基于 S 盒的数字图像置乱技术

眭新光 罗 慧
(西南电子电信技术研究所重点实验室,成都 610041)

摘 要 数字图像置乱技术,作为数字图像信息隐藏的预处理和后处理,其主要目的是将一幅有意义的图像变成一幅杂乱无章的图像,用以增加数字图像信息隐藏算法抵抗非法攻击的能力,从而增加安全性。本文以图像信息安全问题为背景,介绍了通常用于分组密码系统中的 S 盒的理论基础,提出了一种基于 S 盒的数字图像置乱方法,同时讨论了置乱算法的周期性。实验结果表明,算法具有很好的置乱效果。

关键词 信息安全 信息隐藏 S 盒 数字图像置乱 周期性
中图法分类号: TN911.73 **文献标识码**: A **文章编号**: 1006-8961(2004)10-1223-05

Digital Image Scrambling Based on S-box

SUI Xin-guang, LUO Hui
(*Key Laboratory, Southwest Institution of Electron & Telecom Techniques, Chengdu* 610041)

Abstract The main aim of digital image scrambling, which is used as the pre-processing or post-processing in image information hiding, is to transform a meaningful image into a meaningless or disordered image in order to enhance the power to resist invalid attack and in turn enhance the security. This paper introduces the academic foundation of S-box that is usually applied to group cryptosystem with image information security as its background, and then presents a method of digital image scrambling based on S-box and discusses the periodicity of the arithmetic. The algorithm is proved to be efficient with experiments.

Keywords information security, information hiding, S-box, digital image scrambling, periodicity

1 引 言

随着计算机技术、通信技术、信息处理技术和智能化网络技术的飞速发展和广泛应用,数字化信息可以以各种形式在网络上迅速便捷地传输。然而由于网络的开放性特点,使得任何人都可以在网络上自由地获取他感兴趣的任何东西,这就使得信息的安全性倍受关注。在网络通信中,往日因存储量大和传输占用带宽大而让人们望而却步的数字图像也由于存储技术和网络通信技术的发展而在网络通信中占有越来越多的比率。

数字图像有其固有的一些特殊性质,如 2 维的自相似性、相关性、大数据量等。随着计算机技术的发展,人们在图像信息安全方面做了许多有益的探索,并取得了一定成果,其中之一即图像信息隐藏技术。作为信息安全领域的后起之秀,图像信息隐藏技术用于保密通信有自己的优势,因而近年来成为国内外研究的热点,特别是在图像隐藏、图像分存、数字水印等方面。数字图像置乱技术,作为数字图像信息隐藏的预处理和后处理,其主要目的是将一幅有意义的图像变成一幅杂乱无章的图像,使其所要表达的真实信息无法直观地得到。它可以增加数字图像信息隐藏算法抵抗非法攻击的能力,以增加安全性。

在数字图像置乱方面,已有许多比较有效的方法,如基于 Arnold 变换、幻方、Hilbert 曲线、Conway 游戏、Tangram 算法、IFS 模型、Gray 码变换、仿射模变换、多相滤波等方法[1~9]。本文从分组密码中 S 盒的高度非线性性和扩散性出发,提出了一种基于 S 盒新数字图像置乱方法,并通过实验验证了算法的有效性。

2 S 盒

S 盒是分组密码中的一个计算部件,是一个高

收稿日期:2003-06-16;改回日期:2004-05-18

度非线性的输入/输出真值表，其作用是使得明文和密钥产生充分的混淆和扩散。

S 盒的设计思想是这样的：将非线性度高、混淆和扩散性能好的密码函数作为分组密码的运算部件。考虑到这些密码函数的运算量很大，将其在各种自变量下的函数值预先计算好并做成输入/输出真值表，在实际应用时只需要根据输入值来调用表中相应的函数值即可。

例如，在 DES(data encryption standard)加密算法中，可以用到多达 8 个 S 盒(表 1 所示为其中的 S_1)。

表 1 S 盒(S_1)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

每个 S 盒都是 4 行和 16 列，6 比特输入，4 比特输出。由输入的首尾两比特确定 S 盒中的行，由输入的中间 4 比特确定 S 盒的列，其对应行和列处的值(4 比特表示)即为输出值。

实际上，每个 S 盒的每一行都是整数 0～15 的一个置换(即可逆变换)。

在 DES 的加密算法中，S 盒具有差分扩散功能，因而能抗差分攻击，同时由于它又是高度非线性的，每一个 S 盒的输出都不是它的输入的线性或仿射函数，因而能抵抗线性攻击。

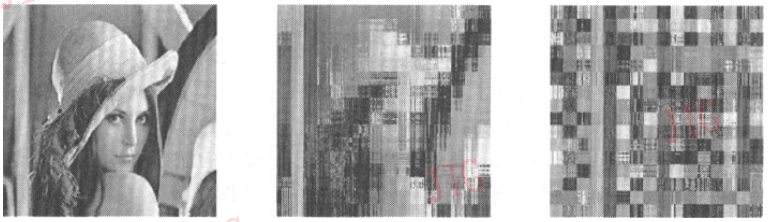
3 S 盒在数字图像置乱中的应用

数字图像置乱的目的是在 2 维的层次上，对数字图像的色彩、位置或者频率进行扰乱，使之成为一幅杂乱无章的图像，即使被非法攻击者截获，不知道恢复方法也无可奈何。此外，由于数字图像的大数据量以及庞大的明文空间，想要利用统计分析的方法将消耗巨大的工作量，在实现上是极其困难或者是得不偿失的。

数字图像置乱有基于位置空间、色彩空间和频率空间的置乱变换，即改变像素的位置或色彩而置乱图像。但是要从置乱的图像恢复出原图像，必须保证原始图像与变换图像之间的变换是可逆的或者是周期性的(即通过若干次变换就可以回复到初始状态)。而每个 S 盒的每一行都是整数 0～15 的一个置换，因而其变换是可逆的。

3.1 基于位置的置乱

由于 S 盒的每一行都是 0～15(共 16 个数)的一个置换，8 个 S 盒共有 32 个置换。把图像的每 16 行(列)分为一小组(利用一个置换来进行位置置乱)，每 32 个小组构成一个大组，利用 S 盒的 32 个置换来对图像的一个大组(32 个小组)进行行(列)置换，从而可以得到位置置乱的图像。图 1 是一个位置置乱的实例。



(a) 原图像 (b) 行列置乱图 (c) 行列及区域置乱图

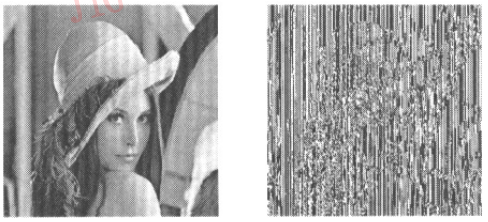
图 1 位置置乱实例

图 1(b)是经过行和列置乱的图像，从图中可以看出，尽管图像已经变得比较乱，但是还可以看出图像的轮廓。这是由于 S 盒的每一行都是 0～15 的置换，从而图像的行(列)置乱都是在 16×16 的块内进行的，只是在这个区域内打乱了图像像素的位置，而块与块之间的位置关系并没有被打乱。而图 1(c)是在行和列置乱的基础上又进行了区域置乱，打破了块与块之间的位置关系，从而达到了比较理想的置乱效果。

3.2 基于灰度的置乱

由于 S 盒的每一行都是 0～15 的一个置换，而 0～15 可以用二进制的 4 个比特表示，从而每一个置换都可以看作 4 比特串到 4 比特串之间的一个置换。利用这种关系，可以对图像进行灰度置乱。由于灰度图像的每个像素用 8 个比特表示，可以对其高 4 位和低 4 位分别进行置换，从而达到置乱的效果。具体作法是：把图像每 16 个像素分为一组，利用 S 盒的 32 个置换对这 16 个像素(16 字节，共 32 个 4

位比特串)分别进行置换。图 2 是一个变换实例。

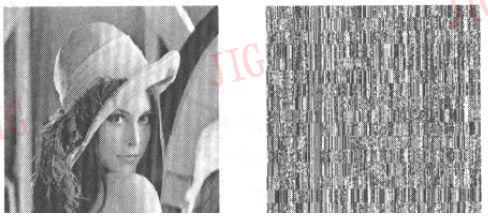


(a) 原图像　　(b) 灰度置乱图

图 2　灰度置乱实例

3.3　基于位置和灰度的置乱

既对图像进行位置置乱(打乱行、列及区域的位置关系),又对图像进行灰度置乱(改变灰度值)。图 3 是一个变换实例。



(a) 原图像　　(b) 位置及灰度置乱图

图 3　位置加灰度置乱实例

4　置乱算法的性能分析

4.1　算法的复杂性分析

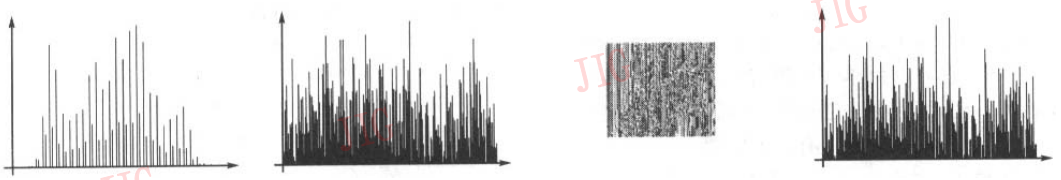
由于算法采用 S 盒置乱,直接调用真值表,而没有涉及函数的具体计算,整个算法中只有少量的加法运算和逻辑运算。例如,在灰度置乱中,对每个像素,只涉及两次“移位”运算,一次“与”运算,调用两次真值表,一次“加”运算。对于一幅 $M\times N$ 的图像,总共需要 $M\times N$ 次“加”运算,$M\times N$ 次“与”运算,$2\times M\times N$ 次“移位”运算,$2\times M\times N$ 次调用真值表。因而算法复杂性很低,计算速度非常快,置乱以及解置乱方便快捷。

4.2　置乱的效果分析

一幅图像的概貌可以通过其灰度直方图来描述。例如,如果一幅图像的灰度直方图比较展开,那么它看起来就比较清晰柔和;如果直方图对比度小,则看起来不自然;如果直方图的动态范围较小,则看起来不清楚。因而可以通过直方图来分析置乱的效果。

对于一幅类似白噪声的图像,其直方图充满整个区域,而且分布应该比较均匀。同时,对于类似白噪声的图像,任意截取其中的某个小区域,其直方图分布应该与整个图像的直方图分布相似,也就是直方图的分布具有自相似性。

图 4 就是对置乱前后图像的直方图的一个比较(由于位置置乱不改变图像的直方图,这里只对灰度置乱的直方图进行比较)。其中,图 4(a)为图 2(a)图像的直方图,图 4(b)为经过灰度置乱后,即图 2(b)的直方图,图 4(c)是从图 2(b)中任意截取的一块小区域,图 4(d)是截取出来的小块图像的直方图。从图中可以看出,经过置乱后图像的直方图充满整个区域,而且分布比较均匀。用直方图的相似度来定量地描述置乱的效果。



(a) 原图直方图　　(b) 置乱后直方图　　(c) 置乱后截取图　　(d) 截取图直方图

图 4　置乱直方图比较

设两图像灰度直方图分别为 $h_1(k),h_2(k),k=0,1.\cdots,G-1$ 则定义直方图的相似度为

$$\alpha=1-\frac{\sum_{k=0}^{G-1}|h_1(k)-h_2(k)|}{\sum_{k=0}^{G-1}|h_1(k)+h_2(k)|} \qquad (1)$$

对于一幅纯噪声的图像,其直方图分布应该是均匀的,即 $h(i)=h(j),\forall\, i,j\in\{0,1,\cdots,G-1\}$。这里原始图像与白噪声图像的直方图相似度 $\alpha=0.19$,置乱后的图像与白噪声图像的直方图相似度 $\alpha=0.81$,截取小图像与白噪声图像的直方图相似度 $\alpha=0.69$,而截取部分与整幅置乱图像的直方图相似

度 $\alpha=0.85$。

这说明经过置乱后图像类似于白噪声，置乱效果良好。

4.2 置乱的安全性分析

一个 0～15 的置换有 16！=20 922 789 888 000 种可能性，由于本算法使用了 8 个 S 盒共 32 个 0～15 的置换，因而 32 个置换共有 $(16!)^{32}=1.8\times10^{426}$ 种可能性。对于非法攻击者来说，即使知道了置乱的方法，但要从 1.8×10^{426} 种可能的置换中分析出算法所采用的置换，其运算量是非常巨大的。如果采用穷搜索的方法，平均需要搜索约 10^{426} 种置换，这在实现上也是很困难的。

另外，从密码学的角度来讲，每个 0～15 的置换都是有限域 GF(2^4)到 GF(2^4)的一个置换，32 个置换相当于一个 GF(2^{128})到 GF(2^{128})的置换。因此，本方法相当于一套分组很大(16 个字节共 128 比特)的分组密码，使信源明文的统计特性被隐蔽得很深，以至于对其统计分析是极其困难的。

因此，置乱后的图像是安全的。

5 基于 S 盒变换的周期性

S 盒的每一个置换都是 0～15 的置换，用矩阵可以表示成

$$(y_0,y_1,\cdots,y_{15})=(x_0,x_1,\cdots,x_{15})\boldsymbol{A} \quad (2)$$

其中，$x_i,y_i\in\{0,1,\cdots,15\}(i=0,1,\cdots,15)$，$x_i\neq x_j$，$y_i\neq y_j(i\neq j)$，而 $\boldsymbol{A}=\begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,15} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,15} \\ & \cdots & \cdots & \\ a_{15,0} & a_{15,1} & \cdots & a_{15,15} \end{bmatrix}$，矩阵 $\boldsymbol{A}$ 的每一行(列)都只有一个元素等于 1，而其余元素等于 0，它可以由单位矩阵经过有限次交换行和交换列得到，因而存在逆矩阵，从而变换是可逆的。

对于变换的周期性，有以下定理。

定理 1 对于给定的 N 和矩阵 $\boldsymbol{A}$，变换

$$(y_0,y_1,\cdots,y_{n-1})=(x_0,x_1,\cdots,x_{n-1})\boldsymbol{A}(\mathrm{mod}\ N) \quad (3)$$

其中，$\boldsymbol{A}=\begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,N-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,N-1} \\ & \cdots & \cdots & \\ a_{N-1,0} & a_{N-1,1} & \cdots & a_{N-1,N-1} \end{bmatrix}$，$a_{i,j}$ 为整数，$y_0,y_1,\cdots,y_{n-1},x_0,x_1,\cdots,x_{n-1}\in\{0,1,\cdots,N-1\}$ 有周期性的充分条件是 $|\boldsymbol{A}|$ 与 N 互素，此处 $|\boldsymbol{A}|$ 是 $\boldsymbol{A}$ 的行列式值[6]。

应用于 S 盒的置换有 $N=16$，而 $|\boldsymbol{A}|=\pm1$(交换行和列的位置不改变行列式的代数值，而只改变其符号)，因而 $|\boldsymbol{A}|$ 与 N 互素，变换存在周期性。

对于置乱周期的具体求法，可以通过求得每一个置换的周期，然后对 32 个置换的周期取最小公倍数，就可以得到这里置乱的周期。从实验的角度得到的每个置换的周期如下：

{14,33,36,33,14,36,12,12,16,14,44,12,14,10,42,14,14,12,36,14,14,55,36,14,44,30,36,30,26,44,44,14}。

从而可以得到置乱的周期为 720 720。

6 结 论

数字图像置乱是近年来新兴起来的研究课题，人们在这一方面已做过许多有益的探索，取得了不少成果。但是，寻找一种安全而又简单的置乱方法，一直是数字图像置乱研究的内容。本方法与基于 Gray 码变换的置乱方法有相似之处。但是，从密码学的角度来讲，基于 Gray 码变换的置乱由于是 GF(2^4)到 GF(2^4)的一个置换，其分组太小，很难抵抗对明文的统计分析，而本方法的分组很大(16 个字节共 128 比特)，使信源明文的统计特性隐蔽得很深，以至于对其统计分析是极其困难的。

从上述实验结果和性能分析的结果来看，基于 S 盒的置乱效果较好，实现方便。用作数字图像信息隐藏的预处理或后处理是非常有效的。

参 考 文 献

1 邹建成，铁小匀. 数字图像的二维 Arnold 变换及其周期性[J]. 北方工业大学学报，2000，**12**(1)：10～14.

2 Ding Wei，Yan Wei-qi，Qi Dong-xu. Digital image scrambling technology based on gray code [A]. In：Proceedings of International Conference on CAD/CG [C]，Shanghai，P. R. China，1999.

3 李国富，邹建成，齐东旭. 广义 Gray 码及其在数字图像置乱中的应用[A]. 见：全国第二届信息隐藏学术研讨会论文集[C]，北京，2000：1～6.

4 Qi Dong-xu，Ding Wei，Li Hua-shan. Tangram algorithm：image transformation for storing and transmitting visual secrets [A]. In：Proceedings of the 9'st International Conference of CAD/CG[C]，Shenzhen，P. R. China，1997，(1)：135～139.

5 李国富. 正交拉丁变换的周期性及其在数字图像置乱中的应用[A]. 见：全国第三届信息隐藏学术研讨会论文集[C]，西安：西安电子科技大学出版社，2001：1～7.

6 齐东旭，邹建成，韩效宥. 一类新的置乱变换及其在图像信息隐蔽中的应用[J]. 中国科学(英文版)，2000，**30**(5)：440～448.
7 Creusere C D, Mitra S K. Efficient image scrambling using polyphase filter banks[A]. In: Proceedings of International Conference On Image Processing[C], Austin, Texas, USA, 1994：81～85.
8 Joo K S, Bose T. Image scrambling using 2-D periodically shift variant filters[J]. Midwest Symposium on Circuits and Systems, 1995，**1**(8)：478～481.
9 BAI Sen, CAO Chang-Xiu. A novel algorithm for scrambling the details of digital image[A]. In: Proceedings of the World Congress on Intelligent Control and Automation (WCICA), Shanghai, P. R. China, 2002，**2**：1333～1336.

眭新光　1978 年生。现为西南电子电信技术研究所博士研究生。主要研究方向为信息安全、图像图形处理以及图像目标识别。
E-mail：hffsxg@sina.com

罗　慧　1979 年生。现为西南电子电信技术研究所硕士研究生。主要研究方向为移动通信。

3D 工作站图形加速卡再晋升

——艾尔莎发布新一代 ELSA ATI FireGL X3-256

艾尔莎(ELSA)最近推出 ELSA ATI FireGL X3-256 工作站图形加速卡，凭借新的图形引擎，以中端价位在 AGP 领域为 3D 工作者带来高端的性能和增强的功能。这款工作站图形加速卡能够让用户建立更加复杂的视觉场景设计，在数字内容创作(DCC)、计算机辅助设计(CAD)、视觉预览(Pre-Visualization)和地理信息系统(GIS)工作中，将比当前 FireGL 产品提升 30%的性能。

作为 ELSA FireGL 工作站图形加速卡家族的扩充，ELSA ATI FireGL X3-256 为用户提供了高端的特性，如可搭建多屏幕显示的双 DVI 输出，双链路模式连接提供的 9M 像素显示，Quad-buffer 立体 3D 输出，12 条像素管线，6 条几何引擎，增强子像素精度以及 256M 容量的 GDDR3 显存等。凭借这些新特性，ELSA ATI FireGL X3-256 能够令用户有效地运行所有“领袖级”3D 应用软件，如 3ds max、Catia、MAYA、SOFTIMAGE|XSI 以及 SolidWorks 等等，并能发挥出这些软件的所有优势。

FireGL X3-256 在保持高画质和复杂外形的同时能够提供更高级的 3D 模型和动画，符合当前高级 3D 用户对硬件和软件相适配的综合标准。借助 FireGL 工作站图形加速卡，SolidWorks 用户能够通过 RealView 功能即时显示完整的 shaded rendered 模型。新的 FireGL X3-256 在 CAD 和视像工作方面拥有丰富的新特性，更加具有优势，为 SolidWorks 用户提供了进一步增强的产品。

在现有的 FireGL X2-256t、FireGL X1、FireGL Z1、FireGL T2-128、FireGL T2-64s 基础上，FireGL ATI X3-256 的加入完善了 FireGL 家族的 AGP 产品线。再加上 PCI Express 产品线的 FireGL V7100、FireGL V5100、FireGL V3200 和 FireGL V3100，ELSA 为 OEM 厂商、工作站系统集成商以及广大图形工作站用户提供了更大的选择空间。