ISSN: 2834-7706

Review Article

Journal of Mathematical Techniques and Computational Mathematics

Visual Cryptography Using Neighborhood Based Encryption Techniques in The Framework of Cellular Automata

M.Venugopal[1], E.G. Rajan[2], and Venkata Raman[3]

[1]*Professor ECE Department, Megha Institute of Engineering and Technology for Women.*

[2]*President of Pentagram Research Centre.*

[3]*Director Advanced data research Centre.*

***Corresponding author:**
Venugopal, M. (2022). Megha Institute of Engineering and Technology for Women.

Submitted:08 Nov 2022;**Accepted:**15 Nov 2022;**Published:** 18 Nov 2022

Citation: Venugopal, M., Rajan, E, G., Raman, V. (2022). Visual Cryptography Using Neighborhood Based Encryption Techniques in The Framework of Cellular Automata. *J Math Techniques Comput Math*, 1(2), 133-137.

Abstract

Security of digital data during data communication, data exchange, data authentication is very important. Many authentication techniques are used to secure data. Visual cryptography is one of the methods which creates signatures by applying nonlinearity into the data. The signatures consist of cipher and the key. At the receiving end if the key and the cipher match then the authentication is done. Through this visual cryptography technique, the users hide information securely based on key authentication. This paper discusses another approach to visual cryptography using neighborhood-based encryption techniques in the framework of cellular automata. A cellular automaton has a grid of cells. This cell has either value 0 or 1. These values are changed to next state level in a discrete way with respect to time using some fixed rule. A 'Cellular Automaton' (CA) is a 2-dimensional finite array of lattice points called cells together with an updating rule that involves values of a cell and of some predetermined neighborhood cells. Cellular automaton rules for visual cryptography are defined. These rules consist of Neighborhood generation phase and signature generation phase. A sample array is considered. Using cellular automaton rules encryption and decryption is done on sample array.

Introduction

Cellular Automata (Cellular Cryptography)

In a simple way, the cellular automata have a grid of cells. This cell has either value 0 or 1. These values are changed to next state level in a discrete way with respect to time using some fixed rule. The value of a cell at a position (i) is let ki. The simple rule to get a new value for this cell is shown in the equation:

$$K_i = Ø\ (a_{i-1}, a_i, a_{i+1})$$

where Ø is a Boolean function to specify a rule. The following characteristics help to construct a cellular automata (CA). CA has discrete states, homogeneous in character synchronously updated, has a deterministic rule and spatially local rules. This characteristic makes analysis and simulation much easier. CA is viewed as a mathematical and also as a computational system. A simple two-dimensional CA is capable of universal computation. The evolution of CA can be computed to do encryption, and the evolution begins from the initial conditions. Any physical system satisfying differential equations may be approximated as CA by introducing finite difference and discrete variables.

Two -Dimensional Cellular Automata

For two-dimensional CA a square lattice is considered as shown in the Table 1.1.

Table 1.1 Nine neighbor CA rule (Moore proposed)

64	128	256
32	1	2
16	8	4

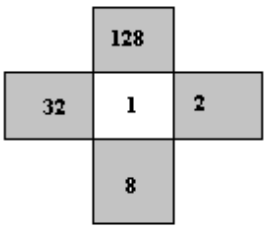


Figure 1.1 5-Neighbour (von Neumann proposed)

The eight rules mentioned in table 1.1 are called fundamental rules of CA and they are known as linear rules of CA. A five neighbor square CA evolve with as

$$a_{i,j}^{(t+1)} = \emptyset[a_{1,1}(t), a_{1,1+1}(t), a_{1+1,1}(t), a_{1,1-1}(t), a_{1-1,1}(t)]$$

As shown in the Figure 1.1, the value of the Centre cell is expanded depending on the values of the shaded cells.

In this paper, also proposed a cellular automata of dimension 2 as graphic crypto systems i.e. crypto systems to encrypt image define by pixels. These crypto systems have several differences compared to the visual schemes proposed to date. For this reason, we denote this cryptography as graphic cryptography (cellular cryptography). The proposal begins by considering plane text message, use a cellular automata algorithm of dimension 2 to encrypt the message which we call as cipher image and finally decrypt the original information.

Related Work

Franciszek seredynski, Pascal Bouvry Alber, Y.Xomaya et al., discussed 'Cellular automata computations and secret key cryptography', cellular automaton rules to generate pseudo-random number sequence for key generation [1]. Puhua Guan et al., presented in his paper titled 'Cellular automaton public-key cryptosystem ' how to Implement cellular automaton public-key cryptosystem [21]. Marco Tomassini, Mathieu perrenoud et al., describes in his paper titled 'Nonuniform cellular automata for cryptography' Considered One & two dimensional non-uniform cellular automata to generate a single key from pseudo random bit sequences [3]. S. Nandi, B.K. Kar, P. Pal Chaudhuri et al., explains in his paper titled 'Theory and applications of cellular automata in cryptography' how 'The cellular automata rules like rule 90 and 150 can be applied for generating high quality pseudo random number to generate a key in stream ciphers. L. H. Encinas et al., explain in their paper titled 'Encryption of images with 2-dimensional cellular automata how a graphic system can be designed using cellular automata. Franciszek Seredynski, presented in his paper titled 'Sequential and parallel cellular automata-based scheduling algorithm' the important features of the cellular automata is parallelism. Gonzalo_Alvarez Mara~n_on et al., have proposed in their paper titled 'Graphic cryptography with pseudorandom bit generators and cellular automata' a new graphic symmetrical cryptosystem. Haibo Zhang et al., have explained in their paper titled 'Visual cryptography for general access structure using pixel-block aware encoding' multi pixel encoding mechanism.

Feng liu and Chuan kun wu et al., explain in their paper titled 'Optimal XOR based (2, n)-visual cryptography schemes state key laboratory of information security' experimental results of a visual cryptography scheme for (2, n).

Proposed System

Another approach to visual cryptography is the use of neighborhood-based encryption techniques in the framework of cellular automata. A 'Cellular Automaton' (CA) is a 2-dimensional finite array of lattice points called cells together with an updating rule that involves values of a cell and of some predetermined neighborhood cells. Cellular automata are of three types and they are based on the type of arrays used, namely (i) linear array, (ii) two-dimensional array] and (iii) three-dimensional array. Each cell is assigned a cell variable ξ which ranges over a set of N values, say 0, 1, 2, N-1. A cell is addressed in the following manner: (i) $\xi_{i,}$ where $\xi_{i,l}$ and ξ_{i+1} are its left and right immediate neighbors in the case of linear array; (ii) $\xi_{i,j}$ where $\xi_{i-1,j}$, $\xi_{i+1,j}$, $\xi_{i,j-1}$, and $\xi_{i,j+1}$ are its top, bottom, left and right immediate neighbors in the case of two dimensional array. Similar kind of addressing is done for the three-dimensional array also. An updating formula, say in the case of a linear array is of the form $\xi_i^{t+1} = \Phi[\xi_{i-1}^t, \xi_i^t, \xi_i^t+1]$ where ξ_{t+1}^i is the value of the i^{th} cell in the next instant of time t+1, ξ_{i-1}^t, ξ_i^t, ξ_{i+1}^t are the values of $(i-1)^{th}$ cell, i^{th} cell and $(i+1)^{th}$ cell respectively at present instant of time t. One can generalize the updating formulas for the two- and three-dimensional arrays also. Based on the preliminary details about cellular automata, a novel approach to visual cryptography is proposed here in the next section.

Cellular Automata Rules for Visual Cryptography

Let us consider an array shown in Fig. 1.2.

0	1	0	0
0	0	0	1
0	0	0	0
1	0	0	0

Figure 1.2: Sample array to be encrypted

This array is encrypted using the visual cryptography [32] technique as described in this section [63]. The procedure consists of two phases, namely (i) neighborhood generation phase and (ii) signature generation phase. Both are briefly explained below.

Neighborhood Generation Phase

$$0 \Rightarrow \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix} \qquad 1 \Rightarrow \begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{matrix}$$

Every cell in a pixel array corresponding to an ASCII character should be represented by a 3x3 cell array. This is implemented with the help of two updating formulas which are shown in figure 1.3

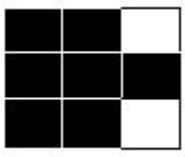
Application of these two formulas to an (m x n) array corresponding to an ASCII character would lead to array size expansion of 3mx3n. Once the array size is increased, the visual signatures are

created using various updating formulas. Details are presented in the following.

Signature Generation Phase

Signatures are generated using cellular automata updating formula pairs, one for generating signature #1 and the other for signature #2. Both signatures are visual patterns of size 3x3. One such formula pair is shown in figure 1.4.

0	0	0
0	0	0
0	0	0

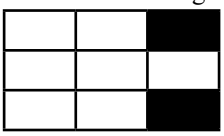


Insert figure from original

Updating Formula #1 for Generation of Signature #

0	0	0
0	1	0
0	0	0

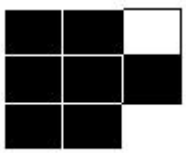
⇨



Updating Formula #2 for Generation of Signature #2

0	0	0
0	1	0
0	0	0

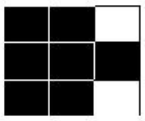
⇨



Updating Formula #3 for Generation of Signature #1

0	0	0
0	0	0
0	0	0

⇨



Updating Formula #4 for Generation of Signature #2

Fig. 1.4: Updating formulas for signature generation

One can see from figure 1.4 that signature #1 and signature #2 visually complement each other after encrypting '1' and they remain the same after encrypting '0'[21]. One can make use of a number of 3x3 neighborhood cellular automata updating rules for signature generation. Details about these rules are explained in the sequel.

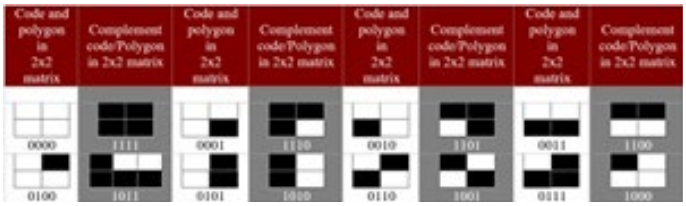
Types of Cellular Automata Formulas

Usually a cellular automaton updating rule is applied to all the cells in an array at a particular instant of time in parallel. Such rules are called 'Global Rules'. One can also apply many different updating rules to cells, in the sense that each cell value is processed by one updating rule and this rule differs from cell to cell. In such a case, the rules are called 'Local Rules'. In the case of visual cryptography, an updating rule called VCR consists of four formulas as shown in Fig. 1.4. A VCR may be a global rule or a set of local rules. A global rule is a deterministic rule whereas a set of local rules can be deterministic or random rules. It goes without saying that use of random updating rules would yield maximum crypto analytic complexity.

Defining neighborhood is an important activity for creating updating rules. Two cases are considered in this study.

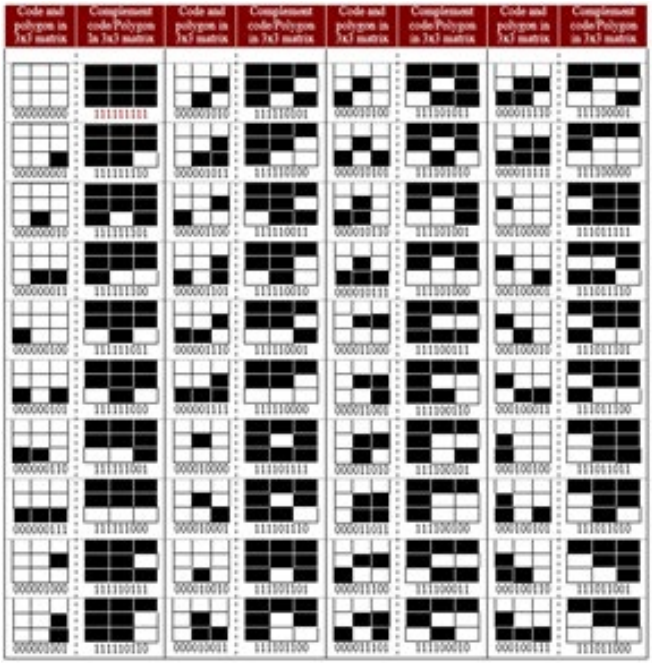
Case #1: Neighborhood 2x2

Eight pairs of patterns are generated in 2x2 neighborhood. Each pair consists of a pattern and its complementary pattern. All eight pairs are listed below.



Case #2: Neighborhood 3x3

One can construct 256 pairs of patterns when 3x3 neighborhood structure is used in the lattice expansion phase. Few pairs are listed below.



Having thus created a rule space consisting of 256 pairs of patterns in a 3x3 neighborhood, one can look into the possibilities of using them in visual cryptography. Four types of applications of the rule space to visual cryptography were tried and results analyzed.

Application type #1
A single pattern substitution formula is applied to both '0' and '1' to create signature #1. The same pattern substitution formula is applied to '0' and its complementary formula to '1' to create signature #2.

Application type #2
One fixed pattern substitution formula is applied to '0' and a different formula to '1' to create signature #1. Alternatively, signature #2 is created by applying the same fixed formula which was applied to '0' and the complementary formula which was applied to '1' while creating signature #1.

Application type #3
Randomly chosen pattern substitution formulas from the rule space are applied to '1's' and a fixed pattern substitution formula to '0' to create signature #1. Alternatively, signature #2 is created by applying the same formulas which were applied to '0's' and the complementary formula which was applied to '1' while creating signature #1.

Application type #4
Randomly chosen pattern substitution formulas from the rule space are applied to '1's' and again randomly chosen pattern substitution formulas from the rule space are applied '0's' to create signature #1. Alternatively, signature #2 is created by applying the same formulas which were applied to '0's' and the complementary formulas which were applied to '1's' while creating signature #1.

Use case studies were made using the above four types of applications and results analyzed.

Complexity Analysis

A pixel array matrix corresponding to an ASCII character consists of two values, that is, a '0' and a '1'. Let the number of 1's in the binary pattern of an ASCII character be 'n' and that of 0's be 'k', so that the total number of cell values in the pixel array is n+k.

Consider a 3x3 neighborhood structure. In this case, any of the 256 signature pairs could be used to encode each '1'. Assume that there are 'n' number of '1' and 'k' number of '0'. Then one can have 256n random possibilities of encrypting all 1's and 256k random possibilities of encrypting all 0's.

So, one can expect 512(n+k) coding patterns in visual cryptography when 3x3 matrix is used for neighborhood generation.

Usually an ASCII character as mentioned is represented in a 7x9 raster array of cells as 1's and 0's, which amounts to saying that 63 cells define an ASCII character. Each cell is further expanded to a 3x3 cell array, meaning all 63 cells in the original 7x9 array are expanded to a total of 567 cells of array size 21x27, and this expanded cell array is treated here as a cellular automaton array. Visual cryptographic signatures are created from this 21x27 array using cellular automata rules, be it a global rule or a local rule or a random rule. Only random rules are considered here.

Visual encryption is understood here as the pair of signatures #1 and signature #2. One can create 512567 signature pairs for encrypting one ASCII character. For example, an I- button would have a security code which is a sequence of 128 ASCII characters out of which the first 64 contains user information and the remaining 64 randomly generated every time a transaction is made. The point to be noted here is that all 128 ASCII characters are encrypted using visual encryption formulas.
Based on the above details, the total complexity involved in this technique amounts to number of visual encryption possibilities. Assume that the server makes use of a random number generator with each number denoting one possibility and that the generator is modeled as a random process characterized by a uniform probability distribution $f(x) = \frac{1}{d-c}$ function. In such a case, the following holds:

Mean = $\mu = \frac{c+d}{2}$

Standard Deviation = $\sigma = \frac{d-c}{\sqrt{12}}$

A uniform distribution has equally likely values over the range of possible outcomes, say c to d. This means the probability of choosing a visual pattern pair for creating visual cryptographic signatures is equally likely.

To summarize, a hacker can decode a visual pattern pair in an I-button and server with a probability of $1/_{512}{}^{567}{}^{128}$

Conclusions

This paper provides results due to a comprehensive study made on the problem of identifying a feasible solution to enhance the security features in smart devices for example I- button based access control and communication.

Presently I-button technology is used in various access control, security and authentication applications supported by secured hash authentication and multiple password protection schemes. These kinds of security techniques are not robust and they are found to be amenable for hacking with minimum efforts.

To enhance the security to next level, visual cryptography using cellular automata has been introduced. Further complexity analysis has been verified and found that, it is impossible for a hacker to decode the information in signatures in short time.

As future work, the results found in this paper could be applied to other security authentication devices like ATM, RFID, Smart card etc., without changing their corresponding security protocols.

Compliance with Ethical Standard

I thank Dr. E. G. Rajan for the research support given to me while preparing this manuscript. The manuscript is prepared with proper understanding and assessment of the content. The financial support to research and publishes paper is not a conflict between the authors, as financial matters are supported by author Dr. M. Venu gopal. The author supports money through his monthly salary. We declare that we have not received any financial support from any organization. Publish of manuscript in the journal is purely academic interest.

We declare that we do not have any conflict of interest in publishing this paper.

We state that no involvement of animals in our research and this article studies does not involve human participation in the research. Also, this research and manuscript has not handled any confidential data.

Competing Interest

There is no financial and non-financial interest to undermine the objectivity, integrity and values of publication by the influence of the authors related to data analysis and interpretation. Also, the financial competing interests, potential employment interest, personal financial interest, non-financial interest does not exist in publishing this manuscript.

Research Data policy and Data availability statement

We state that all the data in this manuscript is original and authors have no reservations in sharing the data available in the manuscript.

References

1. Seredynski, F., Bouvry, P., & Zomaya, A. Y. (2004). Cellular automata computations and secret key cryptography. parallel computing, 30(5-6), 753-766.
2. Seredynski, F., & Zomaya, A. Y. (2002). Sequential and parallel cellular automata-based scheduling algorithms. IEEE Transactions on Parallel and Distributed Systems, 13(10), 1009-1023.
3. Marañón, G., Encinas, L. H., Encinas, A. H., Rey, Á. M. D., & Sánchez, G. R. (2003, September). Graphic cryptography with pseudorandom bit generators and cellular automata. In International Conference on Knowledge-Based and Intelligent Information and Engineering Systems (pp. 1207-1214). Springer, Berlin, Heidelberg.
4. Rio Piedras, P. R. (1987). Cellular automaton public-key cryptosystem. Complex Systems, 1, 51-57.
5. Tomassini, M., & Perrenoud, M. (2000). Nonuniform cellular automata for cryptography. Complex Systems, 12(1), 71-82.
6. Nandi, S., Kar, B. K., & Chaudhuri, P. P. (1994). Theory and applications of cellular automata in cryptography. IEEE Transactions on computers, 43(12), 1346-1357.
7. Hernández Encinas, L., Martín del Rey, Á., & Hernández Encinas, A. (2002). Encryption of images with 2-dimensional cellular automata.
8. Franti, E., & Dascalu, M. (2006). Simulator for testing cellular automata cryptographic algorithms. WSEAS Transactions on Information Science and Applications, 3(7), 1383-1388.
9. Moratelli, C. R., Cota, Ï., & Lubaszewski, M. S. (2006, August). A cryptography core tolerant to DFA fault attacks. In Proceedings of the 19th annual symposium on Integrated circuits and systems design (pp. 190-195).
10. Zhang, H., Wang, X., Cao, W., & Huang, Y. (2008). Visual Cryptography for General Access Structure Using Pixel-block Aware Encoding. J. Comput., 3(12), 68-75.
11. Dorrendorf, L., Gutterman, Z., & Pinkas, B. (2009). Cryptanalysis of the random number generator of the windows operating system. ACM Transactions on Information and System Security (TISSEC), 13(1), 1-32.
12. Liu, F., & Wu, C. (2014, October). Optimal XOR based (2, n)-visual cryptography schemes. In International workshop on digital watermarking (pp. 333-349). Springer, Cham.
13. Lan, J., Goh, W. L., Kong, Z. H., & Yeo, K. S. (2010, November). A random number generator for low power cryptographic application. In 2010 International SoC Design Conference (pp. 328-331). IEEE.
14. Abdulla, S. (2010). New visual cryptography algorithm for colored image. arXiv preprint arXiv:1004.4445.
15. Kishore, M., & Kiran, S. K. (2011, July). A novel encryption system using layered cellular automata. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 6-8).
16. Kar, B., Rao, D. C., & Rath, A. K. (2011). Generating pns for secret key cryptography using cellular automaton. International Journal of Advanced Computer Science and Applications, 2(5).
17. Liu, F., & Wu, C. (2011). Embedded extended visual cryptography schemes. IEEE transactions on information forensics and security, 6(2), 307-322.
18. Chiu, P. L., & Lee, K. H. (2011). A simulated annealing algorithm for general threshold visual cryptography schemes. IEEE transactions on information forensics and security, 6(3), 992-1001.
19. Milea, P. L., Teodorescu, M., Muller, R., Dragulinescu, M., Oltu, O., Tiplea, G., ... & Pompilian, S. Cellular Automata Applications for Renewable Energy Monitoring.
20. Chavan, P. V., & Atique, M. (2012, December). Design of hierarchical visual cryptography. In 2012 Nirma University International Conference on Engineering (NUiCONE) (pp. 1-3). IEEE.
21. James, D., & Philip, M. (2012, January). A novel anti phishing framework based on visual cryptography. In 2012 International conference on power, signals, controls and computation (pp. 1-5). IEEE.
22. Kulikowski, K. J., Karpovsky, M. G., & Taubin, A. (2007). Robust codes and robust, fault-tolerant architectures of the advanced encryption standard. Journal of systems Architecture, 53(2-3), 139-149.

Copyright: *©2022 Venugopal, M. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.*