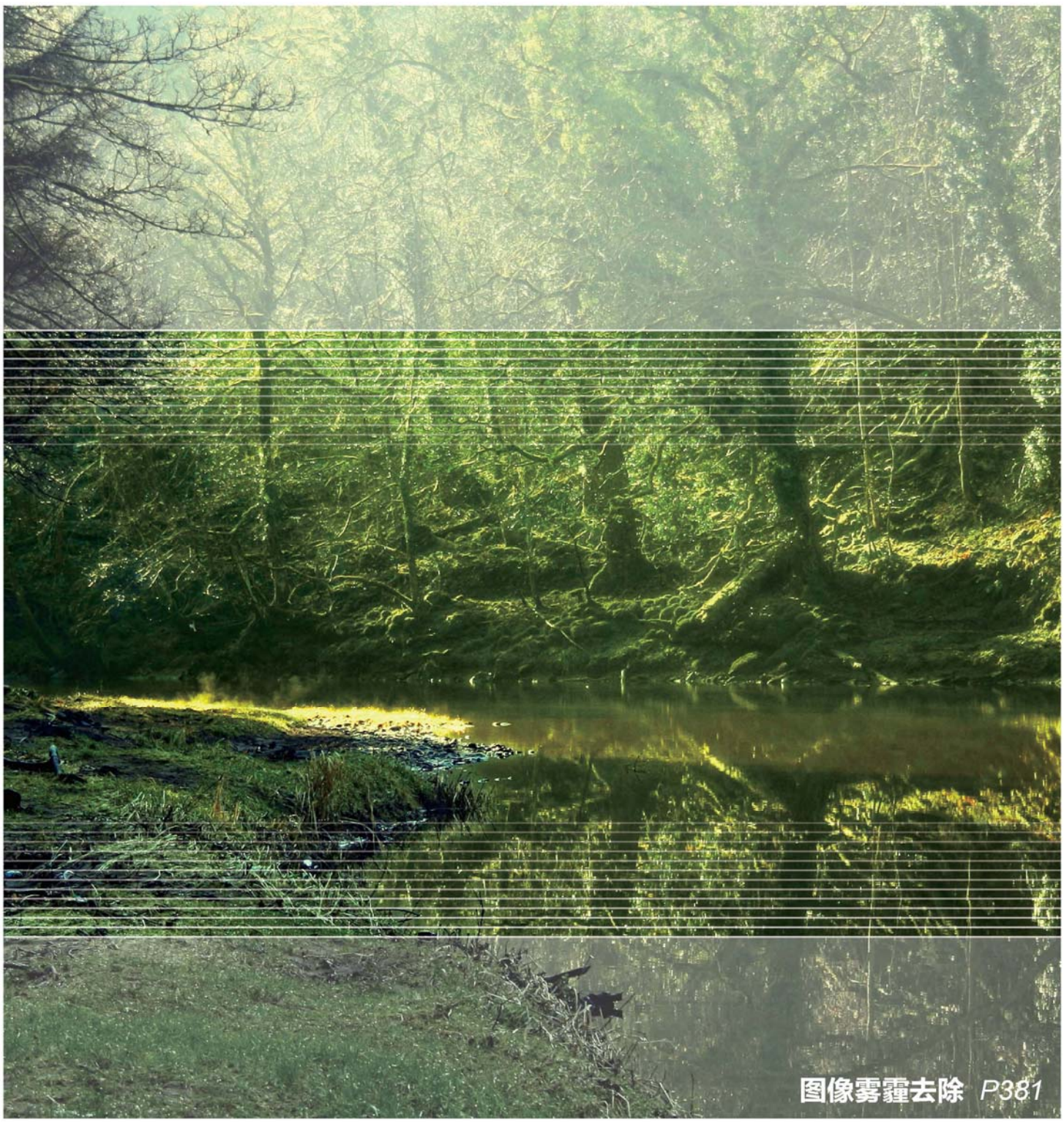
JIG
JOURNAL OF IMAGE AND GRAPHICS

中国图象图形学报

主办：中国科学院遥感与数字地球研究所
中国图象图形学学会
北京应用物理与计算数学研究所

2014
03
VOL.19

ISSN1006-8961
CN11-3758/TB



图像雾霾去除 P381

中国图象图形学报

刊名题字：宋健 | 月刊（1996年创刊）

第19卷第3期（总第215期）
2014年3月16日

中国精品科技期刊
中国国际影响力优秀学术期刊
中国科技核心期刊

主管单位 中国科学院
主办单位 中国科学院遥感与数字地球研究所
中国图象图形学学会
北京应用物理与计算数学研究所

主　　编 李小文
编辑出版 《中国图象图形学报》编辑出版委员会
邮政信箱 北京9718信箱
邮　　编 100101
电子信箱 jig@irsa.ac.cn
电　　话 010-64807995
网　　址 www.cjig.cn

广告经营许可证 京朝工商广字第0361号
总 发 行 北京报刊发行局
订　　购 全国各地邮局
海外发行 中国国际图书贸易集团有限公司
（邮政信箱：北京399信箱　邮编：100048）
印刷装订 北京科信印刷有限公司

Journal of Image and Graphics

Title inscription: Song Jian | Monthly, Started in 1996

Superintended by Chinese Academy of Sciences
Sponsored by Institute of Remote Sensing and Digital Earth, CAS
China Society of Image and Graphics
Institute of Applied Physics and Computational Mathematics

Editor-in-Chief LI Xiaowen
Editor, Publisher Editorial and Publishing Board of Journal of Image and Graphics
P.O.Box 9718, Beijing, P.R.China
Zip code 100101
E-mail jig@irsa.ac.cn
Telephone 010-64807995
Website www.cjig.cn

Distributed by Beijing Bureau for Distribution of Newspapers and Journals
Domestic All Local Post Offices in China
Overseas China International Book Trading Corporation
(P.O.Box 399, Beijing 100048,P.R.China))
Printed by Beijing Kexin Printing Co., Ltd.

CN 11-3758/TB
ISSN 1006-8961
CODEN ZTTXFZ

国外发行代号 M1406
国内邮发代号 82-831
国内定价 50.00元

2014年3月 第19卷 第3期（总第215期）
中国图象图形学报
Zhongguo Tuxiang Tuxing Xuebao

目次

控制关键帧选择的H.264熵编码加密算法(第358页)

显著性检测指导的高光区域修复(第393页)

由灭点进行径向畸变的自动校正(第407页)

Volume 19, Number 3
Published March 16, 2014

CONTENTS
JOURNAL OF IMAGE AND GRAPHICS

H.264 video entropy coding encryption by controlling key frames(P358)

Algorithm for highlight area inpainting guided by saliency detection(P393)

Automatic approach of lens radial distortion correction based on vanishing points(P407)

E-mail: jig@irsa.ac.cn
Website: www.cjig.cn
Tel: 010-64807995

中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS

中图法分类号：TN911.7　　**文献标识码**：A　　**文章编号**：1006-8961(2014)03-0365-08

论文引用格式：曲长波,杨晓陶,袁铎宁. 小波域视觉密码零水印算法[J]. 中国图象图形学报,2014,19(3):365-372.[DOI:10.11834/jig.20140304]

小波域视觉密码零水印算法

曲长波[1], 杨晓陶[1], 袁铎宁[2]

1. 辽宁工程技术大学软件学院, 葫芦岛　125105;
2. 辽宁工程技术大学工商管理学院, 葫芦岛　125105

摘　要：**目的**　传统零水印算法需要构造包含图像特征的水印数据,这样构造的水印往往是无意义的。在已有视觉密码鲁棒水印算法基础上,结合零水印思想,提出小波域视觉密码零水印算法。**方法**　零水印不仅仅是由载体图像生成的,而是其与水印信息共同制造的视觉秘密图份。算法产生2幅图份:主图份(图像特征信息)和所有权图份(零水印)。首先,将载体图像通过合理置乱,去除像素相关性;其次,对置乱后的图像做小波变换,再将小波低频子带分块并对各块做奇异值分解,通过比较块特征值与块特征值均值生成过渡矩阵;然后,将生成的过渡矩阵结合2×2视觉秘密图份算法生成主图份;最后,结合主图份和秘密水印信息产生所有权图份,同时将其保存到认证中心。**结果**　针对零水印信息不够直观,在不对载体进行任何改动的情况下,将有意义二值图像作为零水印嵌入到载体图像中去。即使在很强的鲁棒干扰环境中,本文方法仍然比传统的零水印算法表现出色。**结论**　提出了一种可靠的图像版权认证零水印算法。实验结果表明,算法具有良好的安全性,同时对多种图像处理具有很好的鲁棒性。

关键词：零水印;版权认证;小波变换;奇异值分解;视觉密码;视觉秘密图份

Zero-watermarking visual cryptography algorithm in the wavelet domain

Qu Changbo[1], Yang Xiaotao[1], Yuan Duoning[2]

1. *College of Software, Liaoning Technical University, Huludao*　125105, *China*;
2. *College of Business Administration, Liaoning Technical University, Huludao*　125105, *China*

Abstract: **Objective** Traditional zero-watermarking algorithm requires characteristic image watermark data. Using these methods, it is often necessary to construct meaningless watermarks. Based on the existing visual cryptography robust watermarking algorithm, combined with zero-watermarking, we present a new visual cryptography zero wavelet domain zero watermarking algorithm. We need to embed the meaningful binary image into the original image, without changing the original image. **Method** A zero watermark is not only generated by the carrier image but it is co-produced with the visual watermark secret shares. The proposed algorithm generates two parts: one is the main map component (image feature information) and the other is the ownership chart parts (zero watermark). First of all, using the rational scrambling on the carrier image, it removes the pixel correlation. Second, doing the wavelet transform, the wavelet sub-bands are blocked and the singular value decomposition with each of the blocks is produced. After those steps, we compare each block's characteristic value and the mean value of each block. As a result of that, we can get the transition matrix. Third, the transition matrix is combined with a 2×2 visual secret sharing algorithm to generate the main sharing. Finally, by combining the main sharing with the secret watermarking information, we produce the proprietary sharing and save it to the certification center.

收稿日期:2013-07-16;**修回日期**:2013-10-09

基金项目:国家自然科学基金项目(70971059)

第一作者简介:曲长波(1963—　),男,高级工程师,1990年于大连理工大学获机械装备与制造专业学士学位,主要研究方向为数字图像处理、信息隐藏。E-mail:fx_qcb@126.com

中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS
Vol. 19, No. 3, Mar. 2014

Result Aiming at zero-watermarking information is not very intuitive, in the conditions of not making any changes to the carrier image, we could embed the meaningful binary image into the carrier image. Even in highly robust disturbance environment, this method also has a better performance than the traditional zero-watermarking algorithm. **Conclusion** The presented zero-watermarking algorithm of image copyright authentication is a very reliable way to achieve our goals. As shown by our experiment, this algorithm has a good security. In addition to this aspect, it is also more robust when confronted with many different types of image processing.

Key words: zero-watermarking; copyright authentication; discrete wavelet transform (DWT); sigular value decomposition (SVD); visual cryptography; visual secret sharing

0 引 言

数字水印技术作为一种有效解决图像版权、内容认证和完整性保护等问题的新型技术,近些年来有很快速的发展[1]。但是传统的水印技术需要向原始载体图像中嵌入水印信息,这影响了图像的原有信息,在很多对图像内容要求很高的应用中是不允许的[2]。为克服以上缺点,温泉等人[3]提出了零水印方案。零水印的核心思想是在不修改原始宿主图像数据的前提下,利用图像内部特征构造零水印。零水印有效地解决了图像透明性和鲁棒性之间的矛盾,在最近的几年受到很多学者的关注,如:金军提出基于元胞自动机的图像水印算法[4];赵春晖等人[5]提出基于压缩感知的零水印算法;韩绍程等人[6]提出基于非下采样剪切波变换和 QR 分解的鲁棒零水印算法。

但是这些零水印算法都需要考虑构造既包含有效特征又比原图像数据量尽量少的水印数据[7]。这样生成的水印往往是无意义的二值序列,虽然有相对丰富的水印识别算法以防止水印之间的混淆,但是对于发生版权纠纷的双方来说并不够直观。在引入视觉密码技术之后,可以将有意义的二值图像作为零水印图像。视觉密码技术是新兴的数字水印技术,最近几年国内外已有一定的相关文献。文献[8]提出了一种基于视觉密码的多用户多图像版权保护方案;Abusitta 等人[9]提出了一个基于空域的视觉密码共同所有权保护方案,该方案的鲁棒性受限于空域算法本身;Bharathi[10] 等人提出了基于 Halftone 和视觉密码的图像水印算法,鲁棒性测试效果依然不够理想;Rawat 等人[11]引入分数傅里叶变换,提出基于分数傅里叶变换的视觉密码图像版权保护算法,但只是增加了 2 个安全密钥,没有充分利用分数傅里叶变换的时频分析特性,虽然在一般图像处理方面,鲁棒性有较大的提升,但是在剪切、缩放等几何攻击方面效果依然欠佳;文献[12]与文献[13]将视觉密码和离散余弦变换相结合,提出了离散余弦变换(DCT)域的视觉密码鲁棒水印算法。文献[12]算法的能量集中性并不优秀,所以效果并不理想。文献[13]具有非常高的安全性,但是算法计算复杂,得到的认证数据量大,这与零水印“比原图像数据量尽量少”这一原则相违背。

针对上述视觉密码算法所表现出的鲁棒性不佳,抗攻击能力差等问题,将视觉密码和零水印思想相结合提出了小波域视觉密码零水印算法。将原始图片通过小波变换和奇异值分解产生 2 个图份:主图份(图像特征信息)和所有权图份(零水印)。实验结果表明,算法不仅具有较高的安全性,而且可以对抗多种鲁棒攻击,是一种可靠的零水印方案。

1 视觉密码

视觉密码(visual Cryptography)把包含秘密信息的黑白图像称为秘密图像(secret image),利用视觉密码加密后,得到多个图份(share),密码破译者从任意一幅图份中都无法得到秘密图像的任何信息。而解密过程很简单,只需将图份叠在一起,得到的组合即为解密后图像,不需任何复杂的数学运算。文献[14]中 Noar 和 Shamirl 同时提出了(k, n) VSS (visual secret sharing)——视觉秘密图份算法。其中,n 表示将秘密图像分成 n 个图份,k 表示至少需要 k 幅图份才能还原原始秘密图像。

2×2 VSS 算法:假设原始图像的尺寸为 $M \times N$,则它可以分为两个尺寸为 $2M \times 2N$ 的图份。新图份使用 2×2 的像素块代表原图像的每一个像素。这样需要加密的秘密图像就转化成两个各自独立的图份。通过堆叠两个对应块的像素,可以得到秘密图像信息。同时每个像素对应的 2×2 块都是由数量相等的 2 个白色和 2 个黑色像素组成。

图 1 为视觉密码的应用实例。将图 1(a)“视觉密码”二值图像经过 2×2 VSS 变换得到两幅图份：图 1(b)和图 1(c)，将两幅图份叠加得到解密图像(图 1(d))。原始图像尺寸为 128×128 像素，得到的两幅图份和解密结果尺寸均是 256×256 像素。

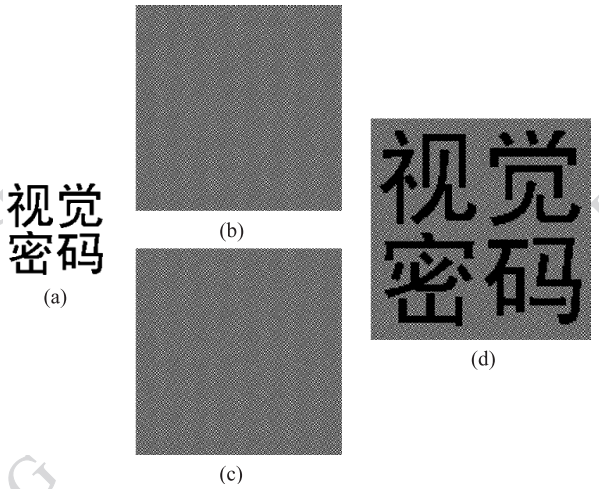


图 1　视觉密码实例

Fig. 1　Visual password instance

2　视觉密码零水印算法

2.1　零水印生成算法

本文算法中零水印是通过视觉密码所生成的所有权图份。零水印的生成通过两步来实现：1)主图份生成算法，将原始图像置乱并对其进行离散小波变换(DWT)、奇异值分解(SVD)处理生成主图份；2)所有权图份生成算法，通过主图份和水印信息生成所属权图份。

2.1.1　主图份生成算法

主图份的构建过程也就是提取载体图像的特征信息的过程。首先对原始载体图像 $\boldsymbol{I}(m\times n)$ 进行充分置乱，除去图像像素相关性；其次对置乱后的载体图像进行 2 次 DWT 变换；然后对小波低频系数按 4×4 分块并对每一系数块做 SVD 处理，同时收集最大特征值生成二进制过渡矩阵；最后通过过渡矩阵得到主图份。具体方法如下：

1)通过密钥 K，对原始载体图像 $\boldsymbol{I}$ 充分置乱加密，生成置乱后载体—实际载体 $\boldsymbol{S}$。

2)对实际载体 $\boldsymbol{S}$ 进行 l 级小波变换，得到低频子带 $\boldsymbol{cA}_{11}$。

3)对 $\boldsymbol{cA}_{11}$ 按 4×4 系数分块，生成 $B_{ij}(i\in 1,2,\cdots,m/4, j\in 1,2,\cdots,n/4)$；并对 B_{ij} 作 SVD 处理，同时取出每一块的最大特征值组成矩阵 $\boldsymbol{X}$。

4)按照如下规则，由 $\boldsymbol{X}$ 生成二进制过渡矩阵 $\boldsymbol{b}$，即

$$b_{ij}=\begin{cases}0 & \boldsymbol{X}_{ij}<\mathrm{mean}(\boldsymbol{X})\\ 1 & \text{其他}\end{cases} \tag{1}$$

式中，mean($\boldsymbol{X}$)表示取 $\boldsymbol{X}$ 的均值。

5)由过渡矩阵 $\boldsymbol{b}$ 生成主图份，方法如下：

if　$b_{ij}==1$

$$\boldsymbol{M}_{ij}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix};$$

else　$$\boldsymbol{M}_{ij}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix};$$

end

由此可以得到主图份 $\boldsymbol{M}$。

2.1.2　所有权图份(零水印)生成

在得到主图份 $\boldsymbol{M}$ 之后，结合有意义水印 $\boldsymbol{w}$ 可以生成所有权图份(零水印)$\boldsymbol{O}$。将生成的所有权图份 $\boldsymbol{O}$ 送到相关认证中心保存，以作为日后版权保护的凭证。所有权图份 $\boldsymbol{O}$ 生成方法为

$$\boldsymbol{O}_{ij}=\begin{cases}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} & w_{ij}=1 \text{ 且 } \boldsymbol{M}_{ij}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\\ \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} & w_{ij}=1 \text{ 且 } \boldsymbol{M}_{ij}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\\ \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} & w_{ij}=0 \text{ 且 } \boldsymbol{M}_{ij}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\\ \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} & \text{其他}\end{cases} \tag{2}$$

2.2　所有权识别

所有权识别过程相当于零水印的提取过程。识别过程需要经过攻击后的载体图像 $\boldsymbol{I}'$ 和从认证中心(CA)得到的所有权图份 $\boldsymbol{O}$，还有置乱密钥 K。所有权识别的步骤 1)—5)和主图份生成算法很相似。具体识别过程如下：

1)从认证中心得到密钥 K，对原始载体图像 $\boldsymbol{I}'$ 充分置乱加密，生成置乱后载体—实际载体 $\boldsymbol{S}'$。

2)对实际载体 $\boldsymbol{S}'$ 进行 l 级小波变换，得到低频子带 $\boldsymbol{cA}'_{11}$。

3)对 $\boldsymbol{cA}'_{11}$ 按 4×4 系数分块，生成 $B'_{ij}(i\in 1,2,\cdots,m/4, j\in 1,2,\cdots,n/4)$。并对 B'_{ij} 做 SVD 处理，同时取出每一块的最大特征值组成矩阵 $\boldsymbol{X}'$。

4)由 $\boldsymbol{X}'$ 生成二进制过渡矩阵 $\boldsymbol{b}'$，即

中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS
Vol. 19, No. 3, Mar. 2014

$$b'_{ij}=\begin{cases}0 & \boldsymbol{X}'_{ij}<\text{mean}(\boldsymbol{X}')\\ 1 & \text{其他}\end{cases} \tag{3}$$

式中，mean($\boldsymbol{X}'$)表示取$\boldsymbol{X}'$的均值。

5)由过渡矩阵$\boldsymbol{b}'$生成主图份$\boldsymbol{M}'$，方法如下：

if $b'_{ij}==1$

$\boldsymbol{M}'_{ij}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$;

else $\boldsymbol{M}'_{ij}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$;

end

6)将生成的主图份$\boldsymbol{M}'$和由认证中心得到的所有权图份$\boldsymbol{O}$相覆盖(点乘)，得到尺寸为$2m\times 2n$的认证矩阵$\boldsymbol{R}=\boldsymbol{M}\cdot\boldsymbol{M}'$。

7)通过处理得到生成水印，即

$$w'_{ij}=\begin{cases}1 & \sum_{i=1}^{2}\sum_{j=1}^{2}R_{ij}<2\\ 0 & \sum_{i=1}^{2}\sum_{j=1}^{2}R_{ij}\geqslant 2\end{cases} \tag{4}$$

得到生成的水印$\boldsymbol{w}'$。由于是有意义水印，即使通过肉眼的直接识别也可以确定原始载体版权归属。

3 实验结果

3.1 实验参数说明

为了检验所提出算法的有效性，进行了多组实验。有意义水印选择32×32“版权保护”二值水印，水印图像如图2(a)所示。实验载体图像选择512×512×8“Lena. bmp”、“baboon. bmp”、“bridge. bmp”灰度图像，原始载体图像如图2(b)—(d)所示。本文置乱方法选择吴慧琳等人[15]提出的置乱方法，初始化参数详见文献[15]。原始载体选择haar小波为基的2级DWT变换。

(a) (b) Lena (c) baboon (d) bridge

图2 水印图像和原始图像

Fig. 2 Watermark and original images

3.2 鲁棒性攻击实验

数字水印的鲁棒性是衡量数字水印好坏的重要的指标之一。本文采用归一化相关系数(NC)来衡量，即

$$NC(x_1,x_2)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}x_1(i,j)x_2(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}x_1(i,j)^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}x_2(i,j)^2}} \tag{5}$$

式中，x_1、x_2分别表示初始水印和提取的水印。

为了检测水印的鲁棒性，对Lena、baboon、bridge 3幅图分别进行了多组攻击实验。相对来说Lena有较小的细节，纹理信息少；baboon的细节信息和纹理信息相对比较复杂；bridge图细节信息比较均匀，纹理信息比较多。同时选择相对复杂，辨认难度大的“版权保护”4个汉字作为水印。实验攻击内容包括：加性噪声攻击、滤波攻击、JPEG压缩、剪切攻击、缩放攻击、旋转攻击等。其中由于噪声攻击具有随机性，得到的结果往往处于动态变换，对于噪声攻击分别进行10次实验取平均值。实验结果如表1—表3所示，其中高斯噪声(均值为0，方差0.01～0.1)，椒盐噪声(噪声密度为0.01～0.1)和旋转攻击(顺时针旋转0.5°～5°)对比效果如图3—图5所示。

4 实验结果分析

4.1 透明性和安全性分析

由于载体本身没有变化，所以攻击者无论使用何种方法都检测不出图像是否含有水印。2×2VSS将原始载体图像分成2个图份，即使算法公开，在没有密钥的前提下很难生成图像的主图份，即使密钥泄露攻击者侥幸得到主图份，由于没有水印信息，攻击者是不可能得到所有权图份的。生成所有权图份的水印为有意义水印，攻击者同时也不能通过载体图像得到水印信息，这样就不能通过所有权图份识别水印，更不可能篡改。

表 1　Lena 图像 3 种算法性能对比

Table 1　Three algorithms performance of Lena

攻击类型	参数说明	PSNR 值	本文算法		文献[11]算法		文献[13]算法	
			NC 值	提取的水印	NC 值	提取的水印	NC 值	提取的水印
高斯低通滤波	模板大小为 5×5，σ=0.5	40.853 8	0.999 1		0.998 3		0.999 1	
中值滤波	模板大小为 5×5	31.240 8	0.996 5		0.990 4		0.993 6	
均值滤波	模板大小为 5×5	28.294 6	0.992 2		0.988 7		0.986 7	
JPEG 压缩	质量因子为 20	32.671 1	0.996 5		0.986 9		0.982 1	
剪切攻击	左上剪切 1/16	18.206 8	0.993 9		0.986 1		0.976 8	
	左上剪切 1/4	11.874 6	0.983 9		0.801 1		0.907 6	
缩放攻击	1/2 倍双线性缩放	32.402 7	1		0.993 9		0.997 6	
对比度增强	增强 100%	16.761 8	0.978 1		0.950 2		0.960 3	

表 2　baboon 图像 3 种算法性能对比表

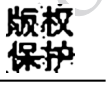
Table 2　Three algorithms performance of baboon

攻击类型	参数说明	PSNR 值	本文算法		文献[11]算法		文献[13]算法	
			NC 值	提取的水印	NC 值	提取的水印	NC 值	提取的水印
高斯低通滤波	模板大小为 5×5，σ=0.5	33.000 9	0.998 3		0.985 2		0.994 2	
中值滤波	模板大小为 5×5	22.635 0	0.982 7		0.961 6		0.960 8	
均值滤波	模板大小为 5×5	22.397 6	0.990 4		0.942 4		0.985 1	
JPEG 压缩	质量因子为 20	26.172 1	0.992 2		0.968 9		0.965 4	
剪切攻击	左上剪切 1/16	17.703 7	0.988 3		0.959 9		0.975 4	
	左上剪切 1/4	11.704 5	0.975 2		0.764 5		0.844 6	
缩放攻击	1/2 倍双线性缩放	24.421 3	0.996 5		0.979 4		0.987 6	
对比度增强	增强 100%	17.476 3	0.987 8		0.954 8		0.974 8	

中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS
Vol. 19, No. 3, Mar. 2014

表 3　bridge 图像 3 种算法性能对比表

Table 3　Three algorithms performance of bridge

攻击类型	参数说明	PSNR 值	本文算法		文献[11]算法		文献[13]算法	
			NC 值	提取的水印	NC 值	提取的水印	NC 值	提取的水印
高斯低通滤波	模板大小为 5×5,σ=0.5	34.300 8	0.999 1		0.995 7		0.998 7	
中值滤波	模板大小为 5×5	24.023 7	0.993 9		0.972 4		0.977 5	
均值滤波	模板大小为 5×5	23.179 6	0.993 0		0.971 4		0.974 2	
JPEG 压缩	质量因子为 20	27.013 1	0.998 3		0.991 3		0.989 7	
剪切攻击	左上剪切 1/16	16.623 2	0.990 4		0.988 3		0.984 3	
	左上剪切 1/4	11.121 2	0.973 1		0.825 6		0.885 7	
缩放攻击	1/2 倍双线性缩放	25.682 8	0.997 4		0.983 6		0.990 5	
对比度增强	增强 100%	16.337 1	0.985 2		0.965 7		0.977 8	

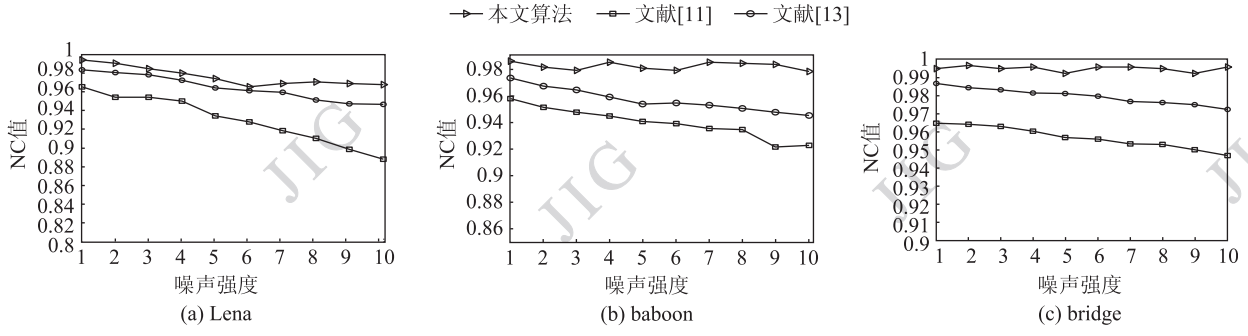


图 3　高斯噪声效果对比图

Fig. 3　Gaussian noise effect comparison chart

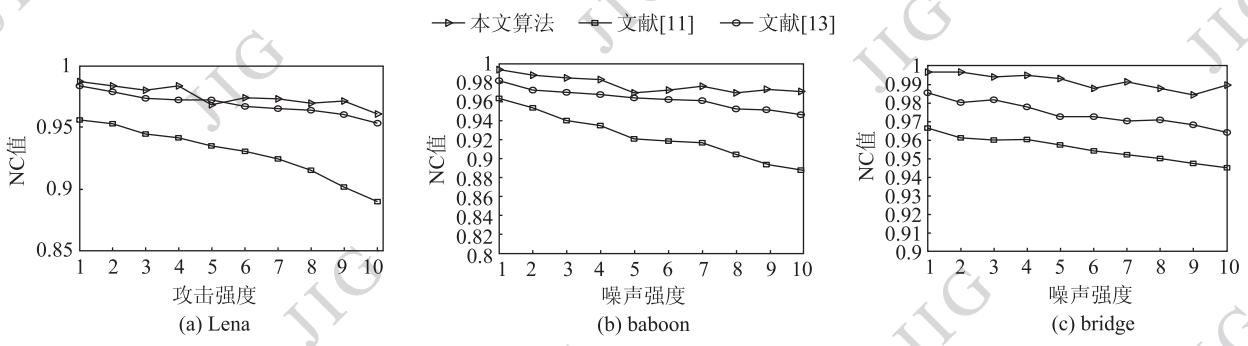


图 4　椒盐噪声效果对比图

Fig. 4　Salt & pepper noise effect comparison chart

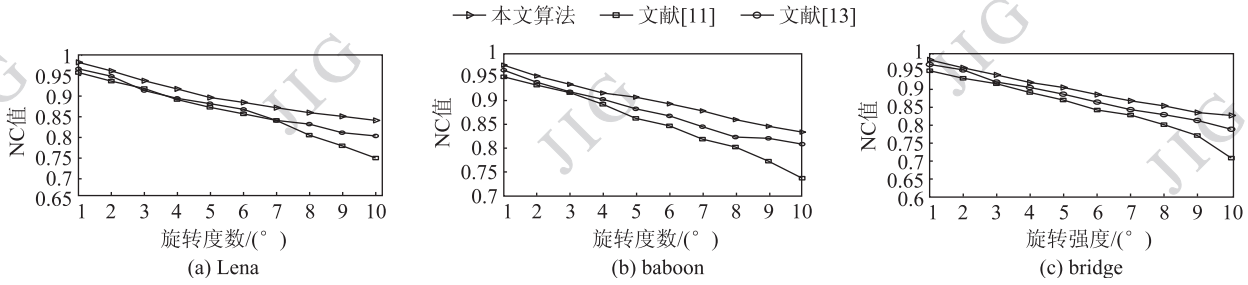


图 5　旋转攻击效果对比图

Fig. 5　Rotate attack effect comparison chart

4.2　鲁棒性分析

通过表 1—表 3 可以看出包括加性噪声攻击，高斯低通滤波攻击，均值、中值滤波攻击，JPEG 压缩等一般图像处理，本文算法有非常良好的鲁棒性。主要是由于算法将原始图像通过 DWT 变换，得到了能量集中的低频子带，而 SVD 的使用则对外界的“扰动”有良好的抵御能力。同时由于生成主图份时，过渡矩阵是由各个系数块能量与所有块能量均值之间的大小关系决定的。这样即使是比较剧烈的和有破坏性的图像处理对这种能量关系的影响不会非常大，所以可以提取到相对完整的水印信息。

面对如剪切攻击和旋转攻击，本文算法依旧表现出很强的优势性。对于剪切、旋转攻击，虽然攻击本身对能量大小关系变化较大，但是可以通过提升置乱效果将这种影响均匀的分担到所有图像块中，仍然可以得到很好的实验结果。从 NC 值这一定量的指标来看本文算法对比文献[11]、文献[13]算法，还是有一定的提升。

4.3　与文献[11]、文献[13]算法比较

本文算法与文献[11]、文献[13]相比，无论是直接观察还是定量的 NC 值分析都有很大的优势。这主要是由于文献[13]算法采用 DCT 变换分离图像能量，虽然 DC 值能集中大量的原始图像能量，但是由于不是比较能量之间的大小关系，在图像受到外界“影响”较大时，生成的主图份会发生很大变化。文献[11]虽然引入 SVD 变换和分数傅里叶变换，但算法本身仅仅增加了系统的安全密钥个数，没有充分利用分数傅里叶变换的时频分析能力。尤其是文献[11]选择通过伪随机序列选取图像块，而不是充分置乱，这样在对抗剪切攻击的时候，鲁棒性实验的表现不能令人满意。对比之下本文算法使用良好的图像置乱方法；较好地获得载体图像的特征信息，由于视觉密码技术本身具有很强的鲁棒性，所以得到了良好的实验结果。

5　结　论

针对传统零水印算法大多为无意义水印，在已有视觉密码鲁棒水印算法基础上结合零水印思想，提出了小波域视觉密码零水印算法。算法中通过使用改进的视觉秘密图份算法和有意义水印制造视觉图份。这样不但实现了将有意义水印作为零水印嵌入到原始载体图像中去，同时获得了良好的视觉效果，又充分提高了算法的鲁棒性。实验结果表明，该算法对多种图像处理具有良好的安全性和很好的鲁棒性。在今后的工作中，希望能在抵抗更大强度的剪切、旋转等几何攻击方面进行探索。

参考文献(References)

[1] Zeng G R, Qiu Z D. Evaluation model for robustness of digital watermarking [J]. Acta Phys. Sin., 2010, 59(8): 5871-5880. [曾高荣, 裘正定. 数字水印的鲁棒性评测模型[J]. 物理学报, 2010, 59(8): 5871-5880.]

[2] Zhao C H, Liu W. Block compressive sensing based image semi-fragile zero-watermarking algorithm [J]. Acta Automatica Sinica, 2012, 38(4): 609-617. [赵春晖, 刘巍. 基于分块压缩感知的图像半脆弱零水印算法[J]. 自动化学报, 2012, 38(4): 609-617.]

[3] Wen Q, Sun T F, Wang S X. Concept and application of zero-watermark [J]. Acta Electronic Sinica, 2003, 31(2): 214-216. [温泉, 孙锬锋, 王树勋. 零水印的概念与应用[J]. 电子学报, 2003, 31(2): 214-216.]

[4] Jin J. Multiple zero-watermarks algorithm based on cellular automata [J]. Journal of Optoelectronics · Laser, 2009, 20(3): 382-387. [金军. 基于元胞自动机的多重零水印算法[J]. 光电子·激光, 2009, 20(3): 382-387.]

[5] Zhao C H, Liu W. Mutual support dual watermark algorithm based on compressive sensing [J]. Acta Electronica Sinica,

2012,40(4):681-687.[赵春晖,刘巍. 基于压缩感知的交互支持双水印算法[J]. 电子学报,2012,40(4):681-687.]

[6] Han S C, Zhang Z N, Zhang Y J. Robust zero-watermark algorithm based on non-subsampled sheaa-let ransform and QR decomposition [J]. Journal of Optoelectronics · Laser, 2012, 23(10):1957-1964.[韩绍程,张兆宁,张玉金. 基于非下采样剪切波变换和QR分解的鲁棒零水印算法[J]. 光电子·激光,2012,23(10):1957-1964.]

[7] Zhang L B, Ma X Y, Chen Q. Image zero-watermarking algorithm based on region of interest [J]. Journal on Communications, 2009,30(11A):117-120.[张立保,马新悦,陈琪. 基于感兴趣区的图像零水印算法[J]. 通信学报,2009,30(11A):117-120.]

[8] Liu F, Wu C K. Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners[J]. Information Security, IET, 2011, 5(2):121-128. DOI: 10.1049/iet-ifs.2009.0183

[9] Abusitta A H. A visual cryptography based digital image copyright protection [J]. Journal of Information Security, 2012, 3:96-104.

[10] Bharathi M, Charanya R, Vijayan T. Halftone visual cryptography & watermarking [J]. International Journal of Engineering Research & Technology, 2013, 4(2):2747-2752.

[11] Rawat S, Raman B. A blind watermarking algorithm based on fractional Fourier transform and visual cryptography [J]. Signal Processing, 2012, 9(6):1480-1491.

[12] Verma J, Khemchandani V. A visual cryptographic technique to secure image shares [J]. Internationa Journal of Engineering Research and Applications, 2012, 2(1):1121-1125.

[13] Tu S H, Hsu C S. A joint ownership protection scheme for digital images based on visual cryptography [J]. The International Arab Journal of Information Technology, 2012, 9(3):276-283.

[14] Naor M, Shamir A. Visual cryptography[C]//Advances in Cryptology-Eurocrypt'94. Berlin: LNCS 1995, 950:1-12.

[15] Wu H L, Zhou J L, Gong X G, et al. A novel blind watermarking algorithm joint JPEG image encoding and cellular automata [J]. Journal of Electronics & Information Technology, 2012, 34(4): 344-350[DOI: 10.3724/SP.J.1146.2011.00667][吴慧琳,周激流,龚小刚,等. 一种与JPEG图像压缩编码结合的细胞自动机域盲水印算法[J]. 电子与信息学报,2012,34(4):344-350.]