文章编号：2095-2163(2024)03-0154-05 中图分类号：TP309.7；TP391.41 文献标志码：A

基于视觉密码和 DCT-SVD 彩色图像水印技术

孙 蕾，王洪君，刘鑫淇
（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视觉密码和 DCT-SVD 的彩色图像水印算法，通过视觉密码方案将彩色秘密水印图像拆分成 3 份与彩色秘密水印图像等大小的分享份图像，并利用待标记图像、水印图像和密钥生成验证信息和测试图像。由版权所有者提供水印图像和验证信息，密钥交由图像所有者保存。当要验证图像所有者的所有权时，会要求图像所有者提供密钥，结合密钥、测试图像和验证信息便可生成水印，若密钥正确，生成的水印可识别为原始水印。将其中一份分享份图像利用 DCT-SVD 水印算法嵌入到载体图像中并进行攻击测试，利用数字水印的提取算法将分享份图像从遭受常见攻击的载体图像中提取出来，与剩余分享份进行叠加恢复秘密水印图像。实验结果表明，水印具有良好的不可感知性和鲁棒性。

关键词：视觉密码；数字水印；可验证；彩色图像；DCT-SVD

Color image watermarking algorithm based on visual cryptography and DCT-SVD

SUN Lei, WANG Hongjun, LIU Xinqi
(College of Mathematics and Computer, Jilin Normal University, Siping 136000, Jilin, China)

Abstract: This article proposes a color image watermarking algorithm based on visual cryptography and DCT-SVD. The color secret watermark image is divided into three shared images of the same size as the color secret watermark image through a visual cryptography scheme. Verification information and test images are generated using the image to be labeled, watermark image, and the key. The watermark image and verification information are provided by the copyright owner, and the key is saved by the image owner. When verifying the ownership of the image owner, the image owner is required to provide a key, which can be combined with the key, test image, and verification information to generate a watermark. If the key is correct, the generated watermark can be recognized as the original watermark. One of the shared images are embedded into the carrier image using the DCT-SVD watermark algorithm and attack testing is conducted. Finally, the digital watermark extraction algorithm is used to extract the shared image from the carrier image that has been commonly attacked, and it is overlaied with the remaining shared images to recover the secret watermark image. The experimental results show that watermarks have good imperceptibility and robustness.

Key words: visual password; digital watermark; verifiable; color image; DCT-SVD

0 引 言

随着网络通信技术的成熟和媒体信息的数字化，数字信息也能方便和快速地通过电子设备传输，计算机的普及与应用使简单的复制粘贴就可以轻易篡改他人的创新成果，盗版现象、版权信息泄露的问题正日益凸显。保护研究者的创新成果已成为一个重要的问题，目前关于保护数字作品的产权，研究者们提出了许多技术方案，其中数字水印技术一直是保护知识产权的重要方法[1-2]。针对均匀量化算法容易造成非均匀分布载体信息局部失真的问题，李莹莹[3]研究了基于扩展变换的对数水印算法。杨永生[4]提出一种数字水印技术在高校秘密档案管理中的应用方法。杨娜娜[5]提出一种数字水印在矢量地图中的应用方法。在此基础上，傅楚君等学者[6]提出一种基于 DCT 离散余弦变换的数字水印算法，提高了数字水印的鲁棒性。饶俊慧等学者[7]提出了一种融合 DCT 离散余弦变换与 SVD 奇异值变换的半脆弱水印算法，解决了半脆弱水印的鲁棒性问题。而赵久影等学者[8]则致力于针对像素拓展度问题的研究提出了基于像素不扩展视觉密码的可逆水印方法。针对数字水印鲁棒性与透明性之间

作者简介：孙 蕾(1997-)，女，硕士研究生，主要研究方向：密码学、信息安全、视觉密码；刘鑫淇(1999-)，女，硕士研究生，主要研究方向：密码学、信息安全、视觉密码。
通讯作者：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、视觉密码。Email：jlnuwhj@ sina.com

收稿日期：2023-03-28

的问题，曲长波等学者[9-10]、李春艳[11]又提出了基于视觉密码和边缘检测的零水印算法。熊祥光[12]提出了一种空域强鲁棒零水印方案，用来解决空域水印的鲁棒性问题。李春艳[13]提出基于最高有效位(Most Significant Bit，MSB)的视觉密码零水印算法，提高了水印的安全性。近年来，数字水印技术被应用于视频版权保护领域并取得一定的效果，但在水印鲁棒性和视频透明性方面还需要加强。高鹏[14]针对鲁棒视频水印算法进行研究，提出鲁棒视频水印算法。数字水印技术应用于彩色图像版权保护领域的研究有了进一步扩展。吴军等学者[15]提出一种基于彩色图像的双重水印算法，在保证图像质量的前提下，可见水印具有较好的视觉可见性，不可见水印的抗几何攻击能力得到了提升。

本文基于有意义分享的视觉密码方案，将彩色水印图像分成 3 份有意义的分享份，并利用标记图像、密钥和彩色水印图像生成验证信息和测试图像；将 3 个分享份中的一幅分享份图像利用离散余弦变换(DCT)和奇异值分解(SVD)方法嵌入到载体图像中。在需要进行验证时，从载体图像中提取分享份图像，将提取出的分享份图像与其余 2 张分享份图像进行叠加，恢复水印图像；利用验证信息、密钥和测试图像进行判断是否能够识别出原始水印图像，用以验证图像所有者的所有权。

1　视觉密码

1.1　视觉密码概述

视觉密码(Visual Cryptography Scheme，VCS)最早是由 Shamir 和 Naor 正式提出，并形成一个新研究热点，涉及数学、密码学、信息论、概率论、计算复杂度理论和其他计算机应用技术等领域，具有自身独特的恢复简单性。视觉密码方案是将秘密图像根据规则拆分成 n 份分享份，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，就可实现秘密信息的恢复，而少于 K 个人的分享份叠加在一起得不到任何秘密信息[16]。参与者不需要学习复杂的密码学知识，依靠人类视觉系统就可以获取秘密信息。

1.2　(2,2)视觉密码方案

(2,2)视觉密码方案使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像素块、还是一个白像素块，在进行加密时分存图像都需要被一黑一白两个像素块表达，所以整体长度变宽。(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的大小一致，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

Table 1　(2, 2) encryption rules for pixel non-extended visual cipher scheme

秘密图像像素	分享份 1	分享份 2	叠加结果
□	■	■	□
	□	□	□
■	■	□	■
	□	■	■

2　离散余弦变换

离散余弦变换(Discrete Cosine Transform，DCT)是可分离的变换，变换核为余弦函数。DCT 除了有一般的正交性质外，其变换的基向量能很好地描述人类语音信号和图像信号的相关特征。因此，在对语音信号、图像信号的变换中，DCT 变换被认为是一种准最佳变换[17-18]。DCT 变换是以一组不同频率和幅值的余弦函数和来近似一幅图像，实际上是傅里叶变换的实数部分。离散余弦变换有一个重要的性质，即对于一幅图像，其大部分可视化信息都集中在少数的变换系数上。因此，离散余弦变换经常用于图像压缩，如国际压缩标准的 JPEG 格式中就采用了离散余弦变换。在傅里叶变换过程中，如果被展开的函数就是实偶函数，那么在其傅里叶变换中只包含余弦项，即离散余弦变换。DCT 变换先将图像函数变换成偶函数形式，再对其进行二维离散傅里叶变换，因此 DCT 变换可以看成是一种简化的傅里叶变换。

对于时间序列 $f(x)$，这里，$x = 0,1,\cdots,N-1$，其一维离散余弦变换的定义，见式(1)：

$$F(u) = \alpha_0 c(u) \sum_{x=0}^{N-1} f(x) \cos \frac{(2x+1)u\pi}{2N} \quad (1)$$

其中，$u = 0,1,\cdots,N-1$，$\alpha_0 = \dfrac{2}{\sqrt{N}}$，$c(u) = \begin{cases} \dfrac{1}{\sqrt{2}}, & u = 0 \\ 1, & u \neq 0 \end{cases}$

一维离散余弦反变换的定义，可写为：

$$f(x) = \alpha_1 \sum_{u=0}^{N-1} c(u) F(u) \cos \frac{(2x+1)u\pi}{2N} \quad (2)$$

3 奇异值分解

奇异值分解(SVD)是对矩阵进行分解,但是和特征分解不同,SVD 并不要求分解的矩阵为方阵。在 SVD 中对于一个 $m \times n$ 大小的矩阵,可以定义矩阵的 SVD 数学公式为:

$$A = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{T}} \tag{3}$$

其中,$\boldsymbol{U}$ 是一个 $m \times n$ 矩阵;$\boldsymbol{\Sigma}$ 是一个 $m \times n$ 矩阵,除主对角线上的元素外全为 0,主对角线上的每个元素都为奇异值;$\boldsymbol{V}$ 是一个 $n \times n$ 的矩阵;$\boldsymbol{U}$ 和 $\boldsymbol{V}$ 满足 $\boldsymbol{U}^{\mathrm{T}}\boldsymbol{U} = \boldsymbol{I}$, $\boldsymbol{V}^{\mathrm{T}}\boldsymbol{V} = \boldsymbol{I}$。

4 水印算法

4.1 水印的生成和添加

利用有意义分享的(3,3)视觉密码方案,以二进制形式对彩色水印图像进行读取并生成 3 份分享份,再进行初始化,使水印图像的像素存储在这 3 个共享份中。读取标记图像,将待标记的 RGB 图像压缩成与 3 个共享份相对应的颜色,为每个图像流分别使用 3 个水印分享份产生 3 个验证矩阵;接收输入参数,即要标记的图像、水印和秘钥,再返回验证矩阵;用随机生成器的种子传递密钥,对验证矩阵初始化并计算验证矩阵,所有验证图像存储在一个 RGB 图像中,形成水印分享份。选取其中一张分享份图像嵌入到载体图像中,嵌入时采用 DCT-SVD 的嵌入方式,具体嵌入步骤如下:

(1)对 64×64 像素大小的水印图像进行猫脸变换,得到置乱后的水印图像 $\boldsymbol{M}'$;

(2)对 512×512 像素大小的载体图像分割成互不重叠的 8×8 的小方块后对每个小块进行 *DCT* 离散余弦变换,取变换矩阵中的中频系数构成 4×4 的矩阵 $\boldsymbol{B}_{ij}(i = 1,2,\cdots\cdots,m;\ j = 1,2,\cdots\cdots,n)$;

(3)对 $\boldsymbol{B}_{ij}$ 矩阵进行奇异值分解 *SVD*,取得最大的奇异值构成矩阵 $\boldsymbol{A}$,再对 $\boldsymbol{A}$ 进行奇异值分解;

(4)将置乱后的水印图像矩阵 $\boldsymbol{M}'$ 叠加到矩阵 $\boldsymbol{S}$ 上,其嵌入公式如下所示:

$$\boldsymbol{D} = \boldsymbol{S} + \alpha\boldsymbol{W}' \tag{4}$$

$$\boldsymbol{D} = \boldsymbol{U}_1\boldsymbol{S}_1\boldsymbol{V}_1^{\mathrm{T}} \tag{5}$$

$$\boldsymbol{A}' = \boldsymbol{U}\boldsymbol{S}_1\boldsymbol{V}^{\mathrm{T}} \tag{6}$$

(5) 将 $\boldsymbol{A}'$ 中相应的元素替换 $\boldsymbol{B}_{ij}$ 中的最大奇异值,将变换后的中频系数矩阵 $\boldsymbol{B}_{ij}$ 还原到相应的块中;

(6)对每一块嵌入了水印信息的矩阵进行逆 *DCT* 变换,最后得到嵌入了水印图像信息的图像 $\boldsymbol{I}'$。

4.2 水印的验证和提取

首先,读取测试图像,根据颜色分流将测试图像分成 3 份,读取验证图像,生成验证息;接受输入参数,即测试图像、验证矩阵和密钥,再返回测试水印;利用随机数生成测试水印矩阵,随机数生成的种子可产生随机数阵列,计算测试水印矩阵;最后,读取秘密传递密钥后验证是否可识别出原始水印。对嵌入到载体图像中的水印分享份图像进行提取,水印提取算法步骤如下:

(1)将嵌入水印图像后的载体图像 $\boldsymbol{I}'$ 分成 8×8 的小块,并对每一个小块进行 *DCT* 离散余弦变换;

(2)获取每一块中的 16 个中频系数,构成矩阵 $\boldsymbol{B}_{ij}'$,然后对其进行奇异值分解 *SVD*,取最大奇异值构成矩阵 $\boldsymbol{A}'$;

(3)设需要提取的水印图像为 $\boldsymbol{W}'$,提取公式为:

$$\boldsymbol{A} = \boldsymbol{U} * \boldsymbol{S} * \boldsymbol{V} * \boldsymbol{T} \tag{7}$$

$$\boldsymbol{D} = \boldsymbol{U}_1 * \boldsymbol{S}_1 * \boldsymbol{V}_1^{\mathrm{T}} \tag{8}$$

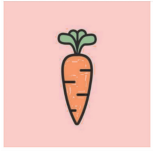
$$\boldsymbol{W}' = (\boldsymbol{D} - \boldsymbol{S})/\alpha \tag{9}$$

(4)将提取出来的水印图像经过猫脸逆变换,得到水印图像。

5 仿真实验和安全性分析

以 *Matlab*2020*a* 为实验平台对本文算法进行了实验验证和各种攻击测试,实验采用 768×1024 和 512×512 大小的彩色图像作为标记图像、彩色水印图像,载体图像为测试图像,如图 1 所示。

(a) 待标记图像 768×1024 Baboon.jpg



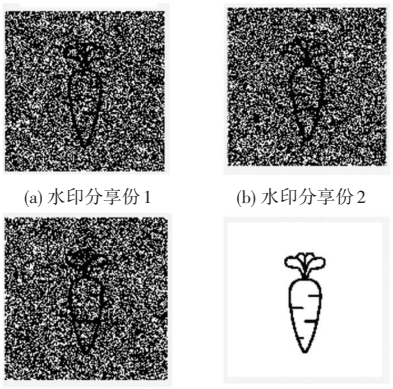
(b) 水印图像 512×512 4.jpg

(c) 原载体图像

图 1 本文实验所用测试图像

Fig. 1 Test images used in the experiments of this paper

水印图像基于有意义共享的(3,3)视觉密码方案生成的 3 张分享份图像和分享份叠加后所得到的水印图像,如图 2 所示。

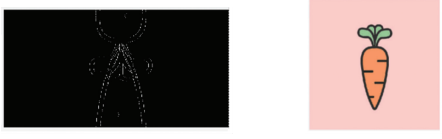


(a) 水印分享份 1　(b) 水印分享份 2　(c) 水印分享份 3　(d) 水印分享份叠加后图像

图 2　视觉密码方案生成的水印分享份及叠加后恢复的水印图像

Fig. 2　Watermark share copies generated by the visual password scheme and the recovered watermark image after overlaying

实验过程中得到的测试水印和利用测试水印、验证图像恢复的原始水印图像如图 3 所示。

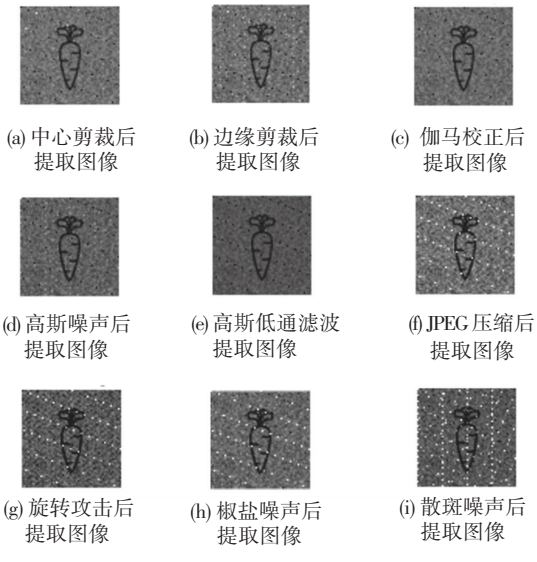


（a）测试水印　（b）原始水印

图 3　测试水印和验证后得到的原始水印图像

Fig. 3　Test watermark and original watermarked image obtained after verification

对嵌入水印后的载体图像进行了椒盐噪声、中心剪裁等攻击后进行水印分享份的提取结果如图 4 所示。



(a) 中心剪裁后提取图像　(b) 边缘剪裁后提取图像　(c) 伽马校正后提取图像

(d) 高斯噪声后提取图像　(e) 高斯低通滤波提取图像　(f) JPEG 压缩后提取图像

(g) 旋转攻击后提取图像　(h) 椒盐噪声后提取图像　(i) 散斑噪声后提取图像

图 4　遭受各种攻击测试后提取的水印分享份图像

Fig. 4　Watermarked share image extracted after being tested with various attacks

受攻击后提取的水印分享份图像与剩余分享份进行叠加后的实验结果如图 5 所示。

(a) 边缘剪裁叠加结果　(b) 椒盐噪声叠加结果　(c) 中心剪裁叠加结果

(d) 散斑噪声叠加结果　(e) 旋转攻击叠加结果　(f) 压缩攻击叠加结果

(g) 高斯低通滤波叠加结果　(h) 高斯噪声叠加结果　(i) 中心剪裁叠加结果

图 5　攻击测试后提取的水印分享份图像与剩余分享份叠加结果

Fig. 5　Results of overlaying the extracted images of watermarked shares with the remaining shares after the attack test

由以上仿真实验结果可知，当载体图像分别遭受旋转攻击、JPEG 压缩攻击、中心剪裁攻击、及边缘剪裁攻击、高斯低通滤波攻击、椒盐噪声和高斯噪声等攻击下提取出的水印图像同嵌入水印图像之间没有明显区别，证明水印图像能够抵抗常见的攻击，有良好鲁棒性。

利用归一化系数（*NC* 值）和结构相似数（*SSIM* 值）来评估提取的图像与原始图像相互间的差异，归一化系数（*NC* 值）的数学表达式为：

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)W'(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W'(i,j)}} \tag{10}$$

其中，原始水印中像素以 $W(i,j)$ 为单位，所提取水印的像素以 $W'(i,j)$ 为单位。

研究可知，*NC* 值愈趋近 1，说明 2 张图像越相似。

给定 2 张图像为 X、Y，这 2 张图像在结构上的相似性可用式(11)求得：

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + u_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{11}$$

其中，μ_x 表示衡量图像 x 的亮度；μ_y 表示衡量图像 y 的亮度；σ_x 表示衡量图像 x 的对比度；σ_y 表示衡量图像 y 的对比度；σ_{xy} 表示衡量 x、y 两张图像的结构对比。

结构相似性范围在 −1 至 1 之间，在 2 张图像完

全相同的情况下,*SSIM* 等于 1。

嵌入之前的水印图像和在受到攻击后提取的水印 BG 图像及原始载体图像与嵌入水印后的载体图像计算得到 *NC* 值和 *SSIM* 值见表 2。

表 2 常见攻击

Table 2 Common attacks

攻击类型	水印图像 *NC* 值	水印图像 *SSIM* 值	载体图像 *NC* 值	载体图像 *SSIM* 值
椒盐噪声	0.962 4	0.903 2	0.997 5	1.000 0
JPEG 压缩	0.965 2	0.906 0	0.998 1	0.999 1
中心剪裁	0.991 6	0.899 9	0.977 4	0.999 5
边缘剪裁	0.984 1	0.903 7	0.903 0	0.997 3
伽马校正	0.994 8	0.999 0	0.998 1	0.995 9
高斯噪声	0.987 5	0.900 1	0.998 2	0.999 1
高斯低通滤波	0.992 2	0.999 3	0.999 8	0.999 6
旋转攻击	0.938 3	0.901 8	0.832 2	0.992 2
散斑噪声	0.908 7	0.906 7	0.976 7	0.996 3

由表 2 可知,2 张水印图像和载体图像计算的 *NC* 值和 *SSIM* 值都接近 1,表明水印能够抵抗伽马校正、散斑噪声、椒盐噪声等攻击,说明载体图像的感知质量较好,水印鲁棒性较强。

6 结束语

本文提出了一种基于视觉密码和 DCT-SVD 的彩色图像水印算法,通过视觉密码方案将彩色秘密水印图像拆分成 3 份与彩色秘密水印图像等大小的分享份图像,并利用待标记图像、水印图像和密钥生成验证信息和测试图像。利用密钥、测试图像和验证信息便可生成水印,若密钥正确,则生成的水印可识别为原始水印。选取其中一份分享份图像利用 DCT-SVD 水印算法嵌入到载体图像中并进行攻击测试,最后利用数字水印的提取算法进行水印的提取。实验结果表明,在遭受常见攻击后提取出的水印分享份图像,与剩余分享份进行叠加仍能恢复秘密水印图像,遭受攻击后提取的水印分享份图像与原水印分享份图像的 *NC* 值和 *SSIM* 值很接近 1,相似度较高。

参考文献

[1] 吴海涛,詹永照. 数字水印技术综述 [J]. 软件导刊,2015, 14 (8): 45-49.

[2] 赵博. 基于数字水印的图像内容认证研究[D]. 长春:吉林大学, 2018.

[3] 李莹莹. 基于扩展变换的数字水印算法研究[D]. 南京:东南大学, 2018.

[4] 杨永生. 数字水印技术在高校秘密档案管理中的应用[J]. 长春工程学院学报(自然科学版),2022,23(1):96-99.

[5] 杨娜娜. 数字水印技术在矢量地图中的应用[J]. 地理空间信息,2022,20(2):114-118,122.

[6] 傅楚君,兰胜坤. 基于 DCT 变换的数字水印算法[J]. 网络安全技术与应用,2020(7):49-51

[7] 饶俊慧,吴晓云. 融合 DCT 与 SVD 的半脆弱图像水印算法研究[J]. 计算机仿真,2022,39(7):507-511.

[8] 赵久影,王洪君. 基于像素不扩展视觉密码的可逆水印[J]. 智能计算机与应用,2020,10(1):80-83.

[9] 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.

[10] 曲长波,杨晓陶,袁铎宁. 平衡多小波视觉密码零水印算法[J]. 计算机工程,2014,40(9):178-182.

[11] 李春艳. 基于图像边缘信息的视觉密码零水印算法[J]. 软件导刊,2016,15(3):178-180.

[12] 熊祥光. 空域强鲁棒零水印方案[J]. 自动化学报,2018,44(1):160-175.

[13] 李春艳. 基于 MSB 的视觉密码零水印算法[J]. 大理学院学报,2015,14(12):26-29.

[14] 高鹏. 鲁棒视频水印算法的相关研究[D]. 杭州:杭州电子科技大学, 2018.

[15] 吴军,孙像君,李慧慧. 一种基于彩色图像的双重水印算法 [J]. 电视技术, 2018, 42 (2): 101-109,114.

[16] NAOR M, SHAMIR A. Visual cryptography[M]//De SANTIS A. Advances in Cryptology—Proceedings of Eurocrypt. Heidelberg:Springer,1995:1-12.

[17] 张亚峰,何丹丹,李宁. 基于 DCT 算法的数字水印技术研究[J]. 精密制造与自动化, 2018 (4): 14-16.

[18] 韦晓林. 基于 DCT 的数字水印改进算法 [J]. 电子产品世界, 2019, 26(2): 88-90.

[19] 石杰. 基于 DCT 域的 JPEG 图像数字水印算法[D]. 北京:北京印刷学院, 2019.

[20] 陈小娥. 基于 Arnold 和 DCT 变换的鲁棒性图像数字水印算法[J]. 湖州师范学院学报, 2018, 40 (10): 24-29.