

一种 DWT 与 DCT 相结合的图像水印算法

杜肖山, 廖述剑

(太原理工大学 信息工程学院, 山西 太原 030024)

摘要:文中提出了一种 DWT 与 DCT 相结合的灰度图像盲水印算法。该算法首先对二值有意义水印进行 Arnold 置乱以及 logistic 混沌加密预处理,其次对灰度载体图像进行二级小波分解,选取逼近子图 LL2 和细节子图 LH2、HL2、HH2 嵌入水印。嵌入时对 4 个子带分别进行分块 DCT 变换,然后运用改进型相交换中频系数的办法将预处理后的水印分块嵌入 4 个子带,不同的子带采取不同的嵌入强度,以增强鲁棒性和实现盲提取。实验结果表明,该算法对图像加噪、滤波、剪切、锐化、JPEG 压缩、直方图均衡化等攻击有较强的鲁棒性。

关键词:图像水印;离散余弦变换;离散小波变换;Arnold 置乱;混沌加密;盲提取;鲁棒性

中图分类号:TP309.7;TP391

文献标识码:A

文章编号:1673-629X(2011)01-0147-04

A Novel Image Watermarking Algorithm Based on DWT and DCT

DU Xiao-shan, LIAO Shu-jian

(Institute of Information Engineering, Taiyuan University of Technology, Taiyuan 030024, China)

Abstract: Proposes a blind robust image watermarking algorithm based on DWT and DCT. Firstly, the binary meaningful watermark image is preprocessed by Arnold scrambling and logistic chaotic encryption. Secondly, after decomposing the gray cover image into the secondary layer, four bands (LL2, HL2, LH2, and HH2) are selected to embed watermark. Apply block DCT to each band and employ an improved approach to embed watermark by switching a pair of middle frequency coefficients. The embedding intensity varies with different sub-bands in order to enhance the robustness and realize blind detection. Finally, experimental results show that the algorithm has strong robustness to image adding noise, filtering, cutting, sharpening, JPEG compression, histogram equalization, and other attacks.

Key words: image watermark; discrete cosine transform; discrete wavelet transform; Arnold scrambling; chaotic encryption; blind detection; robustness

0 引言

随着计算机网络以及多媒体技术的迅猛发展,数字图像、音频、视频等数字媒体已得到广泛的应用,随之而来的数字媒体的信息安全和版权保护问题日益突出^[1]。为防止数字产品被侵权、盗版和随意篡改,结合了传统密码学领域认证和鉴别的特点又与被保护数据紧密结合的数字水印技术受到越来越多人的重视,成为一个非常热门的研究领域^[2]。

对于图像水印,空间域算法直接修改图像的像素,特点是算法简单、计算复杂度低,但鲁棒性较差,典型的有:最低有效位法(LSB)算法、patchwork 算法等^[3]。变换域方法通常改变部分系数来隐藏水印:DCT 域的方法主要集中于交换、修改部分中频系数、

基于量化等^[4],也有方法将水印嵌入到直流成分以进一步增强鲁棒性;DWT 域除可借鉴 DCT 域的一些方法,因其良好的时频特性也可采用不同的嵌入强度将水印嵌入不同子带^[5]。文献[6]结合 DWT 与 SVD(奇异值分解)嵌入水印,获得很好的鲁棒性,但 SVD 算法并不能完全实现盲提取。

文中将经过置乱和加密的水印信息采用不同的强度分块嵌入灰度载体图像二级小波分解的逼近子图 LL2 和细节子图 LH2、HL2、HH2。嵌入过程中对各子带结合了分块 DCT 交换、修改一对中频系数的思想,以实现盲提取和获得水印不可见性与鲁棒性的折中。实验表明,该算法对各种常规攻击有较强的鲁棒性。

1 水印预处理

文中采用二值有意义图像作为待嵌入水印。嵌入前,首先对其进行 Arnold 置乱,在一定程度上消除相邻像素间的相关性,然后采用 logistic 混沌序列加密,

收稿日期:2010-04-27;修回日期:2010-07-01

作者简介:杜肖山(1986-),男,山西运城人,硕士研究生,研究方向为网络安全、数字图像处理;廖述剑,副教授,研究方向为网络安全、计算机辅助测试。

进一步增强安全性。

1.1 水印图像置乱

Arnold 变换简单且有周期性,文中采用其对水印图像置乱,二维 Arnold 变换公式如下^[7]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \quad (1)$$

式中 N 为图像矩阵阶数, $(x, y) \in \{0, 1, 2, \dots, N-1\}$ 表示图像一个像素点原始位置, (x', y') 为经过置乱之后像素点的新位置, $\text{mod} N$ 保证 x' 和 y' 仍属于集合 $\{0, 1, 2, \dots, N-1\}$ 。

1.2 水印图像混沌加密

混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程,这种过程既非周期又不收敛,并且对初始值有极其敏感的依赖性。一类非常简单却被广泛研究的动力系统是 logistic 映射,其定义如下:

$$x_{k+1} = \mu x_k (1 - x_k) \quad k = 0, 1, 2, 3 \dots \quad (2)$$

其中, $0 \leq \mu \leq 4$ 称为分枝参数, $x_k \in (0, 1)$, 当 $3.5699456 \dots < \mu \leq 4$ 时, logistic 映射工作于混沌态,分枝参数 μ 和初值 x_0 可作为水印系统的密钥。

2 水印的嵌入与提取

2.1 水印嵌入算法

以大小为 $M \times M$ 的灰度图像 H 和 $N \times N$ 的二值水印图像 W 为例,嵌入过程如下:

(1) 运用 Arnold 变换对二值有意义水印 W 进行 8 次置乱,置乱后的水印图像记为 W' 。

(2) 选取初值 $x_0 = 0.12315$, 设置分枝参数 $\mu = 4$, 运用公式(2)产生长度为 $N \times N$ 的 logistic 混沌序列记为 m , 对 m 进行运算 $\text{mod}(1000 \times m, 256)$ 得到序列 m' , 再将 m' 中各值先转换为 uint8 型后进行二值化产生长度为 $N \times N$ 的 0、1 二值序列 m'' 。

(3) 按行读取 W' 得到的 0、1 二值序列分别与 m'' 中的各个值对应相异或,结果仍然重新写回 $N \times N$ 的图像矩阵 W' ,实现混沌加密。

(4) 对载体图像 H 进行二级小波分解,若在细节子图 LH1、HL1、HH1 嵌入水印易受各种滤波、噪声、JPEG 压缩的影响,所以本算法选取逼近子图 LL2、细节子图 HL2、LH2、HH2 嵌入水印以获得较强的鲁棒性。

(5) 将步骤(3)获得的 W' 分成 4 块,如图 1 所示,将水印块 1、2、3、4 分别对应嵌入 LL2、HL2、LH2、HH2 子带。

(6) 对于逼近子带 LL2,先进行 8×8 分块,互不重叠,并对每个子块分别进行 DCT 变换^[8],选取一对中频系数嵌入水印,记为 BLOCK(4,5)、BLOCK(5,4),

使得:

1	2
3	4

图 1 水印分块方法

当水印信息为 0 时, $\text{BLOCK}(4,5) \leq \text{BLOCK}(5,4)$, 如不满足,相交换系数值;

当水印信息为 1 时, $\text{BLOCK}(4,5) > \text{BLOCK}(5,4)$, 如不满足,相交换系数值。

(7) 为增强鲁棒性,相交换系数后进一步修改系数值,方法如下^[9]:

当水印位为 0,即 $\text{BLOCK}(4,5) \leq \text{BLOCK}(5,4)$, 若 $\text{BLOCK}(5,4) - \text{BLOCK}(4,5) < \alpha$ 时,则将 BLOCK(5,4) 值增加 $\alpha/2$, BLOCK(4,5) 值减少 $\alpha/2$;

当水印为 1,即 $\text{BLOCK}(4,5) > \text{BLOCK}(5,4)$, 若 $\text{BLOCK}(4,5) - \text{BLOCK}(5,4) < \alpha$ 时,则将 BLOCK(4,5) 值增加 $\alpha/2$, BLOCK(5,4) 值减少 $\alpha/2$ 。

α 取值由多次反复试验确定,兼顾水印透明性和鲁棒性,本算法中取 $\alpha = 14$ 。

(8) 对嵌入水印后各 8×8 子块进行逆 DCT 变换。

(9) 细节子带 HL2、LH2、HH2 嵌入水印方法与逼近子带 LL2 基本相同,唯一区别就是把嵌入强度值 α 改为 β ($\beta > \alpha$), β 取值也由多次反复试验确定,取 $\beta = 28$ 。

(10) 将获得的变换域含水印图像进行二级小波逆变换,完成水印嵌入过程。

2.2 水印提取算法

水印提取是嵌入的逆过程,具体方法如下:

(1) 对含水印图像进行二级小波分解,选取子带 LL2、HL2、LH2、HH2 提取水印。

(2) 对 4 个子带分别进行 8×8 分块 DCT 变换,比较每块 BLOCK(4,5)、BLOCK(5,4) 大小确定水印信息:若 $\text{BLOCK}(4,5) \leq \text{BLOCK}(5,4)$, 水印位为 0, 否则, 水印位为 1。把每个子带提取出的水印信息按嵌入过程中图 1 方式重新合成 $N \times N$ 的整体 W 。

(3) 以 $x_0 = 0.12315$, $\mu = 4$ 产生与嵌入过程步骤(2)相同的二值序列 m'' 。

(4) 按行读取 W 得到的 0、1 二值序列分别与 m'' 中的各个值对应相异或,结果仍然重新写回 $N \times N$ 的图像矩阵 W ,实现混沌解密。

(5) 将混沌解密水印做 8 次 Arnold 反置乱变换,获得最终原始嵌入的二值有意义水印。

3 实验结果与分析

文中算法全部由 MATLAB7.0.1 编程实现,限于篇幅,仅选取 $512 \times 512 \times 256$ 的 Lena 灰度图像作载体、

$32 \times 32 \times 2$ 有意义二值图像作为待嵌入水印。为衡量算法优劣,采用峰值信噪比(PSNR)来评价原始载体图像和嵌入水印后图像之间的差别,其值越大,不易感知性越好^[10]。用归一化互相关系数(NC)来评价提取出的水印与原始嵌入水印之间的差别,其值越大,鲁棒性越强。公式如下^[11]:

$$\text{PSNR} = 10 \lg \frac{M \times N \times 255^2}{\sum_{i=1}^M \sum_{j=1}^N [W(i,j) - W'(i,j)]^2} \quad (3)$$

式中 $M \times N$ 为图像大小, $W(i,j)$ 、 $W'(i,j)$ 表示嵌入水印前后图像位置 (i,j) 处的灰度值,当 $\text{PSNR} \geq 38\text{dB}$ 时,人眼即分辨不出两幅图像的差别^[12]。

$$\text{NC} = \frac{\sum_{i=1}^M \sum_{j=1}^N W(i,j) \times W'(i,j)}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N W^2(i,j)} \sqrt{\sum_{i=1}^M \sum_{j=1}^N W'^2(i,j)}} \quad (4)$$

式中 M 与 N 仍为图像大小, $W(i,j)$ 、 $W'(i,j)$ 表示原始水印与提取出水印在位置 (i,j) 处的灰度值,NC 值越接近于 1 越好。原始载体图像和待嵌入水印图像如图 2 所示,原始水印经 Arnold 置乱及混沌加密预处理,效果如图 3 所示。可以看出之前的有意义水印已经混乱不堪,类似于高斯噪声,增加了安全性。



太原
理工

(a) 原始载体图像

(b) 待嵌入水印

图 2 原始载体图像及待嵌入水印



(a) 经 Arnold 置乱

(b) 经混沌加密

图 3 Arnold 置乱及混沌加密效果

采用文中算法嵌入水印后效果如图 4(a) 所示,其峰值信噪比(PSNR)达到 38.0566,具有良好的不可见性。在没有任何攻击下提取出水印经恢复后如图 4



太原
理工

(a) 嵌入水印后图像

(b) 提取出经恢复后水印

图 4 嵌入后图像及提取经恢复后水印

(b) 所示,归一化相似度(NC)为 1,可以完全不失真地提取出原始水印。

对嵌入水印后图像进行各种常规攻击测试,然后提取并恢复水印与原始水印比较,计算 NC 值,评价该算法的鲁棒性,测试结果如图 5 所示。

对于各种攻击测试客观评价标准如表 1 所示。

表 1 鲁棒性攻击测试评价标准

编号	攻击类型	PSNR/dB	NC
a	JPEG 压缩(Q=50)	34.2733	0.9914
b	JPEG 压缩(Q=35)	33.5948	0.9665
c	剪切左上角 1/16	18.0650	0.9987
d	剪切左上角 1/4	11.9371	0.9710
e	中间剪切 1/16	18.1509	0.9827
f	添加高斯噪声($\sigma^2 = 0.002$)	26.7338	0.9794
g	添加脉冲噪声(intensity=0.005)	28.0361	0.9894
h	添加乘积性噪声(intensity=0.01)	25.4576	0.9693
i	直方图均衡化	19.0779	0.9974
j	高斯低通滤波($4 \times 4, \sigma^2 = 0.5$)	29.4577	0.9695
k	中值滤波(3×3)	34.3247	0.9888
l	二阶巴特沃斯高通滤波器(锐化)	6.8719	0.9442

由图 5 和表 1 可看出,对于 JPEG 压缩,在质量因子为 50 甚至达到 35 的情况下,依然可以较好地提取出水印;对于各种剪切攻击,由于是在频域嵌入水印信息,嵌入后水印分布于整个图像,所以对剪切有较好的鲁棒性;对于添加高斯、脉冲、乘性噪声,均可较好地提取出水印;而对于高斯低通滤波、中值滤波攻击,由于未在载体图像小波分解第一层细节子带嵌入水印,故表现出较好的鲁棒性;而因在载体图像小波分解第二层细节子带嵌入了一定量水印信息,将含水印图像用二阶巴特沃斯高通滤波器滤波(锐化),也可在一定程度上提取出水印,算法有一定的抗锐化攻击能力;对于直方图均衡化攻击,也表现出较好鲁棒性。

4 结束语

文中提出的 DWT 与 DCT 相结合的灰度图像盲水印算法,通过一系列仿真实验表明对于图像加噪、滤波、剪切、锐化、JPEG 压缩、直方图均衡化等常见攻击有较强的鲁棒性。但是,所提出的算法为获得较好的不可见性与较强的鲁棒性以及实现盲提取,水印嵌入容量受一定的限制,对于 $512 \times 512 \times 256$ 的灰度图像仅嵌入了 $32 \times 32 \times 2$ 的二值图像,嵌入容量需进一步提升。另外,如果应用到实际中,对于旋转、缩放甚至一些更加复杂的攻击仍然有待于进一步增强鲁棒性。



图 5 各种攻击后含水印图像及提取出经恢复的水印

参考文献:

- [1] Cox I J. Secure Spread Spectrum Watermarking for Multimedia [J]. IEEE Transactions on Image Processing, 1997, 6 (12): 1673-1687.
- [2] 孙圣和, 陆哲明, 牛夏牧, 等. 数字水印技术及应用 [M]. 北京: 科学出版社, 2004.
- [3] 廖晓峰, 金渊智, 张艳珂, 等. 一种统计特性的数字水印算法 [J]. 重庆大学学报, 2009, 32(8): 882-886.
- [4] Voloshynovskiy S, Pun T, Fridrich J, Memon N. Security of data hiding technologies [J]. Signal Processing, 2003, 83(10): 2065-2067.
- [5] 王伟静, 赵苑苑. 基于小波域的数字水印算法 [J]. 计算机技术与发展, 2009, 19(4): 122-124.
- [6] Bhatnagar G, Raman B. A new robust reference watermarking scheme based on DWT-SVD [J]. Computer Standards & Interfaces, 2009, 31(5): 1002-1013.
- [7] 朱贤坤, 张贵仓, 吕宝成, 等. 小波分块的鲁棒性数字水印算法 [J]. 计算机工程与应用, 2008, 44(34): 93-94.
- [8] 胡彦, 陈昭炯. MATLAB 在数字水印中的应用 [J]. 计算机工程, 2003, 29(7): 184-186.
- [9] 张伟, 陈新龙, 詹斌. 基于 DCT 的图像水印算法研究与实现 [J]. 计算机技术与发展, 2009, 19(9): 157-159.
- [10] 张兆礼, 赵春晖, 梅晓丹. 现代图像处理技术及 Matlab 实现 [M]. 北京: 人民邮电出版社, 2001.
- [11] 初勇波, 冯子亮. 一种空间域和频率域结合的数字水印算法 [J]. 计算机工程与应用, 2008, 44(8): 115-116.
- [12] 林代茂. 信息安全——系统的理论与技术 [M]. 北京: 科学出版社, 2008.