Cryptanalysis of an Image Encryption System Based on Cellular Automata

Ying LIU *

Chongqing Jiaotong University, Chongqing 400074, China

***Abstract* — In recent years, much efforts have been made to utilize Cellular Automata, CA, for cryptography due to its intrinsic nature of simple infrastructure and complex behavior. A CA-based image encryption system was presented by Chen et al. in [20-22]. Although it outperforms some traditional cryptosystems in speed and key size, we find that it is defective and vulnerable to chosen-plaintext attack. We propose some minor modifications and further investigate their effects on the security and performance of the cipher.**

Keywords - Cellular automata; encryption; decryption; cryptanalysis

I. INTRODUCTION

Cellular automata (CA) were first introduced by von Neumann and Ulam as simple models to study the growth of crystals and the problem of self-replicating systems. A number of modular components called cells are arranged in the form of a regular lattice structure and make up of the topology of CA. Along with the executing of local rule, the state of a cell may evolve within a finite set according to the previous states of its neighbors as well as itself. Despite of the simple construction of cellular automata, they always exhibit highly complex behavior. Therefore, it attracted much concerns in the community of computable theory, mathematics, theoretical biology, microstructure modeling and information security [1-5].

In a 2-D square space of $N \times N$ cells, the specified cell $C(i, j)$ with its immediate North, South, West and East cells form the von Neumann neighborhood. If we denote the state of cell $C(i, j)$ at stage t by $v_{i,j}(t)$, the dynamics of each cell can be expressed as

$$v_{i,j}(t+1) = f_{i,j}(v_{i-1,j}(t), v_{i+1,j}(t), v_{i,j}(t), v_{i,j-1}(t), v_{i,j+1}(t)) \quad (1)$$

where $f_{i,j}(\cdot)$ is a Boolean function for two-state CA and defines the rule. Since the cellular automata were always constructed on a finite grid, the universe would be a rectangle instead of an infinite plane. In order to deal with the cells on the edges, we may assign null or periodic boundary conditions to them. In null boundary configurations, the boundary cells are assumed to have 'null' (logic '0' or a fixed value as an extended version) dependency. While the periodic boundary is one in which the extreme cells are adjacent to each other [6]. The local rules applied to each cell can be either identical or different. These two possibilities are termed as uniform and hybrid CA respectively [7]. Practically, we may expect to realize Eq. (1) by XOR gates in hardware for simplicity and flexibility. Thus it can be simplified as

$$v_{i,j}(t+1) = C_0 \oplus (C_1 v_{i-1,j}(t) \oplus C_2 v_{i+1,j}(t) \oplus C_3 v_{i,j}(t) \oplus C_4 v_{i,j-1}(t) \oplus C_5 v_{i,j+1}(t)) \quad (2)$$

which is an affine function in Galois field GF（2） and corresponds to 1-bit programmable additive CA (PACA).

As complexity models, cellular automata were can be employed as tools for cryptography. The first cryptographic scheme using cellular automata went back to middle eighties when Wolfram proposed the CA as a pseudorandom bit generator [5,8]. In [9], Nandi et al. devised a class of block and stream ciphers in terms of the group property of CA. Gutowitz [10] and Guan [11] also used CA to design the public-key cryptography. For further interest, a thorough reading of [12-18] and the references therein is advised. Such persistent efforts about CA-based cryptography are owing to two essential reasons. One is that cellular automata which is a simple structure can generate pseudorandom patterns. The other is that cellular automata can be efficiently implemented by VLSI and do parallel computing [19].

Recently, a novel image security system based on the replacement of the pixel values using recursive cellular automata substitution is presented by Chen et al. [20-22]. [20] and [21] focus on the architecture design and hardware implementation of the new image cryptosystem. The authors have accomplished simulations of the re-configurable 2-D von Neumann 16×16 CA by CANDENCE tools and have also implemented the circuit synthesis using the SYNOPSYS tools with the TSMC 0.18um cell-library. From the perspective of algorithm, [22] reconstructed and improved the system with more iterations performed. Although they thought that the proposed progressive CA encrypted substitution satisfied both confusion and diffusion properties and had a great potential for image encryption, we have found that it is insecure. We also give some minor modifications that do not thoroughly change the structure of the cryptosystem and investigate their contributions to the security and performance of the cipher.

The remaining of this paper is organized as follows. In Section 2, we describe the CA-based image encryption system. The approach to break the cipher is subsequently presented in Section 3. Section 4 makes some attempts to

improve the function of the system while conclusions are drawn in Section 5.

II. IMAGE SECURITY SYSTEM BASED ON RECURSIVE CELLULAR AUTOMATA SUBSTITUTION

The basic idea of the proposed image encryption/ decryption method is to change the pixel values by data reformation and CA substitution. Symmetric key of the cryptosystem is composed of four parts, i.e. data reformation key, GCAT-type selection key, CA key and iteration key. The data reformation key has two bits that are used to reformat the data of the image sequence $A(k,l)$, where $0 < k < M$ and $0 < l < N$ for a $M \times N$ image, as 4-bit (002), 8-bit (012), 16-bit (112) or 32-bit (102). The 3-bit GCAT-type selection key is used to select a particular type of GCAT which will be discussed later. The CA key is used for a chosen CA rule number, initial data, boundary conditions and linear permutations to generate a CA key stream for CA substitution. While the iteration key is used to repeat the encryption process with specified times to obtain a more random encrypted image [22]. Once the reformation key was selected, the size of CA is thus decided. Based on the determined CA configuration, we repeat the CA encryption/decryption scheme several times as below.

Initially, we use the CA key with $(6+n)+N^2+4N+n_\omega$ bits to assign a specific CA evolution. The first $(6+n)=\left(6+\lceil 2\log_2 N\rceil\right)$ bits are rule-controlled data that specify CA rule numbers, according to the size of CA. The next N2 bits are initial data denoting the initial conditions. While the following 4N bits indicate the boundary conditions. After T evolutions, a $T \times N$ N-bit generalized CA sequence is thus obtained. It is obvious that such a sequence have $(T \times N)!$ possible permutations.Since $(T \times N)!$ may be a huge number, we use only $n_\omega = \log_2(T \times N) = \log_2 T + \log_2 N = n_T + n_N$ bits to represent and generate a specific permutation, called a linear permutation. Notably, n_T bits and n_N bits are used to specify the time step and location, respectively, of the starting point for retrieving the $T \times N$ N-bit generalized CA data to generate a new sequence of N-bit CA data for encryption and decryption [22].

Represent the reformatted sequence of N-bit input data as $F(i)$, $0 \le i \le L_1 - 1$, and the sequence of N-bit CA data as $CA_p(i)$, $0 \le i \le L_1 - 1$, we define the recursive CA-encrypted substitution:

CA encryption:

$$\begin{cases} E(0) = F(0), \\ E(i) = [F(i) + GCAT(E(i-1), CA_p(i))] \bmod 2^N, 1 \le i \le L_1 - 1. \end{cases} \quad (3)$$

$GCAT\ (E(i-1), CA_p(i))$ means that $E(i-1)$ and $CA_p(i)$ execute the generalized CA transform. The general form of GCAT can be expressed as

$$GCAT\,(E(i-1), CA_p(i)) = \begin{cases} ((E(i-1)+L_S) \oplus CA_p(i)) \bmod 2^N, \\ \overline{((E(i-1)+L_S) \oplus CA_p(i))} \bmod 2^N, \end{cases} \quad (4)$$

where $0 \le L_s \le 2^N - 1$ are values of level shift. The logic operation $\oplus$ can also be replaced by multiplication as in [21], and we will investigate its contribution to attack resistance in Section 4. Since 3-bit type selection key were used to specify the type of GCAT, [22] selected only six optional GCATs in simulation as below:

Type 1:

$$EXOR\ (E(i-1), CA_p(i)) = E(i-1) \oplus CA_p(i), \quad (5)$$

Type 2:

$$NEXOR\ (E(i-1), CA_p(i)) = \overline{E(i-1) \oplus CA_p(i)}, \quad (6)$$

Type 3:

$$ALU\_1(E(i-1), CA_p(i)) = ((E(i-1)+128) \oplus CA_p(i)) \bmod 2^N, \quad (7)$$

Type 4:

$$ALU\_2(E(i-1), CA_p(i)) = \overline{((E(i-1)+128) \oplus CA_p(i))} \bmod 2^N, \quad (8)$$

Type 5:

$$ALU\_3(E(i-1), CA_p(i)) = ((E(i-1)+1) \oplus CA_p(i)) \bmod 2^N, \quad (9)$$

Type 6:

$$ALU\_4(E(i-1), CA_p(i)) = \overline{((E(i-1)+1) \oplus CA_p(i))} \bmod 2^N, \quad (10)$$

Recursive CA decryption algorithm is just the inverse procedure of encryption. Based on the same CA sequence and GCAT type, plaintext can be exactly retrieved via CA decryption until the number of iterations is reached:

CA decryption:

$$\begin{cases} D(0) = E(0), \\ D(i) = [E(i) - GCAT(E(i-1), CA_p(i))] \bmod 2^N, 1 \le i \le L_1 - 1. \end{cases} \quad (11)$$

Several simulations were performed to test the properties of the CA-based image encryption system in [20-22]. Experiment results indicated that the performance of the proposed system was superior to that of RC4, Triple-DES and AES, since it has shorter keys as well as shorter CPU encryption/decryption time. Chen et al. also claimed that it was perfectly secure in the sense of confusion property, diffusion property and complicated cryptanalysis. Nevertheless, we further find that the proposed cryptosystem is vulnerable to chosen-plaintext attack as given in next section.

III. CHOSEN-PLAINTEXT ATTACK

With Kirchoff's principle, the cryptanalyst knows exactly the design and the operation of the cryptosystem under study except the secret key [23]. In order to determine the key that was used, one can capitalize on any procurable plain and cipher text. Though cryptanalyst can yield no information by observing the coded image because of the system's secrecy, key materials may still be deduced by exploring the relation between raw data and encrypted data.

Consider the four parts which constitute the secret key, data reformation key is most essential since it determines the size of input data and scale of CA. One essential defect of the recursive CA-encrypted substitution is that, no matter how many iterations are performed, the first N bits of the plaintext are invariable as in Eq. (3). Therefore, for any plain/cipher text pair, we only have to check their identical prefix to find out the reformation key. However, false positive (i.e. the false results which appear to be valid in current step) may occur when $E_n(1) = F(1), E_n(2) = F(2), \cdots, E_n(k) = F(k)$ ($1 \le k \le 7$) for some specific $F(k)$ (for example, $GCAT(F(0), CA_p(1)) = 0$) or iteration numbers n (for example, $n = 2^N$). Under these circumstances, we can investigate some other plain/cipher text pairs or inspect its feasibility when deducing other key parts to rule it out.

Assume that the GCAT-type selection key is known, the GCAT can thus be expressed as $GCAT(E(i-1), CA_p(i)) = (\hat{E}(i-1) \oplus CA_p(i)) \bmod 2^N$, where $\hat{E}(i-1) = (E(i-1) + L_S) \bmod 2^N$ or $\hat{E}(i-1) = ((2^N - 1) \oplus (E(i-1) + L_S)) \bmod 2^N$ in terms of whether bit inversion is operated. For any plaintext $F(0), F(1), \cdots$, we have ciphertext $E_n(0), E_n(1), \cdots$ after n iterations. Since $E_r(0) = F(0)$ ($1 \le r \le n$) is fixed for each iteration, the next ciphertext $E_n(1)$ is definitely achieved:

$$E_n(1) = (F(1) + n(\hat{E}(0) \oplus CA_p(1))) \bmod 2^N. \quad (12)$$

To deduce the iteration key, we choose another plaintext $F'(0), F'(1), \cdots$, where $\hat{E}'(0) = \overline{\hat{E}(0)}$. Since $\overline{\hat{E}(0)} \oplus CA_p(1) = \overline{\hat{E}(0) \oplus CA_p(1)}$, the sum of ciphertext $E_n(1)$ and $E_n'(1)$ can be written as

$$E_n(1) + E_n'(1) = (F(1) + F'(1) + n(2^N - 1)) \bmod 2^N \quad (13)$$

Then $n = k2^N + (F(1) + F'(1) - E(1) - E'(1)) \bmod 2^N$ ($k = 0,1,\cdots$) is derived, here the span of k is very limited because the number of iterations must be small enough to consistent with system efficiency.

Put n into equation (12) and solve the congruence expression of first degree according to Theorem 1, we further obtain the value of $CA_p(1)$.

Theorem 1. For any positive integer m and integer a that satisfy $(a, m) \mid b$, the solutions of congruence expression

$$ax \equiv b (\bmod\ m) \quad (14)$$

are

$$x \equiv \frac{b}{(a,m)} \cdot \left(\left(\frac{a}{a,m} \right)^{-1} (\bmod \frac{m}{(a,m)}) \right) + t \frac{m}{(a,m)} (\bmod m) \quad (15)$$

where $t = 0,1,\cdots,(a,m) - 1$ and (a,m) is the greatest common divisor of a, m.

Until now, multiple groups of GCAT type, iteration numbers and $CA_p(1)$ are achieved. However, since there are few groups in amount, we can check their correctness using other plain/cipher text pairs to find out the valid one.

According to the parity of iteration numbers, we then decode the rest of CA sequence.

Without loss of generality, we assume that $CA_p(1), CA_p(2), \cdots, CA_p(i-1)$ ($2 \le i \le L_1 - 1$)

are known before we calculate $CA_p(i)$. For any plain/cipher text pairs, the i th ciphertext $E_n(i)$ can be expressed as a combination of arithmetic and logical operations:

$$E_n(i) = (F(i) + \hat{E}_1(i-1) \oplus CA_p(i) + \cdots + \hat{E}_n(i-1) \oplus CA_p(i)) \bmod 2^N. \quad (16)$$

It is obvious that (16) is a nonlinear equation in one variable $CA_p(i)$. If n is odd, it has a unique solution.

Representing the k th bit of $\hat{E}_1(i-1)$, $(E_n(i) - F(i)) \bmod 2^N$ and $CA_p(i)$ as a_r^k, b^k, CA^k respectively, let

$c^k = \sum_{r=1}^{n} a_r^k$ and P^k be the k th carry bit of , we have relationship of t $\hat{E}_1(i-1) \oplus CA_p(i) + \cdots + \hat{E}_n(i-1) \oplus CA_p(i)$ h e parameters in Table 1 in terms of odd n.

Table I. Relationship among P^k, c^k, b^k and CA^k

P^k	c^k	$n - c^k$	b^k	CA^k
0	even	odd	0	0
0	even	odd	1	1
0	odd	even	1	0
0	odd	even	0	1
1	odd	even	1	1
1	even	odd	1	0
1	even	odd	0	1
1	odd	even	0	0

Therefore, $CA_p(i)$ can be figured out through the pseudocode in Table 2 as follows.

Table II. Decode $CA_p(i)$

```
Initialize P = 0
For k = 1,2,⋯,N
Determine CA^k according to P^k, c^k, b^k as in Table 1
If CA^k = 0
P ← P + c^k 2^(k-1)
else
P ← P + (n − c^k)2^(k-1)
```

When n is even, the for ementioned method is infeasible and there are multiple solutions. If N is small, brute force attack can be considered to calculate $CA_p(i)$. However, the size of CA scales up to 32 dimensions. As a result, we also recur to chosen-plaintext attack and rule out the false positives the same as determining the unique reformation key.

Choosing plaintext $F(0), F(1), \cdots, F(i)$ ($2 \le i \le L_1 - 1$) such that $\hat{F}(0) = CA_p(1)$, $\hat{F}(1) = CA_p(2), \cdots, \hat{F}(i-1) = 0$, we have

$$E_n(i) = (F(i) + nCA_p(i)) \bmod 2^N. \quad (17)$$

Then $CA_p(i)$ is achieved by Theorem 1.

Gaining the CA sequence is equivalent to obtaining the CA key. Nevertheless, we can go even further.

First, we perform the reverse linear permutation to generate a $T \times N$ N-bit sequence starting from the specific time step and location and rearrange it into T $N \times N$ -bit planes of CA evolution. Then we solve the affine function (2) and check the consistency between bit planes. If there are more than one inconsistency, the bit planes are adjusted by cycling N bits as a stream of $T \times N \times N$ bits. Else, the rule-controlled data and specific time step and location are thus achieved. At last, we can plainly deduce the initial configurations and boundary conditions to complete the CA key. In fact, we do not have to decode all CAP(i) on account of the procedure mentioned above.

It is worth noting that the number of plain/cipher text pairs we choose depends on the parity of iteration numbers n. In addition, some arbitrary plain/cipher text pairs are also used. Since different scale and algorithm may concern, the complexity of cryptanalysis varies in terms of the secret key.

IV. DISCUSSION ON MODIFICATIONS

We discuss some minor modifications to the image cryptosystem and study their effects.

Any modifications on CA sequence generator are insignificant since they are not conducive to secure CAP(i). Using non-affine CA together with affine CA may improve the difficulty to deduce the rule-control data. Nevertheless, the truth table can still be derived from enough bit planes.

In GCAT, the XOR operator can also be replaced with multiplication. Hence the generalized CA transform (4) degenerates to arithmetic operation. Under this circumstance, though all $E_n(i)$ can be expressed as a linear congruence equation, we can not use the method in Section 3 to deduce iteration numbers n any longer. Fortunately, the range of n is quite limited considering the length of iteration key and system efficiency. Therefore, we can exhaustively inspect n and rule out all the false positives as before.

Introducing a random initial vector (IV) as the first plaintext is another modification. Meanwhile, the ciphertext

$E_n(IV)$ must be encrypted afterwards, or else it will expose the IV because $E_n(IV) = IV$. Since IV is different for distinct plaintexts, the reformation key is thus secure. Though the options of CA size and iteration numbers are very restricted and it seems possible to decode the parameters N, n and $CA_p(1)$ via brute force attack if N is small, we however can not eliminate the false positives on account of the one-off initial vector.

At last, we consider about permuting the cipher text $E_r(0), E_r(1), \cdots, E_r(L_1 - 1)$ $(1 \le r < n)$ after each iteration. In this instance, one ciphertext can be affected by any plaintext and CA data $CA_p(i)$. So, our proposed attack does not work anymore. And it's a compromise between security and system efficiency.

V. CONCLUSION

In this paper, a fundamental defect of the image cryptosystem based on the replacement of the pixel values using recursive cellular automata substitution is found, and a novel chosen-plaintext attack scheme is presented. For various secret keys, the attacks may be different in the number of chosen plain/cipher text pairs as well as the algorithm. We also discussed some minor modifications and investigated their contributions to the security and performance of the cipher. However, even if they are resistant to our proposed attack, careful cryptanalyses must also be conducted by the cryptographic community before the application.

ACKNOWLEDGEMENT

The paper is subsidized by The national natural science foundation Project (51208538), The open fund project of ministry of education(SLK2014B05), respectively.

REFERENCES

[1] Y.P.Zhang,W. Liu,S. Cao,Z. Zhai and X.Nie.Digital image encryption algorithm based on chaos and improved DES[J], *Systems Man and Cybernetics*, vol. 27,pp. 474 - 479 ,2009.

[2] L. Yu, Z.Wang and W.Wang.The application of hybrid encryption algorithm in software security[J], *Consumer Electronics Communications and Networks*, vol. 67,pp. 669 - 672 ,2013.

[3] Yarahmadi, A. , Moarefi, N. and Setayeshi, S, Implementing Cellular Automata with Dissimilar Rule on Serial Base[J] , *Computer Modeling and Simulation (EMS)*,vol. 54,PP. 334 – 337, 2010.

[4] Ishida, T. , Inokuchi, S., Continuity of Inverse Transition Relations of 2-Neighborhood Cellular Automata[J], *Computing and Networking (CANDAR)*,Vol. 124,PP. 495 – 499,2013.

[5] Roy, S. , Nandi, S. , Dansana, J. and Pattnaik, P.K., Application of cellular automata in symmetric key cryptography[J], *Communications and Signal Processing*,vol. 12,PP. 572 - 576,2014.

[6] N. Ganguly, B. K. Sikdar, A. Deutsch, G. Canright and P. Pal Chaudhuri, A survey on cellular automata[J], *Technical Report, Center for High Performance Computing, Dresden University of Technology*,2003.

[7] Ping Wei , Xu An Wang and Xiaoyuan Yang, Proxy Re-encryption from CLE to CBE [J], *Computational Intelligence and Security (CIS)*, vol. 33, pp. 339 – 342,2010.

[8] Ranaee, I. , Nia, M.M. , Jahantigh, R. and Gharib, A., Introducing a new algorithm for medical image encryption based on chaotic feature of cellular automata [J],*Internet Technology and Secured Transactions*, vol. 431,PP. 582 – 587,2013

[9] Kumaravel, A. , Meetei, O.N., An application of non-uniform cellular automata for efficient cryptography[J],*Information & Communication Technologies*,vol.241,PP. 1200 - 1205,2013.

[10] Feng Bao, Cryptanalysis of a partially known cellular automata cryptosystem[J],*Computers IEEE Transactions* ,vol. 97, pp. 1493 - 1497 ,2004

[11] Jingyang Gao, Hai Cheng, Ziheng Yang and Qun Ding ,The research and design of embed RSA encryption algorithm network encryption card driver[J], *Sensor Network Security Technology and Privacy Communication System (SNS & PCS)*,vol.77,PP. 83-87,2013.

[12] F. Seredynski, P. Bouvry and A. Y. Zomaya, Cellular Programming and Symmetric Key Cryptography Systems[J], *in: E. Cantú-Paz et al. (Eds.), Genetic and Evolutionary Computation – GECCO*, 2003, *LNCS 2724, Part II, Springer*, vol.132,pp. 1369-1381, 2003.

[13] Leong, M.P., Naziri, S.Z.M. and Perng, S.Y., Image encryption design using FPGA [J], *Electrical, Electronics and System Engineering*, vol. 8,pp. 27-32,2013.

[14] Mahmood, A. , Dony, R. And Areibi, S., An adaptive encryption based genetic algorithms for medical images [J],*Machine Learning for Signal Processing*, vol. 1,PP.1-6,2013.

[15] N. Ganguly, A. Das, B. Sikdar, and P. Chaudhuri, Cellular Automota Model for Cryptosystem[J],*Proc. Cellular Automata Conf.*, 2000.

[16] Chin-Feng Lin,Shun-Han Shih,Jin-De Zhu and Sang-Hung Lee, Implementation of an offline chaos-based EEG encryption software[J],*Advanced Communication Technology (ICACT)*,vol.81,pp. 430 – 433,2012

[17] S. Sen, C. Shaw, R. Chowdhuri, N. Ganguly, and P. Chaudhuri, Cellular Automata Based Cryptosystem (CAC) [J], *Proc. Fourth Int'l Conf. Information and Comm. Security (ICICS02)*,PP. 303-314,2002.

[18] Rajput, A.S. ; Mishra, N. ; Sharma, S, Towards the growth of image encryption and authentication schemes [J],*Advances in Computing, Communications and Informatics*, vol. 34,PP. 454 - 459,2013.

[19] Nandi, Subrata , Roy, Satyabrata and Nath, Siddhartha etc., 1-D group cellular automata based image encryption technique[J], *IEEE Transactions on Computers*, PP. 521 - 526,2014.

[20] Torres-Huitzil, C, Hardware realization of a lightweight 2D cellular automata-based cipher for image encryption[J],*Circuits and Systems*, vol.1,PP. 1-4,2013.

[21] R. J. Chen, Y. T. Lai and J. L. Lai, Architecture design and VLSI hardware implementation of image encryption/decryption system using re-configurable 2D Von Neumann cellular automata[J], *Circuits and Systems*, vol,15,pp. 451-456,2006.

[22] R. J. Chen and J. L. Lai, Image security system using recursive cellular automata substitution[J],*Pattern Recognition*, vol. 142,PP.1621-1631,2007.

[23] Kadir, R. ,Shahril, R. and Maarof, M.A., A modified image encryption scheme based on 2D chaotic map [J],*Computer and Communication Engineering (ICCCE)*, vol.1,PP.1-5,2010.