 1 to 4 are repeated two times. Finally, a shuffled array is achieved.

INTERTWINING LOGISTIC MAP

Intertwining logistic map [5] is expressed mathematically as:

$x_{n+1} = [\mu \times k_1 \times y_n \times (1 - x_n) + Z_n\ ]\ MOD\ 1$

$y_{n+1} = [\mu \times k_2 \times y_n + Z_n \times\ (1 + x^2)\ ]\ MOD\ 1$

$Z_{n+1} = [\mu \times (k_3 + y_{n+1} + x_n\ ) \times\ \mathrm{Sin}(Z_n)]\ MOD\ 1$

Here $\mu \in (0 \text{ and } 3.9)$, $k_1 > 33.5$, $k_2 > 37.9$ and

$k_3 > 35.7$.

DIFFUSION PROCESS

Diffusion is a process which is used to conceal statistical properties in the test image in a way that even small change reflects more than fifty changes in the generated cipher or vice versa [7]. Ii = [(Ii $\oplus$ Ii-1) + [CAi × F mod 256] $\oplus$ Ii+1] mod 256 ,Here i ∈ (1, M × N × 3), Ii (present pixel), Ii-1 (earlier pixel) and Ii+1 (following pixel) of the test image. CAi (CA including ith key stream) and F denotes the scaling factor. The Diffusion process has the ability to improve the mathematical features of the test picture and secure the model resistant from known attacks.

ENCRYPTION PROCESS

The Encryption method is presented in Figure 1.

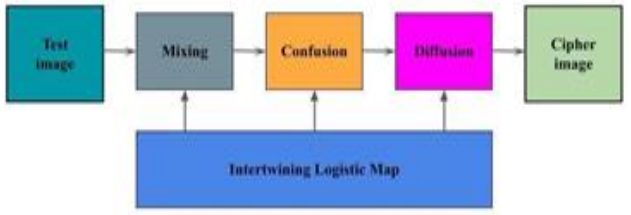

Figure 1: Encryption Process

It is carried out in the following ways: First, the test image is arranged into a linear array.

- Then, the generated linear array image is mixed with the random number generated using the Intertwining Logistic map.
- The next step is shuffling, helps in the reduction of correlation among neighboring pixels.
- Finally, Confusion and diffusion processes are applied for making the model efficient against the differential and statistical attacks.
- Then a cipher image is generated and for the recovery of the original image, the process of decryption is in the exact opposite manner of the process of encryption.

4. RESULTS AND DISCUSSION

The proposed image encryption model has been tested for various security assessment parameters like differential attacks, NPCR and UACI scores, key sensitivity and brute force attacks [8].

Brute Force Resistance: In this type of attack, all the possible key combinations are used to find out any relation. A smaller length of key can be distributed using this process. A bigger length of key needs complex computing and takes a larger time. In this paper the model proposed, a secret key of 128-bits has been used which is immune to brute force attacks [9].

Histogram analysis

Distribution of pixels is represented by histogram. Statistical attacks should be resistive against the proposed model and for that uniformly distribution of the cipher's histogram. Cipher generated using the proposed algorithm underwent histogram analysis and pixel distribution found to be distributed uniformly as shown in Figure 2(a-f). Uniform distribution makes the model resistive because the chances for recovery of the original image from cipher becomes very complex [10].

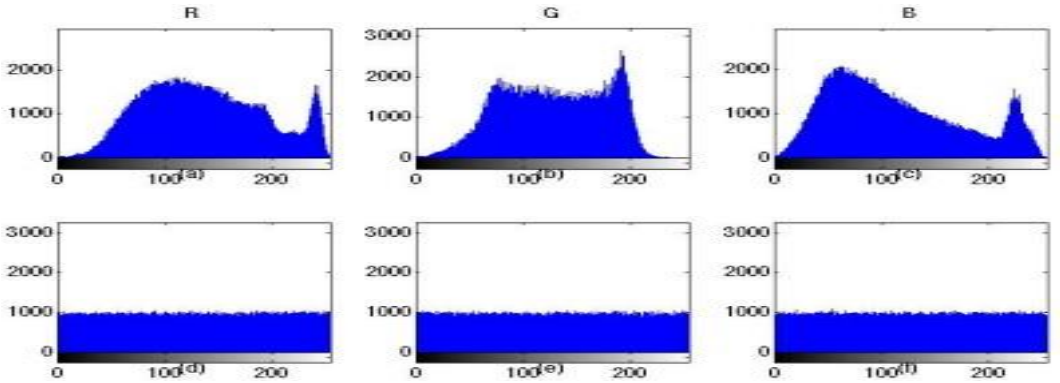

Figure 2: Represents plain and cipher images histogram for analysis

Correlation analysis:

The calculation of resistance for cellular automata with the help of correlation analysis based on the properties of diffusion models. To obtain a safe correlation coefficient among the nearby pixels the approximation value should be almost 0. The parameter r_X represents correlation coefficient.

Differential Attack: NPCR and UACI parameters are used for the analysis of cipher images. The difference among the pixels for the in the cipher images is analyzed.

$$\text{NPCR} = -\frac{\sum_{i,j} DI(i,j)}{M * N} * 100\%$$

$$\text{UACI} = \frac{\sum_{i,j} \frac{CI(i,j) - CI'(I,J)}{255}}{M * N} * 100\%$$

CI and CI' are cipher images with one bit pixel difference.

if

CI (i; j) = CI'(i; j)

then DI (i; j) = 0

Otherwise

DI (i; j) = 1

Table: Results

Types of Chaotic Map	Cellular Automata	Intertwining Logistic Map
NPCR	99.67	99.61
UACI	33.42	33.33

5. Conclusion

An image encryption model with dynamic key and Cellular Automata based dynamic systems emerges with the better results. Cellular Automata has been used to achieve better randomness in the model. With the help of secret keys, sub-keys and control parameters, a higher degree of chaotic behavior has been achieved. Sensitivity of the model has been validated with respect to change even for a single bit in secret key or plaintext. The secret key length is 128-bits, so it resists brute force attacks.

References

1. M. Boyraz, E. Çimen, M. Güleryüz, Z. Yıldız, A chaos-based encryption application for wrist vein images, CHAOS Theory. Appl. 3 (2021) 3–10.
2. N. Pareek, V. Patidar, K. Sud, Cryptography using multiple one dimensional chaotic maps, Communications in Nonlinear Science and Numerical Simulation 10 (7), 2005, pp. 715-723.
3. X. Chai, X. Fu, Z. Gan, Y. Lu, Y. Chen, A color image cryptosystem based on dynamic dna encryption and chaos, Signal Process. 155(2018)44–62, https://doi.org/10.1016/j.sigpro.2018.09. 029.
4. G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, I.J. Bifurc. Chaos 16 (2006) 2129–2151, https://doi.org/10.1142/S021812740601 5970.
5. W. Zhou, X. Wang, M. Wang, D. Li, A new combination chaotic system and its application In a new bit-level image encryption scheme, Opt Laser. Eng. 149(2022), 106782,
6. Cao C, Sun K, Liu W. A novel bit-level image encryption algorithm based on 2d-licm hyper chaotic map. Signal Process2018;143:122–33. doi:10.1016/j.sigpro.2017.08.020.
7. Zheng JM, Zeng QX. The unified image encryption algorithm based on a composite chaotic system. Multimeda Tools App 2022.https://doi.org/10.1007/s11042-022-134 61.
8. X.-Y. Wang, Z.-M. Li, A color image encryption algorithm based on hopfield chaotic neural network, Opt Laser. Eng. 115 (2019) 107–118, https://doi.org/10.1016/j.Optlaseng.2018.11.010.
9. Wu Y, Zhou YC, Saveriades G, Agaian S, Noonan JP, Natarajan P. Local Shannon entropy measure with statistical tests for image randomness. Inform Sci 2013;222: 323–42.
10. Zhou S, Wang XY, Zhou WJ, Zhang C. Recognition of the scale-free interval for calculating the correlation dimension using machine learning from chaotic time series. Physica A 2022;588:126563.
11. Ye G, Huang X. An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing 2017;251:45–53. doi:10.1016/j.neucom.2017.04.016.
12. Kumar, Vimal, and Rakesh Kumar. "A cooperative black hole node detection and mitigation approach for MANETs." In Innovative Security Solutions for Information Technology and Communications: 8th International Conference, SECITC 2015, Bucharest, Romania, June 11-12, 2015.

13. Kumar, V., Shankar, M., Tripathi, A.M., Yadav, V., Rai, A.K., Khan, U. and Rahul, M., 2022. Prevention of Blackhole Attack in MANET using Certificateless Signature Scheme. Journal of Scientific & Industrial Research, 81(10), pp.1061-1072.
14. Kumar, V. and Kumar, R., 2015. An adaptive approach for detection of blackhole attack in mobile ad hoc network. Procedia Computer Science, 48, pp.472-479.
15. Kumar, V. and Kumar, R., 2015, April. Detection of phishing attack using visual cryptography in ad hoc network. In 2015 International Conference on Communications and Signal Processing (ICCSP) (pp. 1021-1025). IEEE.
16. Kumar, V. and Kumar, R., 2015. An optimal authentication protocol using certificateless ID-based signature in MANET. In Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3 (pp. 110-121). Springer International Publishing.