文章编号：2095-2163(2021)08-0173-05 中图分类号：TP309.7 文献标志码：A

基于视觉密码的 DWT-SVD 水印技术

高 淼，王洪君
（吉林师范大学 计算机学院，吉林 四平 136000）

摘 要：本文提出基于视觉密码的数字水印技术，利用像素不扩展的(2,2)视觉密码方案，将秘密图像拆分成两个与秘密图像等大小的分享份图像，把两个分享份图像利用 DWT-SVD 水印算法嵌入到载体图像中，最后利用数字水印的提取算法，将两个分享份图像提取出来，进行叠加恢复秘密图像。基于视觉密码提取出来的分享份不会泄露秘密信息的任何内容，从而保证了秘密信息的安全性。实验结果表明，此方案可以抵抗常见的攻击行为。

关键词：视觉密码；数字水印；像素不扩展；DWT；SVD

DWT-SVD watermarking technology based on visual cipher

GAO Miao，WANG Hongjun
（College of Computer Science，Jilin Normal University，Siping Jilin 136000，China）

【Abstract】 A digital watermarking technique based on visual cipher is proposed. By using the (2,2) visual cipher scheme without pixel expansion，the secret image is divided into two shared images of the same size as the secret image，and the two shared images are embedded into the carrier image using DWT-SVD watermarking algorithm. Finally，two shared images can be extracted by the digital watermark extraction algorithm，and then the secret images can be recovered by superposition. Based on the security of visual password，the extracted shared images will not reveal any contents of the secret information，so as to ensure the security of the secret information. And the experimental results show that this scheme can resist the common attacks.

【Key words】 visual cipher；digital watermarking；pixel unextended；DWT；SVD

0 引 言

随着计算机的普及应用，简单的复制粘贴就可以轻易的篡改他人的创新成果，盗版现象越发猖獗，版权信息泄露愈演愈烈[1]。如何保护研发者的创新成果是一个重要的问题，目前关于如何保护数字作品的知识产权，研究者们提出了许许多多的技术方案，其中数字水印技术一直是维护知识产权的重要方法。数字水印就是在载体图像上嵌入可以代表研究者身份的水印信息，在需要产权维护时，将水印信息从载体图像中提取出来，进行验证，维护产权的合法权益。

为了解决数字水印鲁棒性与透明性之间的问题，温泉等人提出了零水印算法，零水印是指没有把水印信息嵌入到载体图像中去，所以不会对载体图像的完整性起到影响[2]；在此基础上曲长波等人又提出了基于视觉密码和边缘检测的零水印算法[3-4]；Rain 等人又提出基于离散小波的零水印算法，把载体图像进行小波变换，然后将与载体图像相似的部分分成 4×4 个子块，将每个子块都进行奇异值分解，最后实现零水印的生成[5]；李春燕又实现了像素不扩展的盲水印算法，基于像素不扩展的(2,2)视觉密码方案修改载体图像的空间域实现[6]。

本文基于(2,2)像素不扩展视觉密码方案，将版权信息图像拆分成与版权信息图像大小相同的两个分享份图像，然后将两个分享份图像进行奇异值分解，再把载体图像先进行一级小波变换，其中 LL 子带是载体图像的近似图像，再将 LL 子带进行一级 Haar 小波变换，取 LL2 子带与 HH2 子带，进行奇异值分解，把两个分享份分别嵌入到 LL2 与 HH2 中去，完成在载体图像上嵌入两个水印图像。在需要进行版权验证时，使用数字水印的提取算法，把两个分享份提取出来，进行叠加，完成版权信息图像的恢复。因为基于视觉密码学，所以即使水印提取算法泄露，提取出的分享份也不会暴露任何版权信息。

作者简介：高 淼(1997-)，女，硕士研究生，主要研究方向：视觉密码；王洪君(1965-)，男，博士，教授，硕士生导师，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：2021-06-15

1 视觉密码

1.1 视觉密码概括

视觉密码学是在 1994 年由 Naor 和 Shami 提出来的,是一个全新的密码学理论,其不再需要复杂的数学计算与高深的数学理论知识,而是将秘密形成一幅图像,然后将秘密图像根据规则拆分成 n 个分享份,将 n 个分享份分发给 n 个参与者,当 n 个参与者中 k 个人($k \leqslant n$)将自己的分享份叠加在一起,就可以实现秘密图像的恢复[7]。参与者不在需要学习复杂的密码学知识,仅仅需要一双肉眼就可以获取秘密信息。但是传统的秘密学会产生像素扩展等问题,导致恢复的图像与原始图像大小不一,针对这一问题,王洪君等人提出像素不扩展的(2,3)视觉密码方案,根据传统方案进行拆分的分享份图像都是杂乱无章没有规律的图像,容易受到攻击[8];所以又提出具有掩盖图像并且像素不扩展的(2,2)视觉密码方案[9]。

1.2 (2,2)视觉密码方案

传统的(2,2)视觉密码方案,会让恢复出来的秘密图像长度变为原来的二倍,存在像素扩展,因为原始秘密图像中无论一个黑色像素块还是一个白色像素块,在进行加密时分存图像中都需要被一黑一白两个像素块进行表达,所以使整体长度变宽。(2,2)像素不扩展视觉密码方案是指恢复出来的秘密图像与原始秘密图像大小一样,在原始秘密图像中一个黑色像素块或者一个白色像素块,在进行加密时,分存图像也只需要一个像素块进行表达,加密规则见表 1。

表 1 (2,2)像素不扩展视觉密码方案加密规则

Tab. 1 (2,2) pixels do not extend the encryption rules of the visual cipher scheme

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

由数字 0 代表白色,数字 1 代表黑色,进行异或运算。两个分存片颜色相同,叠加恢复出来的秘密图像颜色是白色;两个分存片颜色不同,叠加恢复出来的秘密图像颜色是黑色。

2 离散小波变换 DWT

变换域水印算法是水印算法的重心,包括离散傅里叶变换(DFT),离散余弦变换(DCT),离散小波变换(DWT)。本文主要使用 Haar 小波变换,Haar 小波具有构造简单、计算方便的特点。利用 Haar 小波变换,将二维图像进行一级分解与二级分解,如图 1 和图 2 所示。

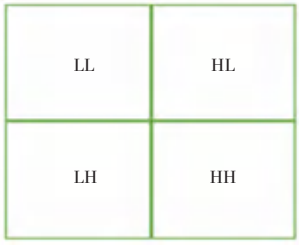


图 1 一级 Haar 小波变换

Fig. 1 First-order Haar wavelet transform

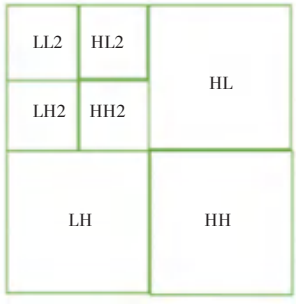


图 2 二级 Haar 小波变换

Fig. 2 Second-order Haar wavelet transform

LL 是低频水平子带;LH 是高频水平子带;HL 是高频垂直子带;HH 是高频对角线子带。低频水平子带与原始图像非常相似,包含了图像的大多数细节,只是大小发生了变化,其它的 3 个子带只包含图像的边缘细节。

3 奇异值分解 SVD

奇异值分解是线性代数中最常用的一种矩阵分解,图像可以看成是由许多非负标量组成的矩阵。

SVD 可以用来提取图像的特征值,实现图像的降维与压缩,应用到数字水印中去可以提高水印的鲁棒性,图像在经过 SVD 分解后可以拆分成 3 个矩阵,分为左奇异值矩阵 $\boldsymbol{U}$,奇异值矩阵 $\boldsymbol{S}$,右奇异值矩阵 $\boldsymbol{V}$,在奇异值矩阵中,奇异值由大到小排列成对角矩阵。R 代表实数域,矩阵 $\boldsymbol{A}$ 的大小为 MXN。

矩阵 $\boldsymbol{A}$ 的奇异值分解可以表示为式(1):

$$\boldsymbol{A} = \boldsymbol{U} \sum \boldsymbol{V}^{\mathrm{T}}. \tag{1}$$

其中,$\boldsymbol{U} \in R^{MXN}$,$\boldsymbol{V} \in R^{MXN}$ 是正交矩阵,$\sum \in$

R^{MXN} 是一个非对角线上都是 0 的矩阵，在对角线上的元素满足 $\sigma^1 \geqslant \sigma^2 \geqslant \ldots \geqslant \sigma^r > \sigma^{r+1} = \sigma^M = 0$。

4　水印算法

4.1　水印添加

利用(2,2)像素不扩展方案将数字水印图像拆分成两个分享份，利用 Haar 小波变换，将载体图像进行二级 Haar 小波变换，得到子带 LL2、HH2，将 LL2 与 HH2 都进行奇异值分解，将分享份 1 进行奇异值分解，并将分解后的奇异值矩阵，加到 LL2 奇异值上，将分享份 2 进行奇异值分解，并将分解后的奇异值矩阵，加到 HH2 奇异值上，实现数字水印的添加。

水印嵌入算法的步骤如下：

(1)分别读取原始图像 I，水印分享份 1 图像 W 和水印分享份 1 图像 WW；

(2)原始图像 I 进行 Haar 小波二级变换，得到 LL2 与 HH2；

(3)LL2 与 W 进行奇异值分解，然后完成水印的嵌入，嵌入公式(2)~(4)：

$$LL3 = US\,V^T, \tag{2}$$

$$W = U^W\,S^W\,V^{WT}, \tag{3}$$

$$S^* = S + \propto S^W. \tag{4}$$

其中，$\propto$ 代表嵌入水印的强度。

(4)将 HH2 与 WW 进行奇异值分解，然后完成水印的嵌入，嵌入公式(5)~(7)：

$$HH3 = U^h\,S^h\,V^{hT}, \tag{5}$$

$$W = U^{WW}\,S^{WW}\,V^{WWT}, \tag{6}$$

$$S^{**} = S^h + \propto 1\,S^{WW}. \tag{7}$$

其中，$\propto 1$ 代表嵌入的水印强度。

(5)利用公式(8)和(9)：

$$LL3^* = U\,S^*\,V^T, \tag{8}$$

$$HH3^* = U^h\,S^{**}\,V^{hT}. \tag{9}$$

实现 SVD 的逆变换得到 $LL3^*$ 和 $HH3^*$，再利用 Haar 小波的逆变换得到含义水印的图像 IW。

4.2　水印提取

对得到的载体图像进行 Haar 小波二级变换，提取出新的 LL2 子带和新的 HH2 子带，将两个新的子带进行奇异值分解，从新的奇异值上求出嵌入水印的奇异值，从而求出水印的矩阵，进行水印的提取。

水印提取算法的步骤如下：

(1)分别读取嵌入水印图像 IW 与原始水印图像 I；

(2)对嵌入水印的图像 IW 进行 Haar 小波二级变换，得到新的 LL2 与 HH2；

(3)利用公式(10)~(12)提取出水印 W；

$$S^* = U^T LL3^*\,V, \tag{10}$$

$$S^W = (S^* - S)/\propto, \tag{11}$$

$$W = U^W\,S^W\,V^{WT}. \tag{12}$$

(4)利用公式(13)~(15)提取出水印 WW。

$$S^{**} = U^{hT} HH3^*\,V^{hT}, \tag{13}$$

$$S^W = (S^{**} - S^h)/\propto 1, \tag{14}$$

$$WW = U^{WW}\,S^{WW}\,V^{WWT}. \tag{15}$$

5　Matlab 实验结果

载体图像是 512×512 的 Lena 图像，如图 3 所示；秘密图像是 128×128 的图像，如图 4 所示。嵌入的水印图像是两幅，分别是秘密图像基于(2,2)像素不扩展视觉密码方案的分享份 1 与分享份 2，都是 128×128 的图像，如图 5(a)，(b)所示。图 6 是嵌入两幅分享份水印图像的载体图像按照水印提取算法从载体图像提取出的两份分享份水印图像如图 7(a)，(b)所示，提取出的两份水印分享份图像进行叠加恢复出秘密图像，如图 7(c)所示。

图 3　载体图像 512×512

Fig. 3　Carrier image 512×512

图 4　秘密图像 128×128

Fig. 4　Secret image 128×128

(a) 分享份 1 图像 128×128 (b) 分享份 2 图像 128×128

(a) Share 1 image 128×128 (b) Share 2 image 128×128

图 5 秘密图像的分享份图像

Fig. 5 A shared image of the secret image

图 6 嵌入两个分享份的载体图像 512×512

Fig. 6 Carrier image 512×512 embedded with two shares

(a) 提取分享份 1 图像 128X128 (b) 提取分享份 2 图像 128X128 (c) 恢复的秘密图像 128X128

(a) Extract share 1 image (b) Extract share 2 image (c) Restored secret image

图 7 提取出的分享份图像及恢复图像

Fig. 7 Extract the shared image and restore the image

在整个实验中,利用峰值信噪比(PSNR)来评价嵌入水印后载体图像的质量。PSNR 的数学表达式(16)如下:

$$PSNR = 101g(\frac{255^2}{MSE}), \quad (16)$$

其中, MSE 的数学表达式(17) 为:

$$MSE = \frac{1}{MXN}\sum_{i=1}^{M}\sum_{j=1}^{N}(P_{i,j}-P'_{i,j})^2. \quad (17)$$

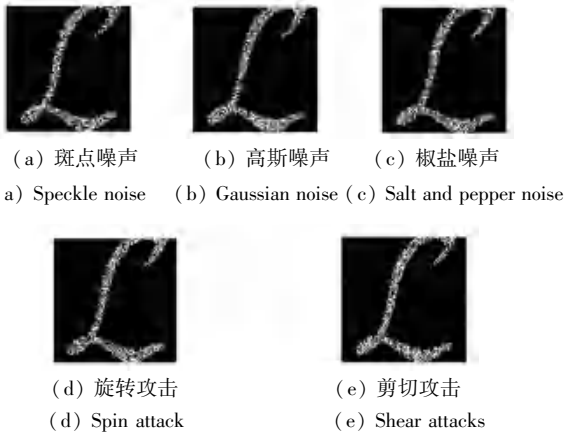
其中, $P_{i,j}$ 代表原始载体图像的像素值, $P'_{i,j}$ 代表嵌入水印后的像素值,PSNR 的数值越大,代表嵌入水印后的载体图像与原始载体图像越相似, $PSNR$ 的数值越小,代表嵌入水印后的载体图像与原始载体图像区别越大。

一般来说,当 $PSNR$ 的数值超过 30,人眼就无法分辨出嵌入水印的图像与原始图像的区别。原始载体图像与嵌入水印后的载体图像峰值信噪比达到 69.213 4,所以在人类的视觉系统下进行观察,两幅图片几乎看不见差异,当峰值信噪比达到正无穷的时候,两张图像完全相同,没有差异。

对嵌入的水印进行攻击后,判断提取出的水印图像与原始水印图像的差异,由归一化相关(NC)进行评价,数学表达式(18)如下:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}W(i,j)\ W'(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}W(i,j)^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}W'(i,,j)^2}}. \quad (18)$$

其中, $W(i,j)$ 代表原始水印的像素, $W'(i,j)$ 代表提取出来的水印像素, NC 值越接近 1,表示提取出来的水印与原始水印越相似,不同攻击下提取出的水印恢复的秘密图像如图 8 所示。



(a) 斑点噪声 (b) 高斯噪声 (c) 椒盐噪声

(a) Speckle noise (b) Gaussian noise (c) Salt and pepper noise

(d) 旋转攻击 (e) 剪切攻击

(d) Spin attack (e) Shear attacks

图 8 各种攻击下秘密图像恢复效果

Fig. 8 Secret image restoration effect under various attacks

$PSNR$ 值是由原始载体图像与接受各种攻击的水印嵌入图像计算出来的,NC 值是原始秘密图像的分享份水印与经受各种各样攻击后提取出来的分享份水印计算出来的,见表 2。

表 2 常见攻击

Tab. 2 Common attacks

攻击类型	$PSNR$	第一个水印分享份 NC	第二个水印分享份 NC
斑点噪声	63.413 7	0.993 2	0.903 8
高斯噪声	63.264 9	0.917 9	0.953 6
椒盐噪声	63.510 4	0.991 7	0.899 0
旋转	61.643 5	0.904 2	0.861 4
剪切	64.362 0	0.947 3	0.999 8

6 结束语

本文将像素不扩展的(2,2)视觉密码方案与

(下转第 182 页)