基于耦合触发细胞自动机的图像加密算法

夏学文[1] 李元香[2] 曾 辉[1]

(武汉大学计算机学院 武汉 430079)[1] (武汉大学软件工程国家重点实验室 武汉 430072)[2]

摘 要 提出了一种基于一维触发细胞自动机的图像加密技术。根据图像文件类型的特点,在加密前对图像进行了简单的预处理,将每个像素点的信息分割成两部分;相应地,密钥也被分成两部分,从而将原始图像信息分成两部分并加密。本加密系统采用的是对称耦合式的触发细胞自动机结构,一方面,加密算法和解密算法可以共享该结构,从而降低了硬件的实现代价;另一方面,基于此结构,对加密后的信息进行了密钥共享和分存,确保只有在同时获得一对密文时才能正确解密。触发细胞自动机的反转规则由子密钥流和图像信息本身共同决定,而且在细胞状态迭代的过程中能自适应地进行调整。密钥空间,即反转规则表,随着细胞自动机邻居半径增大呈指数增长,所以可以根据不同的安全性要求,通过增加细胞自动机的邻居半径来实现。仿真实验证实了该算法的有效性,并得到了较好的加密效果。

关键词 图像加密,触发细胞自动机,密钥共享与分存,对称耦合结构

中图法分类号 TP301.6 **文献标识码** A

Image Encryption Algorithm Based on Coupled Toggle Cellular Automata

XIA Xue-wen[1] LI Yuan-xiang[2] ZENG Hui[1]

(College of Computer, Wuhan University, Wuhan 430079, China)[1]

(State Key Laboratory of Software Engineering, Wuhan University, Wuhan 430072, China)[2]

Abstract A novel image encryption algorithm, which is based on one dimension cellular automata (1-D CA), was proposed. Before encryption, unlike other algorithms, a simple pretreatment was adopted to conceal visual information of original image, which was separated into two parts according to its information characteristic. These two parts were encrypted parallelly. Since secret key was divided into two subkeys corresponding to two subsections of image, only obtaining two parts of cipher text could receive decrypt correctly. The key of this encryption system is the inverse rules of toggle cellular automata which is not only based on secret key generated by a keystream generator, but also depends on image itself. Furthermore, symmetrical-coupled structure of CAs simplifies the cryptosystem's hardware. The proposed image encryption method satisfies the properties of confusion and diffusion due to the wonderful CA substitution as well as the pretreatment. The characteristics of the proposed image encryption system are sharable hardware structure by encryption and decryption, key sharing, self-adaptive inverse rules, very large number of keys and favorable fault tolerance. Simulation results for gray image show that the proposed image encryption method works as out expectations.

Keywords Image encryption, Toggle cellular automata, Key divided-deposit, Symmetrical-coupled

1 引言

随着 Internet 技术的飞速发展,通过网络交换信息已经成为一个主要的信息交流手段。图像信息形象、生动,因而被广泛利用。通过 Internet 交换、发布图像信息不但方便快捷,不受地域限制,而且可以为数据拥有者节省大量的费用,但这也同时为不法分子利用网络技术获取未授权数据提供了渠道。因此,图像拥有者为了保护自身的利益,就需要可靠的图像数据加密技术。

与传统的文本信息不同的是,数字图像具有数据量大、冗余度高等特点,因此不宜利用传统的基于文本信息的加密技术进行加密。近年来,针对数字图像的这些特点,许多学者提出了各种不同的数字图像加密技术,其基本思想可以分为像素位置置乱[1,2]、像值变换[3,4]和位置置换与像值变换相结合[5]等3类。

像素位置置乱的本质是改变原始图像中各像素点的位置,使其变成一个看似毫无意义的图像,从而防止信息的泄露。较具代表性的就是 Arnold 置换算法[6],该算法在置换迭代的初期具有很好的置乱效果,但由于动力系统固有的特性,经过一定次数的迭代后,各像素点会回到其最初的位置,从而恢复成原始图像,即 Arnold 置换算法具有周期性。所以,如果加密算法泄露后,攻击者可以从任一密文开始进行有限次

到稿日期:2008-03-04 本文受国家自然科学基金(60473014),国家博士学科点科研基金项目(20030486049)资助。

夏学文(1974—),男,博士研究生,研究方向为细胞自动机、演化算法、信息安全,E-mail:laughkid@163.com;李元香(1962—),男,博士,教授,研究方向为演化算法、并行算法。

的迭代来非法获得原始图像。另一典型的像素位置置乱算法是幻方置换算法。该算法将一幅图像 $A(n\times n)$ 映射成一个 n 阶的幻方矩阵 $B_{n\times n}$，通过对 $B_{n\times n}$ 的初等变换来实现图像 A 中像素位置的置乱。然而，由于 $B_{n\times n}$ 是一个有限阶的矩阵，因此和 Arnold 算法一样，其初等变换也具有周期性，一旦置乱算法泄露，真实信息就很容易被窃取。基于置乱技术的图像加密技术总体上来说可以等效为对图像矩阵进行有限步的初等矩阵变换，从而打乱图像像素的排列位置。但初等矩阵变换是一线性变换，其保密性不高[7]。

与像素位置置乱算法不一样的是，像值变换是通过改变像素值[3]，而不是改变像素位置来实现信息的隐藏。然而，由于图像信息具有其自身的统计特性，而且其密钥空间一般都很小，因此简单地变换像素值很难抵御有效的攻击。所以很少单纯采用像值变换进行图像加密，而是将其与像素位置置乱算法相结合对图像进行加密。

基于混沌系统的图像加密技术[8]是一种典型的位置置乱与像值变换相结合的方法。该方法具有无周期性以及对初始状态及参数极其敏感等特性。其安全性依赖于密钥流生成器（即混沌系统）所生成密钥流的随机性。但 Dedieu[9] 通过研究指出：混沌系统对参数的敏感性不仅意味着保密性，攻击者反而可以利用这一特点，用参数自适应同步控制的方法对混沌系统的参数（即密钥）进行辨识，从而达到破译的目的。而且低维混沌系统的保密性能还有待于进一步提高[10]。

近年来，利用细胞自动机（Cellular Automata，CA）进行密码系统的设计吸引了众多学者，其原因就在于细胞自动机能通过简单的转换规则来实现复杂的行为模式。1985 年，Wolfram[11] 首次利用细胞自动机来生成密钥流，此后很多研究表明[12-14]，可以通过提高细胞自动机结构的复杂性来提高密钥流的安全性（即随机性）。2002 年，张传武[15] 提出了一种基于触发细胞自动机的加密算法，该算法具有较大的密钥空间和较简单的硬件结构。

本文提出了一种基于耦合结构的触发细胞自动机的图像加密技术。根据图像像素信息的特点，将图像像素信息分成两部分，即高位部分和低位部分，并对高位部分进行了简单的处理从而达到有效隐藏信息的目的。相应地，密钥也分成两部分，用来分别对高位和低位进行加密。此外，本加密算法还利用密钥分存技术来提高算法的安全性。实验分析表明，该方法具有较高的加密效率和安全性。

2 对称耦合触发细胞自动机模型

2.1 触发细胞自动机

细胞自动机（Cellular Automata，CA）是一种时间、空间和状态都离散的动力系统，具有规整、模块化以及内在并行性，便于软件和硬件实现等特点，这使得细胞自动机尤其适合应用于密码学。在细胞自动机中，有一类具有特性性质的细胞自动机，其细胞单元的转换状态与其领域状态配置中的某个单元的状态值之间存在线型关系，即改变领域状态配置中这一单元的状态值将直接导致转移状态的改变，称这种转移状态与其领域状态配置中的某位状态具有线性关系的规则称为反转规则，这类细胞自动机称为触发细胞自动机[16]。触发细胞自动机的迭代过程可简单描述为：

$$1+S_i^{t+1}=f(S_{i-r}^t\cdots,1+S_{i+j}^t,\cdots S_{i+r}^t)\quad -r\leqslant j\leqslant r \qquad (1)$$

其中，$S_i^t\in\{0,1\}$ 表示第 i 个细胞在 t 时刻的状态，r 为细胞自动机的规则半径，j 为触发细胞，$+$ 为模 2 运算，即异或运算。当 $j=-r$ 时，即最左边的细胞为触发细胞，我们称之为左触发细胞自动机；同理，当 $j=r$ 时，我们称之为右触发细胞自动机。表 1 为邻居半径 $r=1$ 的右触发细胞自动机的反转规则表。

表 1 右触发细胞自动机（规则为 90）

S_{i-1}^t	S_i^t	S_{i+1}^t	S_i^{t+1}	S_{i-1}^t	S_i^t	S_{i+1}^t	S_i^{t+1}
0	0	0	0	0	0	1	1
0	1	0	0	0	1	1	1
1	0	0	1	1	0	1	0
1	1	0	1	1	1	1	0

2.2 反转规则表

利用触发细胞自动机的特性，就可以构造任意规则半径的细胞自动机的反转规则表。对于规则半径为 r，$S\in\{0,1\}$ 的一维细胞自动机，其规则表的大小为 2^{2r+1}。以右触发细胞自动机为例，构造半径为 r 的反转规则表的过程如下：

输入：长度为 2^{2r} 的任意二进制串 $(b_{2^{2r}-1},b_{2^{2r}-2},\cdots,b_0)$；

输出：长度为 2^{2r+1} 的反转规则表 T：$(t_{2^{2r+1}-1},t_{2^{2r+1}-2},\cdots,t_0)$；

算法：

1. $i=2^{2r}-1$；
2. 若 $b_i=0$，则 $t_{2i}=0,t_{2i+1}=1$；若 $b_i=1$，则 $t_{2i}=1,t_{2i+1}=0$；
3. $i=i-1$；若 $i\geqslant 0$，转 2；
4. 结束。

例如，当 $r=1$ 时，若输入的二进制位串是：1101，则构造出的右触发细胞自动机的规则号为 166。

由反转规则表的构造算法可以知道，对于任意触发细胞自动机，可以构造出 $2^{2^{2r}}$ 个不同的反转规则表。

2.3 对称耦合触发细胞自动机

耦合细胞自动机是指不同细胞自动机在迭代的过程中是相互影响、相互作用，从而共同决定整个 CA 系统的演化状态。本文采用的是由两个右触发 CA 组成的对称耦合系统，具体迭代过程可用下式表示：

$$\begin{cases}S_{(A,i)}^{t+1}=f(S_{(B,i-r)}^t\cdots,S_{(A,i)}^t,\cdots S_{(B,i+r)}^t)\\ S_{(B,i)}^{t+1}=g(S_{(A,i-r)}^t\cdots,S_{(B,i)}^t,\cdots S_{(A,i+r)}^t)\end{cases} \qquad (2)$$

其中，$S_{(A,i)}^t$ 表示触发细胞自动机 A 中第 i 个细胞在 t 时刻的状态。

由(2)可以看出，A 中细胞 i 的演化不仅与其自身的状态有关，还与 B 中对应位置细胞的邻居状态有关，相应地，B 中细胞 i 的化不仅与其自身的状态有关，还与 A 中对应位置细胞的邻居状态有关。这样两个细胞自动机通过状态之间的相互作用和共同演化来决定着整个 CA 系统的演化，从而构成一个耦合结构的触发细胞自动机。本文将采用右触发细胞自动机构造耦合细胞自动机，即：

$$\begin{cases}1+S_{(A,i)}^{t+1}=f(S_{(B,i-r)}^t\cdots,S_{(A,i)}^t,\cdots 1+S_{(B,i+r)}^t)\\ 1+S_{(B,i)}^{t+1}=g(S_{(A,i-r)}^t\cdots,S_{(B,i)}^t,\cdots 1+S_{(A,i+r)}^t)\end{cases} \qquad (3)$$

3 算法原理

3.1 算法描述

对于一幅数字图片，其每个像素点的大部分信息都集中在该像素灰度值的高位部分，因此，如何在加密前有效地隐藏这些高位部分所含的信息将会十分重要。本文中，每个像素点的灰度值(m-bits)被切分为两个部分：高两位部分 $P_h=(P_{m-1},P_{m-2})$ 和 $P_l=(P_{m-3},P_{m-4},\cdots,P_0)$ 低位部分。相应地，长度为 m-bits 的随机位流 k 也将被分成两部分 k_h 和 k_l，并保证 P_h 与 k_h 的长度之和等于 P_l 与 k_l 的长度之和。加密时，每个像素将分为两部分并行加密，即由 P_h 与 k_h 组成的高位部分和由 P_l 与 k_l 组成的低位部分。因此整幅图片可依此方法将像素点的信息与随机位流各分成两部分，并将相应部分组合成待加密的高位部分 H 和低位部分 L。加密时根据定义的块长度来逐次加密 H 和 L 中相应长度的一对明文块；接收方收到一对密文块进行解密后，再根据明文中的数据结构最终将像素的有效信息从解密后的明文中得到。下面我们仅就长度为 n 比特的一对明文块 $H:(h_{n-1},h_{n-2},\cdots,h_0)$ 和 $L:(l_{n-1},l_{n-2},\cdots,l_0)$ 来介绍加密和解密算法。需要注意的是，H 和 L 加密的过程是并行进行的，而其内部却是逐位进行的。

假定细胞自动机的邻居半径为 r，加密、解密算法可描述如下。

加密算法

1. 定义迭代参数：$I=n,J=m$；

2. 将 H 和 L 分别对两个长度为 n 的循环移位寄存器 R_h 和 R_l 进行初始化，即：$R_h:(r_{n-1},r_{n-2},\cdots,r_0)=(h_{n-1},h_{n-2},\cdots,h_0)R_l:(r_{n-1},r_{n-2},\cdots,r_0)=(l_{n-1},l_{n-2},\cdots,l_0)$；

3. 根据 R_h 和 R_l 中第 $n-2$ 位到第 $n-2^{2r}-1$ 位，即 $(r_{n-2},r_{n-3},\cdots,r_{n-2^{2r}-1},)$ 分别与子密钥流 K 逐位进行异或运算，并根据运算的结果分别确定 R_h 和 R_l 的反转规则表 T_h 和 T_l；

4. 将 R_l 中 $(r_{2r-1},\cdots,r_0)$ 值作为 T_h 的地址进行查表，得到 x；将 R_h 中 $(r_{2r-1},\cdots,r_0)$ 值作为 T_l 的地址进行查表，得到 y；

5. 将 R_h 中 r_{n-1} 与 x 进行异或，即：$r_{n-1}=r_{n-1}\oplus x$，将 R_l 中的 r_{n-1} 与 y 进行异或，即：$r_{n-1}=r_{n-1}\oplus y$；

6. R_h 与 R_l 同时循环左移一位；

7. $I=I-1$，如果 $I>0$，转到 3；

8. $J=J-1$，如果 $J>0$，则 $I=n$，转到 3；

9. 结束。

当合法用户得到密文块时，可以按如下过程进行解密：

1. 定义迭代参数：$I=n,J=m$；

2. 将得到的一对密文块分别对循环移位寄存器 R_h 和 R_l 进行初始化；

3. R_h 和 R_l 同时循环右移一位；

4. 根据 R_h 和 R_l 中第 $n-2$ 位到第 $n-2^{2r}-1$ 位，即 $(r_{n-2},r_{n-3},\cdots,r_{n-2^{2r}-1},)$ 分别与子密钥流 K 逐位进行异或运算，并依运算的结果分别确定 R_h 和 R_l 的反转规则表 T_h 和 T_l；

5. 将 R_l 中 $(r_{2r-1},\cdots,r_0)$ 值作为 T_h 的地址进行查表，得到 x；将 R_h 中 $(r_{2r-1},\cdots,r_0)$ 值作为 T_l 的地址进行查表，得到 y；

6. 将 R_h 中 r_{n-1} 与 x 进行异或，即：$r_{n-1}=r_{n-1}\oplus x$，将 R_l 中 r_{n-1} 与 y 进行异或，即：$r_{n-1}=r_{n-1}\oplus y$。

7. $I=I-1$，如果 $I>0$，转到 3；

8. $J=J-1$，如果 $J>0$，则 $I=n$，转到 3；

结束。

3.2 系统硬件结构

通过对加密、解密过程的比较可以看出，加解密方案只有两点不同：循环移位寄存器的方向相反；移位与异或运算的次序不同，加密时是先运算后移位，而解密时时先移位后运算。因此可以将加、解密系统共享一个功能模块，该结构由两个双向移位寄存器、两个反转规则表、两个规则生成部件、两个异或运算单元、两个双向移位寄存器的移位控制单元以及一个密钥流生成器组成，硬件结构如图 1 所示。

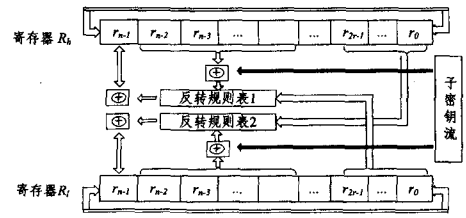

图 1 加密系统结构图

3.3 算法正确性证明

由于本文选取的图片的灰度值都是 8 比特，细胞自动机的规则半径 $r=1$，不失一般性，我们将通过单个像素的加、解密过程来证明该算法的正确性。

如前所述，首先将该像素的灰度值 $(p_7,p_6,\cdots,p_0)$ 和随机位流 $(k_7,k_6,\cdots,k_0)$ 进行分割和重组，得到高位、低位部分，再对耦合的细胞自动机系统中的两个细胞自动机 CA_h 和 CA_l 分别进行初始化，得到待加密的两部分明文，这里分别用 $(P_{h7},P_{h6},\cdots,P_{h0})$ 和 $(P_{l7},P_{l6},\cdots,P_{l0})$ 表示。加密迭代过程可表示如下（CA_h 和 CA_l 中第 j 个细胞在第 i 次迭代加密后的状态分别用 $E_{h(i,j)}$ 和 $E_{l(i,j)}$ 表示）：

CA_h：	P_{h7}	P_{h6}	$\cdots$	P_{h1}	P_{h0}
	$E_{h(1,7)}$	$E_{h(1,6)}$	$\cdots$	$E_{h(1,1)}$	$E_{h(1,0)}$
	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
	$E_{h(n-1,7)}$	$E_{h(n-1,6)}$	$\cdots$	$E_{h(n-1,1)}$	$E_{h(n-1,0)}$
	$E_{h(n,7)}$	$E_{h(n,6)}$	$\cdots$	$E_{h(n,1)}$	$E_{h(n,0)}$
CA_l：	P_{l7}	P_{l6}	$\cdots$	P_{l1}	P_{l0}
	$E_{l(1,7)}$	$E_{l(1,6)}$	$\cdots$	$E_{l(1,1)}$	$E_{l(1,0)}$
	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
	$E_{l(n-1,7)}$	$E_{l(n-1,6)}$	$\cdots$	$E_{l(n-1,1)}$	$E_{l(n-1,0)}$
	$E_{l(n,7)}$	$E_{l(n,6)}$	$\cdots$	$E_{l(n,1)}$	$E_{l(n,0)}$

当接收方收到密文对以后（分别用 $(C_{h7},C_{h6},\cdots,C_{h0})$ 和 $(C_{l7},C_{l6},\cdots,C_{l0})$ 表示），对密文进行解密的迭代过程可表示如下（CA_h 和 CA_l 中第 j 个细胞在第 i 次迭代解密后的状态分别用 $D_{h(i,j)}$ 和 $D_{l(i,j)}$ 表示）：

CA_h：	C_{h7}	C_{h6}	$\cdots$	C_{h1}	C_{h0}
	$D_{h(1,7)}$	$D_{h(1,6)}$	$\cdots$	$D_{h(1,1)}$	$D_{h(1,0)}$
	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
	$D_{h(n-1,7)}$	$D_{h(n-1,6)}$	$\cdots$	$D_{h(n-1,1)}$	$D_{h(n-1,0)}$
	$D_{h(n,7)}$	$D_{h(n,6)}$	$\cdots$	$D_{h(n,1)}$	$D_{h(n,0)}$
CA_l：	C_{l7}	C_6	$\cdots$	C_{l1}	C_0
	$D_{l(1,7)}$	$D_{l(1,6)}$	$\cdots$	$D_{l(1,1)}$	$D_{l(1,0)}$
	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
	$D_{l(n-1,7)}$	$D_{l(n-1,6)}$	$\cdots$	$D_{l(n-1,1)}$	$D_{l(n-1,0)}$

$$D_{l(n,7)} \quad D_{l(n,6)} \quad \cdots \quad D_{l(n,1)} \quad D_{l(n,0)}$$

根据前面的算法描述我们知道，加、解密时每次迭代包括两个过程：移位和运算，为了证明的方便，我们在这两个过程中定义了一个中间状态。例如，在加密时，CA_h 中第 i 个细胞在第 n 次迭代过程中，经过异或运算后的状态可用 $E'_{h(n,i)}$ 表示；而在解密时，CA_h 中第 i 个细胞在第 n 次迭代过程中，经过移位后的状态可用 $D'_{h(n,i)}$ 表示。

由于加密(解密)过程中每次迭代步骤是相同的，所以这里我们只需证明 $(D_{h(1,7)}, D_{h(1,6)}, \cdots, D_{h(1,0)}) = (E_{h(n-1,7)}, E_{h(n-1,6)}, \cdots, E_{h(n-1,0)})$ 和 $(D_{l(1,7)}, D_{l(1,6)}, \cdots, D_{l(1,0)}) = (E_{l(n-1,7)}, E_{l(n-1,6)}, \cdots, E_{l(n-1,0)})$。根据加、解密算法和所采用的对称耦合结构的特性，这里我们只证明前，后者的证明方法与之类似。

证明：根据上面的加密迭代过程，可以有：

经过异或运算后：

$$\begin{cases} E'_{h(n,7)} = f(E_{l(n-1,1)}, E_{l(n-1,0)}, E_{h(n-1,7)}) \\ E'_{h(n,6)} = E_{h(n-1,6)} \\ \cdots \\ E'_{h(n,0)} = E_{h(n-1,0)} \end{cases} \tag{4}$$

经过循环左移后：

$$\begin{cases} E_{h(n,7)} = E'_{h(n,6)} = E_{h(n-1,6)} \\ E_{h(n,6)} = E'_{h(n,5)} = E_{h(n-1,5)} \\ \cdots \\ E_{h(n,1)} = E'_{h(n,0)} = E_{h(n-1,0)} \\ E_{h(n,0)} = E'_{h(n,7)} = f(E_{l(n-1,1)}, E_{l(n-1,0)}, E_{l(n-1,7)}) \end{cases} \tag{5}$$

$(E_{h(n,7)}, E_{h(n,6)}, \cdots E_{h(n,0)})$ 即为待传输的密文。在式(4)、(5)中，反转规则 f 由 $(E_{h(n-1,6)}, E_{h(n-1,5)}, E_{h(n-1,4)}, E_{h(n-1,3)})$ 和子密钥 K 共同确定。

同样地，当正确收到密文 $(C_{h7}, C_{h6}, \cdots, C_{h0})$ 后也需进行类似的处理过程。

经过循环右移后：

$$\begin{cases} D'_{h(1,7)} = C_{h0} = E_{h(n,0)} \\ D'_{h(1,6)} = C_{h7} = E_{h(n,7)} \\ \cdots \\ D'_{h(1,0)} = C_{h1} = E_{h(n,1)} \end{cases} \tag{6}$$

经过异或运算后：

$$\begin{cases} D_{h(1,7)} = g(D'_{l(1,1)}, D'_{l(1,0)}, D'_{h(1,7)}) \\ D_{h(1,6)} = D'_{h(1,6)} = E_{h(n,7)} \\ \cdots \\ D_{h(1,0)} = D'_{h(1,0)} = E_{h(n,1)} \end{cases} \tag{7}$$

在式(7)中，反转规则 g 由 $(D'_{h(1,6)}, D'_{h(1,5)}, D'_{h(1,4)}, D'_{h(1,3)})$ 和子密钥 K 共同确定。由式(6)、(7)可知：$(D'_{h(1,6)}, D'_{h(1,5)}, D'_{h(1,4)}, D'_{h(1,3)}) = (E_{h(n,7)}, E_{h(n,6)}, E_{h(n,5)}, E_{h(n,4)})$，即 $f=g$。

根据以上结果以及对称耦合结构的性质可知：

$$\begin{cases} D_{h(1,6)} = E_{h(n,7)} = E_{h(n-1,6)} \\ D_{h(1,5)} = E_{h(n,6)} = E_{h(n-1,5)} \\ \cdots \\ D_{h(1,0)} = E_{h(n,1)} = E_{h(n-1,0)} \end{cases} \tag{8}$$

由以上结果可知：

$$\begin{cases} D'_{l(1,1)} = E_{l(n,2)} = E_{l(n-1,1)} \\ D'_{l(1,0)} = E_{l(n,1)} = E_{l(n-1,0)} \end{cases} \tag{9}$$

即有：$D_{h(1,7)} = g(D'_{l(1,1)}, D'_{l(1,0)}, D'_{h(1,7)})$

$= f(E_{l(n-1,1)}, E_{l(n-1,0)}, E_{h(n,0)})$

$= f(E_{l(n-1,1)}, E_{l(n-1,0)}, f(E_{l(n-1,1)}, E_{l(n-1,0)}, E_{h(n-1,7)}))$

如果 $E'_{h(n,7)} = f(E_{l(n-1,1)}, E_{l(n-1,0)}, E_{h(n-1,7)}) = E_{h(n-1,7)}$，则 $_{h(1,7)} = f(E_{l(n-1,1)}, E_{l(n-1,0)}, E_{h(n-1,7)}) = E_{h(n-1,7)}$。

如果 $E'_{h(n,7)} = f(E_{l(n-1,1)}, E_{l(n-1,0)}, E_{h(n-1,7)}) = \overline{E_{h(n-1,7)}}$，则 $D_{h(1,7)} = f(E_{l(n-1,1)}, E_{l(n-1,0)}, \overline{E_{h(n-1,7)}}) = \overline{E'_{h(n,7)}} = E_{h(n-1,7)}$。即 $D_{h(1,7)} = E_{h(n-1,7)}$。

由式(8)和上式，有：$D_{h(1,i)} = E_{h(n-1,i)}$，$0 \leqslant i < 8$。

对于其他不同的明文块长度和邻居半径的 CA 具有同样的结果。

至此说明此算法的加、解密是正确的。

4 实验结果与分析

本文利用两个触发 CA 构成的对称式耦合加、解密系统对 128×128 的灰度值为 8 比特的 Lenna 图按照所述的算法进行加、解密。结果如图 2 所示。

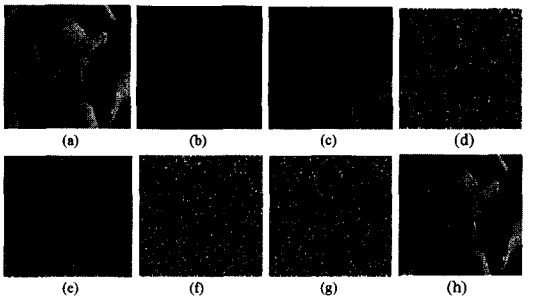

图 2 加密结果：(a)原始图像；(b)混合子密钥前的低位部分；(c)混合子密钥前的高位部分；(d)混合子密钥后的低位部分；(e)混合子密钥后的高位部分；(f)加密(d)后的结果；(g)加密(e)后的结果；(h)解密后的图像

4.1 高位信息的隐藏

根据算法我们知道，加密前每个像素的灰度值将分成两部分：P_h 和 P_l。相应地，具有与像素灰度值相同长度的随机位流也分成两部分：k_h 和 k_l。由于高位部分 P_h 包含着绝大部分该灰度值的信息，因此在加密前可先对其进行简单的预处理。处理方法是将 P_h 移位，其它部分填充上 k_h；图3给出了对图片 lenna 的不同处理结果，从中可以看出，当像素灰度值的高两位移至最低两位，前 6 位填充上 6 位的子密钥 k_h 时，隐藏效果最好。由于 P_l 所含信息较少，因此不进行移位处理，而是直接将高位部分填充上 k_l。

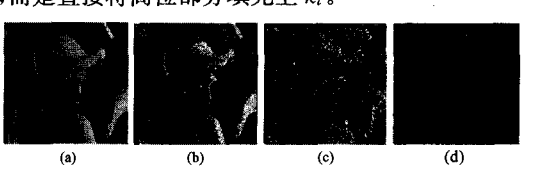

图 3 不同混合方式的结果：(a)原始图像；(b) P_h 保持在原位，k_h 填充低 6 位；(c) P_h 右移 1 位，k_h 填充其它位；(d) P_h 右移至最低 2 位，k_h 填充其它位；

4.2 统计特性

通常来讲，一幅图像上的像素点的信息具有某种统计特性，因此，如果加密后的图像置乱效果不好，就可能通过统计

分析被破译。本文分别对图片 lenna 和一幅全黑图片(即像素灰度值全为 0)进行了加密,对加密前后的结果进行了直方图分析,结果如图 4 所示。从原始图像与加密图像的直方图可以直观地看出,加密图像具有较好的置乱效果。

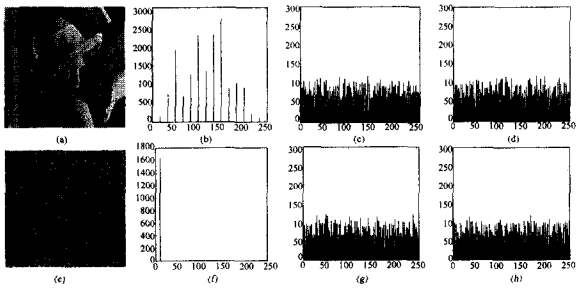

图 4 原始图像和加密后的图像直方图对比(a)原始图像"lenna";(b)"lenna"灰度值直方图;(c)、(d)分别为"lenna"加密后高、低位部分灰度直方图;(e)纯黑图片;(f)纯黑图片的灰度直方图;(g)、(h)分别为加密后高、低位部分灰度直方图

为了进一步精确地测试加密后图像的置乱效果,本文还对加密后的图像进行了随机性测试。DIEHARD 测试集[17]和 ENT 测试集[18]是两种较常用的随机性测试方法,前者甚至被认为是最严格的测试方法之一,但由于该测试集需要至少 10M 字节的测试数据,所以本文将采用 ENT 测试集来检验利用本加密方法加密后的图像的随机性。ENT 测试集包含 4 个指标:熵(entropy,Ent)、算法平均值(Arithmetic mean value,Amv)、线性相关系数(Serial correlation coefficient,Scc)和 chi-分布(chi-distribution,Chi)。各项指标的理想值分别为:$Ent=8$,$Amv=127.5$,$|Scc|=0$,$10\%\leqslant Chi\leqslant 90\%$。

本文对图像 lenna 进行不同轮次的加密所得到的高、低位部分密文 C_h 和 C_l 进行了测试,结果如表 2 所列。可以看出,当加密次数小于 3 时,Chi 测试指标未能通过,以往的研究也表明该指标是最难达到的;当加密轮次大于 3 时,所有的测试指标的结果都很理想。

表 2 不同加密轮次下的密文的随机性

Encryption round	Cipher text	ENT	AMV	SCC	CHI
1	C_h	7.9369	127.6228	0.00309	Failed
	C_l	7.8343	128.3983	0.02382	Failed
2	C_h	7.9797	127.3351	0.01476	Failed
	C_l	7.9689	127.6181	0.01225	Failed
3	C_h	7.9852	126.3654	0.01058	Failed
	C_l	7.9859	128.8422	−0.0058	10%
4	C_h	7.9863	127.5369	0.00842	50%
	C_l	7.9863	127.4450	−0.0028	50%
5	C_h	7.9874	126.9293	0.01979	25%
	C_l	7.9880	126.7076	−0.0088	50%

通过以上仿真结果可以看出本加密算法具有较优的置乱效果,能有效抵抗唯密文攻击。

4.3 密钥空间

在加密和解密过程中,密钥由 CA 系统本身和子密钥流共同决定。半径为 r 的细胞自动机系统有 2^{2r+1} 种状态,同时有 $2^{2^{2r+1}}$ 种规则,由于采用的是两个状态为一组的反转规则,所以每个细胞自动机实际的密钥空间有 $2^{2^{2r}}$。本文采用的是由两个触发细胞自动机组成的对称耦合结构,而且各自采用自己的反转规则,因此密钥空间为 $2^{2^{2r}}\times 2^{2^{2r}}$。如果取 $r=4$,则密钥空间可达到 $2^{2^{2r}}\times 2^{2^{2r}}\approx 1.34\times 10^{154}$,且当 r 每增加 1 时,密钥空间增加为自身的 16 次方,即 $K_{r+1}=K_r^{16}$。通过分析可知本加密系统的密钥复杂度呈指数增长,因此采用穷举搜索密钥是不可能的,即系统在计算上是安全的。

由于对同一图像加密时,每次引入的随机数都不同,所以每次得到的密文也不同,但解密后所得到的图像却是相同的,很难得到唯一的明文-密文对。因而可以抵抗已知明文和已知密文攻击。

4.4 密钥分存机制

密钥分存[2]的概念是由 Shamir 在 1979 年提出的,其思想是把密钥 K 分解成 n 个子密钥 k_i,$0\leqslant i<n$,并且满足任意 $m(1\leqslant m\leqslant n)$ 个子密钥的组合才能恢复密钥 K,而若少于 m 个子密钥则不能获得密钥 K 的任何信息,也就是密码学上称之为门陷技术。

由加密算法和加密系统结构图可以看出,寄存器 R_h 和 R_l 所对应的 CA_h 和 CA_l 的反转规则表,即系统的密钥,并不是由自己本身的细胞状态直接决定,而是由与其耦合的 CA 的某些细胞和子密钥流共同确定。这种性质使得加密后的两部分密文不能单独解密,即加密系统的密钥是分存在这两部分密文中的,只有同时拥有这一对密文才能正确解密。这种密钥分存机制进一步增强了系统的安全性。

4.5 容错性

和文本信息不一样的是,图像信息允许有一定的差错出现,即在不影响合法用户对图像真实信息的理解的前提下,允许图像在网络传输过程中有一定的失真现象。本文在不同的网络传输误码率情况下对图像 lenna 进行了仿真实验,结果如图 5 所示。

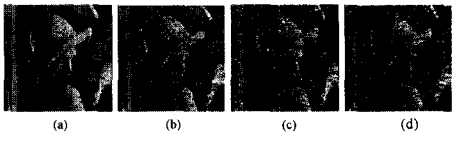

图 5 不同误码率下的解密结果,误码率依次为:(a) 1%;(b) 10%;(c) 20%;(d) 30%

实验结果表明,当网络误码率小于 20%时,合法用户将接收到的加密图像文件解密后基本不影响对原始图像的理解。当误码率达到 30%时,解密后的图像会对原始图像的理解造成一定的影响,但可以通过一些图像处理算法从一定程度上解决该问题。因此可以看出,本算法具有较好的容错性。

结束语 本文给出了一种基于耦合结构的触发细胞自动机的数字图像加密算法。在本算法中,图像像素信息被分成两部分,并对高位部分进行了简单的预处理以有效隐藏图像的真实信息。在加密的过程中,高位部分和低位部分并行地迭代加密而且相互作用,通过这种加密方式实现了密钥分存和共享,即只有同时正确地获得加密后的高、低位密文才能正确解密。算法的密钥由图像本身和子密钥共同决定,而且在进行迭代加密的过程中是不断变化的。从算法来看,本文采用的加、解密规则都具有迭代结构,适合于用计算机快速实现。实验结果也表明,本算法的迭代轮数不需要选择太多,因而算法的执行效率较高。从硬件实现上来看,由于加密和解密可共享同一硬件结构,因此简化了实现的代价。

参 考 文 献

[1] 丁玮,齐东旭.数字图像变换及信息隐藏技术[J].计算机学报,1998,21(9):838-843

[2] Shamir A. How to share a secret[J]. Communications of ACM, 1979,22(11):612-613

[3] Naor M, Shamir A. Visual cryptography // Proc. of Eurocrypt '94. 1994:1-12

[4] Cao Zhenfu. A threshold key escrow based on public key cryptosystem[J]. Science in China (Series E),2001,44(4):441-448

[5] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal,1994,28(4):656-715

[6] Salam F,Marsden J,Varaiya P. Arnold diffusion in the swing equations of a power system[J]. IEEE Trans. Circuits and Systems,1984,31(8):29-42

[7] 李昌刚,韩正之,张浩然.图像加密技术综述.计算机研究与发展[J],2002,39(10):1317-1324

[8] Matthews R. On the derivation of a Chaotic encryption algorithm[J]. Cryptologia,1989,13(1):29-42

[9] Hedieu D, Ogorzalek M J. Indentifiability and identification of chaostic systems based on adaptive synchronization[J]. IEEE Trans. on Circuits and Systems,1997,44(10):948-962

[10] Yang T,Yang Linbao,Yang Chunmei. Application of neural networks to unmasking chaotic secure communication[J]. Physica D,1998,124:248-257

[11] Wolfram S. Cryptography with cellular automata[J]. Advances in Cryptology,1985:429-432

[12] Nandi S,Kar B K,Pal P. Chaudhuri,Theory and application of cellular automata in cryptography[J]. IEEE Trans. on Computer,1994,43(12):1346-1356

[13] Seredynski F,Bouvry P,Zomaya A Y. cellular automata computations and secret key cryptograpgh[J]. Parallel computing, 2004,30(5):753-766

[14] Guan S-U,Zhang Shu. Maric Therese Quieta. 2-D CA Variation With Asymmetric Neighborship for Pseudorandom Number Generation[J]. IEEE Trans. on computer-aided design of integrated circuits and systems,2004,23(3):378-388

[15] 张传武,沈野樵,彭启宗.细胞自动机反向迭代加密技术研究[J].计算机学报,2004,27(1):125-129

[16] Gutowitz H,Victor J D,Knight B W. Local structure for cellular automata[J]. Physica D,1987,28:18-48

[17] Marsaglia G. Diehard. [OL]. http://stat. fsu. edu/~geo/diehard. html,1998

[18] ENT test suit. [OL]. http://www. fourmilab. ch/random,1998

(上接第 213 页)

以提取无冗余的关联规则集。同时由算法看到,关联规则是利用概念之间的量化关系提出的,所以该算法更适用于在大型形式背景上进行关联规则的提取。

参 考 文 献

[1] Wille R. Restructuring lattice theory: an approach based on hierarchies of concepts// Rival I, ed. Ordered Sets. Dordrecht: Reidel, 1982:445-470

[2] Ganter B, WIlle R. Formal Concept Analysis: Mathematical Foundations. Berlin: Springer-Verlag, l999

[3] Yao Y Y. Concept lattices in rough set theory // Proceedings of 2004 Annual Meeting of North American Fuzzy Information Processing society. Canada,2004:796-801

[4] Qu K S,Liang J Y,Wang J H,et al. The algebraic properties of concept lattice. Journal of Systems Science and Information, 2004,2(2):271-277

[5] 谢志鹏,刘宗田.概念格的快速渐进式构造算法.计算机学报,2002,25(5):490-495

[6] 曲开社,翟岩慧,梁吉业,等.形式概念分析对粗糙集理论的表示及扩展.软件学报,2007,18(9):2174-2182

[7] Zupa B, Bohance M. Learning by discovering concept hierarchies. Artificial Intelligence,1999,109(1-2):211-242

[8] Tonella. Using a concept lattice of decomposition slices for program understanding and impact analysis. IEEE Transactions on Software Engineering,2003,29(6):495-509

[9] Qu Kai-She,Zhai Yan-Hui,Liang Ji-Ye,et al. Study of decision implications based on formal concept analysis. International Journal of General Systems,2007,36(2):147-156

[10] 张文修,徐宗本,梁怡,等.包含度理论.模糊系统与数学,1996,10(4):1-9

[11] 张文修,梁怡.不确定性推理原理.西安:西安交通大学出版社,1996

[12] 梁怡,张文修.模糊规则的谐调度和矛盾规则的排除方法.计算机学报,1997,20(10):947-952

[13] 张文修,梁广锡,梁怡.包含度及其在人工智能中的应用.西安交通大学学报,1995,29(8):111-116

[14] 梁吉业,徐宗本,李月香.包含度与粗糙集数据分析中的度量.计算机学报,2001,24(5):544-547

[15] Agrawal R,Imielinski T,Swami A. Mining association rules between sets of items in large databases// Proceedings of the ACM SIGMOD Conference on Management of Data. WashingtonD. C, 1993:207-216

[16] 曲开社,翟岩慧.偏序集、包含度与形式概念分析.计算机学报,2006,29(2):219-226

[17] 苗夺谦,王国胤,刘清,等.粒计算:过去、现在与展望.科学出版社,2007

[18] 翟岩慧,曲开社,曹桃云.基于矩阵秩的概念格生成算法.电脑开发与应用,2006,19(5):11-12