# A New Image Encryption Scheme Based on Two-Dimensional CA Joint With CWQ Method

Zhang Xiaoyan[1], Wang Chao[2], Sun Zhiren[1], Zhang Zanbo[3, 4]

(1. School of Mathematics and Computer Science, Institute of Mathematics, Nanjing Normal University, Nanjing 210097, China
(2. College of Software, Nankai University, Tianjin 300071, China
(3. Department of Computer Science, Sun Yat-sen University, Guangzhou 510275, China
(4. Department of Computer Engineering, Guangdong Industry Technical College, Guangzhou 510300, China

**Abstract** CA is the abbreviation of cellular automata which are dynamical systems with discrete space and time. Considerable interest has been shown over the past decade in the use of cellular automata in cryptography. The aim of this paper is to present a new scheme for image encryption, which combines two-dimensional CA approach we proposed in Moore neighborhood on the graph structure of square lattice and CWQ method based on quad-tree structure. First, the two-dimensional CA encryption approach can strengthen the system' s security more greatly than the confusion-only CWQ method. Second, CWQ method enhances the confusion property of the two-dimensional CA approach which satisfies avalanche effect and the property of diffusion. Moreover, an important feature of the proposed scheme is that it has very large number of security keys and simple operations which are especially useful for digital image encryption.

**Key words** image encryption, cellular automata, quad-tree structure, graph theory, wavelet

**CLC number** O157. 5 **Document code** A **Article ID** 1001-4616(2008 01-0001-07

# 基于二维 CA和 CWQ方法的图像加密方案

张晓岩[1], 王 超[2], 孙志人[1], 张赞波[3, 4]

(1. 南京师范大学数学与计算机科学学院, 数学研究所, 江苏 南京 210097
(2. 南开大学软件学院, 天津 300071
(3. 中山大学计算机科学系, 广东 广州 510275
(4. 广东轻工职业技术学院计算机工程系, 广东 广州 510300

[摘要] 细胞自动机简称 CA, 是具有离散的空间和时间特性的动力系统. 在过去的 10多年里, 细胞自动机在密码系统和信息安全方面的应用得到了人们相当大的关注和兴趣. 本文给出了一种结合格图结构摩尔邻域的二维 CA 方法和基于四叉树结构的 CWQ 方法的图像加密方案. 首先, 二维 CA的加密方法可以比仅进行混淆作用的 CWQ 方法更有效地提高系统的安全性. 其次, CWQ方法可以加强具有雪崩效应和扩散性质的二维 CA方法的混淆性质. 方案具有大密钥量且简单易行适用于数字图像加密等特点.

[关键词] 图像加密, 细胞自动机, 四叉树结构, 图论, 小波

As the rapid progress of Internet in the digital world today, network security and data encryption has become a critically important issue. Traditional cryptographic algorithm does not fit to image encryption because of different characteristic between digital data and image data. Innovative encryption techniques need to be developed for the wide use of multimedia technology and the improvement in network transmission. Image encryption is neces-

**Received date:** 2007-09-18.

**Foundation item:** Supported by the NNSF(10671095 , China Postdoctoral Science Foundation(20070421028 , Jiangsu Planned Projects for Postdoctoral Research Funds(0602023C , Science& Technology Innovation Fund of Nankai University (2006019 and the Scientific Research Foundation of Guangdong Industry Technical College(2005 - 11 .

**Biography:** Zhang Xiaoyan, born in 1978, doctor, majored in graph theory. E-mail Royxyzhang@ gmail com

sary for multimedia internet applications and is useful for providing special security demands in privacy, intellectual properties, medical imaging and military image databases, etc Many encryption algorithms have been proposed to protect digital images and videos However, there are still some potential weakness existing in many image encryption schemes Numerous techniques were proposed to get the aim of supporting special functions of diverse multimedia services in different environment which are referred to Ref [ 1 ~ 3]. Cellular automata were originally proposed by John von Neumann as formal models of self-reproducing organisms Physicists and biologists began to study cellular automata for the purpose of modeling in their respective domains In the present era, cellular automata have been used for computing or as models of chemical, VLSI circuits, parallel multiprocessor architecture, image processing pattern recognition and cryptographic application So cellular automata are now being studied from many widely different angles The main challenge is to associate a given phenomenon with the evolving automata field In this paper, we focus on the cryptographic application of two-dimensional CA for image Wolfram[ 4] proposed the first cryptographic application of a CA. Nandi et al[5] presented a block and stream cipher based on CA. Cryptographic security examination of the two stage programmable CA has been given in [ 6]. Chen et al[7] presents a method for image encryption based on permutation of the pixels of the image by the SCAN methodology and replacement of the pixel values using a progressive CA substitution Some cryptographic applications of CA are summarized in [ 8]. Sutner[ 9] studies CA with additive rules on finite undirected graphs We propose an image encryption approach based on two-dimensional CA in Moore neighborhood on the graph structure of square lattice

Wavelet transform is now used in image compression and encryption more and more widely Some wavelet compression methods take advantage of progression to encode the image data from approximate parts to details Embedded Zero-tree Wavelet[10] is a very effective coding technique based on partial order of wavelet coefficients by magnitude with a set partitioning sort algorithm, ordered bit plane transmission, and exploitation of self similarity across different scales of the image wavelet transform. A variation version of the Embedded Zero-tree Wavelet called Set Partitioning in Hierarchical Trees was given in [ 11]. These methods are used effectively by taking advantage of the relationship of graph structure, especially tree structure between a node and its child-nodes Lian and Wang[12] proposed a wavelet coefficient confusion method based on quad-tree structure, called CWQ method They showed that the method is suitable for image or video encryption in network transform with real-time requirement, especially in mobile multimedia network because of low cost and realizing bit rate control easily. Whereas, wavelet transform has the feature of energy convergence which may do some help to statistical analysis So some encryption strengthened method are needed for the system' s security. In [ 12], Sign Encryption method( SE and Approximate Coefficients Encryption( ACE method are used for the purpose after applying CWQ method. Our new image encryption scheme incorporates the two-dimensional CA approach we proposed and CWQ method in [ 12]. Differ with CWQ + SE+ ACE method, the two-dimensional CA approach are used before taking CWQ method The joint two-dimensional CA approach and CWQ method for encrypting image has several advantages First, the two-dimensional CA encryption approach can strengthen the system' s security greatly and the confusion effect can be compared to that of CWQ + SE + ACE method which is discussed in Section 3. And CWQ method enhance the confusion property of the two-dimensional CA approach which satisfies avalanche effect and the property of diffusion Moreover, the new image encryption scheme satisfies the characteristics of convenient realization, very large number of security keys, the characteristics of less computational complexity, fast encryption speed and low cost which are suitable for multimedia applications

## 1 Background

A cellular automata is a discrete dynamical system that consists of an arrangement of basic components called cells together with a transition rule The cells have a finite number of states which are updated synchronously according to a specified local rule A standard formal definition of classic CA is given as follows

A $d$-dimensional CA, $\mathscr{A}$, consists of six parts, $(\mathbf{Z}^d, Q, \Pi, \mathscr{B}, f, \rho_f)$. Underlying space $\mathbf{Z}^d$ represents a $d$-dimensional orthogonal coordinate system. Suppose that every cell is specified by the point whose coordinates are $(x_1, x_2, \cdots, x_d)$ on $\mathbf{Z}^d$. $Q$ is a finite set, the elements of which are the states of $\mathscr{A}$. A configuration is a map $C: \mathbf{Z}^d \to Q$. The set composed of all possible configurations is called configuration space $\Pi$. Configuration is often related to time Let $C_t$ denote the configuration at time $t$, then the state of a certain cell $c$ at time $t$ is denoted as $C_t(c)$. Suppose that the coordinates $(x_1, x_2, \cdots, x_d)$ specify a certain cell $c$, then $\mathscr{B} = \{(y_1, y_2, \cdots, y_d): |y_i - x_i| \leqslant 1, 1 \leqslant i \leqslant d\}$ is denoted as the cell's neighborhood Obviously, there are exact $3^d$ cells in every cell's neighborhood $f$ is a local rule acting on a cell's neighborhood and a local transition function with $3^d$ variables The values of the function and its variables are taken from $Q$. $\rho_f$ represents the global transformation on $\Pi$ induced by $f$. If $\rho_f$ acts on $C_t$, we can get $C_{t+1}$ where every cell's state is the result coming from the action of $f$ on its neighborhood, i e, $C_{t+1} = f(C_t(B(c)))$, $\forall c \in \mathbf{Z}^d$. $\rho_f$ is then often caused the evolution or next state transformation configurations being the states of the system. It plays an essential role in practicing CA.

Because image is made up of pixels specified by two-dimensional plane coordinates, we take a two-dimensional CA as the example to describe concretely. $\mathbf{Z}^2$ is the underlying space of two-dimensional CA. The cells are arranged in the form of a square lattice structure The intersection of the squares form the cells of the automation. We can use $(a, b)$ to specify every cell whose state is assumed to be 0 or 1 and whose neighborhood is the set consisting of nine cells $(a \pm 1, b)$, $(a, b \pm 1)$, $(a \pm 1, b \pm 1)$ and $(a, b)$. The neighborhood is the so-called Moore neighborhood which is formed by the specified cell, $(a, b)$, with its eight nearest neighbors Local rule $f$ can be expressed in equations $f(000000000) = \varepsilon_1$, $f(000000001) = \varepsilon_2$, $\cdots$, $f(111111111) = \varepsilon_{512}$ where $\varepsilon_i \in \{0, 1\}$ and $i \in \{1, 2, \cdots, 512\}$. We represent the local rule $f$ by $\varepsilon_1 \varepsilon_2 \cdots \varepsilon_{512}$ conveniently. For example, $f = 0x(BDE26401)^{16}$ represents a 128 bit hexadecimal number, i e, 512 bit binary number, combined by 16 copies of the same hexadecimal number $BDE26401$ together Suppose that the original configuration is $C_0$ at time $t = 0$, and the states of cells in the neighborhood of a cell whose state is $x_0$ are $x_0, x_1, \ldots, x_8$. Then the state of the cell is $f(X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8)$ at time $t = 1$. All cells' states can be obtained in the same way We put the states together to gain configuration $C_1$ which can be considered as the result of global transformation $\rho_f$ acting on $C_0$. Furthermore, $C_2$, $C_3$, $C_4$, $\cdots$ can be generated in succession.

For an encryption application the plaintext is $p$ and the ciphertext is $c$, then the so-called avalanche effect is as follows: a small change (e g, 1 bit) in $p$ should result in a big change in $c$, and a small change in the local rule $f$ should yield a significant change in the ciphertext Suppose that a certain cell is specified by $(x_1, x_2)$. Denote $\{(y_1, y_2, \cdots, y_d): |y_i - x_i| \leqslant 2, 1 \leqslant i \leqslant d\}$ as the cell's 2-neighborhood The state of every cell in two-dimensional CA at time $t = 1$ is decided by the action of local rule $f$ on the states of cells in its neighborhood at time $t = 0$ But its state at time $t = 2$ relies on the action of local rule $f$ on the states of cells in its 2-neighborhood at time $t = 0$ Analogically, its state at time $t = n$ rests with the action of local rule $f$ on the states of all cells whose coordinates are not in excess of its coordinates over $n$ at time $t = 0$ So when $n$ is large enough, CA will be affected markedly by avalanche effect which contains two aspects, one is that when a certain cell's state is changed at time $t = 0$, the states of a large-scale cells will be affected at time $t = n$, the other is that when the original configurations of two CA are same completely but nuanced between the two CA in local rules, the configurations at time $t = n$ will be of astonishing difference The fact above is also one of the theoretical basis that our encryption scheme depends on in our paper

We denote

$$\{(y_1, y_2): |y_i - x_i| \leqslant j, 1 \leqslant i \leqslant 2, j \in \mathbf{Z}^+\}$$

as the cell's $j$-neighborhood, generally. Note that there are 25 cells in every cell's 2-neighborhood, and the number of independent variables of local rule achieves $2^{25}$. Then the set of local rules would contain

$$2^{225} = 2^{33554432}$$

elements Similar to 1-neighborhood local rule, we represent the 2-neighborhood local rule $g$ by

$$\varepsilon_1\varepsilon_2\cdots\varepsilon_{33554432}.$$

For example,

$$g = 0x(D3AB593C05EB87A9)^{524288}$$

represents a 8388608 bit hexadecimal number, i e , 33554432 bit binary number, combined by 524288 copies of the same hexadecimal number

$$D3AB593C05EB87A9$$

together A $j$-neighborhood local rule can be represented similarly where $j\geqslant 3$.

The quad-tree structure decomposes a $2^N\times 2^N$ image block into an $(N-n_0+1)$-level hierarchy, where all blocks at level $n$ have size $2^n\times 2^n$, $0\leqslant n_0\leqslant n\leqslant N$. This structure corresponds to a rooted tree, in which every node, i e , every $2^n\times 2^n$ block, has 0 or 4 children Nodes with children are called internal nodes, while those without any children are called leaf nodes, i e, it is not further subdivided For each node in a tree, we define its level to be the number of edges in the shortest path from the node to the root The height of the tree is defined to be the maximum of the levels of its nodes The tree can be represented by a series of bits that indicate termination by a leaf with a "0" and branching into child nodes with a "1". The quad-tree structure is commonly used in image coding to decompose an image into separate spatial regions to adaptively identify the type of quantizer used in various regions of an image. Many compression and encryption algorithms based on quad-tree structure is especially suitable for portable devices that may not have too much computing power Because of their low computational complexity, these methods are very efficient

Wavelet transform has become powerful in image and video compression and encryption Some wavelet coefficient confusion methods which are the encryption methods combining with the wavelet compression methods have been proposed, such as CWW method, CWF method and CWQ method referred in [12]. CWW method permutes wavelet coefficients among the whole image. CWF method permutes wavelet coefficients among the same frequency subband CWQ method permutes wavelet coefficients among the child-nodes that have the same parent-node. In CWQ, the approximate coefficients and lowest detail coefficients are confused in the same manner as CWF method, while the rest coefficients are confused based on quad-tree structure. To the same size image, the key spaces of the confusion methods are different from each other Compared to CWW method and CWF method, CWQ method is of the smallest key space, whereas, CWQ method can get the best bit rate control result and is faster than CWW and CWF methods in the encryption speed.

We take advantage of the virtues of both two-dimensional CA approach and CWQ method to present a new image encryption scheme as follows

## 2 Joint Image Encryption Scheme

The boundary conditions that are used in CA depend on the specific physics of the system being modeled Because every image is on finite plane while unbounded plane $\mathbf{Z}^2$ is infinite, we must deal with the trouble for the purpose of applying two-dimensional CA. If we consider the image to be on a topological anchor ring, i e , the right border of the image laps the left one and the top border superposes the bottom one, then every pixel has nine ones( including itself in its neighborhood in the image Without loss of generality, we take black-and-white binary image for example to illustrate how to encrypt image by applying two-dimensional CA approach combined with CWQ method We can consider that black or white represents 1 or 0 of cell's state, respectively, in a black-and-white binary image $M$. Alice and Bob agree on two selected various neighborhood local rules which are a 1-neighborhood local rule $f$ and a 2-neighborhood local rule $g$ with an iteration time $t=n$ besides CWQ key in advance In the encryption stage Alice does the following operations

**Step 1** Generating an random black-and-white binary image $R_M$ of the same size as the message $M$. Let $C_0(R_M)=R_M$.

**Step 2** Obtaining $C_n(R_M) = (gf)^n(R_M)$ and $N_0 = C_n(R_M)$ Ý $M$, where Ý represents the operation of XOR.

**Step 3** Getting $N_1 = \mathrm{CWQ}(N_0$ and sending $(R_M, N_1$ to Bob

In the decryption stage Bob does the following operations

**Step 1** Getting $C_n(R_M) = (gf)^n(R_M)$ and $N_0 = \mathrm{CWQ}^{-1}(N_1)$.

**Step 2** Recovering $M = C_n(R_M)$ Ý $N_0$ because $N_0 = C_n(R_M)$ Ý $M$.

Note that the image encryption algorithm based on two-dimensional CA can also be used for gray-scale image Let $(P_{i\times j})_{W\times H}$ be the gray-scale matrix of a gray-scale image and transform every $P_{i\times j}$ ( between 0 and 255 into a binary array, i e , $P_{i\times j} = d^0_{i\times j}d^1_{i\times j}\cdots d^7_{i\times j}$, then the gray-scale image $(P_{i\times j})_{W\times H}$ is equivalent to eight binary images $(d^k_{i\times j})_{W\times H}$, $0\leqslant k\leqslant 7$. Thus, our algorithm can be used to encrypt a gray-scale image easily Similarly, we can use this algorithm to encrypt a color image

## 3 Experimental Result

We take the 256 × 256 sized image Cameraman, choose a 1-neighborhood local rule $f$ and a 2-neighborhood local rule $g$ where

$f = (BDE2640A)^{16}$ and

$g = (D3AB593C05EB87A9)^{524288}$.

The left part of Fig 1 is the original gray-scale image $M$ which is encrypted by our algorithm. The encryption result $N_1$ are shown in the right part of Fig 1. The confusion effect of $N_1$ can be compared to that of Fig 3 in [12]. It is obvious that the new encryption scheme of two-dimensional CA approach joint with CWQ method make the image more confusion than the CWQ method even if combined with SE and ACE methods After deciphering the right part of Fig 1 by performing the process of decryption, we can get the recovered image which is identical to the original image, the left part of Fig 1.

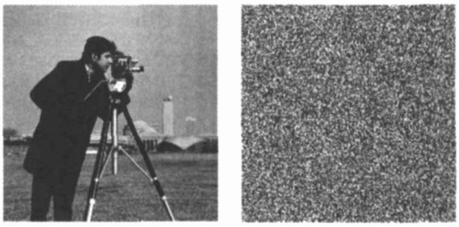

**Fig.1 Original image $M$ and cipher-image $N_1$**

## 4 Discussions and Conclusions

Just as our discussion above, when $n$ is large enough, the value of each pixel at time $t = n$ is determined strictly by local rule $f$, $g$ and the values of all pixels at time $t = 0$, which causes that our proposed system satisfies obvious avalanche effect and diffusion property For example, if we alter local rule $gf$ just a little such as changing the value of $gf(010010101)$ to be $1 - gf(010010101)$, we can obtain a new cipher-image $N_2$, i e , the left part of Fig 2, after encrypting Cameraman image once more without changing the other factors

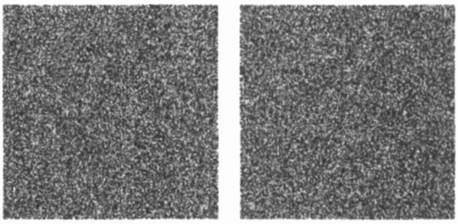

**Fig.2 New cipher-image $N_2$ and result image $N_3$ of performing XOR operation on $N_1$ and $N_2$**

Next, we can get $N_3$, the right part of Fig 2, to display the pixel-wise absolute difference of the two cipher-images $N_1$ and $N_2$ through the operation of XOR on them. This fact shows that the two cipher-images have no similarities even though the local rules differ by only one value

Since wavelet transform has the feature of energy convergence which may do some help to statistical analysis, it is essential for an eavesdropper, Charlie, to find the local rules $f$, $g$ and time $n$ that can be considered as part of the key of our algorithm. From the discussion in Section 1, we know that the set of independent variables of 1-neighborhood local rule $f$ contains 512 elements which means that there are $2^{512}$ local rules in two-dimensional CA. And the range of local rule can be widened further if we replace 1-neighborhood by 2-neighborhood There are 25 cells in every cell' s 2-neighborhood, and the number of independent variables of local rule achieves $2^{25}$. Then the set of local rules would contain $2^{2^{25}} = 2^{33554432}$ elements that make the amount of keys of our algorithm larger than ever with little affect on the speed of encryption and decryption But if we widen the neighborhood furthermore by replacing 2-neighborhood with 3-neighborhood, then the set of local rules would contain $2^{2^{49}} = 2^{562949953421312}$ elements, since there are 49 cells in every cell's 3-neighborhood A 3-neighborhood local rule has better avalanche effect than a 2-neighborhood local rule naturally because the state of a cell would be affected by the states of cells in its larger neighborhood It seems that it is better for us to choose a 3-neighborhood local rule instead of a 2-neighborhood local rule Whereas, it is unpractical for us to implement the computer simulation for that a 3-neighborhood local rule would need too large memory. For a 1-neighborhood rule $f$ which can be represented by $\varepsilon_1\varepsilon_2\cdots\varepsilon_{511}\varepsilon_{512}$ it needs 512 bit( or 64 byte to be stored in memory, since every $\varepsilon_i$ takes 1-bit Then, for a 2-neighborhood rule $g$ that can be represented by $\varepsilon_1\varepsilon_2\cdots\varepsilon_{33554431}\varepsilon_{33554432}$, it needs 33554432 bit ( or about 4MB to be stored in memory. Further, a 3-neighborhood rule $h$ needs 64 T ( or 65536 G byte to be stored in memory which is impossible in practice However, we can take another idea and get a 3-neighborhood local rule $gf$ by acting a 1-neighborhood rule $f$ first, then acting a 2-neighborhood rule $g$ again Then, the state of a cell will also be affected by the states of cells in its 3-neighborhood, i e , the combined local rule $gf$ is actually a 3-neighborhood local rule We only need 4MB + 64B memory to store the 3-neighborhood local rule $gf$ that can be realized easily in practice This idea is applied in our encryption scheme. Note that $gf = g$ when $f$ is an identical transformation, so the key space must be larger than 233554432 However, the key space cannot achieve $2^{512} \times 2^{33554432} = 2^{33554944}$ for a combined 3-neighborhood local rule $gf$ since two different group combined local rules maybe become a same combined local rule For example, when $g_1$ and $g_2$ take some special local rules, say $g_1 = g_2 = (0, \cdots, 0)$, then $g_1f_1 = g_2f_2 = (0, \cdots, 0)$ although $f_1 \leqslant f_2$. Whereas, since such cases only take a small portion and $fg \neq gf$ in CA in general, the key space would be close to $2^{512} \times 2^{33554432} = 2^{33554944}$. Actually, this idea can be generalized by combining more 1-neighborhood local rules and 2-neighborhood local rules to get larger neighborhood local rules which can strengthen avalanche effect and enlarge the key space while take small memory in practice.

Besides avalanche effect and diffusion properties, the property of confusion of two-dimensional CA can be enhanced by CWQ method which is good at confusing image Take a $K \times K$ sized image and $L$-layer wavelet transform for example, the key space of CWQ method[12] is $[(N/2^L)^2!]^4 \times (4!)^{3\times\sum_{l=2}^{L}(N/2^L)^2}$. So the eavesdropper Charlie must contend with searching through near $2^{33554432} + [(256/2^L)^2!]^4 \times (4!)^{3\times\sum_{l=2}^{L}(256/2^L)^2}$ key space if $K = 256$ And almost perfect guess of $f$, $g$ and $n$ makes decryption impossible after the cipher-image $N_0$ is confused by CWQ method again. The volume of security key of the scheme we proposed is much larger than $10^{9536}$ which is the lower bound of the volume of security key introduced in [7] for images of size 256 × 256 The discussion of encryption speed of CWQ method has been shown in [12]. We analyze the computing complexity of the encryption process by two-dimensional CA. Assume the size of either original black-and-white binary image $M$ or random bit-pattern $R_M$ is $l \times w$. Then, we act the local rule $gf$ on $R_M$ $n$ times successively For every pixel with state value $x_{i0}$ during each iteration, we first search the states of its 9 neighbors, say $x_{i0}$, $x_{i1}$, $\cdots$, $x_{i8}$, in its 1-neighborhood Then, we replace $x_{i0}$ by the new state value $f(x_{i0}, x_{i1}, \cdots, x_{i8})$ for the pixel The time complexity of this process is only $O(1)$ if the local rule $f$ has been saved in the memory Similarly, the process also takes $O(1)$ time for the action of a 2-neighborhood local rule $g$. The total time for searching and replacing is $O(l \times w)$ in each iteration Since the iteration number is $n$, the computing complexity for obtaining $(gf)^n(R)$ is $O(n \times l \times w)$. We should execute the operation of XOR on $(gf)^n(R)$ and $M$ which costs $O(l \times w)$ time Since a gray-scale image can be considered as the combination of eight binary images, the sum of complexity for gaining cipher-image $N_0$ is $O(8 \times n \times l \times w) + O(8 \times l \times w) = O(n \times l \times w)$. For a fixed number $n$, the computational complexity is only $O(l \times w)$.

Cellular automata can exhibit fascinatingly complex behavior by dealing with the relations between the part and the whole It has been applied in other studies widely and tied in many problems such as the Conway's game which is actually a two-dimensional CA with special local rule Howard Gutowitz, a discrete dynamical system scientist, designed a CA − 1. 1 algorithm based on cellular automata This is a block encryption algorithm with key of 1088 bits, which is very effective in VLSI circuits and has been protected by patent right Due to the universality of CA model, more applications can be found in traditional cryptography and image processing

## [References]

[1] Yuan C, Zhu B B, Wang Y, et al Efficient and fully scalable encryption for MPEG−4 FGS[C] // Proc IEEE Int Symposium on Circuits and Systems, 2003(2: 620-623

[2] Wee S J, Apostolopoulos J G. Secure scalable streaming enabling transcoding without decryption[C] // Proc IEEE Int Conference on Image Processing, 2001(1: 437-440.

[3] Tosun A S, Feng W C. Lightweight security mechanisms for wireless video transmission[C] // Proc IEEE Int Conference on Information Technology: Coding and Computing, 2001: 157-161.

[4] Wolfram S. Cryptography with cellular automata[C] //Advances in Cryptology-CRYPTO 85, Lecture Notes in Computer Science, 1985(218: 429-432

[5] Nandy S, Kar B K, Chaudhuri P. Theory and applications of cellular automata in cryptography[J]. IEEE Trans Comput, 1994, 43: 1 346-1 357.

[6] Mihaljevic M. Security examination of certain cellular automata based key stream generator[C] // ISITA 96− 1996 IEEE Int Symp Inform Theory and Appl, 1996: 246-249.

[7] Chen R, Lu W, Lai J. Image encryption using progressive cellular automata substitution and SCAN[C] // IEEE ISCAS, 2005(2: 1 690-1 693.

[8] Chaudhuri P P, Chaudhuri D R, Nandi S, et al Additive Cellular Automata: Theory and Applications[M]. New York: IEEE Press, 1997.

[9] Sutner K. Additive automata on graphs[J]. Complex Systems, 1998, 2(1: 1-28.

[10] Shapiro J M. Embedded image coding using zerotrees of wavelet coding[J]. IEEE Transactions on Signal Processing, 1993, 41(12: 3 445-3 462

[11] Said A. A new fast and efficient image code based on set partitioning in hierarchical trees[J]. IEEE Transactions on Circuits and Systems for Video Technology, 1996(6: 243-250

[12] Lian S, Wang Z. Comparison of several wavelet coefficients confusion methods applied in multimedia encryption[C] // Proc Int Conference on Computer Networks and Mobile Computing, 2003: 372-376

[责任编辑: 陆炳新]