

An Image Watermarking Algorithm Based on Dual Scrambling in Wavelet Transform Domain

XU Xiao-yong, FAN Ji-qiu, XIONG Si-can

School of Mathematics and Information Science, East China Institute of Technology, Fuzhou Jiangxi 344000, China

E-mail: xxy20050052@yahoo.com.cn, fanjiqiu@sina.com, xsc060@126.com

Abstract: A digital watermarking algorithm by dual scrambling with Arnold transform and chaotic encryption in Wavelet Transform Domain was proposed. Firstly, the digital watermarking was scrambled randomly by Arnold transform, and then encrypted by logistic mapping. The encrypted watermarking was embedded into low frequency band. The process of watermarking extracted is the inversion of the process of watermarking embedded. Finally, the watermarking extracted was obtained after the anti-Arnold transformation. The experiments indicate that the algorithm not only enables the watermarking to have very good invisibility, but also makes the watermarking has very good robustness to the general image attacks, such as scaling, rotation, cropping, noise, filter, JPEG compression and so on.

Keywords: Arnold transform; chaotic encryption; wavelet transform; digital watermarking; robustness

一种基于双重置乱的小波变换域图像水印算法

许小勇, 樊继秋, 熊思灿

东华理工大学数学与信息科学学院, 江西, 抚州, 344000

E-mail: xxy20050052@yahoo.com.cn, fanjiqiu@sina.com, xsc060@126.com

【摘要】提出了一种基于 Arnold 变换和混沌加密双重置乱的小波变换域图像水印算法。本算法先将数字水印进行 Arnold 变换, 然后将置乱后的水印图像采用 logistic 映射对原始水印图像进行置乱, 将处理后水印图像嵌入宿主图像小波域的低频系数中。水印提取是嵌入过程的逆过程, 将提取出的水印图像进行混沌解密、Arnold 反置乱变换得到原始水印图像。实验结果表明: 该算法具有很好的不可见性, 且对一般的图像处理如缩放、旋转、剪切、噪声、滤波、JPEG 压缩等具有较好的鲁棒性。

【关键词】Arnold 变换; 混沌加密; 小波变换; 数字水印; 鲁棒性

1. 引言

随着网络技术的飞速发展及 Internet 的普及, 数字媒体的版权问题越来越引起人们的关注。数字水印技术^{[1] [2] [3]}是信息隐藏技术的一个重要研究方向, 近年来得到了迅速地发展, 为数字作品的版权侵犯、非法复制和篡改及完整性认证等问题提供了一种可行的解决途径。

本文提出了一种基于 Arnold 变换和混沌加密双重置乱的小波变换域图像水印算法。对数字水印进行 Arnold 置乱再用混沌进行加密, 将加密后的水印嵌入到原始载体图像的小波变换域, 水印信息分布在整个原始图像中。大量的仿真实验结果证明该算法嵌入的水印具

有很好的透明性和鲁棒性。

2. 水印图像的置乱处理

使用置乱技术的目的是将水印图像噪声化, 使得图像的能量尽可能的均匀分布, 可有效提高隐藏信息的安全性和鲁棒性。目前使用较多的置乱技术主要有: Arnold 变换、幻方、Hilbert 曲线、Radon 变换、Gray 码变换、混沌置乱等。本文利用了 Arnold 变换和混沌加密相结合的方法来对水印图像进行置乱处理。

2.1 Arnold 变换^{[4] [5]}

数字图像可看作是二维连续曲面上, 按照某一间隔和某种策略进行采样所得到的一个二维离散点的阵列, 即一个图像矩阵。所以, 可令离散图像的像素坐

基金项目: 东华理工大学校长基金 (DHXK1040)

Fund: Donghua University Principal Fund (DHXK1040)

标扩展到另一幅图像上。对于一幅大小为 $M \times N$ 的图像，有下述的 Arnold 变换：

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N, \quad x, y \in \{0, 1, 2, \dots, N-1\} \quad (1)$$

由此做迭代变换记 $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ ，式中右端 $\begin{bmatrix} x \\ y \end{bmatrix}$

为输入，左端为 $\begin{bmatrix} x' \\ y' \end{bmatrix}$ 为输出，考虑其反馈，有

$$P_{i,j}^{n+1} = AP_{i,j}^n \bmod N, P_{i,j}^n = (i, j)^n, n = 0, 1, 2, \dots$$

Arnold 变换实际上是一种点的位置移动，可以迭代地做下去，同时需要指出：Arnold 变换变换具有周期性，当迭代进行到某一步时，将会重新得到原始图像。

2.2 混沌加密

混沌【6】现象是非线性动力系统中出现的类似随机过程"这种过程对初值极其敏感，既非周期又不收敛。Logistic 映射为一种简单并广泛研究和应用的动力系统，其方程定义如下：

$$x_{n+1} = 1 - ux_n, x \in (-1, 1), u \in (0, 2) \quad (2)$$

式中， u 为分叉参数。当 $u \in [1.40114, 2]$ 时，系统进入混沌状态，根据式 (2) 就可以得到一个混沌序列。假设水印图像的大小为 $M \times N$ ，混沌置乱算法步骤：运用 Logistic 映射产生 $M \times N$ 大小的一维混沌序列，按行列的顺序对图像进行降维，生成大小为 $M \times N$ 的一维序列，对混沌序列元素进行大小排列，记下其变换坐标 i ，根据变换坐标 i ，重排一维序列，得到置乱后的一维序列，再对其进行升维操作最终得到置乱后的图像。记录序列元素的变换坐标 i ，就可以根据相同的方法对置乱后的图像进行逆置乱。

2.3 水印双重加密实验结果

以一灰度图像作为水印进行双重加密实验，水印大小为 64×64 ，先对水印进行 18 次 Arnold 变换，再使用混沌进行加密，混沌加密中密钥 $x_0 = 0.65$ ， $u = 1.55$ ，水印加密解密实验效果如图 1 到图 4 所示。



Figure 1. Watermark

图1. 水印



Figure 2. scrambled watermark

图2. 置乱水印



Figure 3. Extracted watermark with wrong key
图3. 用错误密码提取的水印



Figure 4. Extracted watermark with right key
图4. 用正确密码提取的水印

在图 (3) 中 $x_0 = 0.650001$ ， $u = 1.588$ ，虽然 x_0 与密钥相差 0.000001 ，但得到的解密图却完全不一样，这说明混沌加密方法对图像进行加密具有非常强的保密性。

3. 水印的嵌入和提取算法

3.1 水印嵌入位置分析

一个图像作小波分解后，可得到一系列不同分辨率的子图像^[7]，系数呈现金字塔式的结构，且图像能量重新分配，绝大部分能量分布在最低频的小波系数上，和低频稀疏相比，最低频的小波系数具有系数绝对值较大，变化范围大的特点，因此也具有更大的更改空间，可以嵌入更多的水印信息。

在小波域中，高频部分代表了图像的轮廓和纹理等细节信息，在这些地方嵌入水印人眼不易察觉，但经过图像处理或攻击后易丢失，所以高频不宜嵌入水印；低频部分集中了图像的主要能量，说明低频部分有很好的鲁棒性且有较大的视觉容量，在这些地方嵌入水印不易丢失，虽然容易影响图像的质量，但通过控制嵌入因子的大小，仍可保证图像的高保真度。

3.2 水印嵌入算法

基于以上分析，将水印图像嵌入到图像的逼近子图中，具体算法如下：

设 X 代表大小为 $M \times M$ 的原始图像， W 代表大小为 $N \times N$ 水印图像，一般的基于小波多级分解的特性考虑，水印尺寸的选择要小于原始图像尺寸，并且满足 $M = 2^p N$ ，(p 为整数)。水印嵌入算法就步骤如下：

1) 对大小的原始图像进行 3 级小波分解，得到不同分辨率下的多个细节子图 $X_j^k (j, k = 1, 2, 3)$ 和逼近子图 X_3^0 。

2) 对原始水印 W 进行 Arnold 变换进行置乱再进行混沌加密预处理，处理后的水印图像为 W' 。保留置乱次数 k 作为密钥。

3) 将置乱后的水印图像 W' 采用 *db1* 小波进行一级小波分解, 得到一级分辨率下三个细节子图 $W_1^k, (k=1,2,3)$ 和一个逼近子图 W_1^0 。

4) 将置乱后水印的一级逼近子图 W_1^0 嵌入到宿主图像三级小波变换的逼近子图 X_3^0 , 按如下公式嵌入:

$$XW_3^0 = X_3^0 + \alpha W_1^0 \quad (3)$$

α 为嵌入强度因子, 将水印三个细节子图 $W_1^k, (k=1,2,3)$ 作为密钥进行保存, 在提取水印时用到。

5) 对嵌入水印后的小波系数进行 3 级小波重构, 得嵌入水印后的图像 XW 。

3.3 水印提取算法

水印的提取过程是嵌入过程的逆过程, 提取时需要借助于原始图像, 其过程如下:

1) 依次读入原始图像 X 和 XW 。

2) 将原始图像 X 和已嵌入水印图像 XW 分别采用 *db1* 进行三级小波分解, 分别提取出低频逼近子图 X_3^0, XW_3^0 。

3) 按如下公式提取出置乱后水印一级小波分解的逼近子图:

$$W_1^0 = (XW_3^0 - X_3^0) / \alpha \quad (4)$$

4) 将上述得到的 W_1^0 系数与保存的细节子图系数 $W_1^k, (k=1,2,3)$ 一起, 进行一级小波重构得到 W'' 。

5) 根据原混沌密钥和水印图像的尺寸大小求得置乱周期 T , 对 W'' 进行混沌解密后再进行 $T-k$ 次置乱, 便得到最终的提取水印 W 。

4、实验结果及分析

4.1 实验仿真结果

我们采用经典的 Lena 图像 (256×256) 作为测试图像, 以一特殊意义的灰度图像 (64×64) 作为水印, 在 Matlab7.0 环境下进行仿真实验。对原始图像失真度用峰值信噪比(PSNR)^[8] 进行量化评估, 对提取出的水印用归一化相关系数(NC)进行量化评估, 按照上述的方法进行水印的嵌入和提取。计算公式如下:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \quad (5)$$

其中, $MSE = \frac{1}{M \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (f(i, j) - f'(i, j))^2$,

MSE 是均方误差, $f(x, y)$ 和 $f'(x, y)$ 分别为原始图像的像素和嵌入水印后图像的像素值, M, N 分别是图像的宽和高。

$$NC(W, W') = \frac{\sum W(n)W'(n)}{\sqrt{\sum W^2(n)}\sqrt{\sum W'^2(n)}} \quad (6)$$

其中 W 为原水印像素, W' 为提取出来的水印像素。实验结果如图 7、图 8 所示:

图 5 为原始图像, 图 6 为原始水印图像, 图 7 为嵌入水印后的图像, 图 8 为受到任何攻击下提取出的水印图像, 计算得到 PSNR=34.42dB, NC= 0.9976, 说明本文算法使水印有很好的不可见性且水印检测性能稳定。

4.2 鲁棒性检测实验

图像水印的鲁棒性测试, 就是对添加水印后的图像进行各种常见处理后提取出水印, 以验证算法的鲁棒性, 常用的处理手段有尺度变换、旋转、叠加噪声、滤波、锐化、剪切、JPEG 压缩等攻击, 算法攻击测试结果如下:

1) 缩放

图 9 至图 11 为不同缩放攻击后提取出的水印图像, PSNR 和 NC 值见表 1

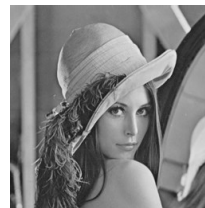


Figure 5. Original image
图 5. 原始图像



Figure 6. Original watermark
图 6. 原始水印图像



Figure 7. Image with watermarking
图 7. 嵌入水印后的图像



Figure 8. Extracted watermark
图 8. 受到任何攻击下提取出的水印图像



Figure 9. 4times
图 9. 4 倍放大

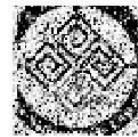


Figure 10. 0.5 times
图 10. 0.5 倍



Figure 11. 0.25times
图 11. 0.25 倍

Table 1. PSNR and NC of zooming attack
表 1 缩放攻击的 PSNR 和 NC

参数	4 倍缩放	1/2 倍缩放	1/4 倍缩放
PSNR(db)	34.42	24.74	22.01
NC	0.9976	0.9248	0.8763

2) 旋转

图 12 至图 16 为不同旋转攻击后提取出的水印图像, PSNR 和 NC 值见表 2

3) 添加噪声

图 17 至图 21 为加入不同噪声后提取出的水印图像, PSNR 和 NC 值见表 3 (数字代表噪声方差)

4) 剪切



Figure 12. clockwise 25°
图 12 顺时针旋转 25°



Figure 13. clockwise 60°
图 13 顺时针旋转 60°



Figure 14. anticlockwise 25°
图 14 逆时针旋转 25°



Figure 15. anticlockwise 60°
图 15 逆时针旋转 60°



Figure 16. anticlockwise 90°
图 16 逆时针旋转 90°

Table 2. PSNR and NC of rotation attack
表 2 旋转攻击的 PSNR 和 NC

参数	顺时针 25°	60°	逆时针 25°	60°	90°
PSNR	11.01	10.21	10.93	10.27	11.19
NC	0.9233	0.9223	0.9264	0.9201	0.9403



Figure 17. Salt and pepper 0.002
图 17 盐椒噪声 0.002



Figure 18. Salt and pepper 0.01
图 18 盐椒噪声 0.01



Figure 19. Gaussian noise 0.001



Figure 20. Gaussian noise 0.005

图 19 高斯噪声 0.001

图 20 高斯噪声 0.005

图 22 至图 25 为剪切攻击后提取出的水印图像, PSNR 和 NC 值见表 4

5) 滤波

图 25 至图 29 为滤波攻击后提取出的水印图像, PSNR 和 NC 值见表 5

6) JPEG 压缩



Figure 21. poisson noise
图 21 泊松噪声

Table 3. PSNR and NC to different attack intensity salt and pepper noise and Gaussian noise and poisson noise
表 3 不同噪声攻击的 PSNR 和 NC

参数	椒盐噪声 0.002	0.01	高斯噪声 0.001	0.005	泊松噪声
PSNR	31.16	25.24	19.95	19.91	26.63
NC	0.9876	0.9544	0.8862	0.9063	0.9669

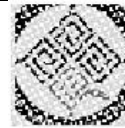


Figure 22. Top left cutting



Figure 23. Center cutting



Figure 24. upper half cutting



Figure 25. painting randomly

Table 4. PSNR and NC of cutting attack
表 4 剪切攻击的 PSNR 和 NC

参数	左上角 1/4	中间 1/4	上半部分	随机涂抹
PSNR	11.54	11.408	8.734	14.45
NC	0.9441	0.9424	0.9089	0.9476



Figure 26. wiener2 [3, 3]
图 26 维纳 2 [3, 3]



Figure 27. wiener2 [5, 5]
图 27 维纳 2 [5, 5]



Figure 28. medfilt2 [3, 3]
图 28 medfilt2 [3, 3]



Figure 29. medfilt2 [5, 5]
图 29 medfilt2 [5, 5]

图 30 至图 34 为 JPEG 压缩攻击后提取出的水印图像 (部分), PSNR 和 NC 值见表 6

图 35、图 36 为 JPEG 压缩质量因子与图像峰值信

Table 5. PSNR and NC of JPEG filter attack
表 5 滤波攻击的 PSNR 和 NC

参数	wiener2 [3,3]	[5,5]	medifilt2 [3,3]	[5,5]
PSNR	33.06	30.41	31.04	27.59
NC	0.9896	0.9608	0.9795	0.9376



Figure 30. 20%
图 30 20%



Figure 31. 40%
图 31 40%



Figure 32. 60%
图 32 60%



Figure 33. 80%
图 33 80%



Figure 34. 90%
图 34 90%

Table 6. PSNR and NC of JPEG compressed attack
表 6 JPEG 压缩攻击后提取出的水印图像

质量因子	90	80	60	40	30	20
PSNR	34.32	32.848	31.59	30.61	30.00	29.09
NC	0.9973	0.9970	0.9949	0.9916	0.9866	0.9771

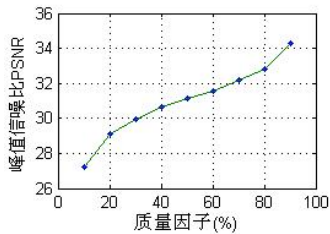


Figure 35. correlations of quality and PSNR
图 35 JPEG 压缩质量因子与图像峰值信噪比 PSNR 关系

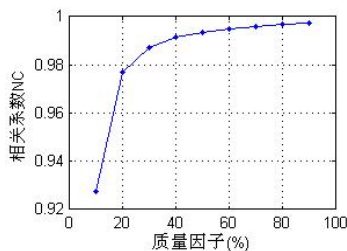


Figure 36. correlations of quality and NC
图 36 相关系数 NC 之间的关系

噪比 PSNR、相关系数 NC 之间的关系。

从以上实验结果可以看出, 该算法具有很好的透明性, 对于常见的攻击如缩放、旋转、剪切、噪声、滤波、压缩等攻击都具有较强的鲁棒性。

5. 结束语

本文提出了一种结合 Arnold 变换、混沌加密的双重置乱技术的小波域图像水印算法。算法在变换域进行水印嵌入, 使得水印信息能很好的分散在原始图像的全部像素中, 并且只对低频信息进行了嵌入, 将水印的高频数据进行了保留, 从而使得算法的鲁棒性得到了加强。仿真实验结果证明: 该算法对于常见的图像处理如缩放、旋转、剪切、噪声、滤波、压缩等攻击都具有较强的鲁棒性。

References (参考文献)

- [1] X.G.Xia, C.Q. Boncelet and G.R.Acre. Wavelet transform based on watermarking for digital images. Optics Express, Vol.3, pp.497-508
- [2] Zhu Zhiyu, Zhang Dai-hua. Watermarking Algorithm Based on DWT and Chaotic Encryption [J], Laser & Infrared, 2006, 36(5), P417420 (Ch).
- [3] 朱志宇, 张代华. 基于离散小波变换和混沌加密的图像水印算法 [J]. 激光与红外, 2006, 36(5): 418-420.
- [4] Wu Ping, Liang Qing. Method for Image Hiding Based on Information Divided-storage and Chaotic Sequences by Wavelet Transform [J], Journal of System Simulation, 2006, 18(9): 2555-2558 (Ch).
- [5] 吴平, 梁青. 一种基于信息分存和混沌序列的小波域信息隐藏方法 [J]. 系统仿真学报, 2006, 18(9): 2555-2558.
- [6] Ding Wei, Yan Weiqi, Qi Dongxu. Digital Image Scrambling Technology Based on Arnold Transformation [J] Journal of Computer Aided Design & Computer Graphics. 2001, 13(4): 20-23 (Ch).
- [7] 丁玮, 闫伟齐, 齐东旭. 基于 Arnold 变换的数字图像置乱技术 [J]. 计算机辅助设计与图形学报, 2001, 13(4): 20-23.
- [8] Huang Waibin, Zhang Dan, Dong Guangchang. An image inverse-scramble algorithm based on Arnold transformation [J]. Applied Mathematics A Journal of Chinese Universities (Ser.A) 2008, 23(1): 99-104 (Ch).
- [9] 黄外斌, 张察, 董光昌. 基于 Arnold 变换的图像逆置乱算法 [J]. 高校应用数学学报, 2008, 23(1): 99-104 (Ch).
- [10] Zhang Xuefeng, Luo Zujun, Gao Chuan. A Digital Image Encryption Algorithm Based on Chaotic Sequences [J]. Computer Engineering and Applications, 2006, 19(2): 61-63 (Ch).
- [11] 张雪峰, 罗祖军, 高川. 基于混沌序列的数字图像加密算法 [J]. 计算机工程与应用, 2006, 19(2): 61-63.
- [12] Xu Chen, Zhao Ruizhen, Gan Xiaobing. Wavelet analysis & application algorithm [M]. Bei Jing: science press, 2004, 137-142
- [13] 徐晨, 赵瑞珍, 甘小冰. 小波分析·应用算法 [M]. 北京: 科学出版社, 2004, 137-142.
- [14] Zou Juan, Jiang Haiyang, Jia shijie, Zeng Jie. Study of Adaptive Digital Watermarking Algorithm Based on Wavelet Transformation [J]. 2009, 30(5), 70-73 (Ch).
- [15] 邹娟, 姜海洋, 贾世杰等. 基于小波变换自适应数字图像水印算法 [J]. 大连交通大学学报, 2009, 30(5), 70-73.