一种定位精确的混沌脆弱数字水印技术

丁 科, 何 晨, 王宏霞
(上海交通大学电子工程系, 上海 200030)

摘 要: 提出了一种特别适用于数字产品的认证、内容篡改证明和完整性证明的脆弱数字水印算法. 原始图像的象素灰度值映射为混沌的初值, 经过若干次迭代生成水印图像, 然后把它嵌入象素灰度值的 LSB(Least Significant Bit) 平面. 利用混沌对初值极端敏感性的特点, 能够精确地定位对加入水印图像的篡改, 并且水印提取不需要原始图像. 实验结果表明了所提出水印方案对篡改证明的有效性, 敏感性以及良好的篡改定位能力.

关键词: 脆弱数字水印; 混沌; 认证
中图分类号: TN919; TP391 文献标识码: A 文章编号: 0372-2112 (2004) 06-1009-04

A Chaotic Fragile Watermarking Technique with Precise Localization

DING Ke, HE Chen, WANG Hong-xia
(Dept. of Electronic Eng., Shanghai Jiaotong Univ., Shanghai 200030, China)

Abstract: A new fragile watermarking scheme is presented, which is capable of authentication, tamper-proofing and integrity verification of digital products. Let the grayscale values of host image map the initial values of the chaotic mapping. The watermark obtained by iterating several times of the chaotic mapping, is embedded into the LSB (Least Significant Bit) plane of host image. The proposed scheme can localize the tampers on the watermarked image by using to the high sensitivity on initial value of the chaotic mapping. Moreover, no host image is needed in watermark extraction. Our simulation results show the effectiveness, sensitivity and localization of tamper-proofing of this technique.

Key words: fragile watermark; chaos; verification

1 引言

近年来, 随着计算机以及多媒体技术的发展, 数字产品的版权保护以及内容认证越来越受到重视, 数字水印就是在这样的背景下产生并受到学术界的广泛关注. 用于版权保护的鲁棒数字水印的研究已经比较深入, 但考虑到数字产品的内容完整性认证, 及传输的多媒体数据的可信度, 这种水印技术还不能完全适应这种要求, 而脆弱水印技术能够实现这一点. 脆弱水印通常应该满足以下特点: (1)不可见性, (2) 对加入水印图像篡改的敏感性, (3) 篡改定位能力, (4) 提取水印不需要原始图像.

文献[1] 把图像低频子带系数通过正、负调制嵌入大于某个给定阈值的小波域系数, 所提出的脆弱水印具有篡改定位能力, 但是定位精度不高, 实现算法复杂, 并且阈值的选取往往比较困难. 文献[2] 在文献[3] 的基础上提出一种具有篡改定位能力的分级脆弱水印, 原始图像分级, 并通过 Hash 函数生成摘要, 和水印异或之后通过私钥加密, 最后嵌入到原始图像的 LSB(Least Significant Bit) 平面, 该算法通过不断分级达使定位精度逐步提高, 其主要优点是克服了文献[3] 中对矢量攻击(VQ attack) 的无效性. 但是该算法由于不同级分享同一个 LSB 平面, 导致嵌入内容互相包含, 所以需要分割算法来解决嵌入时的碰撞问题. 类似这些传统的篡改定位方法[2,3] 一般是基于 Hash 函数对篡改的敏感性, 这种方法的弊端在于: (1) 必须分块, 导致定位不够精确, (2) Hash 函数计算复杂度高, 不适合实时处理, (3) 被认可的安全的 Hash 函数种类少.

本文基于混沌对初值的极端敏感性, 为定位型的认证以及脆弱数字水印技术开辟了一条新的路径. 原始图像的象素灰度值映射为混沌初值经过若干次混沌迭代生成水印图像, 然后嵌入到原始图像的 LSB 平面, 利用混沌对初值的极端敏感性, 能够精确地定位对加入水印图像的篡改, 性能稳定, 原理清晰, 实现速度快, 并且水印的提取不需要原始图像.

2 基于混沌映射的脆弱数字水印技术

2.1 混沌映射

在我们提出的方案中, 多次使用混沌系统产生伪随机序列. 混沌是非线性方程(组) 在某些特定条件下的解, 它的随机输出由一确定的方程(组) 决定. 混沌系统的初始参数可以作为整个水印系统的密钥, 混沌系统良好的随机性能和容易再生的特点增加了系统的安全性能. 考虑一维离散混沌映射

$$f: U \to U,\ U \subset R$$

$$z(n+1) = f(K, z(n)),\quad K \in R,\quad z(n) \in U \qquad (1)$$

其中 $n = 0, 1, \ldots$ 表示迭代次数, K 是控制系统混沌行为的参数. (1) 式迭代 n 次得到实值混沌序列记为

$$Z^n = \{z(1), z(2), \ldots, z(n)\} \qquad (2)$$

收稿日期: 2003-01-29; 修回日期: 2003-08-23
基金项目: 国家高技术研究发展计划(863) (No. 2002AA144110); 中国博士后科学基金(No. 2003033304)

定义如下量化函数

$$V = Q(Z^n, d) \tag{3}$$

其中 $V > \{v_1, v_2, \cdots, v_d \mid v_i \in \{0,1\}\}$, d 表示返回 {0, 1} 比特的个数. 由于混沌对初值的极端敏感性, 因此对于略微不同的初始值, 将得到完全不同的两个序列.

设 $E = \{E_0, E_1, \cdots, E_{q-1}\}$ 是 U 上的一个有限分割, $G_{j=0}^{q-1} E_j = U$, $E_i \cap E_j = \varnothing (i \neq j)$, 其中 q 为分割数. 根据映射 f 的有限分割 E 可得到符号序列 X, 当且仅当测度熵 $h(f) = \log_2 q$ 时, X 为 Bernoulli 序列[6]. 十进制混沌序列可由二进制符号序列 X 顺次取 m 比特得到.

2.2 水印嵌入

水印嵌入算法的框图如图 1 所示.

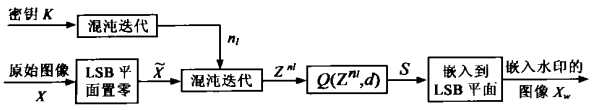

图 1 水印嵌入算法框图

对于大小为 N×N 的原始图像 $X(i,j)$, $(1 \le i, j \le N)$, 其 LSB 平面置零得到 $\tilde{X}(i,j)$. 设映射 C_0 满足 $C_0(X(i,j)) \in \{0,1\}$, 混沌迭代的初值 $z_{i,j}(0)$ 为:

$$z_{i,j}(0) = C_0(X(i,j)) \tag{4}$$

水印信号 $S: S(i,j) \in \{0,1\}$ 由式(5)产生:

$$S(i,j) = Q(Z^n_{i,j}, 1) \tag{5}$$

其中迭代次数 n_l 依次取由系统密钥 K 所产生的十进制混沌序列 $\{n_l \mid 1 \le n_l \le 2^m, l = 1, 2, \cdots, N^2\}$ 中的元素, K 可作为整个脆弱水印系统的密钥.

由此得到嵌入水印的图像

$$X_w = Add(X, S) \tag{6}$$

函数 Add(a, b) 表示把二值平面 b 嵌入到 a 的 LSB 平面的操作.

上述方案由于对每一个象素点都要混沌映射迭代多次, 导致计算复杂度的增大. 下面改进上述方案, 把 X 分割成大小为 c×c 的小块, 对于每个小块 $X_r(i,j)$, $(1 \le i, j \le c)$, 计算

$$z_r(0) = C_0\left(\sum_{i=1}^{c}\sum_{j=1}^{c} X(i,j)\right) \tag{7}$$

$$S_r = Q(Z^n_r, c^2) \tag{8}$$

其中 $\{n_r \mid 1 \le n_r \le 2^m, r = 1, 2, \cdots, \left(\frac{N}{c}\right)^2\}$. 改进算法以每个小块所有象素灰度值的和映射为混沌初值, 每次混沌映射迭代返回小块大小个数的二值序列. 记 S_c:

$$S_c > (S_1, S_2, \cdots, S_{(N/c)^2}) \tag{9}$$

为改进方案的水印, 同上得到嵌入水印的图像

$$X_{cw} = Add(X, S_c) \tag{10}$$

2.3 水印提取及认证

水印提取算法框图如图 2 所示, 对收到的嵌入水印的图像的 LSB 平面置零, 以它的象素灰度值当作混沌的初值, 然后根据由密钥生成的混沌迭代次数, 通过混沌迭代得到水印 S_{ex}.

定义篡改判别矩阵:

$$T(i,j) = \begin{cases} 1, & X(i,j) \text{被篡改} \\ 0, & X(i,j) \text{没被篡改} \end{cases} \tag{11}$$

$$T = |S_{ex} - LSB(X_w)| \tag{12}$$

其中 LSB(·) 定义为取图像的 LSB 平面.

如果 $S_{ex} = LSB(X_w)$, 则 $T = [0]_{N \times N}$, 表明原始图像没有被篡改. 否则矩阵 T 中为 1 的点表示原始图像中被篡改的点.

3 性能分析

3.1 敏感性分析

脆弱水印要求加入的水印不可察觉. 为了衡量嵌入水印图像和原始图像之间的差别, 定义峰值信噪比(PSNR, Peak Signal-to-Noise Ratio)为

$$PSNR = 10\log_{10}\left(\frac{255 \times 255}{\frac{1}{N \times N}\sum_{i=1}^{N}\sum_{j=1}^{N} |X_w(i,j) - X(i,j)|^2}\right) \tag{13}$$

本文把水印信号嵌入到图像的 LSB 平面, 设 P_{el} 为把 0 判成 1 或者把 1 判成 0 的差错概率, 由 LSB 平面每个比特的独立性知, $P_{el} = 0.5$. 计算加入水印的图像和原始图像差值平方的数学期望

$$E(|X_w(i,j) - X(i,j)|^2) = P_{el} \times 1 + (1 - P_{el}) \times 0 = 0.5 \tag{14}$$

由此得到峰值信噪比的数学期望为

$$E(PSNR) = 10\log_{10}\left(\frac{255 \times 255}{\frac{1}{N \times N}\sum_{i=1}^{N}\sum_{j=1}^{N} E(|X_w(i,j) - X(i,j)|^2)}\right) = 51.18\text{dB} \tag{15}$$

可见, 从理论上分析, 本算法将得到很高的峰值信噪比值, 满足脆弱水印对不可察觉性的要求.

3.2 篡改定位能力分析

利用混沌映射对初值极端敏感性的特点, 对加入水印图像的篡改本算法能准确地定位, 从而使之具有内容篡改证明和完整性证明能力.

由混沌的伪随机特性知, 如果点 $X_w(i,j)$ 被篡改, 则经过混沌迭代, 检测到该点被篡改, 即 $T(i,j) = 1$ 的概率为:

$$P\{T(i,j) = 1 \mid X_w(i,j) \text{被篡改}\} = 0.5 \tag{10}$$

所以对于加入水印的图像, 理论上将有 50% 的篡改点被检测到, 并且这些被检测到的篡改点将随机的分布在篡改区域, 从下一节的实验结果可以看到篡改区域的轮廓十分明显. 表 1 是理论上检测到的篡改象素点数和实际检测到的篡改点数的比较.

表 1 理论上检测到的篡改点数和实际检测篡改点数的对比

	实例 1	实例 2	实例 3	实例 4
实际检测到的篡改点数	519	1009	2097	5014
理论检测到的篡改点数	512	1024	2048	4096

3.3 计算复杂度分析

对于一个实用的水印算法, 要求其计算复杂度低, 这样容易实现水印嵌入和提取的实时处理. 本文方案中, 所提出的水印嵌入和提取是两个对称的过程, 他们的计算复杂度是同一个数量级的. 对于嵌入算法, 其计算复杂度由原始图像大小以及混沌迭代的次数决定. 设每个点的混沌迭代的次数的数学

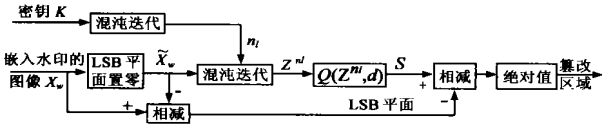

图 2　水印提取及认证过程框图

期望为 $E(n^r)$, 则嵌入算法的计算复杂度为:

$$R_c = O\left(E(n^r)\times\left(\frac{N}{c}\right)^2\right) \tag{17}$$

可见, R_c W1/ c^2. c 值越大, 计算复杂度越低, 但定位精度将随之降低, 所以必须在计算复杂度和定位精度上做折衷考虑.

4　实验结果

用 Matlab 6l 5 模拟本算法, 以一维 Logistic 离散混沌映射为例:

$$z(n+1) = 1-2z(n)^2,\ z(n)\in[-1,1] \tag{18}$$

取分割数为 2, 并且以零为分割点量化实值混沌序列. 实验中以 d= 1 为例, 量化函数 Q 的具体表达式为:

$$V=\begin{cases}1, & z(n)\ge 0\\ 0, & z(n)<0\end{cases} \tag{19}$$

考虑以下一些有实际意义的篡改实验.

411　图像内容修改实验

对于 512@512@8- Jet. 灰度图, 加入水印的图像如图 3(a) 所示, 峰值信噪比为 51. 1dB. 假设把- Jet. 图中飞机机身上的/ US AIR FORCE0 改成/ UN AIR FORCE0 即把字母 S 改成 N, 如图 3(b) 所示, 为了更清晰地观察所篡改的内容, 图 3(d) 和图 3(e) 为该区域篡改前后的放大的图像. 利用本文提出的算法检测所做的篡改, 篡改区域检测结果如图 3(c) 所示, 可见本文算法具有良好的篡改敏感性以及篡改定位能力. 表2比较了本文算法和文献算法的峰值信噪比值.

表 2　本算法与文献算法的 PSNR 的对比

	本文	Kundur[4]	Wang[5]
PSNR(dB)	5111	4310	4215

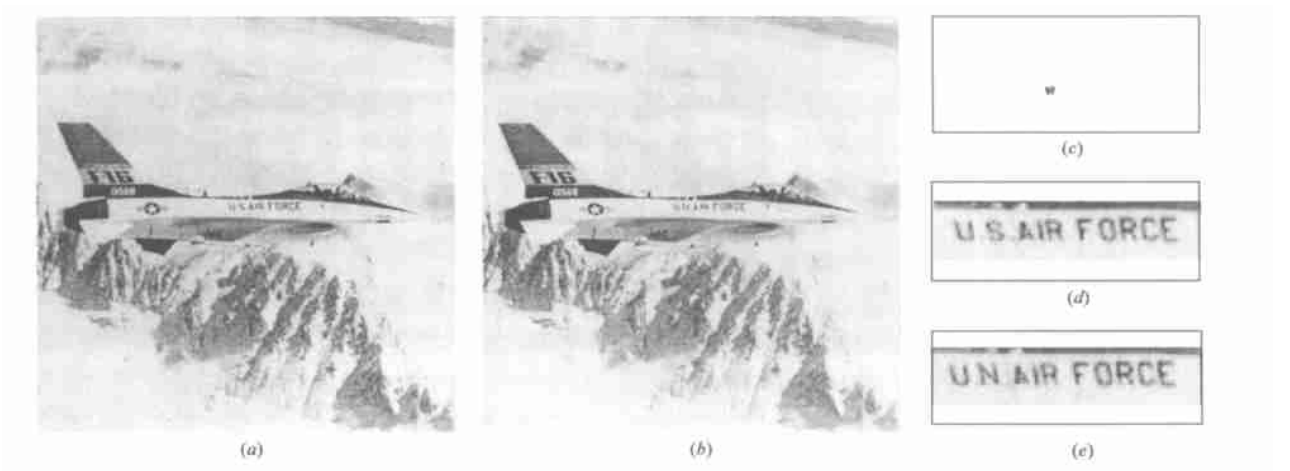

图 3　图像内容修改检测　(a) 篡改前的嵌有水印的图像;　(b) 篡改过的图像;　(c) 篡改检测结果;　(d) 篡改前的放大区域;　(e) 篡改后的放大区域

412　图像内容增加实验

对于 512 @512@8- Peppers. 灰度图, 加入水印的图像如图 4(a) 所示, 峰值信噪比为 511 2dB. 假如在加入水印的图像上再加两个辣椒如图 4(b) 所示, 利用本文的算法来检测这一篡改, 篡改区域检测结果如图 4(c) 所示. 可见本算法对图像内容的篡改能够非常精确地定位, 篡改区域轮廓明显.

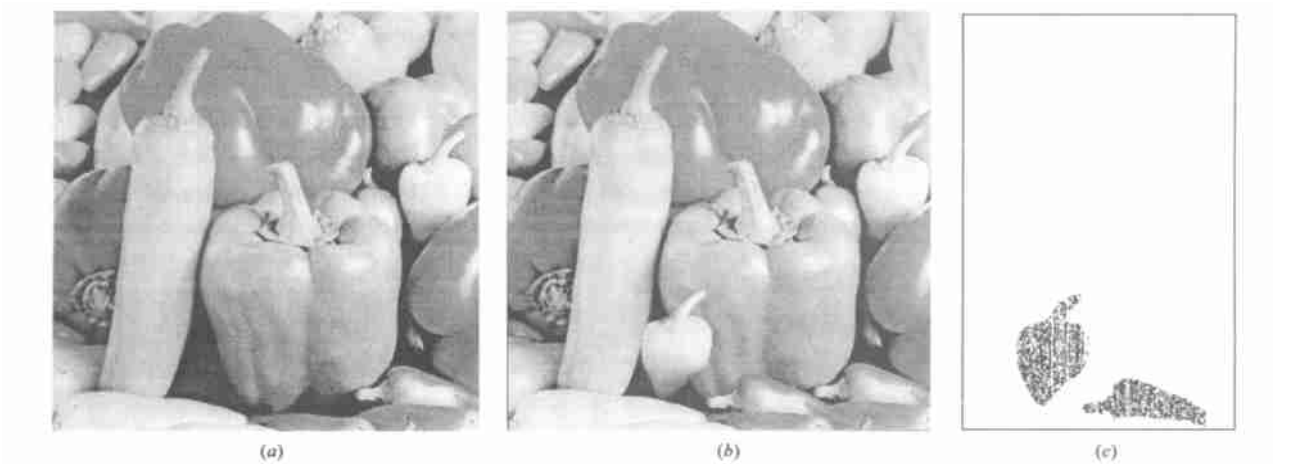

图 4　图像内容增加检测　(a) 篡改前的嵌有水印的图像;　(b) 篡改过的图像;　(c) 篡改检测结果

另外本文算法对常见图像处理操作如加性高斯噪声、JPEG 压缩、抽条、中值滤波、锐化、直方图均衡、纹理化、剪切、高斯模糊等都非常敏感, 对篡改区域都能良好地定位捕捉.

5 结论

提出了一种基于混沌映射的脆弱水印算法, 为定位型的认证以及脆弱数字水印开辟了一条新的路径. 通过修改原始图像的 LSB 平面嵌入水印, 获得了较高的峰值信噪比. 混沌随机序列的应用增加了算法的安全性. 另外, 本算法计算简单, 容易实现, 在提取时不需要原始图像, 并且对于加入水印图像的篡改能够精确的定位, 这些良好的性能大大增加了它的应用范围. 后续的研究可以重点放在公钥水印算法以及对篡改强度的区分等方面.

参考文献:

[1] C S Lu, H Y Mark Liao. Multipurpose watermarking for image authentication and protection[J]. IEEE Trans on Image Processing, 2001, 10(10): 1579- 1592.

[2] M U Celik, G Sharma, E Saber, et al. Hierarchical watermarking for secure image authentication with localization[J]. IEEE Trans on Image Processing. 2002, 11(6): 585- 595.

[3] P W Wong. Public key watermark for image verification and authentication[A]. Proc of 1998 IEEE Int Con on Image Processing[C]. Chicago, IL, USA: IEEE, 1998, 1: 455- 459.

[4] D Kundur, D Hatzinakos. Digital watermarking for telltale tamper proofing and authentication[J]. Proc of the IEEE, 1999, 87(7): 1167- 1180.

[5] Y W Wang, J F Doherty, R E Van Dyck. A wavelet2based watermarking algorithm for ownership verification of digital images[J]. IEEE Trans on Image Processing. 2002, 1(2): 77- 88.

[6] C Liang, S Sun. Chaotic frequency hopping sequence[J]. IEEE Trans on Communications, 1998, 46(11): 1433- 1437.

作者简介:

丁 科 男, 1980 年出生于浙江省余姚市, 2002 年毕业于浙江大学信息与电子工程学系, 获学士学位, 现为上海交通大学通信与信息系统专业硕士, 研究方向为信息隐藏技术, 混沌理论, 智能信息处理等.

何 晨 男, 上海交通大学教授, 博士生导师, 上海交通大学现代通信研究所副所长, 1982 年毕业于南京工学院无线电系, 获工学士, 1985 年毕业于南京工学院通信与电子系统专业, 获工学硕士, 1994 年毕业于日本国立德岛大学研究生院通信与电子系统专业, 获工学博士, 目前的主要研究方向为新一代无线通信系统理论、智能信息处理以及自适应信号处理在通信中的应用, 数字信息隐藏的理论与技术, 信息论与编码理论等.

王宏霞 女, 1973 年出生于河北省赵县, 1996 年毕业于河北师范大学数学系, 获学士学位, 1999 年在电子科技大学获应用数学专业硕士学位, 2002 年获电路与系统专业博士学位, 现为上海交通大学电子工程系博士后, 研究方向为信息隐藏技术, 保密通信, 混沌理论, 神经网络等.