基于混沌特性改进的小波数字水印算法

王丽娜, 于 戈, 王国仁
(东北大学信息科学与工程学院, 辽宁沈阳 110004)

摘 要: 本文基于混沌特性提出一种改进的小波数字水印算法 IWSVD, 即采用混沌模型算法来生成混沌随机序列. 混沌序列{Xn} 对初值极为敏感, 以此随机序列作水印信息, 随机序列不同, 会导致生成的数字水印不同, 保证数字水印信号的唯一性, 因而攻击者伪造水印是不可能的, 检测抵赖也是不可能的. 迭加了水印的图像能抗压缩及抗噪音处理, 该算法健壮性更好.

关键词: 混沌特性; 小波变换; 数字水印; 版权保护
中图分类号: TN911.73 文献标识码: A 文章编号: 0372-2112 (2001) 10-1424-03

An Improved Wavelet Digital Watermarking Algorithm Based on Chaotic Property

WANG Li-na, Yu Ge, WANG Guo-ren
(*School of Information Science and Engineering, Northeastern University, Shenyang, Liaoning* 110004, *China*)

Abstract: An improved wavelet watermarking algorithm based on chaotic property is proposed. The random sequence acted as watermark is generated using chaotic function model. Since the chaotic random sequence is sensitive to initial value, different random sequence causes different watermark, which makes digital watermark be unique. Therefore it is impossible for an attacker to forge digital watermark and to detect repudiately. The embedded watermark is robust to compression and noise addition etc.

Key words: chaotic property; wavelet transform; digital watermarking; copyright protection

1 引言

随着 Internet 中图像和视频信息的快速增长, 对数字信息进行版权保护有着迫切的需求. 数字水印(digital watermark) 技术是保护版权的最好技术. 它的核心是信息隐藏技术. 由于水印信息并不影响作品的宏观内容, 因而水印信息将永久地保存在多媒体作品当中, 任何人若试图从作品中剔除水印都不得不大幅度破坏原作品, 以致到面目全非的地步, 从而保护了作者的合法版权. 一些专家学者提出了不同的水印模式, 例如, Horvatic 等人提出基于安全波谱和听觉感知模型的健壮语音水印算法[1]. Lutoboski 等人提出使用图像的小波系数矩阵的单值分解法生成水印[2]. Swanson 等人提出基于对象的透明的视频水印[3]. 这些研究对数字信息版权保护做出了重要贡献. 但是, 在这些算法中嵌入个人信息时都是以个人信息作种子采用一般的随机数生成方法来生成随机数. 这不具备随机序列对初值敏感这一特性, 因此有可能产生伪造原创作者个人信息来伪造水印现象. 为此本文提出了一种改进的算法. 将图像原创作者本身掌握的一个保密参数当作 x_0. 混沌序列 $\{X_n\}$ 对初值 x_0 极为敏感. 以此序列作水印信息, 因而会导致生成的水印不同, 这样一来保证了水印信号的唯一性, 所以攻击者伪造水印是不可能的, 检测抵赖也是不可能的. 在本文中采用混沌算法来生成随机序列, 健壮性更好.

2 基于混沌特性改进的小波数字水印算法 IWSVD

本文研究对图像嵌入水印, 把水印叠加在图像能量最集中的部分. 小波变换能将图像分解到时域和尺度域上. 所以选择适当的小波基对原图像进行 l 级分解, 对前 l 级的差别分量保留, 不做处理, 对第 l 级的详细分量嵌入水印.

小波变换与傅氏变换的一个区别是小波变换的变换基不唯一. 选择小波函数时通常需要考虑小波的正交性、紧支集和消失矩. 高阶消失矩可以使变换快速衰减, 小波的消失矩越高, 其支集越长. 在 IWSVD 算法中, 采用具有高阶消失矩的紧支正交小波——Daubechies 小波.

2.1 小波 SVD 数字水印算法描述[2]

定义 T 为小波 SVD(Wavelet Singular Value Decomposition) 系数水印转换, 设 $A = A(M, l)$ 是图像 M 在 l 层的相近系数的 $n \times n$ 矩阵, 考虑到 A 的单值分解:

$$A = U \sum V^T$$

其中,

$$U = (u_1, \cdots, u_n)^T \quad V = (v_1, \cdots, v_n)^T \quad \Sigma = \begin{pmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_n \end{pmatrix}$$

U 和 V 是正交矩阵: $U^T U = I$ $V^T V = I$

收稿日期: 2000-09-21; 修回日期: 2001-04-22

设 $\overline{U}=(\overline{u}_1, \cdots, \overline{u}_n)^T$　　$\overline{V}=(\overline{v}_1, \cdots, \overline{v}_n)^T$

是两个随机生成的正交矩阵(密钥相关)

并且 $\overline{\Sigma}=\delta\begin{pmatrix}\overline{\delta}_1 & & \\ & \ddots & \\ & & \overline{\delta}_n\end{pmatrix}$ 是随机生成的对角矩阵(密钥相关).

从 $\overline{U}$ 和 $\overline{V}$ 中取后 d 行来代替 U 和 V 的对应的 d 行, 形成如下两个矩阵 $\tilde{U}$ 和 $\tilde{V}$

$$\tilde{U}=(u_1, \cdots, u_{n-d}, \overline{u}_{n-d+1}, \cdots, \overline{u}_n)^T$$

$$\tilde{V}=(v_1, \cdots, v_{n-d}, \overline{v}_{n-d+1}, \cdots, \overline{v}_n)^T$$

进而构成 $V(A)=\tilde{U}\Sigma\tilde{V}^T$,

$T(A)=A+V(A)$.

在该算法中嵌入个人信息时都是以个人信息作种子采用一般的随机数生成方法来生成随机数. 这不具备随机序列对初值敏感这一特性, 因此有可能产生伪造图像原创作者个人信息来伪造水印现象. 为此本文提出了一种改进的算法, 基于混沌随机序列对初值敏感的特性, 使用混沌模型生成混沌随机序列, 来代替一般的随机数生成.

2.2　基于混沌随机序列对初值敏感的特性提出的改进算法 IWSVD

混沌函数具有伸大拉长和折回重叠的性质, 所以有不可预测性. 混沌序列是一个伪随机序列, 很容易由迭代方程或非线性方程或偏微分方程生成. 考虑如下的非线性迭代方程 $X_{n+1}=f(X_n; \mu_i)$, 这是一个一维多参数的迭代方程, $f(X_n; \mu_i)$ 是变量 X 的非线性函数, i ($i=1, 2, 3\cdots$) 为参数. 对于参数 i 选取适当的值, 可以得到混沌序列 $\{X_n\}$, $\{X_n\}$ 对初值非常敏感. 初始条件的任意小的改变如 1.0e-6, 都会引起完全不同的行为. 其迭代轨迹就会大相径庭, 加上迭代方程本身的特点, 初值成为得到迭代序列的关键因素. 因而 $\{X_n\}$ 可以用作作品原创者的身份"指纹".

对于一维映射: $X_{n+1}=f(X_n \quad \mu_i)$,

由初始条件敏感性可知, 当初始条件 x_0 稍微出现一些偏差 δx_0, 则经过 n 次迭代后, 结果就会呈指数分离, 故 n 次迭代后的误差为:

$$\delta x_n=|f^n(x_0+\delta x_0)-f^n(x_0)|=\frac{df^n(x_0)}{dx}\delta x_0=e^{lE\cdot n}\delta x_0$$

其中　$LE=\frac{1}{n}\ln\frac{\delta x_n}{\delta x_0}=\frac{1}{n}\ln\left|\frac{df^n(x_n)}{dx}\right|$

即是所谓的 Lyapunov 特征指数, 它表征了相邻两点之间的平均指数幅散率. 混沌区是一个特殊的区域, 当 μ_i 在混沌区取值时, 迭代轨迹将以指数级发散. 将这些特点应用到数字水印算法中, 就形成了良好的数字水印改进算法.

本文采用混合光学双稳模型[4]作为混沌源, 它是能生成奇妙吸引子的函数. 该模型可用一个一维非线性迭代方程来描述:

$$X_{n+1}=A_1\sin^2(X_n-X_B)$$

同方程 $X_{n+1}=f(X_n; \mu_i)$ 对比, 可以得到

$$f(X_n; A, X_B)=A_1\sin^2(X_n-X_B) \qquad (1)$$

这里 $A_1=\mu_1$, $X_B=\mu_2$, 这样, 随着参数 A_1 和 X_B 的变化, 系统将从固定点失稳, 经倍周期分叉进入混沌, 在混沌区, 除去其窗口, 系统输出序列 $\{X_n\}$ 是一个很好的随机序列.

生成 $\{S_n\}$ 算法①:

对于混沌序列 $\{X_n\}$

If $X_i>=2/3*A_1$ then $S_i=1$

else $S_i=0$ ($i=1, 2\cdots, n$)

因而从混沌随机序列 $\{X_n\}$ 可以生成 0, 1 比特随机序列 $\{S_n\}$.

将图像原创作者本身掌握的一个保密参数当作 x_0. 利用混沌序列 $\{X_n\}$ 对初值 x_0 极为敏感的特性, 以此序列 $\{X_n\}$ 作水印信息, 因而会导致生成的数字水印不同, 这样一来保证了水印信号的唯一性, 所以攻击者伪造水印是不可能的, 检测抵赖也是不可能的. 改进的 $\overline{U}$ 和 $\overline{V}$ 生成过程描述如下:

Step1 以 x_0 作初值, 使用方程(1)生成 $\{X_n\}$;

Step2 使用生成 $\{S_n\}$ 算法①由 $\{X_n\}$ 生成 $\{S_n\}$;

Step3 将 $\{S_n\}$ 赋给 $\overline{U}$: $\overline{U}\leftarrow\{S_n\}$;

Step4 $x'_0=g(x_0)$; g 为单向函数;

Step5 以 x'_0 作初值, 使用方程(1)生成 $\{X'_n\}$;

Step6 使用生成 $\{S_n\}$ 算法①由 $\{X'_n\}$ 生成 $\{S'_n\}$;

Step7 将 $\{S'_n\}$ 赋给 $\overline{V}$: $\overline{V}\leftarrow\{S'_n\}$.

Step8 以 X_0^+ 作初值, 使用方程(1)生成序列 $\{X_n^+\}$;

Step9 使用生成 $\{S_n\}$ 的算法①由序列 $\{X_n^+\}$ 生成序列 $\{s_n^+\}$;

Step10 将序列 $\{s_n^+\}$ 赋给 Σ: $\Sigma\leftarrow\{s_n^+\}$.

从这个改进的算法可以得到以下结论:

(1)密钥唯一性: 不同的密钥 x_0 产生不等价的水印, 即对任何图像 M, $V^1(M)=\tilde{U}_1\Sigma\tilde{V}_1^T$, $V^2(M)=\tilde{U}_2\Sigma\tilde{V}_2^T$, , 满足 $x_0^1\neq x_0^2\Rightarrow V^1(M)\neq V^2(M)$.

(2)不可逆性: 混沌序列 $\{X_n\}$ 是不可逆的,

$x_0\rightarrow\{X_n\}\rightarrow\{S_n\}\rightarrow\{U_n\}\rightarrow V(A)$ 是不可逆的. 即 x_0 不能根据 $V(A)$ 逆推出来. 不可逆意味着对于任何水印信号 V, 很难找到其它有效水印与该水印信号等价.

(3)不可见性: IWSVD 算法是不可见水印处理系统, 嵌入水印后没产生可见的数据修改, 即加水印后的数字产品相似于原始产品, 即 $M\sim M_w$

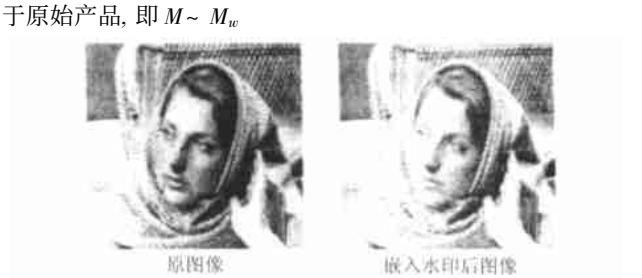

图 1　灰度图像嵌入水印前后效果对比

(4)鲁棒性: 设 M 是原始的产品, 而 M_w 是加水印的产品并且 $D(M_w, V)=1$, 又设 O 是一个多媒体操作算子, 则对于任何 $Y\sim M_w$, $Y=O(M_w)$, 满足 $D(Y, V)=1$, 而且对于任何 $Z=O(M)$, 满足 $D(Z, V)=0$.

2.3　参数对水印的影响

图 2 真彩色图像嵌入水印前后对比

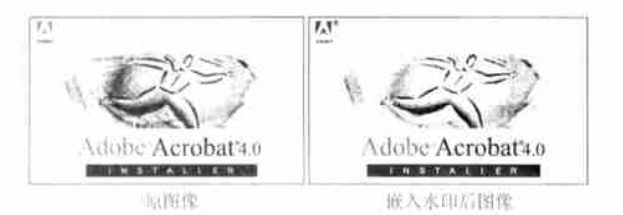

图 3 索引图像嵌入水印前后对比

图像的小波系数水印改变量用 $\| (A) \|$ 来衡量, 它受尺度参数 σ 控制. $V(A)$的随机性由参数 d/n 控制. 因此在加水印的过程中有必要对参数 σ 及 d/n 进行合理的选择和测试. 选择不同的参数, 水印效果是不同的.

3 抗干扰测试

3.1 JPEG 压缩过程和结果

在图像信号的传输过程中, 经常会遇到对图像数据的压缩. 对 256 × 256Lenna 图像用改进的算法水印, 然后对水印图像做不同程度的 JPEG 压缩. 不同压缩质量下的水印检测值曲线如图 4 所示. 水印检测方法描述如下:

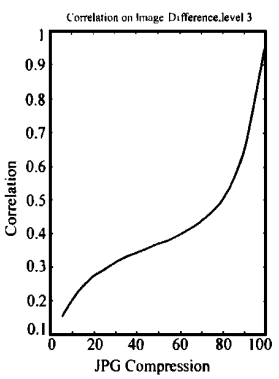

图 4 对应 JPEG 压缩的健壮性性能测试($\sigma = 0.1$, $d/n = 0.9$)

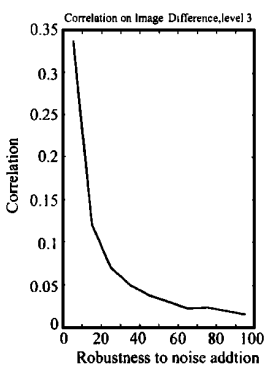

图 5 对应噪音的健壮性性能测试

设 M 代表原图像, 设 N 代表将要测试水印 $V(M)$ 是否存在的图像, 定义 $n \times n$ 矩阵 $B = DCT(B)$ 是 $n \times n$ 矩阵 B 的二维离散余弦变换. 定义 $V(A(M)) = T(A(M)) - A(M)$.

在水印检测和健壮性测试中使用下面的检测函数:

$$d_T(M,N) = \frac{|< V(A(M)), A(N-M) >|}{\| V(A(M)) \| \, \| A(N-M) \|}$$

$$d(M,N) = \frac{|< W(M) - M, N - M >|}{\| W(M) - M \| \, \| N - M \|}$$

$$d_T(M,N) = \frac{|< V(A(M)), A(N-M) >|}{\| V(A(M)) \| \, \| A(N-M) \|}$$

$$d(M,N) = \frac{|< W(M) - M, N - M >|}{\| W(M) - M \| \, \| N - M \|}$$

其中, $< A, B > = \sum_{i,j=1}^{n} a_{ij} b_{ij}$, $\| A \| = < A, A >^{1/2}$

从图 3(计算不同压缩质量下的 d 值)看出水印健壮性较好. 改进的小波 IWSVD 数字水印算法在压缩质量因子达到 15 时水印仍然存在.

3.2 噪声过程和结果

在图像信号的传输过程中, 经常会遇到噪声干扰. 对 256 × 256 Lenna 图像用改进的算法作水印, 然后对水印图像加入高斯白噪声, 做抗干扰测试的水印检测曲线如图 5(计算不同压缩质量下的 d 值)所示. 实验表明健壮性更好. 改进的小波数字水印算法 IWSVD 在噪声幅度达到 15 时水印仍然存在.

4 结论

基于混沌特性改进的小波数字水印算法的优点首先在于其算法简单, 利用小波变换快速、简单的特点; 采用混沌算法来生成随机序列, 健壮性更好. 第二, 这一算法的抗干扰能力强, 因为水印信号隐藏在图像的第 l 级的详细分量中, 即是把水印信息放在图像能量最大的部分-低频部分. Mathworks 公司的 Matlab 实现了改进的小波数字水印算法 IWSVD, 并做了各种健壮性测试. 未来的工作是对该改进的小波数字水印算法, 用遗传算法来优化参数 σ 和 d/n.

参考文献:

[1] P Horvatic, J Zhao, N Thorwirth. Robust audio watermarking based on secure spread spectrum and auditory perception model [A], Information Security for Global Information Infrastructures [C], IFIP/SEC2000: 181-190.

[2] A Lutoborski, A Baldoza, J Vergis. On wavelet-based method of watermarking digital images [R], Dept. of Mathematics, Syracuse Univ., Multi-Sensor Exploitation Branch, Air Force Research Lab., 1998: 9-10.

[3] M D Swanson, B Zhu, B Chau. Object-based transparent video watermarking [A]. IEEE Signal Processing Society 1997 Workshop on Multimedia Signal Processing [C].

[4] H Zhang, J Dai, P Wang. Bifurcation and chaos in an optically bistable liquid-crystal device [J]. Optical Soc. Am B, 1986, 3(2).

作者简介:

王丽娜 女. 1964 年 10 月生于辽宁省营口市. 副教授, 研究领域包括网络安全, 数字水印, 入侵探测. 发表论文 20 余篇, 编著 2 部. 获辽宁省政府科技进步一等奖.