一种不对称公钥数字水印算法

胡延军 马小平 高 莉
(中国矿业大学信电学院,徐州 221008)

摘 要 为了更好地进行版权保护,针对现有数字水印算法存在的缺点,提出了一种新的不对称公钥水印思想,并首先指出目前用于版权保护的鲁棒性数字水印算法所存在的缺点和不对称公钥水印算法的优点,然后提出能克服这些缺点的不对称公钥水印算法思想;同时根据算法模型的需要,设计了一种新的具有较好相关特性的伪随机序列,并对其自相关特性进行了证明;最后具体描述了所提出的算法实例,并进行了仿真试验。试验结果证明,该算法思想是可行的,所设计的算法实例具有较好的鲁棒性和较强的抗攻击能力。

关键词 数字水印 公钥 伪随机序列
中图法分类号: TP309 **文献标识码**: A **文章编号**: 1006-8961(2005)03-0354-06

An Asymmetric Public Key Digital Watermarking Algorithm

HU Yan-jun, MA Xiao-ping, GAO Li
(*School of Communication & Electronic Engineering, China University of Mining and Technology, Xuzhou* 221008)

Abstract A novel asymmetric public key algorithm of robust digital watermarking, which has more potential value in practice, is proposed in this paper. First, the disadvantage of common robust watermarking algorithm is discussed, and the advantage of asymmetric public key watermarking algorithm is described. Then, a kind of asymmetric public method is proposed. To implement the method, a special pseudorandom sequence used as watermark is designed. The construction method of pseudorandom sequences is proposed, and the pseudorandom sequences' correlation characteristic is proved. Furthermore, the detail of asymmetric public key algorithm is proposed. Finally, experiments are done. Experimental results show that the algorithm is robust enough against attacks of the commonly used image processing methods. Also, experimental results show that the algorithm is robust to malicious attacks.

Keywords digital watermarking, public key, pseudorandom sequences

1 引 言

数字水印技术(digital watermarking)目前已成为图像信息防伪领域中的研究热点[1~3]。数字水印技术是一种保护多媒体数据版权,特别是保护数字图像版权的技术[4,5]。其实质是利用多媒体数据中的冗余度,将一定的数据隐藏到多媒体数据中,并以嵌入的数据作为版权信息的一种信息隐藏技术。

数字水印可分为脆弱性水印(fragile watermarking)和鲁棒性版权水印(robust copyright watermarking)[1]。借助于传统的加密技术,目前脆弱性水印已提出了相应的公钥算法[5],但鲁棒性版权水印算法目前还基本上没有相应的公钥算法。文献[6~13]提出的鲁棒性版权水印算法流程示意图如图 1 所示。

这些水印算法主要存在以下两个问题:

(1)由于水印的嵌入算法和检测算法是互逆的,或者说是对称的,因此水印算法不能公开,例如以文献[10]所提的算法为例,该算法核心思想是先将原始图像进行小波分解,然后取其小波逼近子图为嵌入水印信号的载体,并当水印信息为"0",就将小波逼近子图中系数的小数调制为 0.25;而当水印信息为"1"时,就将小波逼近子图中系数的小数调

收稿日期:2003-08-20;**改回日期**:2004-09-22

第一作者简介:胡延军(1974~),男,2004 年获中国矿业大学硕士学位,现为中国矿业大学信息与电气工程学院博士研究生。研究兴趣包括信息隐藏、信息安全、数据通信等。E-mail:yjhu@cumt.edu.cn

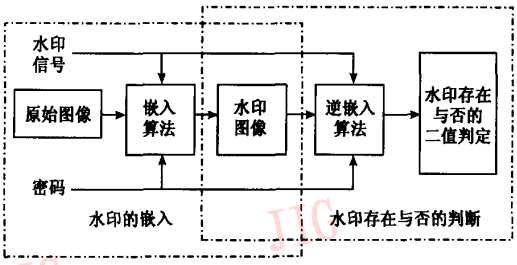


图 1　文献[6~13]提出的鲁棒性版权算法流程示意图

Fig. 1　Robust watermarking algorithmic proposed in[6~13]

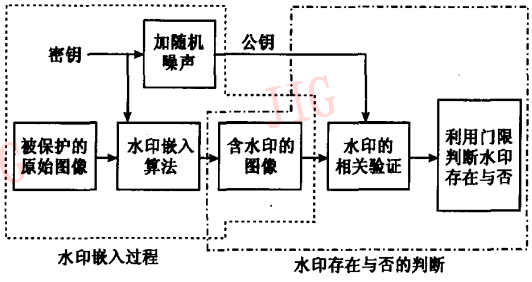


图 2　水印的嵌入和判断存在与否过程示意图

Fig. 2　Watermark embedment & detection process

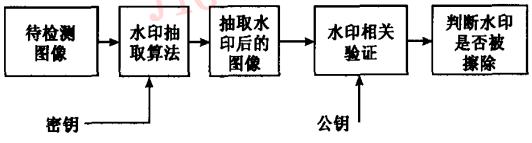


图 3　对版权主张者验证其水印私钥正确与否过程示意图

Fig. 3　Ownership authentication process

制为 0.75;由此可以看出,如果攻击者了解该算法,并将小波逼近子图中的系数部分扰乱,就可以抹去或改造水印信息。

(2)由于水印的嵌入和水印存在的判别均使用相同的密码,因此在提取水印过程中就要求必须公开私有秘钥,可以文献[11]所提的算法为例,若要最后恢复出水印图像,就需要知道置乱序列,而置乱序列一公开,攻击者也就可以抹去或改造水印信息。

这两个问题的存在,就决定了只能由版权所有者或水印嵌入者才可进行水印存在与否的判别,这就限制了这些水印算法的实际应用,而上述两个问题存在的根由,是因为算法自身具有对称非公钥的特性所致,所以研究一种能解决上述两个问题的不对称的公钥水印算法,将具有很高的应用价值。

要解决上述两个问题,不对称的公钥水印算法则应满足如下要求:(1)水印算法的一切细节都可以公开;(2)水印算法在水印嵌入后,应公开一个公钥,而后任何人都可以利用这个公钥来验证图像中是否存在水印,同时又不能利用公钥来去除图像中的水印信号;(3)只有拥有密钥的人才可以去除图像中的水印信号。这样在如何验证版权所有问题上,就可以以版权主张者是否能将水印信号去除为判断依据。

为此,本文提出了一种基于具有特殊相关特性的伪随机序列的不对称公钥数字水印算法。

2　不对称的公钥水印算法

2.1　算法思想

本文设计的不对称公钥水印算法流程如图 2 和图 3 所示。

该算法的基本思想是利用相关技术,首先以某个具有特殊相关特性的序列作为密钥,然后加入信号强度相同的随机噪声作为公钥予以公开。这样,如果要判断是否存在水印,那么只要求判定图像中某特定信号和公钥的相关函数是否和公开的相关函数相同即可。

本文算法不仅可以公开验证水印存在与否过程的任何细节,同时,水印嵌入算法也可以公开(但公开水印嵌入算法,会降低算法的抗攻击能力);而密钥则是作为版权所有者的唯一证明,不能公开。

2.2　作为密钥的伪随机序列

2.2.1　最佳正弦伪随机序列

文献[14]提出:如果 b 是 p 的原根,则 $1/p$ 为 b 进制全循环小数,而且可由该全循环小数产生最佳正弦伪随机序列 $\boldsymbol{x}=\{x_i\}$。由于序列 $\boldsymbol{x}$ 具有良好的随机特性,因此对序列 $\boldsymbol{x}$ 进行 $p-1$ 的周期延拓,可得到以下 $\tau=0\sim p-2$ 时的周期自相关函数

$$R_x(\tau)=\frac{1}{p-1}\sum_{i=1}^{p-1}x_i x_{i+\tau}$$

$$=\begin{cases}\dfrac{p}{2(p-1)} & \tau=0\\ \dfrac{-p}{2(p-1)} & \tau=\dfrac{p-1}{2}\\ 0 & 0<\tau<p-1,\tau\neq\dfrac{(p-1)}{2}\end{cases}\tag{1}$$

其中,$i+\tau$ 可作为 $i+\tau(\mathrm{mod}p)$ 理解。

2.2.2 作为密钥的伪随机序列

尽管最佳正弦伪随机序列具有很好的和独特的相关特性,并且其抗干扰能力也比较强,但不能用它作为水印密钥,因为序列的长度就泄漏了密钥信息。本文在该序列的基础上,设计了一种新的具有较好相关特性,并可作为密钥的随机序列的产生方法。

(1)密钥序列的产生方法

在最佳正弦伪随机序列中的第 k 个数前插入数 I,其中,$1\leqslant k\leqslant p, I\ll p$。

(2)序列的自相关性质

对序列 $\boldsymbol{y}=\{y_i\}$ 进行 p 的周期延拓,当 p 较大时,可得到以下 $\tau=0\sim p-1$ 时的序列自相关函数

$$R_y(\tau)=\frac{1}{p}\sum_{i=1}^{1}y_iy_{i+\tau}\approx\begin{cases}0.5 & \tau=0\\ -0.25 & \tau=\dfrac{p}{2},\dfrac{p}{2}+1\\ 0 & 0<\tau<p-1;\tau\neq\dfrac{p}{2},\dfrac{p}{2}+1\end{cases}\tag{2}$$

其中,$i+\tau$ 作为 $i+\tau(\mathrm{mod}p)$ 理解。

下面对式(2)进行证明:

设最佳正弦伪随机序列为 $\boldsymbol{x}=\{x_i\}$,当 $\tau=0\sim p-2$ 时的周期自相关函数为 $R_x(\tau)$。不失一般性,可设序列 $\boldsymbol{y}=\{y_i\}$ 是由序列 $\boldsymbol{x}$ 在 x_k 后插入某个实数 I(其中,$I\ll p$)所得,并记密钥序列的自相关函数为 $R_y(\tau)$。

证明:

①当 $\tau=0$ 时:

由于 $R_y(\tau)=R_x(0)+\dfrac{I^2}{p}$,且 $p\gg I$,所以 $R_y(\tau)\approx R_x(0)\approx 0.5$

②当 $\tau=1$ 时,

由于 $R_y(\tau)=R_x(1)+\dfrac{I(x_k+x_{k+1})}{p}$,且 $p\gg I$,所以 $R_y(\tau)\approx R_x(1)\approx 0$

③当 $2\leqslant\tau\leqslant k+1$,且 $p\gg I$ 时,$R_y(\tau)=R_x(\tau)+R_x(\tau-1)+\dfrac{I}{p}(x_{k-\tau+1}+x_{k+\tau})-g(\tau)\approx R_x(\tau)+R_x(\tau-1)-g(\tau)$

其中,

$$g(\tau)=\frac{1}{p}\left(\sum_{i=k-\tau+1}^{k}x_ix_{i+\tau}+\sum_{i=0}^{i=k-\tau+1}x_ix_{i+\tau-1}+\sum_{i=k+1}^{p-1}x_ix_{i+\tau-1}\right)$$

$$=\frac{1}{2p}\sum_{i=k-\tau+1}^{k}\left(\cos\frac{2\pi b^{i-1}(1-b^{\tau})}{p}-\cos\frac{2\pi b^{i-1}(1+b^{\tau})}{p}\right)+\frac{1}{2p}\sum_{i=0}^{k-\tau+1}\left(\cos\frac{2\pi b^{i-1}(1-b^{\tau-1})}{p}-\cos\frac{2\pi b^{i-1}(1+b^{\tau-1})}{p}\right)+\frac{1}{2p}\sum_{i=k+1}^{p-1}\left(\cos\frac{2\pi b^{i-1}(1-b^{\tau-1})}{p}-\cos\frac{2\pi b^{i-1}(1+b^{\tau-1})}{p}\right)$$

当 $i=1,2,\cdots,p-1$ 时,则 b^{i-1} 遍历模 p 群中的除 0 外的所有值各 1 次;同时在 $1<\tau\leqslant p$ 情况下,有 $b^{\tau}-1\neq 0\ (\mathrm{mod}p)$ 和 $b^{\tau-1}-1\neq 0\ (\mathrm{mod}p)$,即 $\sum_{i=k-\tau+1}^{k}b^{i-1}(1-b^{\tau})\cup\sum_{i=0}^{k-\tau+1}b^{i-1}(1-b^{\tau-1})\cup\sum_{i=k+1}^{p-1}b^{i-1}(1-b^{\tau-1})$ 将遍历模 p 群中,除 0 外的某 $p-2$ 值各 1 次。

在 $\tau\neq(p-1)/2$ 或 $\tau\neq(p+1)/2$ 条件下,由于有 $\sum_{i=k-\tau+2}^{k}b^{i-1}(1+b^{\tau})\cup\sum_{i=0}^{k-\tau+1}b^{i-1}(1+b^{\tau-1})\cup\sum_{i=k+1}^{p-1}b^{i-1}(1+b^{\tau-1})$ 将遍历模 p 群中除 0 外的某 $p-2$ 值各 1 次;因此可以得到 $g(\tau)=\varepsilon/p\approx 0$(其中,$\varepsilon\in[-2,2]$)。

若 $\tau=(p-1)/2$,则有 $\cos\dfrac{2\pi b^{i-1}(1+b^{\tau})}{p}=1$,$\sum_{i=0}^{k-\tau+1}\cos\left(\dfrac{2\pi b^{i-1}(1+b^{\tau-1})}{p}\right)\cup\sum_{i=k+1}^{p-1}\cos\left(\dfrac{2\pi b^{i-1}(1+b^{\tau-1})}{p}\right)\approx(p-2)/4$。

若 $\tau=(p+1)/2$,则有 $\cos\dfrac{2\pi b^{i-1}(1+b^{\tau-1})}{p}=1$,同时可以得到如下结果:

$$\sum_{i=k-\tau+2}^{k}\cos\left(\frac{2\pi b^{i-1}(1+b^{\tau})}{p}\right)\approx(p+1)/4。$$

综上所述,有 $g(\tau)\approx 1/4$。

④当 $1\leqslant\tau\leqslant k+1$,且 $p\gg I$ 时,则有

$$R_y(\tau)=R_x(\tau)+R_x(\tau-1)+\frac{I}{p}(x_{k-\tau+1}+x_{k+\tau})-h(\tau)\approx R_x(\tau)+R_x(\tau-1)-h(\tau)$$

其中,$h(\tau)=\dfrac{1}{p}\left(\sum_{i=k-\tau+1}^{k}x_ix_{i+\tau+1}+\sum_{i=0}^{i=k-\tau+1}x_ix_{i+\tau}+\sum_{i=k+1}^{p-1}x_ix_{i+\tau}\right)$,其证明类似证明③。

综上所述,式(2)得证。

(3)伪随机序列作为密钥的可行性

从式(2)可以看出,利用本算法产生的序列具有非常独特的相关性质,即由同一个最佳正弦随机序列产生的两个不同序列,其自相关函数非常相似。这就意味着,公开序列的长度和序列具有的自相关

特性,并不表示公开序列。该序列就为算法思想的实现提供了可能。用该序列作为密钥产生的公钥(即密钥加强度相当或稍强的随机噪声后的信号),将不会泄漏密钥的任何信息,而作为必须公开的用于判断水印是否存在的依据,即公钥和密钥之间的相关函数,也不会泄漏密钥的任何信息。

3 水印算法的实现

先定义以下两个函数:

(1)两个序列长度都为 p 的序列 $\boldsymbol{x}=\{x_i\}$ 和 $\boldsymbol{y}=\{y_i\}$,其中 $i=0\sim p-1$。定义其相关函数为

$$R_{x,y}(\tau)=\frac{1}{p}\sum_{i=0}^{p-1}x_i y_{i+\tau} \tag{3}$$

其中,$i+\tau$ 作为 $i+\tau(\mathrm{mod}p)$ 理解。

(2)两个序列长度都为 p 的序列 $\boldsymbol{x}=\{x_i\}$ 和 $\boldsymbol{y}=\{y_i\}$,其中 $i=0\sim p-1$。定义其区别度函数为

$$D(\boldsymbol{x},\boldsymbol{y})=\sum_{i=0}^{p-1}\left|\frac{x_i}{2x_1}-\frac{y}{2y_1}\right| \tag{4}$$

3.1 水印嵌入过程

(1)选择 b 和 p,并先按前述的方法来产生私有密钥伪随机序列 $\boldsymbol{k}^{\mathrm{r}}=\{k_i^{\mathrm{r}}\}$;然后随机产生和密钥长度相同的随机序列 $\boldsymbol{n}=\{n_i\}$;并由下式计算公钥 $\boldsymbol{k}^{\mathrm{k}}$:$\boldsymbol{k}^{\mathrm{k}}=\boldsymbol{k}^{\mathrm{r}}+\boldsymbol{n}$。

(2)先将原始图像 $\boldsymbol{G}_{\mathrm{o}}$ 进行多级小波分解,并对某个小波逼近子图 $\boldsymbol{D}_{\mathrm{o}}$,按照规则 ξ 选取 p 个位置互不相同的小波系数的小数部分来得序列 $\boldsymbol{c}^{\mathrm{o}}=\{c_i^{\mathrm{o}}\}$ $(i=0,\cdots,p-1)$,然后将序列 $\boldsymbol{c}^{\mathrm{o}}$ 按公式 $\boldsymbol{c}^{\mathrm{w}}=\boldsymbol{c}^{\mathrm{o}}+\alpha\cdot\boldsymbol{k}^{\mathrm{k}}$ 转换成序列 $\boldsymbol{c}^{\mathrm{w}}$,其中 α 是水印嵌入强度,也将作为密钥之一;接着,以 $\boldsymbol{c}^{\mathrm{w}}$ 取代 $\boldsymbol{D}_{\mathrm{o}}$ 中的 $\boldsymbol{c}^{\mathrm{o}}$,以便将 $\boldsymbol{D}_{\mathrm{o}}$ 变换成 $\boldsymbol{D}_{\mathrm{w}}$;最后结合其他小波子图对 $\boldsymbol{D}_{\mathrm{w}}$ 进行小波逆变换来得到含水印的图像 $\boldsymbol{G}_{\mathrm{w}}$。

(3)对图像 $\boldsymbol{G}_{\mathrm{w}}$ 进行一次抽取水印工作,首先求出区别度 σ,然后将区间 $\sigma\pm\mu$ 公开,作为版权主张者用于抽取水印的置信区间。

3.2 水印存在与否的验证过程

(1)将图像 $\boldsymbol{G}_{\mathrm{u}}$ 进行多级小波分解,首先得到某个小波逼近子图 $\boldsymbol{D}_{\mathrm{u}}$,然后从 $\boldsymbol{D}_{\mathrm{u}}$ 的系数中按照规则 ξ 选取小波系数的小数部分的序列 $\boldsymbol{c}^{\mathrm{u}}=\{c_i^{\mathrm{u}}\}$;

(2)按公式(3)求出公钥 $\boldsymbol{k}^{\mathrm{k}}$ 的自相关函数(记为 $A(\tau)$),以及序列 $\boldsymbol{c}^{\mathrm{u}}$ 和公钥 $\boldsymbol{k}^{\mathrm{k}}$ 的相关函数(记为 $C(\tau)$);

(3)按式(4)计算 $A(\tau)$ 和 $C(\tau)$ 的区别度 σ,当 σ 小于某一门限值 d 时,就认为存在水印;否则认为水印不存在。

3.3 版权所有证明过程

(1)由版权主张者提供校验密钥序列 $\boldsymbol{k}^{\mathrm{ver}}=\{k_i^{\mathrm{ver}}\}$ 和嵌入强度 $\tilde{\alpha}$;

(2)将图像 $\boldsymbol{G}_{\mathrm{w}}$ 进行多级小波分解,首先得到某个小波逼近子图 $\boldsymbol{D}_{\mathrm{w}}$,然后从 $\boldsymbol{D}_{\mathrm{w}}$ 的系数中,按照规则 ξ 选取位置互不相同的小波系数的小数部分,得到序列 $\boldsymbol{c}^{\mathrm{w}}$,并将序列 $\boldsymbol{c}^{\mathrm{w}}$ 按公式 $\boldsymbol{c}^{\mathrm{e}}=\boldsymbol{c}^{\mathrm{w}}-\alpha\cdot\boldsymbol{k}^{\mathrm{ver}}$ 转换成序列 $\boldsymbol{c}^{\mathrm{e}}$,最后将 $\boldsymbol{D}_{\mathrm{w}}$ 中 $\boldsymbol{c}^{\mathrm{w}}$ 的各个分量用 $\boldsymbol{c}^{\mathrm{e}}$ 中各个分量取代,并将 $\boldsymbol{D}_{\mathrm{w}}$ 化成 $\boldsymbol{D}_{\mathrm{e}}$,再结合其他小波子图对 $\boldsymbol{D}_{\mathrm{e}}$ 进行小波逆变换,即得抽取水印后的图像 $\boldsymbol{G}_{\mathrm{e}}$;

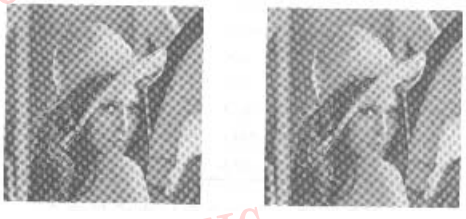
(3)对抽取水印后的图像 $\boldsymbol{G}_{\mathrm{e}}$ 进行水印信号检测,当区别度 σ 值在公开的置信区间 $\sigma\pm\mu$ 内,则说明水印抽取成功,即证明抽取者对该图像拥有版权;否则说明主张者不拥有图像版权。

4 试验结果

以灰度 Lena 图像为原始图像,对水印算法进行了实验仿真,仿真是在 Matlab 6.1 平台上进行的。实验时,取 $p=313$,$b=10$,$\alpha=0.15$;门限值 d 取 50;ξ 规则为取图像小波分解后逼近子图中系数大于 6.2 的前 p 个小波系数的小数部分。

计算可得到和置信区间为 199.0554 ± 10。

(1)添加水印对视觉效果的影响见图 4。



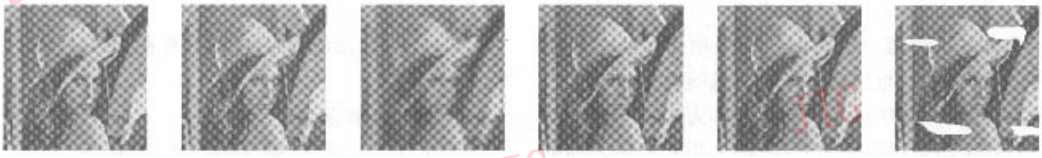
(a) 原始图像　　(b) 加水印后的图像

图 4　添加水印对视觉效果的影响

Fig. 4　Visual effect of watermark on original image

从图 4 可以看出,加水印信号后的图像和原始图像没有什么区别,即水印具有良好的不可感知性,其峰值信噪比(PSNR)为 44.315 1dB,此时区别度 $\sigma=11.4479$。

(2)常见图像处理对水印提取的影响见图 5。其中,图 5(a)是对含水印图像加均值为 0,最大值



(a) 加均值为 0，最大值为 0.1 随机噪声后的图像　(b) 加均值为 0，方差为 0.02 高斯噪声后的图像　(c) 模糊化后的图像　(d) 中值滤波后的图像　(e) 魏纳滤波后的图像　(f) 随机剪切后的图像

图 5　对含水印信号图像进行常见图像处理后的 Lena 图像

Fig. 5　Experiment results of common signal distortions to watermarked images

为 0.1 的随机噪声后的图像；图 5(b)是对含水印图像加均值为 0，方差为 0.02 的高斯噪声后的图像；图 5(c)是对水印图像模糊化后的图像，以仿真图像的打印后再扫描；图 5(d)是对含水印图像进行中值滤波后的图像；图 5(e)是对含水印图像进行魏纳滤波后的图像；图 5(f)是对含水印图像进行随机剪切后得到的图像。

图 5 中各图像水印存在与否的检测结果如表 1 所示。尽管本文的水印算法在图 5(c)试验中的水印提取效果不佳，但由于此时图像的视觉效果已经非常差，因此仍然可以认为算法对各种干扰和各种常见的图像处理都有较强的鲁棒性。特别是对图 5(f)剪切部分重要信号的情况下，其所提取的水印信号仍然可信。

表 1　常见图像处理对水印提取的影响

Tab. 1　Effect of common signal distortions on watermark detection

	峰值信噪比(dB)	区别度 σ 值
图 5(a)	22.692 2	17.275 5
图 5(b)	16.839 0	14.800 3
图 5(c)	20.744 8	80.751 9
图 5(d)	27.857 2	20.664 5
图 5(e)	33.920 2	16.683 4
图 5(f)	15.797 4	28.784 3

(3)JPEG 压缩对水印提取的影响见表 2。

表 2　JPEG 压缩对水印提取的影响

Tab. 2　Robustness to JPEG compress

品质因子	峰值信噪比(dB)	区别度 σ 值
10	30.232 7	13.803 6
20	32.644 4	12.367 6
30	33.888 8	11.837 2
40	34.583 8	11.555 8
50	35.248 9	11.661 7
60	35.818 3	11.731 8
70	36.382 6	11.492 0

从表 2 可以看出，本文提出的算法在品质因子非常小的情况下，仍然能够判断出图像中存在水印信号，这说明该算法能抗 JPEG 压缩。

(4)攻击试验

图 6 是在固定某个嵌入强度下，使用 313 个不同密钥进行抽取水印的试验结果。从图 6 可以看出，如果不拥有正确的嵌入强度，就不能正确的抽取掉水印信号。图 7 是使用产生密钥序列的 k 值来随机产生 313 个 I 值的密钥，且使用正确抽取强度的抽取效果。由该图可以看出，如果降低置信区间的大小，那么产生密钥的参数 I 就成为一个新的秘密限门，这虽可进一步提高算法的对抗穷举法的攻击能力，但这同时会降低算法的抗干扰能力。

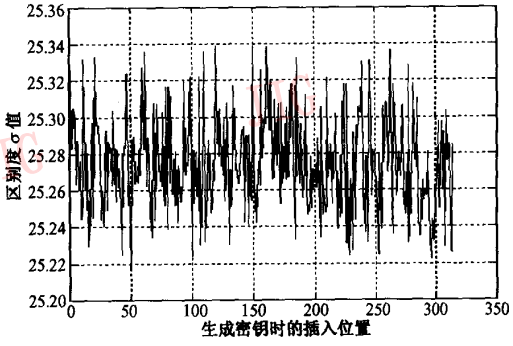


图 6　使用不正确的嵌入强度去除水印的效果

Fig. 6　Experiment results of erasure watermark by using wrong embedment intensity

5　结　论

试验证明，本文提出的用于版权保护的不对称公钥算法是可行的，同时，试验结果还表明，该算法具有较强的鲁棒性，可以抗一般的图像处理攻击。由于本算法的时间复杂度取决于密钥的长度和水印

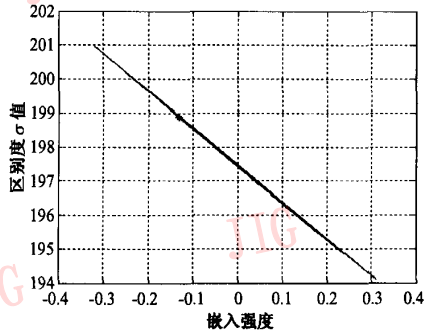


图 7　使用正确的嵌入强度、随机产生密钥去除水印的效果

Fig. 7　Experiment results of era ure watermark by using correct embedment intensity

的嵌入强度的可选空间,因此增加序列的长度、采用多个序列,或嵌入水印时采用多个嵌入强度,则不仅可以延长算法的穷举攻击时间,而且使破解变得更加不可能。当然,在以牺牲抗干扰能力为代价的情况下,密钥的产生参数 I 可作为一个新的秘密限门,用于进一步扩大密钥空间,以提高算法的抗穷举攻击能力。

虽然本算法不需要公开水印的嵌入算法,但一旦水印的嵌入算法泄漏,对某些特定的密钥(如 k 取 p 的时候),水印攻击者利用统计的方法还是有可能检测出密钥,这是本水印算法的不足之处,因此,是否存在作为密钥的更好的序列或是否存在其他的公钥水印算法是今后研究的方向。

参考文献(References)

1 Petitcolas F A P, Anderson R J, Kuhu M G. Information hiding-A survey[J]. Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, 1999, **87**(7): 1062 ~ 1078.

2 Yang Yi-xian, Niu Xin-xin. Review of multi-media information camouflage[J]. Journal of China institute of communications, 2002, **23**(5): 32 ~ 38. [杨义先,钮心忻. 多媒体信息伪装综述[J]. 通信学报, 2002, **23**(5): 32 ~ 38.]

3 Zhang Yu-jin. Image engineering in China: 200[J]. Journal of Image and Graphics, 2003, **8A**(5): 481 ~ 498. [章毓晋. 中国图象工程: 2002[J]. 中国图象图形学报, 2003, **8A**(5): 481 ~ 498.]

4 Liu Zhen-hua, Yin Ping. Information hidden technology and application[M]. Beijing: Science Press, 2002: 77 ~ 82. [刘振华, 尹萍. 信息隐藏技术及其应用[M]. 北京:科学出版社, 2002: 71 ~ 82.]

5 Wong P W. A public key watermark for image verification and authentication [A]. In: Proceedings of the IEEE International Conference on Image Processing (ICIP'98) [C], Chicago, Illinois, USA, 1998, **1**: 455 ~ 459.

6 Cox I J, Kiliant J, Leighton T, *et al.* Secure spread spectrum watermarking for multimedia [J]. IEEE Transactions on Image Processing, 1997, **6**(12): 1674 ~ 11687.

7 Xia Xiang-gen, Boncelet C G, Arce G R. Wavelet transform based watermark for digital image[J]. Watermarking Special Issue of Optice Express, 1998, **3**(12): 497 ~ 511.

8 Hsu Chiouting, Wu Jaling. Hidden digital watermarks in image[J]. IEEE Transactions on Image Proceeding, 1999, **8**(1): 58 ~ 68.

9 Sun Rui, Sun Hong, Yao Tian-reng. Blind watermarking scheme for a spatial-domain digital image[J]. Journal of Huazhong University of Science and Technology (Nature Science), 2002, **30**(4): 81 ~ 83. [孙锐,孙洪,姚天任. 一种空域的数字图像盲水印方案[J]. 华中科技大学学报(自然科学版), 2002, **30**(4): 81 ~ 83.]

10 Wang Huiqin, Li Renhou, Wang Zhi-xiong. Fuzzy adaptive image watermarking algorithm[J]. Journal of Xi'an Jiaotong University, 2002, **37**(2): 182 ~ 185. [王慧琴,李人厚,王志雄. 一种模糊自适应图像水印算法的研究[J]. 西安交通大学学报, 2002, **37**(2): 182 ~ 185.]

11 Zhou Ya-xun, Xu Tie-feng. An invisible signature digital watermarking algorithm based on binary operation [J]. Journal of China Institute of Communication, 2002, **23**(2): 107 ~ 112. [周亚讯,徐铁峰. 基于二值运算的隐形签名数字水印算法[J]. 通信学报, 2002, **23**(2): 107 ~ 112.]

12 Zhang Jun, Wang Neng-chao, Shi Bao-chang. A public watermarking based on chaos map and genetic alogrithm[J]. Pattern Recognition and Artificial Intelligence, 2002, **15**(1): 42 ~ 47. [张军,王能超,施保昌. 基于混沌映射和遗传算法的公开数字水印技术[J]. 模式识别与人工智能, 2002, **15**(1): 42 ~ 47.]

13 Pan J S, Huang H C, Wang F H. A VQ-based robust multi-watermarking algorithm[J]. IEICE Transactions on Fundamentals of Electronics, Communication and Computer Sciences, 2002, **E85-A**(7): 1719 ~ 1726.

14 Hu De-wen. Nonlinear and multivariable system identification[M]. Hunan: National University of Defense Technology Press, 2001: 54 ~ 59. [胡德文. 非线性与多变量系统相关辨识[M]. 湖南:国防科技大学出版社, 2001: 54 ~ 59.]