于唤理, 王洪君, 孟祥凤. 基于 LWT-PCA 算法的水印技术在视觉密码中的应用[J]. 智能计算机与应用,2024,14(11):182-187. DOI:10.20169/j.issn.2095-2163.241128

基于 LWT-PCA 算法的水印技术在视觉密码中的应用

于唤理, 王洪君, 孟祥凤
(吉林师范大学 数学与计算机学院, 吉林 四平 136000)

摘 要: 本文提出了一种基于 LWT-PCA 的数字水印算法在像素不扩展(2,2)视觉密码方案中的应用。算法对载体图像进行一阶提升小波变换,在低频 LL 子带上用主成分分析提取出重要的主成分系数,再用像素不扩展(2,2)视觉密码方案将水印拆分成 2 个分享图像,将其中分享图像 1 嵌入到提取的主成分系数中,提取出来分享图像 1 与分享图像 2 可以恢复出水印。实验结果表明,本文水印算法能抵抗各类常见的攻击,同时保证了水印的隐蔽性。

关键词: 提升小波变换(LWT); 主成分分析(PCA); 视觉密码; 像素不扩展
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 2095-2163(2024)11-0182-06

Application of watermarking technology based on LWT-PCA algorithm in visual cryptography

YU Huanli, WANG Hongjun, MENG Xiangfeng
(College of Mathematics and Computer, Jilin Normal University, Siping 136000, Jilin, China)

Abstract: This paper proposes the application of a digital watermarking algorithm based on LWT-PCA in the pixel non-expansion (2,2) visual cipher scheme. The algorithm performs a first-order boosted wavelet transform on the carrier image, extracts the important principal component coefficients on the low-frequency LL sub-band by Principal Component Analysis, and then splits the watermark into two shared images by using the pixel non-expansion (2,2) visual password scheme. After that, the paper embeds the shared image 1 into the extracted principal component coefficients, and extracts the shared image 1 and the shared image 2 to recover the watermark. Experimental results show that the proposed watermarking algorithm can resist various common attacks and ensure the concealment of watermarks.

Key words: Lifting Wavelet Transform (LWT); Principal Component Analysis (PCA); visual cryptography; the pixel does not expand

0 引 言

随着互联网不断的发展,数字媒体(数字图像、视频、音频等)的传播和获取就变得更容易,不需要在授权的情况下,就可以并不困难地篡改他人的劳动成果,所以如何保护人们的知识产权就成为了一个非常重要的研究课题。其中,数字水印一直都是保护所有权的技术之一,数字水印技术就是在载体图像中嵌入有意义的水印信息,在需要维护所有权的时候,提取出水印信息来验证所有权。

目前,主要图像水印[1-4]的技术分为 2 个方面。一方面是基于空间域的水印技术,通过改变载体图像的灰度值来嵌入水印,但计算复杂度低,鲁棒性弱,很容易遭到破坏。另一方面是基于频域的水印技术,将水印嵌入到载体图像的变换系数中,这样就很难被检测到。曲长波等学者[5-6]提出了小波域视觉密码零水印算法和基于视觉密码和边缘检测的零水印算法,主要对载体图像做离散小波变换(Discre Wavelet Transform,DWT)和奇异值分解的运算,通过比较块特征值求得过渡矩阵,最后与视觉密码结合生成零水印。Wang[7]提出的基于离散小波变换和奇异值分解(Singular Value Decomposition,SVD)

作者简介: 于唤理(1999—),男,硕士研究生,主要研究方向:信息安全,密码学,视觉密码; 孟祥凤(2001—),女,硕士研究生,主要研究方向:信息安全,密码学,视觉密码。
通信作者: 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。Email:jlnuwhj@sina.com。

收稿日期: 2024-01-28

的算法，但该算法鲁棒性较弱。Nasrin 等学者[8-10]提出的基于提升小波变换（Lifting Wavelet Transform，LWT）算法是改进的第二代小波算法，能够保持第一代小波变换的时频局部性，同时改进了第一代小波变换的算法，鲁棒性有所提升。主成分分析[11]（Principal Component Analysis，PCA）是在模式识别领域中一种经典的数据降维算法，可以提取图像中最重要的一部分，来提高鲁棒性。

本文主要研究的是提升小波变换和主成分分析的水印算法与像素不扩展（2，2）视觉密码方案相结合。利用像素不扩展（2，2）视觉密码方案将水印图像拆分成 2 个大小与水印图像相同的分享图像，将其中分享图像 1 与提升小波变换和主成分分析的水印算法相结合嵌入到载体图像中，分享图像 2 放在版权保护中心。本次研究在提取图像时，从嵌入水印的载体图像中提取出分享图像 1，提取出的分享图像 1 和放在版权保护中心的分享图像 2 让 2 个分享图像进行叠加就可以恢复出原始的水印图像。实验结果表明，该算法实现起来简单，得到了较好的效果，并且有很强的鲁棒性。

1　视觉密码

1.1　视觉密码概括

视觉密码（Visual Cryptography Scheme，VCS）是 1994 年由 Naor 和 Shamir[12]提出的一种新型密码学理论，不仅有简单的恢复性，并且具有一次一密的安全性。将秘密图像拆分成 n 个分享图像，将 n 个分享图像分发给 n 个参与者，当有 $k(k \leqslant n)$ 个参与者将自己的分享图像叠加在一起就可以恢复出秘密图像，而少于 k 个参与者叠加自己的分享图像就不会恢复出任何的秘密图像。参与者不需要学习复杂的知识，用眼睛就可以辨认出秘密图像。但由于视觉密码有像素扩展等问题，即分享图像的大小要比原始图像的大了许多，并且有的分享图像，没有意义。针对上述问题，YANG[13]利用恢复图像中黑白像素点在黑色区域和白色区域出现的概率不同，提出了基于概率的可视密码分享方案。王洪君等学者[14]提出了像素不扩展的（2，3）视觉密码方案解决了像素扩展的问题。同时王洪君等学者[15]又提出具有掩盖图像的像素不扩展的（2，2）视觉密码方案，不仅解决了像素扩展的问题，同时还解决了分享图像无意义的问题。李春燕[16]提出基于像素不扩展视觉密码水印算法，通过修改二值图像的基本矩阵来实现水印的嵌入。高淼等学者[17]提出了基于视觉密码的 DWT-SVD 水印技术把 2 个分享图像都嵌入到载体图像中。

1.2　（2，2）视觉密码方案

在传统的（2，2）-VCS 方案中，数字 1 代表黑色像素，数字 0 代表白色像素，$\boldsymbol{S}_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ 和 $\boldsymbol{S}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 分别为白色像素和黑色像素的基础加密矩阵。$\boldsymbol{C}_0$、$\boldsymbol{C}_1$、$\boldsymbol{C}_2$、$\boldsymbol{C}_3$ 是 $\boldsymbol{S}_0$ 和 $\boldsymbol{S}_1$ 做随机列置换后的所有矩阵集合，即：

$$\boldsymbol{C}_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \boldsymbol{C}_1 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix},$$

$$\boldsymbol{C}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \boldsymbol{C}_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

（2，2）像素不扩展视觉密码方案指叠加出来的秘密图像和原始秘密图像大小一样，每一个白色像素点和黑色像素点，都有 2 条加密规则，进行异或运算。2 个分享图像颜色相同叠加出来的秘密图像为白色，2 个分享图像颜色不相同叠加出来的秘密图像为黑色。像素不扩展（2，2）视觉密码加密规则见表 1。

表 1　像素不扩展（2，2）视觉密码加密规则

Table 1　Pixel non-expansion （2，2） visual password encryption rules

原图像中像素	概率/%	分享图像 1	分享图像 2	叠加后的图像
□	50	■□	■□	□□
	50	□■	□■	□□
■	50	■□	□■	■■
	50	□■	■□	■■

2　提升小波变换

提升小波变换（LWT）是采用提升方法构造的第二代小波变换，在图像处理和分析方面 LWT 算法起着重要作用。相比于小波变换，LWT 算法具有更高的效率。LWT 具有以下优点：

（1）算法简便，运算效率快。

（2）易于实现整数变换。

（3）能实现原位计算，计算过程不需要辅助空间，可以节省存储单元。

该算法的基本思想是，将现有的图像分解成多个构造模块，按照步骤完成对信号的分解。步骤主要分为 3 个阶段：分裂（Split）、预测（Predict）、更新（Update），如图 1 所示。

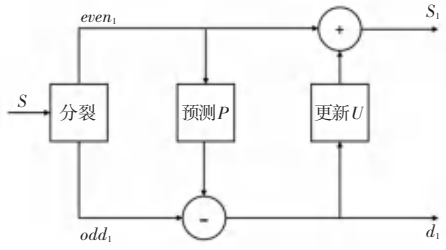


图 1 提升小波变换分解过程

Fig. 1 Lifting wavelet transform decomposition process

(1)分裂。运算过程中,分裂是最基本的内容,对结果的影响较大。客观来说,分裂工作主要是将原始的信号进行分裂处理,分成偶数序列和奇数序列两个互不相交的子集。将输入信号 s 分为 2 个较小的子集,偶数序列 $even_1$ 和奇数序列 odd_1,分解过程表示为:

$$Split(s) = (even_1, odd_1) \tag{1}$$

(2)预测。主要是运用预测算子,以一组序列为基础,对另外一组序列进行科学、合理预测。预测值与实际值的差值越小,相似度越高,所产生的误差为小波系数,奇、偶序列有着紧密的联系,如果给出其中一个序列,则可将另外一个序列预测出来,而且获得的预测值准确度较高。设预测值为 $P(even_1)$,则与实际值之间的差值为:

$$d_1 = odd_1 - P(even_1) \tag{2}$$

(3)更新。更新是提升小波变换的最后一个步骤,由于预测后奇数序列不能保持原始数据,利用预测值把最开始的偶数序列进行更新,更新过程表示为:

$$s_1 = even_1 + U(d_1) \tag{3}$$

其中,U 表示更新算子,s_1 表示原始信号的低频部分。

在经历提升小波变换的一次分解后,就可以从中得到低频部分 s_1 和高频部分 d_1,不断地对低频部分进行提升小波变换就可以对信号做连续分解。提升小波变换的逆变换是通过改变数据流向实现的,也称为提升小波变换的重构过程,如图 2 所示。

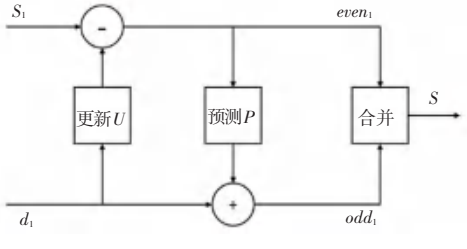


图 2 提升小波变换重构过程

Fig. 2 Lifting wavelet transform reconstruction process

3 主成分分析

主成分分析[8]是一种统计分析方法,同样也是一种有效的数据降维算法。设有 n 个样本 $X_1, \cdots, X_P$, p 维向量 $\boldsymbol{x} = (x_1, \cdots, x_p)^{\mathrm{T}}, i = 1,2,\cdots,n, n > p$,构造样本矩阵如下:

$$\boldsymbol{X} = \begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & & & \\ X_{p1} & X_{p2} & \cdots & X_{pn} \end{bmatrix} \tag{4}$$

主成分的基本计算过程如下。

(1)将样本阵元进行基本的标准化,即:

$$Z_{ij} = \frac{x_{ij} - \bar{x}_j}{s_j},\ i = 1,2,\cdots,n;\ j = 1,2,\cdots,p \tag{5}$$

其中,$\bar{x}_j = \dfrac{\sum_{i=1}^{n} x_{ij}}{n}$, $i = 1,2,\cdots,n; j = 1,2,\cdots,p$,

$s_j^2 = \dfrac{\sum_{i=1}^{n} (x_{ij} - \bar{x}_j)^2}{n-1}$.

(2)求标准化矩阵 $\boldsymbol{Z}$ 的相关系数矩阵 $\boldsymbol{R}$:

$$\boldsymbol{R} = [r_{ij}]\ xp = \begin{bmatrix} 1 & r_{12} & \cdots & r_{1p} \\ r_{21} & r_{22} & \cdots & r_{2p} \\ \vdots & & & \\ r_{p1} & r_{p2} & \cdots & 1 \end{bmatrix} \tag{6}$$

其中,$r_{ij} = \dfrac{\sum Z_{ij} Z_{ij}}{n-1}$, $i, j = 1,2,\cdots,p$。

(3)求相关系数矩阵 $\boldsymbol{R}$ 的特征方程:

$$|\boldsymbol{R} - \lambda \boldsymbol{I}_p| = 0 \tag{7}$$

特征方程就能求出 p 个特征根,即 $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_p \geqslant 0$。从而根据特征值能求出对应的特征向量 $\boldsymbol{e}_i$ $(i = 1,2,\cdots,p)$,再根据特征向量 $\boldsymbol{e}_i$ 来组成相应的特征系数矩阵 $\boldsymbol{U} = (e_1, e_2, \cdots, e_p)^{\mathrm{T}}$。

(4)确认主成分数。其中,主成分的个数至关重要,选择错误就会导致重要数据的丢失。假设取出其中第 i 个特征值,定义第 i 个特征值的贡献占比率为:

$$R_c(r) = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} \tag{8}$$

其中,R_c 表示主成分所占的贡献比率,特征值为 $i = 1,2,\cdots,p$。

然后就能从中算出前 m 个主成分的累计贡献

率 $R_{ac}(m)$：

$$R_{ac}(m)=\frac{\sum_{i=1}^{m}\lambda_i}{\sum_{i=1}^{n}\lambda_i} \tag{9}$$

在使用中，让使用信息的效率达到 85% 以上，即按照 $R_{ac}\geqslant 85\%$ 确定 m 值。

(5)变量转换为主成分。主成分计算公式为：

$$F_j=\boldsymbol{U}_j^{\mathrm{T}}\boldsymbol{Z},\quad j=1,2,\cdots,m \tag{10}$$

4　基于 LWT-PCA 的水印算法

4.1　嵌入水印

利用像素不扩展(2,2)视觉密码方案将水印图像加密生成 2 个分享图像，将分享图像 1 嵌入到载体图像中，将分享图像 2 保存至版权保护中心。因低频区域能包含载体图像的重要信息，所以先对载体图像进行一阶提升小波变换，提取其中的低频区域。将水印嵌入到低频子带的区域中能够很好地抵抗各类攻击，然后将低频区域的每一块图像进行主成分分析，求出每一块图像的主成分，将分享图像 1 嵌入到这些主成分中有较好的鲁棒性，因为这些部分既有高频部分、又有低频部分。假设载体图像 I 是一个灰度图像，水印图像 W 是二值图像。水印嵌入到载体图像算法具体过程如下。

(1)对载体图像 I 拆分成互不重叠的 8×8 的小块，记为 I_n。然后对其中各个子块 I_n 进行一阶提升小波变换，得到一个新的矩阵 $\boldsymbol{I}_n^{\mathrm{LWT}}$。

(2)选取 LWT 变换得到的低频子图 $I_n^{\mathrm{LL}}(i,j)$，对其低频子图进行标准化，然后生成标准化矩阵 $Z(i,j)$。

(3)求出矩阵 $\boldsymbol{Z}(i,j)$ 的相关系数矩阵 $\boldsymbol{R}(i,j)$。

(4)求相关系数矩阵 $\boldsymbol{R}(i,j)$ 的 p 个特征根，顺序按照由大到小的方式进行排列，即 $\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_p\geqslant 0$。

(5)得出特征根的值 λ_i 后，就可以算出特征向量 $\boldsymbol{e}_i(i=1,2,\cdots,p)$，再根据特征向量 $\boldsymbol{e}_i$ 来组成特征矩阵 $\boldsymbol{U}=(e_1,e_2,\cdots,e_p)^{\mathrm{T}}$。

(6)按照 $\boldsymbol{R}_{ac}=\dfrac{\sum_{i=1}^{m}\lambda_i}{\sum_{i=1}^{n}\lambda_i}\geqslant 85\%$ 来确定 m 的值，计算主成分公式为：

$$y_j=\boldsymbol{U}_j^{\mathrm{T}}\boldsymbol{Z},\ j=1,2,\cdots,m \tag{11}$$

(7)利用(2,2)像素不扩展视觉密码方案将水印图像 W 加密生成2幅分享图像，分别为分享图像1和分享图像 2。

(8)将分享图像 1 嵌入到载体图像中，分享图像 2 保存至版权保护中心，嵌入水印公式为：

$$Y'=y+aw \tag{12}$$

其中，a 表示水印的嵌入强度；y 表示嵌入前载体图像的主成分系数；Y' 表示嵌入后含水印载体图像的主成分系数。

(9)最后进行逆 LWT 变换得到载体图像。

4.2　提取水印

当创作者想证明所有权时，利用 LWT 变换和水印强度 a 完成整个提取水印的过程，把提取出的分享图像 1 和分享图像 2 叠加，就可以得到原水印图像。水印提取的完整算法流程如下。

(1)根据嵌入过程中前 6 步的方法算出相应的标准化矩阵、相关系数矩阵、特征根等来求出原始的主成分。

(2)同样根据嵌入过程中前 6 步的方法算出相应的标准化矩阵、相关系数矩阵、特征根等来求出新的主成分。

(3)提取水印公式如下：

$$W=(Y'-y)/a \tag{13}$$

(4)提取出来的水印图像为分享图像 1 与在版权保护中心的分享图像 2 进行叠加就可以恢复出原始水印图像。

5　实验及分析

5.1　图像评价标准

5.1.1　峰值信噪比

峰值信噪比[18](Peak Singal to Noise Ratio，*PSNR*)是用来评价嵌入水印图像后载体图像的客观标准，可作为原始图像和嵌入水印后的载体图像之间的劣化程度的客观评价，评价结果用 dB 来表示。一般来说，当 *PSNR* 的值大于 33 dB 时，人的肉眼就无法区分 2 幅图像的差别。峰值信噪比的值越大，则表示 2 幅图像区别不大；若峰值信噪比的值越小，2 幅图像的差异就能区分出来。*PSNR* 计算公式为：

$$R_{PSN}=10\lg\left(\frac{MN\max(I)^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}(I-I')^2}\right) \tag{14}$$

其中，$\max(I)^2$ 表示原始图像的最大像素值；M 和 N 分别表示图像的大小；I' 表示嵌入水印图像的数据。

5.1.2 归一化相关系数

归一化相关系数[18]是用来评估提取出的水印和原始水印之间的差异的。如果归一化相关系数越接近 1,说明提取出来的图像和原始图像的相似度越接近,反之,则说明 2 幅图像相似度越低。归一化相关系数计算公式为:

$$NC = \frac{\sum_{i=2}^{L} w(i) \times w'(i)}{\sqrt{\sum_{i=1}^{L} w^2(i)} \sqrt{\sum_{i=1}^{L} w'^2(i)}} \quad (15)$$

其中,$w(i)$ 表示原始图像的像素信息;$w'(i)$ 表示提取出来水印的像素信息。

5.2 实验结果及分析

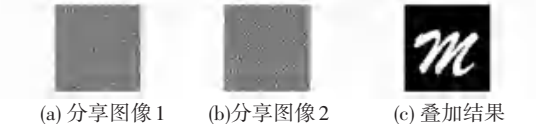
图 3 显示的是载体图像为 512×512 的 lena 灰度图像;图 4 显示的是水印图像为 128×128 的二值图像;图 5(a)显示的是嵌入载体图像的分享图像 1;图 5(b)显示的是送至版权保护中心为的分享图像 2;图 5(c)显示的是 2 幅分享图像叠加后恢复出的水印图像;图 6 显示的是嵌入水印后的载体图像;图 7(a)显示的是嵌入载体图像后提取出来的分享图像 1;图 7(b)显示的是提出来的分享图像 1 和分享图像 2 叠加恢复出来的结果。

图 3 载体图像

Fig. 3 Carrier image

图 4 原始水印图像

Fig. 4 The binary watermark



(a) 分享图像 1 (b)分享图像 2 (c) 叠加结果

图 5 分享图像及叠加结果

Fig. 5 Shared and stacked results

图 6 嵌入水印后的载体图像

Fig. 6 Watermarked image

(a) 提取分享图像 1 (b) 恢复的水印图像

图 7 提取出分享图像及恢复的水印图像

Fig. 7 Extracting the shared image and the restored watermark image

经实验结果得到峰值信噪比为 49.030 9 dB。因峰值信噪比大于 33 dB,就意味着人眼分辨不出原始载体图像和嵌入水印后载体图像的区别,说明 2 幅图像有良好的相似性。

现分别对嵌入水印的算法进行无攻击、高斯噪声、椒盐噪声、泊松噪声、斑点噪声、剪切攻击、旋转攻击,不同攻击下提取的水印也大不相同,如图 8 所示。

(a) 椒盐噪声攻击 (b) 泊松噪声攻击 (c) 高斯噪声攻击

(d) 斑点噪声攻击 (e) 剪切攻击 (f) 旋转攻击

图 8 各种攻击下提取水印恢复的效果

Fig. 8 The effect of extracting watermark recovery under various attacks

现将本文受到各类攻击后的峰值信噪比的值与文献[19]和文献[20]做对比,见表 2。研究中将分享图像 1 和受到各种攻击后提取出来的分享图像 1 计算出来的归一化相关系数与文献[19]和文献[20]做对比,见表 3。

表 2　受各类攻击后的峰值信噪比

Table 2　Peak signal-to-noise ratio after various attacks

攻击类型	峰值信噪比		
	本文	文献[15]	文献[16]
椒盐噪声	44.582 5	47.509 5	46.387 9
泊松噪声	48.185 1	47.322 5	46.975 8
斑点噪声	48.247 1	47.011 4	45.442 8
高斯噪声	48.382 3	47.338 0	45.277 3
剪切	47.819 0	47.029 9	45.353 2
旋转	47.581 8	47.573 4	45.497 0

表 3　受各类攻击后的归一化相关系数

Table 3　Normalized correlation coefficients after various attacks

攻击类型	归一化相关系数		
	本文	文献[15]	文献[16]
椒盐噪声	0.985 59	0.981 95	0.887 79
泊松噪声	0.987 31	0.986 75	0.887 40
斑点噪声	0.990 14	0.984 03	0.882 80
高斯噪声	0.992 76	0.990 98	0.877 06
剪切	0.983 29	0.982 50	0.868 23
旋转	0.954 15	0.988 74	0.867 53

6　结束语

本文将提升小波变换和主成分分析水印技术应用到了像素不扩展(2,2)视觉密码方案中，提出了基于 LWT-PCA 水印算法在视觉密码方案中的应用。不是传统意义上把水印图像直接嵌入到载体图像中，而是利用视觉密码方案拆分成了 2 幅分享图像，把其中 1 幅分享图像嵌入，只有 2 个叠加才可以恢复水印图像，有很好的保密效果，既保护了载体图像的隐私，又保护了水印图像的安全。该算法在受到各种攻击后，依然能很好地提出水印，这也说明算法具有很强的鲁棒性。

参考文献

[1] 吴德阳，张金羽，容武艳，等. 数字图像水印技术综述[J]. 高技术通讯，2021，31(2)：148-162.

[2] 郑秋梅，顾国民，王玉菲，等. 一种新的抗几何攻击的数字算法[J]. 中国石油大学学报(自然科学版)，2012，36(1)：188-192.

[3] 钟莉萍，李君，陈文庆. 数字水印综述[J]. 湛江师范学院学报，2004，25(3)：112-115.

[4] 陈松. 信息隐藏与数字水印技术研究[M]. 北京：新华出版社，2014.

[5] 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.

[6] 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.

[7] WANG Yong. Digital watermarking algorithm based on SVD and DWT [J]. Computer Simulation, 2011, 28 (5): 295-298.

[8] NASRIN M, BEE E K. A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition [J]. Digital Signal Processing, 2014, 33 (10): 134-147.

[9] LEI Baiying, SON I Y, ZHOU Feng, et al. A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition [J]. Signal Processing, 2012, 92 (9): 1985-2001.

[10] VIVEK S V, RAJIB K J, APARAJITA O. Significant region based robust watermarking scheme in lifting wavelet transform domain [J]. Expert Systems with Applications, 2015, 42 (21): 8184-8197.

[11] KUNCHEVA L I, FAITHFULL W J. PCA feature extraction for change detection in multiple unlabeled data [J]. IEEE Transactions on European Networks and Learning Systems, 2014, 25 (1): 69-80.

[12] NAOR M, SHAMIR A. Visual cryptography[C]//Advances in Cryptology—EUROCRYPT′94: Workshop on the Theory and Application of Cryptographic Techniques. Cham: Springer, 1995: 1-12.

[13] YANG C N. New visual secret sharing schemes using probabilistic method [J]. Pattern Recognition Letters, 2004, 25 (4): 481-494.

[14] 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.

[15] 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.

[16] 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.

[17] 高淼，王洪君. 基于视觉密码的 DWT-SVD 水印技术[J]. 智能计算机与应用，2021，11(8)：173-176，182.

[18] ZHENG Qiumei, JIN Xiao, GU Guomin, et al. A digital watermark algorithm based on data matrix [J]. Journal of China University of Petroleum (Edition of Natural Science), 2015, 39 (1): 188-193.

[19] 夏维伟，陈家琪. 基于分块的 DWT 和 PCA 图像水印算法[J]. 电子科技，2017，30(11)：96-99.

[20] 李伟，孙云娟. 基于 LWT-SVD-DCT 算法的水印技术[J]. 洛阳理工学院学报(自然科学版)，2021，31(1)：77-81.