

## 一种基于密钥的水印嵌入位置置乱算法

周翔翔<sup>1</sup>, 尹忠海<sup>2</sup>, 刘守义<sup>1</sup>, 韩毅娜<sup>1</sup>

(1. 空军工程大学 电讯工程学院, 西安 710077; 2. 空军工程大学 理学院, 西安 710051)

(zhouxiangxiang1982@163.com)

**摘 要:**提出了一种基于密钥的数字水印嵌入位置的置乱算法,该算法利用分组移位和混洗操作将水印嵌入位置进行多次置乱。算法简单,实现方便,嵌入位置随机分散,嵌入位置信息的安全仅依赖于—组密钥,在相当程度上达到了较理想的置乱效果,增加了系统的安全性。

**关键词:**数字水印;嵌入位置;密钥;分组移位;混洗

**中图分类号:** TP309 **文献标志码:** A

## Algorithm based on key to confuse watermark embedding positions

ZHOU Xiang-xiang<sup>1</sup>, YIN Zhong-hai<sup>2</sup>, LIU Shou-yi<sup>1</sup>, HAN Yi-na<sup>1</sup>

(1. Institute of Telecommunication Engineering, Air Force Engineering University, Xi'an Shaanxi 710077, China;

2. Institute of Science, Air Force Engineering University, Xi'an, Shaanxi 710051, China)

**Abstract:** An algorithm based on the key to hash the digital watermark embedding positions was presented. The Scrambling algorithm used shifting and shuffling to hash the watermark embedding positions many times. It is very simple and convenient to carry it out, and then the positions are stochastic and dispersive. The security of embedding positions relies on a key, which to a certain extent makes the result of scrambling perfectly, and increases the security of the system.

**Key words:** digital watermark; embedding positions; key; shift; shuffle

## 0 引言

数字水印技术是信息隐藏技术中的一个较为重要的分支。数字水印必须具有透明性、鲁棒性、不可检测性、安全性、自恢复性等特性。早期的水印算法都是在空域上进行,现在大部分算法是在频域上进行,这样大大增强了水印的鲁棒性和安全性。目前用得比较多的是离散余弦变换(DCT)。这种变换的水印算法需要在载体图像中选择一些 $8 \times 8$ 的分块来分别嵌入水印信息,嵌入块选择的好坏直接影响到水印系统的安全性,如何选择这些块是解决水印嵌入的关键。

水印嵌入块的选择应当遵循在整个可选块空间上随机无序选择的原则。如果用密钥直接指定嵌入位置存在以下几个问题:1)不同大小的载体图像需要不同的密钥,以便将水印随机地分布到整幅载体图像中;2)不同大小的水印嵌入时需要的密钥长度不同;3)标识水印实际嵌入位置时要求的密钥长度与水印大小和嵌入版本数有关。这样,导致密钥较长,给密钥管理带来了困难。本文提出的基于密钥的分组移位和混洗算法,对于不同大小的载体图像和不同大小的水印,都能够根据初始的无意义的密钥产生出很好的标识水印嵌入、提取位置的数组,利用这个数组中元素的值标识出水印在载体图像中的实际位置,这些位置都是随机无序的。即使本置乱算法被攻击者获知,由于不知道密钥就无法得知水印嵌入的实际位置,从而进一步增强了水印的抗攻击能力和安全性。

## 1 水印嵌入位置的产生

不可感知性和鲁棒性是水印特性相互矛盾的两个方面,

有效的水印算法必须在这两个方面之间进行折中,在保证不可感知性的前提下,尽可能多地嵌入水印。离散余弦变换(DCT)算法是先将载体图像分成一系列 $8 \times 8$ 块,每个分块可通过DCT变换得到一个 $8 \times 8$ 的DCT块,每个DCT块里只选择4个中低频系数嵌入水印。

设载体图像为灰度图 $I(M \times N \times 256)$ ,其中 $M$ 表示图像水平方向的像素个数, $N$ 表示图像垂直方向的像素个数,256表示图像的颜色数。设水印信息的大小为 $S$ 。为了使水印信息尽可能分散地嵌入载体图像,以增强水印系统的安全性,我们用密钥 $K$ 随机选取一系列 $8 \times 8$ DCT块,DCT块的选取算法具体描述如下:

1) 计算载体图像可分割的DCT块的数目,用 $N_{DCT}$ 表示DCT块的总数目。则 $N_{DCT} = \lfloor \frac{M}{8} \rfloor \times \lfloor \frac{N}{8} \rfloor$ 。

2) 确定需要嵌入水印的DCT块的数目,用 $N_{WM}$ 表示所需的DCT块数。由于每个DCT块里只选择4个低频系数嵌入水印,则 $N_{WM} = S/4$ 。

3) 引入一维数组 $Block[N_{DCT}]$ 标识需嵌入水印的块,初始化为:

$$Block(i) = \begin{cases} 1, & 0 \leq i \leq N_{WM} - 1 \\ 0, & N_{WM} \leq i \leq N_{DCT} - 1 \end{cases}$$

4) 根据密钥 $K$ ,利用分组移位算法将 $Block[N_{DCT}]$ 置乱为 $Block'[N_{DCT}]$ , $Block'[N_{DCT}]$ 的值仍然为“1”或者“0”。

5) 经过上面的操作,用“1”标识的待嵌入水印的DCT块位置已由初始的前 $N_{WM}$ 个分散到整个灰度图像DCT块位置

收稿日期:2007-04-05;修回日期:2007-06-18。

**作者简介:**周翔翔(1982-),男,江苏盐城人,硕士研究生,主要研究方向:计算机辅助技术、信息安全研究;尹忠海(1964-),男,河北沧州人,副教授,博士研究生,主要研究方向:计算机网络与信息安全;刘守义(1950-),男,河北人,教授,博士,主要研究方向:计算机辅助决策与系统仿真;韩毅娜(1965-),女,陕西西安人,讲师,硕士,主要研究方向:计算机应用技术。

空间中。将这些分散的位置信息收集起来,即扫描  $Block'[N_{DCT}]$ ,用  $Positon[N_{WM}]$  存储值为“1”的下标。

6) 对一维数组  $Position[N_{WM}]$  实施多轮混洗,混洗的轮数为密钥  $K$  的长度  $|K|$ ,经过混洗算法的进一步置乱,从而得到的数组即为嵌入水印的实际位置。

同样,在提取水印信息时,根据给定的密钥  $K$  (这个密钥和嵌入密钥相同),利用与嵌入时相同的算法可以得到标识水印嵌入位置的数组,从而正确地将水印信息提取出来。

下面,将详细地描述分组移位算法和混洗算法,以及它们是如何对水印嵌入位置实现置乱的。

## 2 分组移位算法及其置乱初始的水印嵌入位置

### 2.1 分组移位算法的基本构成及其原理

设原始信息是大小为  $N$  的一维数组  $W(t)$ ,  $W'(t)$  为随机置乱后的一维数组。分组移位置乱方法是对原始信息  $W(t)$  的一个全排列。如果设  $W$  为原始信息空间,  $K$  为密钥空间,则对  $W$  的随机置乱算法定义为如下的映射:分组移位算法设计成由  $l$  轮分组移位构成,每轮分组移位的操作取决于该轮读入的密钥,设密钥由  $l$  个字符构成,即  $K = \alpha_1 \alpha_2 \cdots \alpha_l$ 。假设第  $i$  轮读入的密钥字符为  $\alpha_i \in \{1, 2, \cdots, 9, A, B, \cdots, Z\}$ ,每个字符对应一个整数值,其对应关系如下:

$$\alpha_i: 1 \ 2 \ \cdots \ 9 \ A \ B \ \cdots \ Z$$

$$a = f(\alpha_i): 1 \ 2 \ \cdots \ 9 \ 10 \ 11 \ \cdots \ 35$$

整数  $a = f(\alpha_i)$  即为第  $i$  轮分组移位操作中每分组所包含的项数。以本轮操作的  $a = f(\alpha_i) = 3, N = 26$  ( $N$  为原始一维信息的长度) 为例,分组移位操作过程如图 1 所示。



图1 分组移位算法

### 2.2 分组移位算法置乱初始的水印嵌入位置

原始的信息是大小为  $N_{DCT}$  的一维数组  $Block[N_{DCT}]$ ,它的前  $N_{WM}$  项为“1”,其余项为“0”。根据密钥  $K$ ,使用分组移位算法操作后,得到  $Block'[N_{DCT}]$  为随机置乱后的一维数组。 $Block'[N_{DCT}]$  中“1”的分布是分散的。分组移位算法置乱水印嵌入位置的过程组织如下:

读入密钥  $K = \alpha_1 \alpha_2 \cdots \alpha_l$

for  $s = 1$  to  $l$

$a = f(\alpha_s)$ ; //取得本轮置乱算法的密钥

for  $i = 0$  to  $\lfloor \frac{N_{DCT}}{2a} \rfloor \times a - 1$

$j = \lfloor \frac{i}{a} \rfloor a + a + i; Block'(i) = Block(j)$ ;

next  $i$

for  $i = \lfloor \frac{N_{DCT}}{2a} \rfloor \times a$  to  $\lfloor \frac{N_{DCT}}{2a} \rfloor \times a - 1$

$j = \lfloor \frac{i}{a} \rfloor a - 2 \lfloor \frac{N_{DCT}}{2a} \rfloor a + i; Block'(i) = Block(j)$ ;

next  $i$

for  $i = \lfloor \frac{N_{DCT}}{2a} \rfloor \times a$  to  $N_{DCT} - 1$

$j = i; Block'(i) = Block(j)$ ;

next  $i$

next  $s$

## 3 混洗算法及其再次对水印嵌入位置的置乱

### 3.1 混洗算法的原理

本混洗算法使用的是单级互连网络中的混洗交换的思想,算法的目的是分散和混乱原有序列。算法描述如下:

设原始的信息是大小为  $N$  的一维数组  $P(t)$ ,  $P'(t)$  为混洗置乱后的一维数组,需要  $n$  位二进制数来表示数据  $0, 1, \cdots, N-1$ , 则  $N = \lceil \log_2^N \rceil$ 。混洗后  $P'(i)$  与  $P(j)$  对应关系为  $P'(i) = P(j)$ ,  $j = x_{n-1}x_{n-2} \cdots x_1x_0$ ,  $x_{n-1}x_{n-2} \cdots x_1x_0$  是  $j$  的二进制形式。其中  $i$  和  $j$  之间的对应关系为  $Shuffle(j) = i$ ,  $Shuffle$  函数是将处理数据的二进制位中的最左位移到最右位的循环移位。

$$Shuffle(x_{n-1}x_{n-2} \cdots x_1x_0) = (x_{n-2} \cdots x_1x_0x_{n-1})$$

若  $N = 8$ , 则  $Shuffle$  函数的作用效果如图 2 所示。

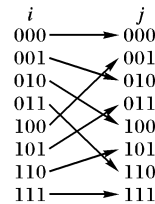


图2  $Shuffle$  函数的作用效果( $N = 8$ )

由此可知,当  $j = x_{n-1}x_{n-2} \cdots x_1x_0$  时,  $i = x_{n-2} \cdots x_1x_0x_{n-1}$ 。

### 3.2 混洗进一步置乱分组移位后的水印嵌入位置

分组移位操作后,水印嵌入位置已经分散到整个载体图像的 DCT 块空间。但仍有一些水印嵌入位置是集中在一起的,且嵌入顺序是按行从左到右的。现在保持水印位置不变,利用混洗算法将嵌入的顺序打乱。

首先扫描分组移位算法后得到的  $Block'[N_{DCT}]$ ,用  $Positon[N_{WM}]$  将  $Block'$  中值为“1”的位置标号存储。实施一次混洗后得到  $result_1[N_{WM}]$ 。满足  $result_1[Shuffle(j)] = Positon[j]$ 。

对一维数组  $Position[N_{WM}]$  实施  $|K|$  轮混洗,从而得到的数组即为嵌入水印的实际位置。

## 4 实验测试效果

### 4.1 水印嵌入位置的产生

我们利用 VC++ 6.0 编程实现了上述算法,下面给出一个实验结果。

载体图像大小为  $256 \times 256$ , 水印大小为 560, 给定的密钥  $K$  为 W3R1A, 则实验结果如图 3。



图3 水印嵌入位置的产生

通过多次与上两个实验相似的测试,可以得知分组移位和混洗的置乱算法产生的水印嵌入位置,遍布整个载体图像 DCT 块。同时,这些嵌入位置的先后顺序与其在载体图像 DCT 块中的位置的顺序无关。

### 4.2 嵌入位置改变测试

这个实验的目的是实施一次本文提出的置乱算法,从水印嵌入位置的初始状态到实施分组移位后的状态,再到混洗

(下转第 2477 页)

钥产生和分发是绝对安全的。所以即使在通信的第四步密文信息被截获,但因为截获者根本不可能知道解密的量子密钥从而也无法获取明文信息。

## 2) 签名的不可伪造性

在该方案中对签名的不可伪造作出了双重保证,首先通信双方在建立量子密钥  $K_{(a,b)}$  的过程中可知道对方的身份,因为  $K_{(a,b)}$  只有通信的双方才拥有,所以消息的接受者能肯定消息的唯一发送者。同时因为只有发送者本人才能知道自己的椭圆曲线加密的私有密  $K_s$ ,因此只有消息的发送者才能对消息做唯一签名。

## 3) 签名的不可重用性

在该方案中采用的单向 Hash 算法使签名成为消息的函数同时由于单向 Hash 函数具有良好的抗碰撞性  $H_{ash}(x) \neq H_{ash}(y)$ ,保证了签名不可能被转换为其他的文件,从而确定了签名的不可重用性。

## 4) 签名的不可抵赖性

Alice 用自己的私钥加密信息摘要得数字签名  $DS$ , Bob 直接利用 Alice 的公钥就可以独立的验证发送者的签名,同时 Bob 也不能否认他收到了发送者的签名,因为只有 Bob 本人拥有解开密文信息的量子密钥。

5) 任何想获取量子密钥的试图都不可能成功。

因为本方案中第三方不能从通信双方公开参数中获取通信双方密钥,特别是当通信者采用一次一密方式加密时系统将是无条件安全的。

## 4 结语

本文利用量子密码在量子信道密钥分配中的安全性及椭圆曲线加密体制在经典秘密通信中的优越性,将二者相结合,提出了一种在经典信道中基于量子密钥的数字签名方案,该方案有可证明的安全性,同时也保证了签名的不可伪造性和不可抵赖性。不足之处是目前量子密钥分配还存在着很多制约因素,最主要的是传输距离、噪声干扰的限制。但相信随着科学技术的不断发展,量子密钥有望突破一些在自由空间和

光纤信道中的传输困难而得到良好的分配和传输。也可能将会与经典安全通信中的优秀算法、方案相结合从而为信息安全提供更强有力的工具。

## 参考文献:

- [1] WIESNER S. Conjugate coding[J]. Sigact News, 1983, 15(1):78-88.
- [2] WOOTERS W K, ZUREK W H. A single quantum cannot be cloned[J]. Nature, 1982, 299: 802-803.
- [3] LUTKENHAUS N. Security against eavesdropping in quantum cryptography[J]. Physics Review A, 1996, 54(1):97-111.
- [4] LUTKENHAUS N. Estimates for practical quantum cryptography[J]. Physics Review A, 1999, 59: 3301-3319.
- [5] BRASSARD G, LUTKENHAUS N, MOR T, et al. Security aspects of practical quantum cryptography[DB/OL]. [2007-05-01]. <http://arxiv.org/df?quant-ph/9911054>.
- [6] HANKERSON D, MENEZES A, CANSTONE S. Guide to elliptic curve cryptography[M]. Heidelberg: Springer, 2004.
- [7] BENNETT C H, BRASSARD G, BREIDBART S, et al. Quantum cryptography, or unforgeable subway tokens[C]// Advances in Cryptology: Proceedings of Crypto 82. New York: Plenum Press, 1982: 267-275.
- [8] CLAUSER J F. Experimental distinction between the quantum and classical field-theoretic predictions for the photoelectric effect[J]. Physical Review Letters, 1974, D9, 853-860.
- [9] BENNETT C H, BRASSARD G. An update on quantum cryptography[C]// Advances in Cryptology: Proceedings of Crypto 84. Berlin: Springer-Verlag, 1984: 475-480.
- [10] BENNETT C H, BESSETTE F, BRASSARD G, et al. Experimental quantum cryptography[J]. Journal of Cryptology, 1992, 5(1):3-28.
- [11] BENNETT C H, WIESNER S J. Communication via one-and two-particle operators on Einstein-podolsky-rosen states[J]. Physical Review Letters, 1992, 69: 2881-2884.
- [12] 郭光灿. 量子密码——新一代密码技术[J]. 物理与工程, 2005, 15(4):1-4, 8.

(上接第 2474 页)

后的状态,通过两大类型的变换,从而可以形象地看出水印嵌入位置和顺序的变化过程。

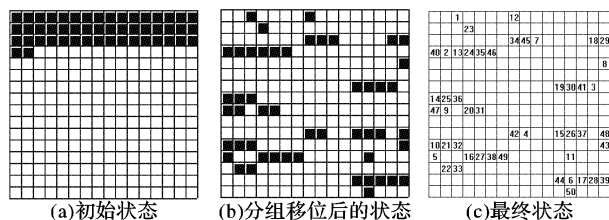


图 4 实验结果

以载体图像大小为  $128 \times 128$ , 水印大小为 200, 给定的密钥  $K$  为 Z15SG94C 为例,载体图像的 DCT 块大小为  $16 \times 16 = 256$ ,嵌入水印需用 50 个 DCT 块,水印嵌入的初始位置设定如图 4(a)。分组移位操作后,结果如图 4(b)所示。保持水印位置不变,利用混沌算法将嵌入的顺序打乱,得到的结果见图 4(c)。

## 5 结语

本文提出的基于密钥的分组移位和混沌算法对于产生随

机分散的水印嵌入和提取位置比较有效,可以广泛用于数字水印系统嵌入位置的选取上。其中,分组移位算法也可用于水印图像的置乱。在水印系统中,嵌入位置用本文提出的算法,水印图像置乱用分组移位算法,就可实现水印系统的单密钥体制。

## 参考文献:

- [1] 刘德鹏,蔡翔云. 水印对象的混沌置乱算法[J]. 云南大学学报:自然科学版, 2006, 28(S1): 145-148.
- [2] 李敏,费耀平. 基于置乱变换的多重数字水印盲算法[J]. 计算机工程, 2006, 32(16): 122-124.
- [3] 陈波,谭运猛,吴世忠. 信息隐藏技术综述[J]. 计算机与数字工程, 2005, 33(2): 21-27.
- [4] KWOK S H. Watermark-based copyright protection system security[J]. Communications of the ACM, 2003, 46(10):98-101.
- [5] YIN ZH, WANG K. Improvements of the definition of image fidelity[C]// Proceedings of the 12th International multi-Media Modelling Conference proceedings. New York: IEEE Press, 2006, 1: 426-429.