Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/53

Image decryption and encryption using a cellular automaton with just two dimensions

Prabhdeep Singh[1], Dibyahash Bordoloi[2], Vikas Tripathi[3]

[1]Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002
[2]Head of the Department, Department of Computer Science & Engineering,Graphic Era Hill University, Dehradun, Uttarakhand India, 248002
[3]Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002

ABSTRACT

In this research, we provide a novel method for encrypting and decrypting both images and data based on the principles of cellular automata (CA). The technique for encrypting and decrypting a block cypher is based on the principles of linear and nonlinear cellular automata. This algorithm's input should be a picture of any dimension. To begin, we take the whole picture as input plain text and transform it to pixels. After that, we use nonlinear CA rules (Complement) on both the plain text and the key. The aforementioned data is then analysed using a single standard PB CA rule. The preceding outputs should then be subjected to an XOR procedure. The output of the XOR operation is then used as the input to the substitution box (S- BOX). Once again, the preceding findings are subjected to standard PB CA guidelines, which are then followed by S-BOX. Similar to how encryption is performed, decryption is performed in reverse. Our suggested technique is more secure than industry standard algorithms like AES and DES because it encrypts and decrypts data in a total of eight rounds and does not rely on any shared information between the plain text and the cypher text.

Keywords: XOR, AES, DES, S-BOX

INTRODUCTION

There are few fields where cryptography is more crucial than in security, defence, medicine, and business, to name a few. How long a cryptosystem can be used to encrypt and decode communications before the 'key' is cracked using cellular automata (CA) principles is a good indicator of its effectiveness. Since the starting state of the CA provides the key to the encryption, and the CA evolves a complex chaotic system from this 'beginning state' that cannot be anticipated, a family of CA-based encryption algorithms offers a particularly promising approach to cryptography.

This section of the paper will be structured as follows. The development of cellular automata is

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/53

discussed in Section II. The literature review is the topic of Discussion III. In Section IV and its subsections, we detail our novel cellular automata-based encryption and decryption technique.

HISTORY

Mathematics, physics, theoretical biology, and microstructure modelling all make use of cellular automata, a discrete model. Tessellation automata, homogeneous structures, and iterative arrays are all names for what we term "Cellular Automata."

The cells in a cellular automation system have just two possible states—on or off—and are arranged in a regular grid. The grid's dimensions need only be limited. Each cell has a collection of neighbouring cells designated for it; these are termed the cell's Neighbors. A new generation is born, with each cell's future state determined by its present state and the nearby cells' future states according to a predetermined rule. The rule used to update the state of cells is typically uniform across all cells, remains constant over time, and is applied uniformly to the whole grid at once. Since the rules of elementary cellular automata reside on the vertices of the 8-dimensional hyper cube, they may all be stated using just 8 bits.

Stanislaw Ulam and John vonNeumann of Los Alamos National laboratory came up with the idea in the 1940s. The use of 2D cellular automata, pioneered by John Conway in the 1970s with his game of life, was investigated to some extent in the 1950s and 1960s.

In the 1980s, Stephen Wolfram undertook a systematic investigation of basic cellular automata, which he defines as having a single dimension. In his 2002 book, "A New Kind of Science," he argued that cellular automata may be used in a wide variety of scientific disciplines. Cryptanalysis and computer hardware are two examples.

Autonomous Systems in Living Cells The definition of a Cellular Automata (CA) is a 4-tuple (D, S, N, R) For where D is a CA dimension.

Where S is the set of all finite states. The N-dimensional neighbourhood space is governed by the R-dimensional collection of local rules.

An ideal parallel processing machine is a set of rules for updating arrays of cell values, which may be any combination of numbers and symbols. This rule determines how a cell value should change with relation to other cell values in the same Neighbourhood.

Fundamental cellular automata B

The first of CA's three essential components is the grid, which consists of a linear arrangement of cells. Put another way, it would lack depth.

There are two groups of states: the contiguous states and the noncontiguous states. a value of 0 or 1 alone.

3 Neighbors: In a one-dimensional neighbourhood, a cell's two neighbours are to its left and

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/53

right.

In the field of cellular automata, there are several approaches to calculate a cell state based on a collection of cells. As in the case of blurring a picture. The new colour of a pixel may be determined by taking the mean of its neighbouring pixels. We also determined that the combined states of a cell's neighbours constitute its new state.

AUTOMATISM OF 2D CELLS, CLASS C

Different types of neighbourhoods may be defined when a d-dimensional grid is taken into account. If we focus on CA in two dimensions, the most frequent neighbourhoods are: First, VonNeumann: Just the four cardinal directions! (Four Distinct Areas) Moore: Two more neighbourhoods are formed when the diagonals are added to the Von Neumann ones. Three-Extended Moore: Increasing the neighborhood's distance by one.

2-D representation of the Moore neighbourhood
2D CA architecture shown in Fig. Both images have a centre cell labelled CELL and its 9 surrounding cells labelled. Each cell in a two-dimensional cellular automaton may be in one of an infinite (or limited) number of states. A cell's state at time t depends on the states of its neighbours at time t-1, and time itself is discrete. There are often two cellular neighbourhoods taken into account while working with 2-D cellular automata. We take into account five cells in the Von Neumann neighbourhood.

All the guidelines for a cellular automaton in two dimensions are shown in Figure 3. Each cell's subsequent state in 2-D eight-neighborhood CA is influenced by the states of both the cell itself and the eight neighbouring cells (Table). Several rules take into consideration such interdependencies. The centre cell stands in for the cell under consideration, while the surrounding cells represent its immediate neighbours. Each cell has a number that corresponds to the rule number (Rule 1, Rule 2, Rule 4, Rule 8, Rule 16, Rule 32, Rule 64, and Rule 128) that defines the current cell's unique dependence on its neighbour.

This set of 8 rules, collectively referred to as the linear rules of cellular automata, is considered to be the most basic laws of cellular automata. For linear rules of cellular automata, the rule number is the mathematical sum of the numbers of the relevant cells if the cell is dependent on two or more neighbours. The 2D CA rule 150 (=2+4+16+128) describes the centre cell's dependence on its four neighbouring cells to the right, left, bottom, and top. 8C0+8C1+8C2+....+8C8=256 is the total number of such rules. Each cell shall be treated the same way under Rule-150.

Literature Survey

Using a one-dimensional cellular automaton, Stephen Wolfram [1] described a stream cypher. The author uses this to deduce a rule for determining what the subsequent values should be. Thus, ai1=ai-1 XOR (ai OR ai+1). There, ai might either be 0 or 1. Here, the author uses the statement to transform the plain text into the encryption text. When Ci=Pi XOR ai, the resulting value is ci. If the sequence ai is known, then doing the same process again will provide the plain text. There is presently no publicly available method that can solve it systematically. An integrated circuit is a

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/53

viable option for efficiently implementing the CA. It has the potential to be employed in a number of high band width cryptography applications and needs less than gate delay periods to create each output bit. According to Stephen Wolfram [2], CA may be utilised as a mathematical model for physics, biology, and computing. The author conducts an in-depth analysis of CA and describes some general characteristics of this behaviour, such as the emergence of certain patterns. The author provides a set of rules that may be used to get the patterns. Each cell simultaneously undergoes this regulation. Cellular automata, as described by Olivier Martin et al. [3], is intricate and exhibits a wide range of behaviours. Discrete CA are straightforward dynamical systems. Numbers and algebraic values are used to derive the whole framework of a state transition diagram. Algebraic methods are used in order to provide a comprehensive examination of global characteristics. The systems often comprise an enormous number of configurations and cycles and cannot be reversed. When it comes to cellular automata, self-organization is considered in terms of a computational process, as stated by Stephen Wolfram [4]. Cellular automata descriptions from dynamical systems theory are augmented with formal language theory. After a certain number of generations, the resulting configuration sets in a cellular automaton evolve into regular languages. It provides several instances. Sizes of minimum grammars for these languages may be used as proxies for the complexity of the corresponding sets. For the most part, this level of complexity is considered to declining with time. It would seem that the limit sets created by some types of cellular automata correlate to more advanced languages. This makes several features of such sets formally incomputable. Undecidability in these and similar dynamical systems is hypothesised to be prevalent. A primarily phenomenological investigation of cellular automata in two dimensions is described, as stated by Norman H. Packard and Stephen Wolfram [5]. Classes of behaviour are discovered qualitatively that are analogous to those seen in one-dimensional cellular automata. Patterns with intricate boundaries, defined by several growth dimensions, may emerge from seemingly simple seeds in two-dimensional cellular automata. Boundaries that execute efficiently continuous movements may evolve from disorder states to form new domains. The exponents of entropies are useful for characterising several global features of cellular automata. The fates of some are less easily determined. Cellular automata, as described by Stephen Wolfram [6], are discrete dynamical systems that exhibit intricate self-organizing behaviour despite their very basic composition. All cellular automata in one dimension are shown to belong to one of four universal classes. We explore what makes the structures formed in these areas distinct. Limit points, limit cycles, and chaotic attractors are all types of behaviour that may be seen in three distinct groups. It is likely that the fourth class can perform universal computations, making certain aspects of its behaviour in infinite time undecidable.

2D Cellular Automata-Based Image Encryption and Decryption

There are XOR (linear cellular automata rule), complement (nonlinear cellular automata rule), substitution (nonlinear cellular automata rule), and permutation (nonlinear cellular automata rule) operations in this method. Non-linear rules are preferable than linear ones when designing a crypto system. However, the two underlying activities of cryptography are the production of confusion (nonlinear CA rule) and diffusion (linear CA rule) [7]. Therefore, both linear (diffusion) and nonlinear (confusion) operations or rules will be used in the creation of every encryption and decryption method in cryptography. A more secure technique may be achieved by using a larger number of nonlinear rules for encryption and decryption in place of a smaller number of linear

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/53

ones.

ENCRYPTION ALGORITHM STEPS

Rule (Complement) for Nonlinear CA and PB CA Rule8. Both the plain text and the key are assumed to be 128 bits in length. To begin, we transform the text into a 4x4 matrix where each cell stores 1 byte (= 8 bits). On this end, we are now applying the rule (complement) of nonlinear cellular automata to every single one of the unadorned texts. The 128-bit key is also represented as a 4x4 matrix, with the nonlinear CA rule (complement) applied to each cell. PB CA rule8 is then applied independently once the complement has been applied. Applying the By applying the periodic boundary (PB) CA rule-8 to each value in the cell of the matrix, we can see that the values in the second row have been moved to the first row, the values in the third row have been moved to the first row, and so on, with the values in the first row being moved to the last row.

The linear rule of cellular automata is provided by the XOR operation applied to the cypher key and cypher text, which in turn provides the diffusion feature of cryptography[8].

A cypher and decryption technique using CA rule c) Substitute Bytes Transformation (S-Box) is shown in Figure 5. (Forward and Inverse Transformation)

Below is a table lookup for the forward substitution byte transformation, known as Sub Bytes. It's an identical copy of the AES table. We plan to create an S-box with a high non-linearity and algebraic degree in the near future. AES S-box, on the other hand, is well-balanced, non-linear, and of a high algebraic degree. In order to generate a permutation of all 256 possible 8-bit values, AES specifies a 16 by 16 matrix of byte values called S-box. Following is the mapping from each state byte to a new byte. Row values are represented by the first four bits of the byte, whereas column values utilise the last four bits. These values in the rows and columns act as indexes into the S-box, from which a specific 8-bit output value is retrieved. Here's an example: the hexadecimal number '95' refers to the value '2A' in row 9, column 5 of the S-box. As a result, the number 95 is converted to the letter sequence 2A.

For example, in the following matrix, applying the PB CA rule 128 to each cell of the matrix, the values in the first row have been shifted to second row, values in the second row have been shifted to third row and so on and values in the last row have been shifted to first row after applying periodic boundary (PB) CA rule-128 to each value in the cell of the matrix. Rule-128 of the Private Banking and Credit Association is a zero-one-one-zero [9].

For example, in the following matrix, applying PB CA rule 32 to each cell, the values in the first column have been moved to second column, second column values have been transferred to third column and third column values have been shifted to first column, and so on[10].

STEPS OF DECRYPTION ALGORITHM

The encrypted text may be converted back to plain text by using a reversible cypher algorithm such as the nonlinear CA rule (compliment), PB CA rule8 (linear), XOR (linear), S-Box (nonlinear), PB CA rule128 (linear), or PB CA rule32 (linear). In this case, the opposites of

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/53

complement, XOR, and S-Box are, in fact, compliment, XOR, and inverse S-Box. Additionally, PB CA Rule 128 is the opposite of PB CA Rule 8, whereas PB CA Rule 2 is the inverse of PB CA Rule 32.

CA rule-2 Periodic Boundary is applied to each cell in the key, as seen in Figure 10. In the following matrix, for instance, the values in the second column have been moved to the first column, the values in the third column have been moved to the second column, and so on, and the values in the first column have been moved to the last column, all as a result of applying the periodic boundary (PB) CA rule-2 to each value in the cell of the matrix.

REFERENCES

1. Kumari, M., Gupta, S., & Sardana, P. (2017). A survey of image encryption algorithms. *3D Research*, *8*(4), 1-35.
2. Zhang, Y. (2017). A chaotic system based image encryption scheme with identical encryption and decryption algorithm. *Chinese Journal of Electronics*, *26*(5), 1022-1031.
3. Zhang, Y., & Tang, Y. (2018). A plaintext-related image encryption algorithm based on chaos. *Multimedia Tools and Applications*, *77*(6), 6647-6669.
4. Younes, M. A. B. (2019). A SURVEY OF THE MOST CURRENT IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES. *International Journal of Advanced Research in Computer Science*, *10*(1).
5. Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. *International Journal of Applied Engineering Research*, *12*(23), 13265-13280.
6. Fu, X. Q., Liu, B. C., Xie, Y. Y., Li, W., & Liu, Y. (2018). Image encryption-then-transmission using DNA encryption algorithm and the double chaos. *IEEE Photonics Journal*, *10*(3), 1-15.
7. Zhang, Y. (2018). Test and verification of AES used for image encryption. *3D Research*, *9*(1), 1-27.
8. Pujari, S. K., Bhattacharjee, G., & Bhoi, S. (2018). A hybridized model for image encryption through genetic algorithm and DNA sequence. *Procedia Computer Science*, *125*, 165-171.
9. Parvaz, R., & Zarebnia, M. (2018). A combination chaotic system and application in color image encryption. *Optics & Laser Technology*, *101*, 30-41.
10. Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., & Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos based S-Box. *Chaos, Solitons & Fractals*, *95*, 92-101.