文章编号：2095-2163(2020)01-0080-04 中图分类号：TP309.7 文献标志码：A

基于像素不扩展视觉密码的可逆水印

赵久影[1]，王洪君[2]
（1 吉林师范大学 数学学院，吉林 四平 136000；2 吉林师范大学 计算机学院，吉林 四平 136000）

摘 要：提出了基于像素不扩展视觉密码的可逆水印算法。首先，二值水印图像通过像素不扩展的视觉密码方案被分割成 2 个分享图像。然后，其中一个分享图像利用水印嵌入算法嵌入到载体图像中，另一个分享图像分配给所有者。最后，利用水印提取算法从嵌入水印后的图像中提取分享图像，叠加提取的分享图像和所有者的分享图像得到原始水印图像，并且无损地恢复载体图像。基于视觉密码的安全性，该算法不会泄露水印的任何信息，保证了原始载体图像的完整性并且不需要第三方和复杂的计算。实验结果表明，此方案能抵抗大多数常见攻击。

关键词：视觉密码；像素不扩展；可逆水印

Reversible watermarking based on pixel unextended visual cryptography

ZHAO Jiuying[1], WANG Hongjun [2]
（1 College of Mathematics, Jilin Normal University, Siping Jilin 136000, China;
2 College of Computer, Jilin Normal University, Siping Jilin 136000, China）

【Abstract】 A reversible watermarking algorithm based on pixel - free visual cryptography is proposed. Firstly, the binary watermarking image is segmented into two shared images through a visual cryptography scheme without expanding the pixels. Then, one of the shared images is embedded into the carrier image using the watermarking embedding algorithm, and the other is assigned to the owner. Finally, the watermarking extraction algorithm is used to extract the shared image from the embedded watermarking image. The binary watermarking image is obtained by superimposing the shared image of the owner and the carrier image which is restored losslessly. Based on the security of visual cryptography, the algorithm does not leak any information of the watermarking, nor does it require third party and complex calculation, which guarantees the integrity of the original carrier image. The experimental results show that this scheme can resist most common attacks.

【Key words】 visual cryptography; pixel non-expansion; reversible watermarking

0 引 言

随着计算机的迅速发展，保护数字产品的版权已成为近年来的一个重要问题。目前，研究人员提出了许多保护数字图像知识产权的技术。其中，数字水印技术就是在载体图像中隐藏有意义的数字水印，以保护版权和完整性检查。当需要证实图像的合法所有权时，可以提取隐藏的水印进行所有权验证。

曲长波等人[1-2]给出了基于视觉密码的零水印算法，对载体图像进行置乱和奇异值分解等操作提取特征矩阵，利用视觉密码生成零水印。零水印算法没有将水印嵌入到载体图像中，所以载体图像不会被修改。侯翔等人[3]给出了一种定位篡改实体组的脆弱水印算法，该算法采用优化的 k 均值聚类进行分组，构建特征参数及混沌映射生成脆弱水印。Li 等人[4]提出了一种基于 DCT 算法的数字水印，利用离散余弦变换对图像像素值和频域系数矩阵进行变换，实现了盲水印的嵌入和提取。文献[5-10]也对数字水印算法进行了研究。罗昊等人[11]提出了一种在加密域中来做直方图平移的可逆水印算法，利用直方图平移的方法实现水印的嵌入和提取，在此过程中不会影响原始载体图像。刘连山等人[12]提出了基于分块的预测差值直方图平移的可逆水印算法。文献[13-16]也提出了不同的可逆水印算法。

本文提出基于像素不扩展视觉密码的可逆水印算法，该算法既能提取水印，又能无损地恢复载体图像。利用(2,2)像素不扩展视觉密码方案将水印分割为 2 幅分享图像。将分享图像中的一个嵌入载体图像中，另一个分配给所有者。提取时，从嵌入水印后的图像中提取分享图像，将这 2 幅分享图像合并显示水印，在此过程中还能完整地恢复载体图像。实验结果表明，该算法实现简单，具有良好的抗攻击能力。

作者简介：赵久影(1994-)，女，硕士研究生，主要研究方向：视觉密码、信息安全、密码学；王洪君(1965-)，男，博士，教授，主要研究方向：密码学、信息安全、网络体系结构。

通讯作者：王洪君 Email：jlnuwhj@ sina.com

收稿日期：2019-10-25

1　视觉密码

1994 年，Naor 和 Shamir[17] 提出了一种新的加密方法，称为视觉密码（VSS）。将一幅秘密图像编码为 n 幅分享图像，然后分发给 n 个参与者，每人一幅分享图像。解密时只需将分享图像打印到透明胶片上，n 幅分享图像中的任意 k 幅或 k 幅以上进行叠加，用人眼即可辨认出秘密图像。传统视觉密码方案的分享图像大小比原秘密图像大，并且分享图像无意义。为了解决上述问题，王洪君等人[18-19] 给出了像素不扩展的（2，3）视觉密码方案和具有掩盖图像的像素不扩展的（2，2）视觉密码方案。李春燕[20] 提出了基于像素不扩展视觉密码的盲水印算法，利用像素不扩展的（2，2）视觉密码的基础矩阵修改载体图像的低位来嵌入水印。

像素不扩展的（2，2）视觉密码方案见表 1。对于一个白（黑）色像素，有 2 条加密规则。对于每一次编码一个白（黑）色像素，随机选择一个加密规则，根据所选的规则将像素分割为 2 个子像素。

表 1　加密规则

Tab. 1　Encryption principles

原图像中像素	分享图像 1	分享图像 2	叠加结果
□	□	□	□
	■	■	□
■	□	■	■
	■	□	■

2　水印嵌入和提取

2.1　水印的嵌入

假设载体图像 H 是一个 $M \times N$ 的灰度图像，水印图像 W 是一个 $m \times n$ 的二值图像。利用密钥 K 产生 $m \times n$ 个随机数，从 $M \times N$ 个像素位置筛选出符合嵌入条件的 $m \times n$ 对像素值。将水印图像 W 利用像素不扩展的（2，2）视觉密码方案分割成 2 幅分享图像，分享 1 嵌入到载体图像中，分享 2 和密钥 K 分配给所有者，根据水印嵌入算法，得到嵌入水印后的载体图像。嵌入水印的算法流程具体如下。

（1）利用密钥 K 产生 $m \times n$ 个随机整数。随机整数对应图像的像素位置，将选取位置的像素值与其相邻的像素值进行比较。每当一对像素值 (x,y) 被读入时，当 $x < y$ 时，则 x,y 要满足如下条件：

$$\begin{cases} 2y - x + 3 \leqslant 255; \\ 3x - 2y - 3 \geqslant 0. \end{cases} \tag{1}$$

反之亦然，否则不能嵌入水印，重新选择嵌入位置。

（2）水印图像 W 利用像素不扩展的（2，2）视觉密码方案分割成 2 幅分享图像（见表 1），分享 1 嵌入到载体图像中，分享 2 分配给所有者。嵌入过程的阐释表述如下。

① 求出每对像素值差值的绝对值 h，差值与 2 作取余运算，余数为 r。

② 分享图像 1 的像素 w 与差值 h 和余数 r 作如下运算得到 q，其数学公式可表示为：

$$q = 2 \times h - r + 2 \times w, \tag{2}$$

③ 判断 (x,y) 的大小关系，先用较小的值与 q 作减法，再用较小的值与 q 作加法，得到嵌入水印后的像素值 (x',y')。x',y' 之间的大小关系与 x,y 之间的大小关系相同。假设 $x < y$，则有：

$$x' = x - q, \tag{3}$$

$$y' = x + q. \tag{4}$$

由此可得 $x' < y'$，同理可以利用较大的值与 q 作加减法得到 (x',y')。

2.2　水印的提取

当所有者想要证明所有权时，利用密钥 K 在嵌入水印位置提取像素值，每当一对 (x',y') 的值被读入时，根据水印的提取算法，得到 w 和 (x,y)，直到把所有像素值都提取出来就得到分享 1，将其与所有者的分享 2 叠加，可以得到原水印图像。将 (x',y') 替换成 (x,y) 就可以恢复原始载体图像。水印提取的完整算法详见如下。

（1）利用密钥 K 提取 $m \times n$ 对嵌入水印的像素值 (x',y')。

（2）比较 (x',y') 的大小，求出 x',y' 的平均值，x',y' 中较小值对应的 x 或 y 为平均值。假设 $x' < y'$，则可得到：

$$x = \frac{x' + y'}{2}, \tag{5}$$

（3）求 x 与 x' 差值的绝对值 s，差值 s 与 4 作取余运算，余数为 t。

（4）被除数为余数 t，除数为 2，得到的商就是嵌入水印图像的像素值 w，余数为 p。

（5）将差值 s，提取的水印像素值 w 和余数 p 作如下运算得到 c，其数学公式可表示为：

$$c = \frac{s - 2 \times w - p}{2} + p, \tag{6}$$

（6）x,y 中，较小值已经确定，较大值即为较小值与 c 的和，得到原载体图像像素对 (x,y)。假设 $x' < y'$，则有：

$$y = x + c, \tag{7}$$

同理，如果嵌入过程利用较大的值与 q 作加减

法得到(x',y'),则提取时,利用较大的值为平均值,较小值即为较大值与 c 的差。

假设有一对灰度值 (x,y),$x, y \in Z, 0 \leqslant x,y \leqslant 255$,嵌入 $w, w \in \{0,1\}$,并恢复 (x,y) 的可逆方法如下。假设:

$$x = 127,\ y = 132,\ w = 0,$$

x,y 满足嵌入条件,则有:

$$x' = 118,\ y' = 136$$

嵌入一对像素 (x',y'),根据水印提取算法提取嵌入值 w 并且恢复原始对 (x,y)。其推导运算过程如下:

$$x = \frac{x' + y'}{2} = 127, \tag{8}$$

$$1 \div 2 = w \cdots r, \tag{9}$$

$$w = 0, \tag{10}$$

$$y = x + c = 132. \tag{11}$$

2.3 实验结果

以 512×512 的 Lena 为载体图像,133×133 的水印图像如图 1 所示,嵌入水印的图像见图 2(a),恢复载体图像见图 2(b)。提取的分享图像 1 见图 3(a)和所有者的分享图像 2 见图 3(b),2 幅分享图像的叠加结果如图 3(c)所示。在实验中,使用峰值信噪比(*PSNR*)来测量嵌入水印后图像的质量。*PSNR* 的计算公式的数学表述如下:

$$PSNR = 10\lg\left(\frac{255^2}{MSE}\right), \tag{12}$$

其中,

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(p_{i,j} - p'_{i,j})^2, \tag{13}$$

式中,$p_{i,j}$ 是原载体图像的像素值,$p'_{i,j}$ 是嵌入水印后图像的像素值。*PSNR* 越大,嵌入水印后的图像与原载体图像越相似。一般来说,如果 *PSNR* 大于 30,人类的眼睛就无法察觉到差异。原载体图像与嵌入水印后的图像的峰值信噪比为43.95,这意味着人眼几乎看不到嵌入水印后的图像与原载体图像的区别。恢复的载体图像与原载体图像的峰值信噪比为正无穷,意味着 2 张图像完全相同。

对嵌入水印后的图像分别引入加噪声、剪切、滤波、缩放等扰动因素。提取的水印由测量值 *NC*(归一化相关)来进行表征,如式(14)所示:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)\,W'(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W'(i,j)^2}}. \tag{14}$$

其中,$W_{i,j}$ 是原始水印的像素值,$W'_{i,j}$ 是提取水印的像素值。如果 *NC* 接近 1,则提取的水印与原始水印相似。不同攻击下提取的水印图像如图 4 所示,*PSNR* 值是被攻击的图像和恢复的载体图像计算出来的,在有攻击和无攻击的叠加结果间测量 *NC* 值,可求得 *PSNR* 和 *NC* 数据见表 2。结果表明,该方案能够抵御常见的攻击。

图 1 原始水印图像

Fig. 1 The binary watermark

(a) 嵌入水印后的图像 (b) 恢复的载体图像

(a) Watermarked image (b) Recovered image

图 2 嵌入水印后的图像及恢复的图像

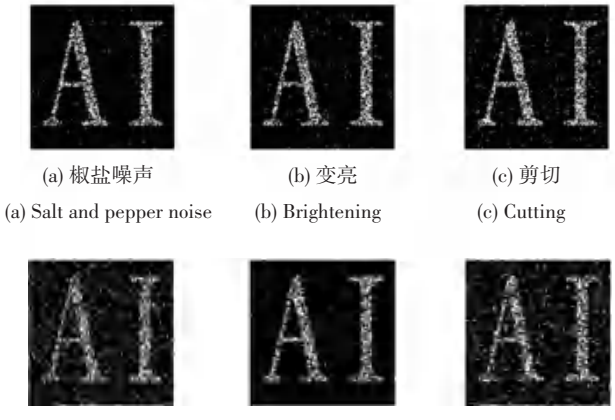
Fig. 2 The watermarked image and recovered image

(a) 分享图像 1 (b) 分享图像 2 (c) 叠加结果

(a) Shared image1 (b) Shared image 2 (c) Stacked result

图 3 分享图像及叠加结果

Fig. 3 Shared and stacked result



(a) 椒盐噪声 (b) 变亮 (c) 剪切

(a) Salt and pepper noise (b) Brightening (c) Cutting

(d) 旋转后还原 (e) 滤波 (f) 缩放

(d) Restore after rotation (e) Filtering (f) Zooming

图 4 不同攻击下提取的水印

Fig. 4 Watermarking extracted under different attacks

表 2　常见攻击

Tab. 2　Common attacks

攻击类型	*PSNR*	*NC*
椒盐噪声	40.651 0	0.977 6
变亮	40.824 9	0.967 0
变暗	40.820 6	0.988 0
剪切	40.902 6	0.945 1
旋转后还原	41.343 8	0.758 6
滤波	40.803 2	0.967 7
缩放	41.307 4	0.755 9

3　结束语

将像素不扩展的视觉密码方案与可逆水印相结合，提出了基于像素不扩展视觉密码的可逆水印算法，既能保证原始载体图像的隐私，又能保证水印的安全。近年来，视觉密码与水印相结合多为零水印算法，零水印算法没有将水印图像嵌入到载体图像中，载体图像不会被修改。其它视觉密码与水印相结合的算法不能完整地恢复载体图像。该算法不仅能正确地提取水印图像，并且能无损地恢复载体图像。对嵌入水印后的图像进行攻击，提取的水印和原始水印图像也较为相似。实验结果表明，该算法能抵御常规的攻击。

参考文献

[1] 曲长波，李栋栋. 基于视觉密码和边缘检测的零水印算法[J]. 计算机应用与软件，2016，33(9)：328-333.

[2] 曲长波，吴德阳. 基于 Curvelet-DSVD 和视觉密码的强鲁棒零水印算法[J]. 计算机应用研究，2019，36(2)：532-537.

[3] 侯翔，闵连权，唐立文. 定位篡改实体组的矢量地图脆弱水印算法[J/OL]. 武汉大学学报(信息科学版)：1-8[2019-09-05]. https://doi.org/10.13203/j.whugis20170404.

[4] LI Haiming, GUO Xiaoyun. Embedding and extracting digital watermark based on DCT algorithm[J]. Journal of Computer and Communications，2018，6(11)：287-298.

[5] 黄樱，牛保宁，关虎，等. 基于图像纹理的自适应水印算法[J/OL]. 北京航空航天大学学报：1-15[2019-08-26]. https://doi.org/10.13700/j.bh.1001-5965.2019.0369.

[6] 梁欣. 基于 DWT 和 SVD 的彩色图像数字水印算法研究[J]. 计算机与数字工程，2019，47(8)：2014-2017.

[7] 张健，刘燕，段鹏刚. 基于离散小波置乱的数字水印实现[J]. 光电技术应用，2019，34(4)：43-47，63.

[8] AHMAD M, ALSHARARI H D. Cryptanalysis and improvement of a digital watermarking scheme using chaotic map [J]. International Journal of Rough Sets and Data Analysis (IJRSDA)，2018，5(4)：61-73.

[9] ERFANNIA A，HATAMLOU A，MAHALLEH F. Watermarking of digital images with the substitution of low-value bits to increase capacity[J]. International Journal of Computer Vision and Image Processing (IJCVIP)，2017，7(4)：41-50.

[10] ZHU Changqing. Research progresses in digital watermarking and encryption control for geographical data[J]. Acta Geodaetica et Cartographica Sinica，2017，46(10)：1609-1619.

[11] 罗昊，谢晓尧，彭长根. 基于直方图平移的加密域可逆水印算法[J]. 郑州大学学报(理学版)，2018，50(2)：29-34.

[12] 刘连山，王晓利，初广辉，等. 基于分块预测的差值直方图平移的可逆水印算法[J]. 山东科技大学学报(自然科学版)，2019，38(4)：74-82，91.

[13] 项世军，杨乐. 基于同态加密系统的图像鲁棒可逆水印算法[J]. 软件学报，2018，29(4)：957-972.

[14] ZHENG Hongchang，WANG Chuntao，WANG Junxiang，et al. A new reversible watermarking scheme using the content-adaptive block size for prediction[J]. Signal Processing，2019，164：74-83.

[15] GAO Lin, GAO Tiegang, ZHAO Jie, et al. Reversible watermarking in digital image using PVO and RDWT [J]. International Journal of Digital Crime and Forensics (IJDCF)，2018，10(2)：40-55.

[16] WU Yuanxin, DIAO Wen, HOU Dongdong, et al. Reversible watermarking on stereo audio signals by exploring inter-channel correlation[J]. International Journal of Digital Crime and Forensics (IJDCF)，2019，11(1)：29-45.

[17] NAOR M, SHAMIR A. Visual cryptography[M]//De SANTIS A. Advances in Cryptology - EUROCRYPT ´94. EUROCRYPT 1994. Lecture Notes in Computer Science. Berlin/Heidelberg：Springer，1995，950：1-12.

[18] 王洪君，牟晓丽，鲁晓颖，等. 像素不扩展的(2，3)视觉密码方案[J]. 吉林大学学报(信息科学版)，2014，32(1)：82-87.

[20] 王洪君，赵腾飞，尚大龙，等. 具有掩盖图像的像素不扩展的(2，2)视觉密码方案[J]. 南京大学学报(自然科学)，2018，54(1)：157-162.

[20] 李春艳. 基于像素不扩展视觉密码的水印算法[J]. 大理大学学报，2017，2(6)：19-21.