

一种基于改进奇异值和子块映射的图像零水印技术

吴德阳^{1,5}, 赵静^{1,5***}, 汪国平^{2,4*}, 张晓丹^{1,5}, 李胜^{2,4}, 唐勇^{1,5**}, 曲长波³

¹燕山大学信息科学与工程学院, 河北 秦皇岛 066004;

²北京大学信息科学技术学院, 北京 100871;

³辽宁工程技术大学软件学院, 辽宁 葫芦岛 125105;

⁴北京大学北京市虚拟仿真与可视化工程中心, 北京 100871;

⁵河北省计算机虚拟技术与系统集成重点实验室, 河北 秦皇岛 066004

摘要 为了解决奇异值最高位在几何攻击下易敏感性和零水印抗几何攻击性能差的问题, 提出一种基于改进奇异值和子块映射的图像零水印技术。首先, 对载体图像进行 Arnold 置乱处理, 消除像素间的相关性。然后, 进行 Curvelet 变换、分块以及奇异值分解以获得载体图像的稳定特征。同时, 提出一种子块映射机制, 将原始的版权图像划分成不同的子块, 并通过子块求和, 使用不同的字符表示水印子块。最后, 将载体图像的特征与水印子块按位进行逻辑运算生成零水印。实验结果表明, 所提出的图像零水印算法在几何攻击、非几何攻击以及组合攻击下具有很强的鲁棒性, 并且生成的零水印信息安全性更高。

关键词 图像处理; 图像零水印; 奇异值分解; 子块映射; 数字水印

中图分类号 TP391

文献标志码 A

doi: 10.3788/AOS202040.2010002

An Image Zero Watermarking Technology Based on Ameliorated Singular Value and Subblock Mapping

Wu Deyang^{1,5}, Zhao Jing^{1,5***}, Wang Guoping^{2,4*},

Zhang Xiaodan^{1,5}, Li Sheng^{2,4}, Tang Yong^{1,5**}, Qu Changbo³

¹College of Information Science and Engineering, Yanshan University, Qinhuangdao, Hebei 066004 China;

²School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China;

³College of Software, Liaoning Technical University, Huludao, Liaoning 125105, China;

⁴Beijing Engineering Technology Research Center of Virtual Simulation and Visualization, Peking University, Beijing 100871, China;

⁵Key Laboratory for Computer Virtual Technology and System Integration of Hebei Province, Qinhuangdao, Hebei 066004

Abstract In order to solve the problem of the sensitivity of the highest singular value bit under geometric attack and the poor anti-geometric attack performance of zero watermark, an image zero watermarking technology based on ameliorated singular value and sub-block mapping is proposed. Firstly, the carrier image was Arnold scrambled to eliminate the correlation between pixels, and then Curvelet transformation, partitioning and singular value decomposition were performed to obtain the stable characteristics of the carrier image. At the same time, a seed block mapping mechanism is proposed to divide the original copyright image into different sub-blocks, and by summing the sub-blocks, different characters are used to represent the water imprint block. Finally, the feature of the carrier image and the water imprint block are logically calculated to generate zero watermark by bit. Experimental results show that the proposed zero-watermarking algorithm has strong robustness under geometric attack, non-geometric attack and combined attack, and the generated zero-watermark information is more secure.

Key words image processing; image zero watermarking; singular value decomposition; sub-block mapping; digital

收稿日期: 2020-05-08; 修回日期: 2020-06-23; 录用日期: 2020-07-06

基金项目: 国家自然科学基金面上项目(61872398, 61632003)、国家自然科学基金(61902340)、河北省自然科学基金(F2018203060)、秦皇岛市科学技术研究与发展计划项目(201602A018)

* E-mail: wgp@pku.edu.cn; ** E-mail: tangyong@ysu.edu.cn; *** E-mail: zhaojing@ysu.edu.cn

watermarking

OCIS codes 100.2000; 110.3055; 110.7410

1 引 言

随着信息技术的飞速发展,数字信息越来越丰富,如文本、音频、图像、视频等,使数据的存储和传输更加方便、快捷。同时,数字图像作为可视化的信息,被广泛应用于通信、信息隐藏等领域,但许多违法者经常使用图像编辑软件对图像信息进行恶意篡改,破坏了原始图像的版权和内容信息。因此,对数字图像的版权保护和信息安全进行研究具有重要的意义^[1-2]。同时,随着网络环境越来越复杂,如何在大强度攻击下提取清晰的版权信息也是数字水印技术所面临的挑战。

传统的数字水印技术主要将版权信息嵌入宿主图像的不可见域中,以达到信息隐藏的目的^[3],当发生版权纠纷时,再通过嵌入算法的逆操作提取版权信息进行版权认证。如 Jane 等^[4]直接将版权水印的奇异值信息嵌入到载体图像的低频域的奇异值上,由于奇异值具有很好的旋转不变性,因此对于常规攻击具有较好的鲁棒性,但该方法在认证过程中需要额外的水印信息才能提取完整的版权图像。而 Thanki 等^[5]通过量化的方式将置乱后的水印信息全部嵌入载体图像的小波系数的水平子带。该方法在版权认证阶段,不需额外的水印信息,认证过程比非盲水印更方便。但由于需要嵌入的水印信息量较大,因此会影响载体图像的透明性。

由于在数字图像中嵌入版权水印会破坏图像的透明性与鲁棒性之间的平衡,也无法保证图像的内容完整性。为此,温泉等^[6]提出零水印的概念,其基本思想是通过提取载体图像的特征,并将其与版权水印进行逻辑运算生成零水印信息,最后将零水印信息注册到版权保护中心。由于零水印技术不需要将版权水印嵌入到载体图像中,在解决版权纠纷问题的同时,还满足了图像信息内容完整性的要求。因此被广泛应用于医疗图像、军事地图、文本等领域的版权保护^[7-8]。现有零水印分为两类,一类是空域零水印,另一类是频域零水印。空域零水印主要利用图像的空间结构特点生成零水印信息。如 Ghadi 等^[9]直接对载体图像进行分块操作,然后计算块均值与整体均值的差值作为雅可比矩阵的输入,用于生成零水印信息。文献^[10-11]利用每一子块的最大奇异值和整体奇异值的均值之间的关系构造特征

矩阵,然后与版权水印生成零水印。由于添加性的攻击对于上述的空间关系是同步变化的,因此在抵抗非几何攻击上表现出较强的鲁棒性。而频域零水印,主要利用离散小波变换(DWT)^[12]、离散余弦变换(DCT)^[13]、Curvelet 变换等将图像空间信息转换成频域信息,然后再选择低频子带进行奇异值分解(SVD)^[14],生成特征矩阵。如 2015 年,Rani 等^[15]将 DWT 应用于每一子块来提取低频子带,同时利用奇异值分解对每一子块的低频子带进行分解,并通过最大奇异值构造特征矩阵,该算法对于常规的图像处理操作得到的水印图像清晰度较好,但对于旋转攻击,最大奇异值突变较大,因此,无法提取清晰的版权图像。2015 年,Waleed 等^[16]将二维码(QR 码)分别与低频信息和 DCT 系数产生两个密钥图份,直接将载体图像与两个密钥信息进行异或运算提取水印图像,该算法对于小范围可以提取清晰度较好的 QR 码水印。但存在两个不足:1) 当载体图像受到较大强度的攻击时,QR 码破坏严重,无法被移动设备识别,导致版权认证失败;2) 算法直接将载体图像的 4 级低频子带作为特征信息与 QR 码进行异或运算,当受到几何攻击时,会导致整体的特征信息发生变化,进而影响算法的鲁棒性。2017 年,Thanh 等^[17]利用一维 DCT 系数构造载体的特征矩阵,并直接与版权水印生成零水印信息。该算法中的水印信息并未进行加密处理,安全性较低,且利用 DCT 系数的关系构造的特征矩阵,在大强度攻击下鲁棒性较差。

本文研究奇异值分解的稳定性及信息加密规则的安全性,提出一种基于改进奇异值和子块映射的新型零水印技术。将改进后的奇异值分解用于提取载体图像的特征矩阵;并提出一种新的加密方法,将版权信息的 2×2 子块元素直接映射成一个 ASCALL 值。由于现有的图像零水印在几何攻击下,空间关系构造的特征矩阵容易发生变化;且在单独使用 DWT、Curvelet 变换时,得到的特征表征能力较弱,进而影响了算法的鲁棒性能,难以保证在复杂环境下版权的清晰度。同时,常用的加密规则大多为打乱图像元素的位置关系,安全性较差。因此本文通过改进传统奇异值分解以及耦合 Curvelet、DWT 来解决最高位敏感性问题。同时提出一种新的加密方法来提高版权信息的安全性。

2 一种基于改进奇异值和子块映射的图像零水印技术

2.1 改进奇异值分解

改进奇异值分解(ASVD)是在传统SVD的基础上进行改进的一种矩阵分解工具,ASVD直接将图像分解为三个矩阵相乘,其中在奇异值矩阵引入一个调控因子 α ,用于控制奇异值的变化,具体表达式为

$$\mathbf{I} = \mathbf{U}\mathbf{\Sigma}^\alpha\mathbf{V}^T, \quad (1)$$

$$\mathbf{\Sigma}^\alpha = \begin{bmatrix} \lambda_{1,1}^\alpha & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & \lambda_{n,n}^\alpha \end{bmatrix}, \quad (2)$$

式中: \mathbf{I} 为载体图像; \mathbf{U} 为左奇异矩阵; $\mathbf{\Sigma}$ 为奇异值矩阵; \mathbf{V}^T 为转置右奇异值矩阵; α 为调控因子; λ 为奇异值,且 $\lambda_{1,1} \geq \lambda_{2,2} \geq \cdots \geq \lambda_{n,n}$ 。

2.2 图像信号处理对奇异值稳定性的影响

几何攻击往往对图像像素的几何位置造成很大的影响,在构造受攻击载体的特征矩阵时仍使用SVD对同一位置分解,就会导致奇异值波动大的情形,载体在受到攻击后奇异值的稳定性决定着零水印的稳定性和唯一性。为此在构造零水印之前,对信号处理与奇异值变化的关系进行分析。假设 \mathbf{I} 为原始载体图像, \mathbf{I}' 为受攻击的载体图像,大小均为 $M \times N$, i 和 j 为图像索引, C 为载体图像 \mathbf{I} 受攻击前后的变化率,计算表达式为

$$C = \frac{\sum_{i=1}^M \sum_{j=1}^N |\mathbf{I}_{i,j} - \mathbf{I}'_{i,j}|}{M \times N} \times 100\%。 \quad (3)$$

将图像的最大奇异值 λ_{\max} 表征图像的重要信息,并通过最大奇异值的变化来反映图像受攻击的强度,用 λ_{\max} 代替(3)式中的 $\mathbf{I}_{i,j}$,得到新的表达式,即

$$C = \frac{|\lambda_{\max} - \lambda'_{\max}|}{M \times N} \times 100\%, \quad (4)$$

式中: λ_{\max} 为攻击前的最大奇异值; λ'_{\max} 为攻击后的最大奇异值;当 $\lambda'_{\max} = \lambda_{\max}$ 时,表明攻击后的图像与原始图像具有同样的特征,而当 $\lambda'_{\max} = 0$ 时,最大奇异值的变化率最大。

为了证实本文ASVD比传统SVD在稳定性上的优越性,假设 λ_{\max}^α 和 λ_{\max} 分别为载体图像攻击前使用ASVD和SVD得到的最大奇异值, λ_{\max}^α 和 λ_{\max} 为载体图像受攻击后分别使用ASVD和SVD得到的最大奇异值,令

$$\begin{cases} b_1 = \lambda_{\max}^\alpha - \lambda_{\max} \\ b_2 = \lambda_{\max} - \lambda_{\max} \end{cases}, \quad (5)$$

式中: b_1 可以简化成如下形式,

$$b_1 = (\lambda_{\max} - \lambda_{\max}) \left(\lambda_{\max}^{\alpha-1} + \lambda_{\max}^{\alpha-2} \lambda_{\max}^1 + \cdots \lambda_{\max} \lambda_{\max}^{\alpha-2} + \lambda_{\max}^{\alpha-1} \right)。 \quad (6)$$

$$\text{同时令 } b_n = \left(\lambda_{\max}^{\alpha-1} + \lambda_{\max}^{\alpha-2} \lambda_{\max}^1 + \cdots \lambda_{\max} \lambda_{\max}^{\alpha-2} + \lambda_{\max}^{\alpha-1} \right),$$

$$b_1 = (\lambda_{\max} - \lambda_{\max}) b_n = b_2 b_n。 \quad (7)$$

由于 $0 < \alpha < 1$,则 $b_n < 1$,所以 $b_1 < b_2$ 。将(7)式代入(4)式,则有

$$\begin{cases} C_{\text{ASVD}} = \frac{|b_2 b_n|}{M \times N} \times 100\% \\ C_{\text{SVD}} = \frac{|b_2|}{M \times N} \times 100\% \end{cases}, \quad (8)$$

式中: C_{ASVD} 为使用ASVD得到的变化率; C_{SVD} 为使用SVD得到的变化率。将两者作差,得到

$$C_{\text{ASVD}} - C_{\text{SVD}} = \frac{|b_2 b_n| - |b_2|}{M \times N} < 0。 \quad (9)$$

综上所述,证明ASVD的变化率要比SVD的小,即ASVD的稳定性比SVD更优。

2.3 子块映射

为了进一步提高算法的安全性和透明性,本文将原有的版权图像进行分块映射,用一个字符表示原始版权信息 2×2 的像素,并将字符转换成ASCALL码,构成映射后的水印信息,具体步骤如下。

步骤1:将大小为 $m \times n$ 的版权水印 \mathbf{w} 按 2×2 个像素划分,记每一子块为 \mathbf{b}^k , k 为子块的个数,划分方式为

$$\mathbf{b}^k = \mathbf{w} / (2 \times 2), \quad k = 1, 2, \dots, m/2。 \quad (10)$$

步骤2:定义子块水印与原始水印之间的映射关系,构造映射矩阵,在 2×2 子块中包含4个“0”的情形仅有一种;子块包含1个“1”的情形则有 C_4^1 种;子块包含2个“1”的情形则有 C_4^2 种;子块包含3个“1”的情形则有 C_4^3 种;子块包含4个“1”的情形则有1种。如下式所示。

$$\mathbf{b}^k = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad k = 1, \quad (11)$$

$$\mathbf{b}^k = \begin{cases} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, & k = 2 \\ \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, & k = 3 \\ \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, & k = 4 \\ \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, & k = 5 \end{cases}, \quad (12)$$

$$\mathbf{b}^k = \begin{cases} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, & k=6 \\ \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, & k=7 \\ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, & k=8 \\ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, & k=9 \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & k=10 \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, & k=11 \\ \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, & k=12 \\ \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, & k=13 \\ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, & k=14 \\ \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, & k=15 \\ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, & k=16. \end{cases}, \quad (13)$$

$$\mathbf{b}^k = \begin{cases} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, & k=12 \\ \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, & k=13 \\ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, & k=14 \\ \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, & k=15 \end{cases}, \quad (14)$$

$$\mathbf{b}^k = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad k=16. \quad (15)$$

步骤 3: 将每个子块映射成一个字符元素, 对划

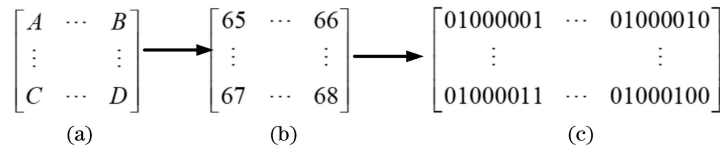


图 1 版权水印预处理过程

Fig. 1 Preprocessing process of copyright watermark

图 1(a)到图 1(b)过程是将字符转换成相应的 ASCII 值, 再将其转换成二进制信息, 特征信息的预处理过程与水印的预处理过程相似。这种预处理方式的特点在于不会损失原有的特征信息, 保留了原有的内容, 同时可以方便构造灰度或彩色零水印。

3 构造零水印与提取版权水印

3.1 构造零水印

假设载体图像 \mathbf{I} 大小为 $M \times N$, 版权标识 w 大小为 $m \times n$ 。在构造零水印之前需要提取载体图像的特征矩阵, 并将预处理过的版权信息与特征矩阵按位进行异或运算生成零水印信息, 如图 2(a) 所示。生成零水印的具体步骤如下。

步骤 1: 为了消除图像像素之间的相关性, 将载体图像 \mathbf{I} 进行 Arnold 置乱^[18], 得到置乱后的载体

分的子块元素进行求和, 并根据子块元素的和表示成一个字符, 具体转换过程为

$$\sum_{i=1}^2 \sum_{j=1}^2 \mathbf{b}_{i,j}^k = 0 \rightarrow A, \quad (16)$$

$$\sum_{i=1}^2 \sum_{j=1}^2 \mathbf{b}_{i,j}^k = 1 \rightarrow \{B, C, D, E\}, \quad (17)$$

$$\sum_{i=1}^2 \sum_{j=1}^2 \mathbf{b}_{i,j}^k = 2 \rightarrow \{F, G, H, I, J, K\}, \quad (18)$$

$$\sum_{i=1}^2 \sum_{j=1}^2 \mathbf{b}_{i,j}^k = 3 \rightarrow \{L, M, N, O\}, \quad (19)$$

$$\sum_{i=1}^2 \sum_{j=1}^2 \mathbf{b}_{i,j}^k = 4 \rightarrow P, \quad (20)$$

式中: i 和 j 为矩阵索引; $k = \{1, 2, \dots, 16\}$ 。

步骤 4: 通过上述子块划分和映射, 将原有版权图像中的 2×2 矩阵像素用一个字符进行表示, 并将映射后的字符转换成 ASCII 码, 用于生成映射后的水印信息。

2.4 特征矩阵与水印图像预处理

由于版权水印经过子块映射后得到版权信息为十进制的灰度图像, 无法直接进行逻辑运算, 为此, 需要将特征矩阵和版权信息进行预处理。同时, 为了构造唯一性强的特征矩阵, 本文直接将每个子块的最大奇异值构造成载体图像的特征矩阵。水印图像预处理过程如图 1 所示。

图像 \mathbf{I}_1 , 置乱方式如下

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod(N), \quad (21)$$

式中: x_1 和 y_1 为置乱后的像素; x 和 y 为原始像素; N 为图像大小。

步骤 2: 将置乱后的载体图像 \mathbf{I}_1 进行 Curvelet 变换获得 Curvelet 的低频信息 I_{cA} , 大小为 $\frac{M}{2} \times \frac{N}{2}$, 并对低频信息 I_{cA} 进行子块划分, 得到各个低频子块 $\mathbf{B}_{i,j}$, 即为

$$\mathbf{B} = I_{cA} / (8 \times 8), \quad i, j \in \{1, 2, \dots, m\}. \quad (22)$$

步骤 3: 将 \mathbf{B} 进行 DWT 变换获得每一子块的小波域低频信息 I_{ccA} 。

步骤 4: 对偶数的低频子块 I_{ccA} 进行 ASVD, 并提取每个子块的最大奇异值 λ^a , 分解方式为

$$\lambda^\alpha = \text{ASVD}(I_{\text{ccA}}), \quad (23)$$

式中: $i, j \in \{2, 4, 6, \dots, 32\}$; α 为调控因子。

步骤 5: 将每一子块的最大奇异值 $\lambda_{i,j}^\alpha$ 构造成为特征矩阵 \mathbf{T} , 大小为 $\frac{m}{2} \times \frac{n}{2}$, 构造方式为

$$\mathbf{T} = \begin{bmatrix} \lambda_{1,1}^\alpha & \cdots & \lambda_{1,\frac{n}{2}}^\alpha \\ \vdots & & \\ \lambda_{\frac{m}{2},1}^\alpha & \cdots & \lambda_{\frac{m}{2},\frac{n}{2}}^\alpha \end{bmatrix}. \quad (24)$$

步骤 6: 将版权图像 w 按照 2.3 节和 2.4 节中的方法进行预处理, 得到预处理后的版权信息 w'_b , 并将特征矩阵 \mathbf{T} 按 2.4 节方式进行处理, 得到处理后的特征矩阵 \mathbf{T}_b , 最后将 \mathbf{T}_b 与 w'_b 按位进行逻辑操作生成零水印信息 \mathbf{Z} , 并将生成的零水印信息注册到版权保护中心, 运算方式为

$$\mathbf{Z} = \text{xor}(\mathbf{T}_b, w'_b), \quad (25)$$

式中: $b \in \{1, 2, \dots, 8\}$ 为字节位。

3.2 版权认证

版权认证过程与零水印构造过程相似, 因此在认证阶段需要提取攻击后载体图像的特征矩阵与零水印进行逻辑运算, 提取原始的版权水印, 大致过程如图 2(b) 所示。提取版权水印的具体步骤如下。

步骤 1: 将受攻击后的载体图像进行 3.1 节中步骤 1~5 的操作, 得到受攻击后的特征矩阵 \mathbf{T}' 。

步骤 2: 将得到的特征矩阵 \mathbf{T}' 与零水印 \mathbf{Z} 按照 (25) 式进行逻辑运算, 提取版权信息 w' 。

步骤 3: 由于步骤 2 提取的版权信息 w' 由字符的 ASCALL 码表示, 因此需要根据子块映射机制的逆操作将其还原成原始的版权信息 w' 。

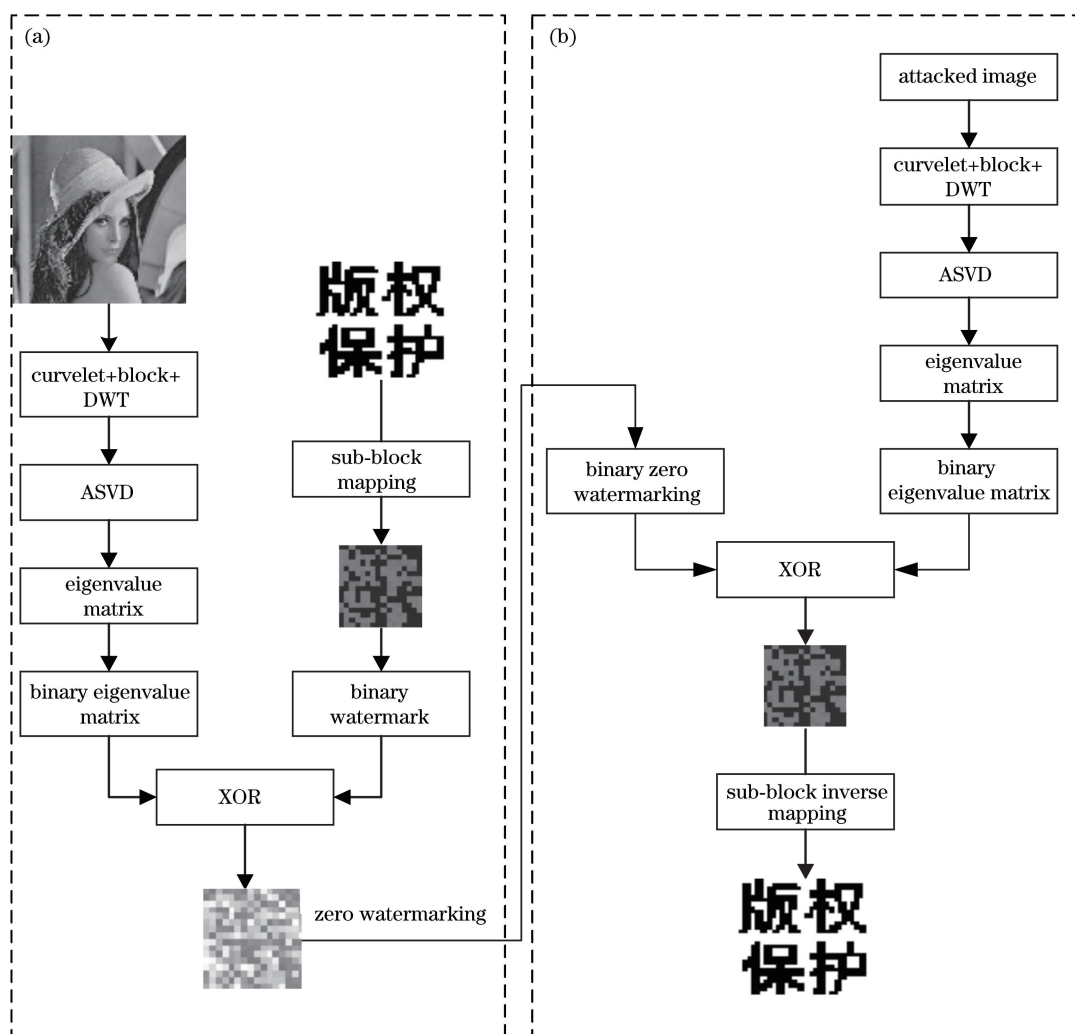


图 2 构造零水印与提取版权水印过程。(a)产生零水印;(b)提取版权水印

Fig. 2 Process of constructing zero watermark and extracting copyright watermark. (a) Generate zero watermark; (b) extract copyright watermark

4 实验结果与分析

4.1 参数说明

为了验证算法的有效性,选择大小为 512×512 的标准灰度图像作为载体图像,如图 3(a)~(i)所

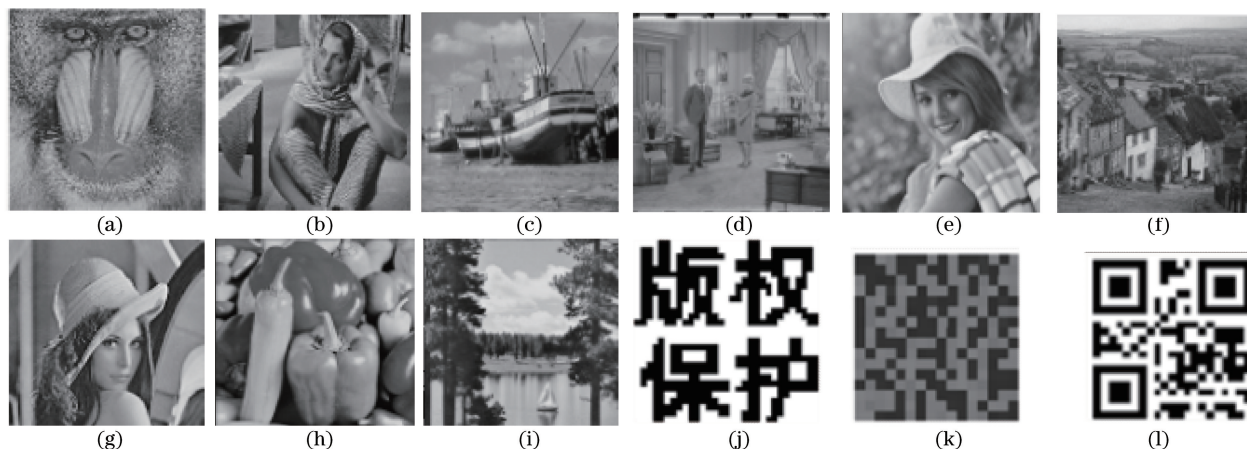


图 3 载体图像与版权水印。(a) Baboon 图像;(b) barbara 图像;(c) boat 图像;(d) couple 图像;(e) elaine 图像;(f) goldhill 图像;(g) lena 图像;(h) paper 图像;(i) sailboat 图像;(j) 版权标识;(k) 映射水印;(l) QR 代码

Fig. 3 Carrier images and copyright watermark. (a) Baboon image; (b) barbara image; (c) boat image; (d) couple image; (e) elaine image; (f) goldhill image; (g) lena image; (h) paper image; (i) sailboat image; (j) copyright logo; (k) watermark mapped; (l) QR code

4.2 评价指标

为了检验算法的性能,本文算法使用归一化相关系数(NC)和误码率(BER)来衡量算法的鲁棒性。

1) 归一化相关系数

归一化相关系数通常用于计算原始水印图像与被提取水印图像之间的相似性,取值范为 $C_N \in [0, 1]$,当 $C_N = 1$ 时,表示两个水印图像完全一致,表明算法的鲁棒性强,当 $C_N = 0$ 时,表示两个水印图像无相关, C_N 值的计算方式为^[19]

$$C_N = \frac{\sum_{i=1}^m \sum_{j=1}^n [W(i, j) \times W'(i, j)]}{\sqrt{\sum_{i=1}^m \sum_{j=1}^n [W(i, j)]^2} \sqrt{\sum_{i=1}^m \sum_{j=1}^n [W'(i, j)]^2}}, \quad (26)$$

式中: W 表示原始水印图像; W' 表示提取的版权水印; i, j 为图像索引; m 和 n 分别表示图像的长和宽。

2) 误码率

误码率表示图像中错误比特数据占总比特数据的比值,通常用于衡量水印算法的鲁棒性,但该衡量指标大都用于计算两幅二值版权图像之间的错误比特数,取值范围 $R_{BE} \in [0, 1]$,值越小表明算法的鲁棒性越好,具体计算方式为^[19]

$$R_{BE} = \frac{b}{m \times n} \times 100\%, \quad (27)$$

示,同时选择大小为 32×32 含有“版权保护”字样的版权标识和二维码作为版权水印,如图 3(j) 和图 3(l)所示。图 3(k)为映射后的水印信息,大小为 16×16 。所有的仿真在 64 位的 Windows 操作系统、matlab2014 软件上进行。

式中: b 为错误的比特数; $m \times n$ 为图像的大小。

4.3 改进奇异值的稳定性实验及选择调控因子

根据上述的改进方案,通过计算载体图像 I 与 I' 之间子块最大奇异值的变化率来选取合适的调控因子。由于本文对载体图像进行分块操作,因此在计算最大奇异值的变化率时,对所有子块的最大奇异值进行平均操作,图 4 所示为在固定强度的攻击下,通过改变调控因子而得到的实验结果。

从图 4 可以看出,最大奇异值的变化率与调控因子呈线性变化关系,随着调控因子逐渐变大,最大奇异值的变化率逐渐升高,变化率越大表明奇异值越不稳定,所选择的调控因子过大。当调控因子大于 0.5 时,最大奇异值的变化率变化较快。当调控因子为 0.9 时,变化率达到最高,其变化程度与传统的 SVD 接近。本文通过理论分析和大量实验测试可得,选择调控因子为 0.2 时,算法在鲁棒性和虚警率之间具有很好的平衡性。

4.4 虚警率实验

为了验证不同载体图像之间零水印的虚警率,分别对图 3 中的 9 幅载体图像进行虚警率测试,并计算两两之间的 NC 值来表示零水印之间的相似度,在此实验中,NC 值越高,表明虚警越高,反之越小,具体实验结果见表 1。

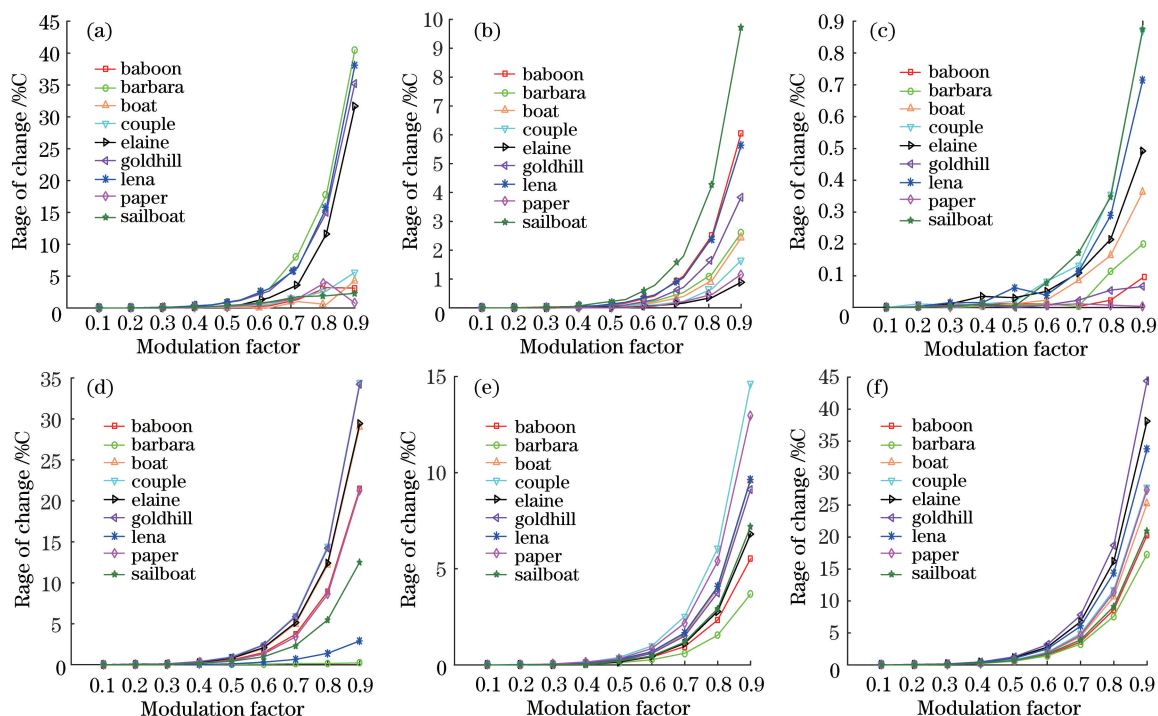


图 4 最大奇异值变化率与调控因子的关系。(a)高斯噪声(0.3);(b)中值滤波(模板大小 11×11);
(c) JPEG 压缩(压缩因子 10);(d)旋转攻击(5°);(e)行列偏移(下移 5 行);(f)剪切攻击(左上角 1/4)

Fig. 4 Relationship between the change rate of maximum singular value and modulation factors. (a) Gaussian noise (0.3);
(b) median filtering (template size 11×11); (c) JPEG compression (compression factor 10); (d) rotation attack
(5°); (e) column and column offset (5 rows down); (f) crop attack (upper left 1/4)

表 1 虚警率实验结果

Table 1 Experiment results of false alarm rate

Item	Baboon	Barbara	Boat	Couple	Elaine	Goldhill	Lena	Paper	Sailboat
Baboon	1.0000	0.4981	0.7067	0.6744	0.7280	0.5317	0.6151	0.6963	0.6087
Barbara	0.4981	1.0000	0.5504	0.6036	0.5129	0.6498	0.5856	0.5682	0.6564
Boat	0.7067	0.5504	1.0000	0.7372	0.7297	0.7150	0.7157	0.6268	0.6793
Couple	0.6744	0.6036	0.7372	1.0000	0.6855	0.7135	0.7638	0.6725	0.7280
Elaine	0.7280	0.5129	0.7297	0.6855	1.0000	0.6703	0.7372	0.6538	0.6391
Goldhill	0.5317	0.6498	0.7150	0.7135	0.6703	1.0000	0.7274	0.5915	0.7355
Lena	0.6151	0.5856	0.7157	0.7638	0.7372	0.7274	1.0000	0.5604	0.7640
Paper	0.6963	0.5682	0.6268	0.6725	0.6538	0.5915	0.5604	1.0000	0.5219
Sailboat	0.6087	0.6564	0.6793	0.7280	0.6391	0.7355	0.7640	0.5219	1.0000

由表 1 可知,9 幅载体图像之间的零水印相似度最低为 0.4981,平均虚警率为 0.6524,而且每幅图像生成的载体特征是唯一的,即使两幅图像之间的相似度达到 0.8 也无法提取清晰的版权信息,同时本文采用子块映射机制对版权信息进行了加密操作,即使得到完整的零水印信息也难以获取原始的版权信息,表明本文算法具有较低的虚警率和较高的安全性。

4.5 鲁棒性实验

4.5.1 非几何攻击

非几何攻击是一种添加性的攻击,主要改变图像像素值的大小,为了测试提出的零水印算法在抵抗非几何攻击时的鲁棒性和稳定性,分别对 9 幅载体图像添加高斯噪声、椒盐噪声和乘性噪声,参数设置为均值 0,方差 0.01 和 0.05;中值滤波、维纳滤波和低通滤波,滤波模板大小为 3×3

和 9×9 ; JPEG 压缩因子为 10 和 50; 具体实验结果见表 2。

由表 2 可知, 9 幅载体图像对于三种不同类型的噪声攻击都得到比较好的 NC 值, 最高值为 1.0000, 最低值为 0.9801, 整体平均值为 0.9916。对纹理丰富的 Baboon 图像添加噪声, 得到的 NC 值仍在 0.9809 以上。在滤波攻击方面, Lena 图像在三种不同的滤波攻击中得到的 NC 值几乎都为 1.0000, Baboon、Barbara、Goldhill 三幅载体图像得

到的整体平均 NC 值为 0.9962, 表明本文算法能有效地抵抗常见的滤波攻击。在 JPEG 压缩攻击方面, 随着压缩强度逐渐降低, NC 值逐渐升高, 在压缩因子为 50 时, 9 幅载体图像得到的 NC 值都在 0.9965 以上, 而在压缩因子为 10 时, 最低的 NC 值仍在 0.9913 以上。由于 Curvelet 变换和 DWT 具有很好的去噪性能, 同时得到的低频子带具有很强的稳定性, 进而使得本文方法在抵抗非几何攻击方面表现出较强的鲁棒性。

表 2 非几何攻击实验结果

Table 2 Experimental results of non-geometry attack

Attack type	Parameter	Baboon	Barbara	Boat	Couple	Elaine	Goldhill	Lena	Paper	Sailboat
Salt & pepper noise	0.01	0.9948	0.9983	1.0000	1.0000	1.0000	0.9974	0.9983	0.9974	0.9965
	0.05	0.9878	0.9913	0.9931	0.9861	0.9948	0.9895	0.9983	0.9922	0.9957
Gaussian noise	0.01	0.9887	0.9931	0.9930	0.9800	0.9922	0.9861	0.9931	0.9904	0.9930
	0.05	0.9809	0.9843	0.9825	0.9660	0.9835	0.9801	0.9844	0.9869	0.9737
Speckle noise	0.01	0.9931	0.9983	0.9965	0.9948	1.0000	0.9948	0.9983	0.9974	1.0000
	0.05	0.9861	0.9983	0.9930	0.9896	0.9965	0.9930	0.9930	0.9931	0.9896
Median filtering	3×3	0.9948	0.9965	1.0000	0.9948	1.0000	0.9983	0.9965	1.0000	0.9895
	9×9	0.9801	0.9913	0.9853	0.9878	0.9965	0.9965	0.9913	0.9931	0.9825
Wiener filtering	3×3	0.9965	0.9983	1.0000	0.9983	1.0000	0.9965	1.0000	1.0000	0.9930
	9×9	0.9931	0.9913	0.9913	0.9965	1.0000	0.9965	0.9948	0.9965	0.9895
Low pass filtering	3×3	0.9913	1.0000	0.9965	0.9983	0.9983	0.9965	0.9983	0.9965	0.9930
	9×9	0.9913	0.9965	0.9948	0.9983	0.9983	0.9965	0.9983	0.9965	0.9860
JPEG compression	10	1.0000	0.9965	0.9913	1.0000	0.9965	0.9939	0.9965	0.9983	0.9965
	50	1.0000	1.0000	0.9965	0.9983	1.0000	0.9983	0.9983	0.9974	1.0000

4.5.2 几何攻击

为了验证算法在几何攻击下的性能, 分别对 9

幅载体图像进行顺时针旋转、行列偏移攻击、剪切攻击, 具体实验结果见表 3。

表 3 几何攻击实验结果

Table 3 Experimental results of geometry attack

Attack type	Item	Baboon	Barbara	Boat	Couple	Elaine	Goldhill	Lena	Paper	Sailboat
Rotation /($^{\circ}$)	1	0.9776	0.9819	0.9755	0.9704	0.9754	0.9755	0.9836	0.9801	0.9577
	2	0.9538	0.9512	0.9549	0.9567	0.9533	0.9613	0.9837	0.9625	0.9376
	5	0.9036	0.9148	0.9109	0.8998	0.8755	0.8977	0.9377	0.8811	0.9038
Cutting	Upper left 1/4	0.9392	0.9705	0.9396	0.9314	0.9447	0.9471	0.9555	0.9623	0.9755
	Center 1/4	0.9368	0.9623	0.9447	0.9461	0.9633	0.9639	0.9515	0.9441	0.9650
	Bottom right 1/4	0.9498	0.9621	0.9416	0.9594	0.9314	0.9737	0.9602	0.9657	0.9477
Move	1 line	0.9948	0.9878	0.9939	0.9913	1.0000	0.9930	0.9983	0.9861	0.9965
	2 line	0.9931	0.9843	0.9869	0.9861	0.9983	0.9792	0.9965	0.9843	0.9869
	5 column	0.9514	0.9586	0.9755	0.9574	0.9684	0.9531	0.9406	0.9492	0.9489

由表 3 可知, 旋转攻击得到的 NC 值较低, 但在旋转 5° 的攻击下, 得到的平均 NC 值仍在 0.9028 以上, 最高 NC 值为 0.9377; 对于行列偏移攻击得到

较好 NC 值, 最高值为 1.0000。由于旋转攻击和行列偏移攻击都会使图像像素的整体位置发生改变, 会造成特征缺少的情形, 因此, 相比于非几何攻击得

到的 NC 值要低,但整体 NC 值仍在 0.9518 以上。主要原因在于本文算法改进了传统奇异值分解,使得构造的特征矩阵在上述攻击下的变化较小,同时子块映射方式有效减少了与载体图像直接接触的面积,在一定程度上提升了算法抵抗旋转攻击和行列偏移攻击的鲁棒性。对于剪切操作,整体得到的 NC 值为 0.9605;由于剪切攻击属于局部攻击范围,只改变剪切位置的像素值大小,当载体图像被剪切时,只有一小部分的特征受到影响,因此,本文算法能够抵抗不同位置的剪切攻击。

4.5.3 组合攻击

为了进一步验证算法的强鲁棒性能和适应性,本节设计 6 组组合攻击实验,组合的攻击类型如下:图 5(a)为高斯噪声(均值为 0,方差为 0.03)+旋转攻击(向右旋转 2°);图 5(b)为剪切攻击(左上角 $1/64$)+高斯噪声(均值为 0,方差为 0.03);图 5(c)为椒盐噪声(均值为 0,方差为 0.05)+JPEG 压缩(压缩因子为 10);图 5(d)为

(模板大小 5×5)+旋转攻击 3° ;图 5(e)为旋转攻击(旋转角度 3°)+行列偏移(下移 3 行);图 5(f)为剪切攻击(中心 $1/64$)+JPEG(压缩因子为 30)。同时从 SIPI 的图像数据库中选取大小为 256×256 的 Airplane 图像和大小为 1024×1024 的 Pentagon 图像用于测试算法在改变图像大小的情况下的鲁棒性,如图 5(e)和(f)所示。由图 5 可以看出,Lena 载体图像经过上述组合攻击后提取的版权水印只发生微小的变化,但仍能清晰地识别出其中的版权信息,而对于复杂结果的二维码水印,在上述各种组合攻击下,仍能通过移动设备扫描出水印信息。尤其在图 5(a)和图 5(b)的组合攻击下,载体图像的质量已经发生了严重的扭曲,但提取的版权图像仍能清晰地识别出版权信息。组合攻击对于载体图像影响较大,除了影响图像的像素值之外,还会改变图像像素的位置,但本文算法采用双变换域和改进奇异值分解,因此能够很好地抵抗复杂的组合攻击。

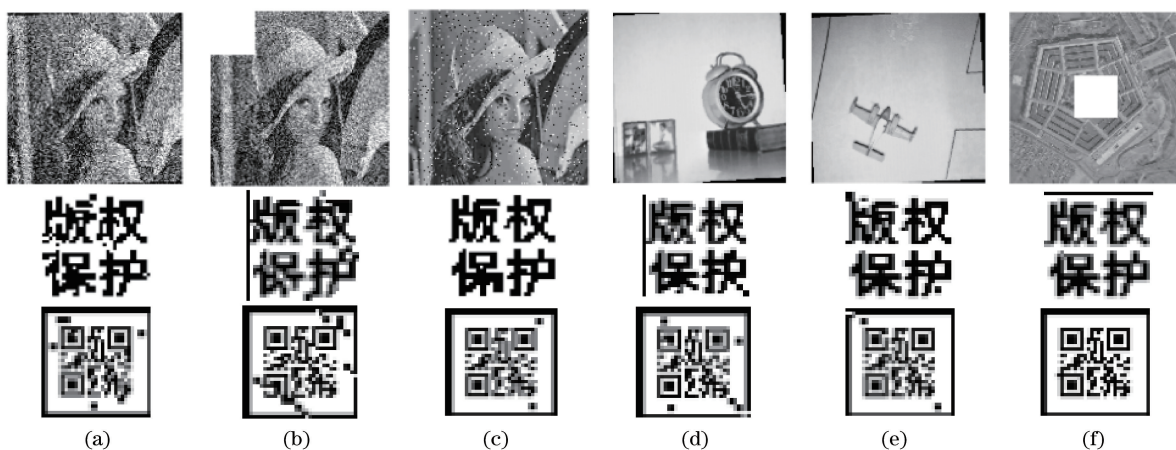


图 5 组合攻击。(a)高斯噪声+旋转攻击;(b)剪切攻击+高斯噪声;(c)椒盐噪声+JPEG 压缩;(d)中值滤波+旋转攻击;(e)旋转攻击+行列偏移;(f)剪切攻击+JPEG

Fig. 5 Combined attack. (a) Gaussian noise + rotation attack; (b) shear attack + Gaussian noise; (c) salt and pepper noise + JPEG compression; (d) median filter + rotation attack; (e) rotation attack + row and column offset; (f) shear attack + JPEG

4.6 安全性能分析

为了验证本文提出的子块映射方法对版权图像加密的安全性和生成零水印的唯一性,利用随机生成的随机矩阵分别对 9 幅载体图像进行攻击测试。同时,为了更加精确地体现子块映射方法的优势,随机矩阵中的数值只限定在 65~80 区间,将生成的 100 个随机矩阵用于提取加密后的版权图像,并计算相应的 NC 值,实验结果如图 6 所示。

由图 6 可以看出,随机生成的 100 个攻击序列提取的水印信息相似度都在 0.5 左右波动,即提取

的版权图像是无法辨别版权归属的。而当使用自身载体图像生成的零水印去提取版权图像时,得到的 NC 值为 1.0000,表明本文提出的零水印方法具有很强的安全性。

4.7 对比实验

为了突出本文算法的优势,分别选择空域强鲁棒零水印方案^[10]和一种基于水印信息的视觉映射特征的图像零水印算法^[17]进行对比实验,载体选择大小为 512×512 的 Lena 图像版权水印选择大小为 32×32 的版权标识,分别如图 3(g)和(j)所示。并

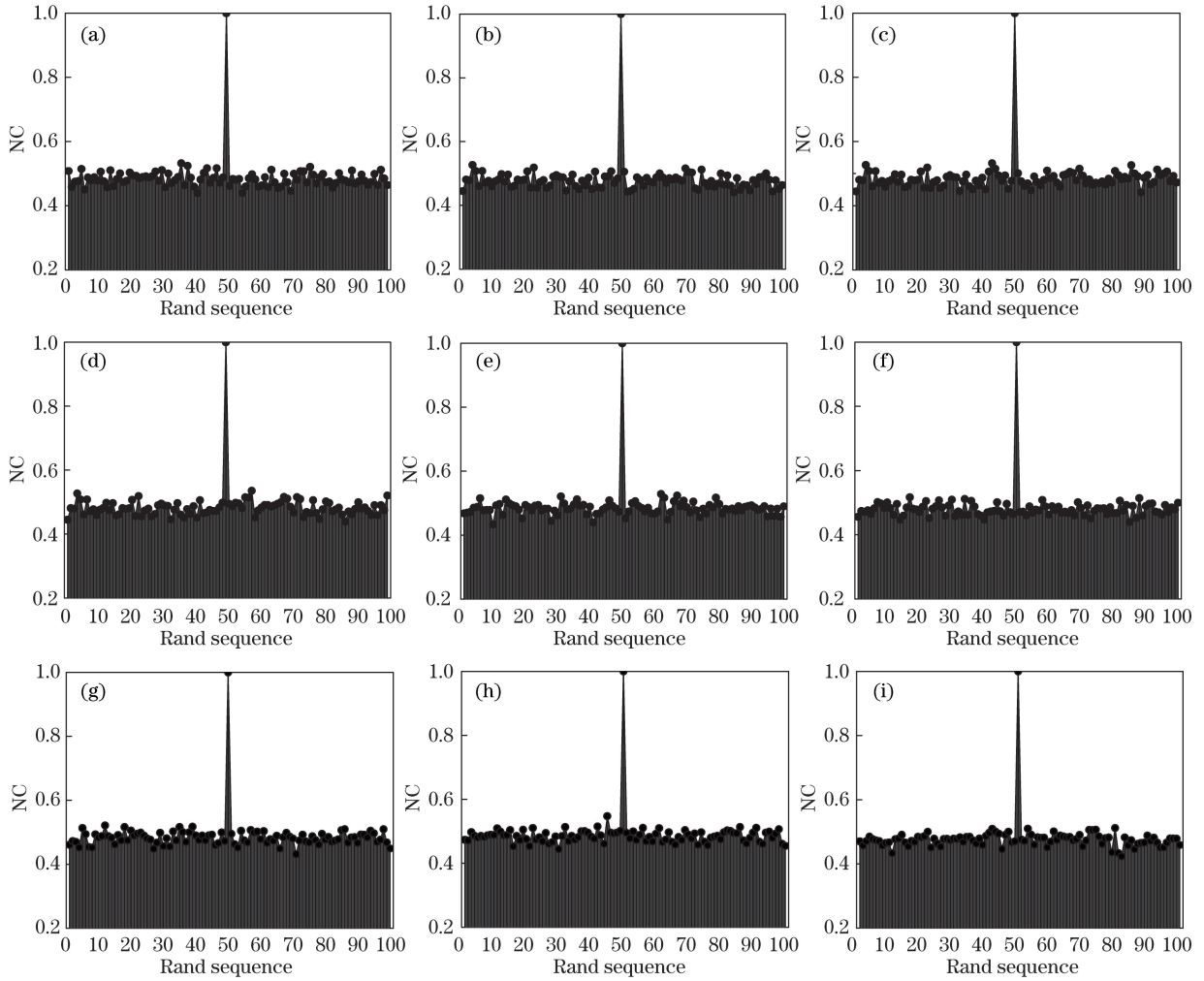


图 6 零水印安全性测试。(a) Baboon 图像;(b) barbara 图像;(c) boat 图像;(d) couple 图像;(e) elaine 图像;
(f) goldhill 图像;(g) lena 图像;(h) paper 图像;(i) sailboat 图像

Fig. 6 Zero watermark security test. (a) Baboon image; (b) barbara image; (c) boat image; (d) couple image;
(e) elaine image; (f) goldhill image; (g) lena image; (h) paper image; (i) sailboat image

分别进行噪声攻击、滤波攻击、JPEG 压缩攻击、旋转攻击、剪切攻击和行列偏移攻击,具体对比实验结果见表 4 和图 7,其中图 7(f)的剪切大小为 128×128 。

表 4 SVD 与 ASVD 的性能对比

Table 4 Performance comparison between SVD and ASVD

Attack type	Parameter	SVD		ASVD	
		NC	BER / %	NC	BER / %
Gaussian noise	0.2	0.3777	52.34	0.9913	0.98
Median filtering	5×5	0.6923	30.57	1.0000	0.00
JPE compression	20	0.5952	39.16	0.9983	0.20
Rotation / ($^\circ$)	2	0.3058	53.91	0.9575	4.79
Cutting	Upper left 1/4	0.9121	9.47	0.9648	3.91
Move	5 line	0.3097	54.39	0.9895	1.17

在表 4 中,SVD 使用的调制因子为 1、ASVD 使用的调制因子为 0.2,在非几何攻击和几何攻击下 ASVD 相比于传统的 SVD 的性能更优,尤其在抵抗几何攻击方面上得到的 NC 值都比 SVD 的高,最大提升幅度为 50%左右,实验结果表明,本文使用的 ASVD 方案与 SVD 相比,更有利于提升算法的鲁棒性能。

如图 7(a)所示,随着噪声攻击强度逐渐增大,三种算法得到的 NC 值逐渐下降,但本文算法下降趋势较为缓慢,且在噪声强度为 0.5 时得到的 NC 值可以达到 0.9200。如图 7(b)所示,在 3×3 的滤波模板时,本文算法、文献[10]算法、文献[17]算法的 NC 值几乎一致,但当模板大于 9×9 时,文献[10]算法和文献[17]算法的 NC 值变化较大,而本文算法的 NC 值几乎不变。如图 7(c)所示,在 JPEG 压缩方面,

三种算法得到的 NC 值变化趋势几乎一致,但本文算法在压缩因子为 10 时,NC 值仍能达到 0.9800 以上,文献[17]算法的 NC 值约为 0.9200 左右。如图 7(d)所示,随着旋转角度逐渐增大,文献[10]与文献[17]算法的 NC 值下降较快,而本文算法变化缓慢,且最低 NC 值也在 0.95 以上。如图 7(e)所示,三种算法

在行列偏移方面的变化趋势大致相同,但本文算法的 NC 值仍在文献[10]、文献[17]算法之上。如图 7(f)所示,对不同位置进行剪切操作,文献[17]算法的 NC 值高于文献[10]和本文算法,但与本文算法的差值约为 0.02,同时本文算法对不同的位置的剪切操作变化较小,稳定性好。

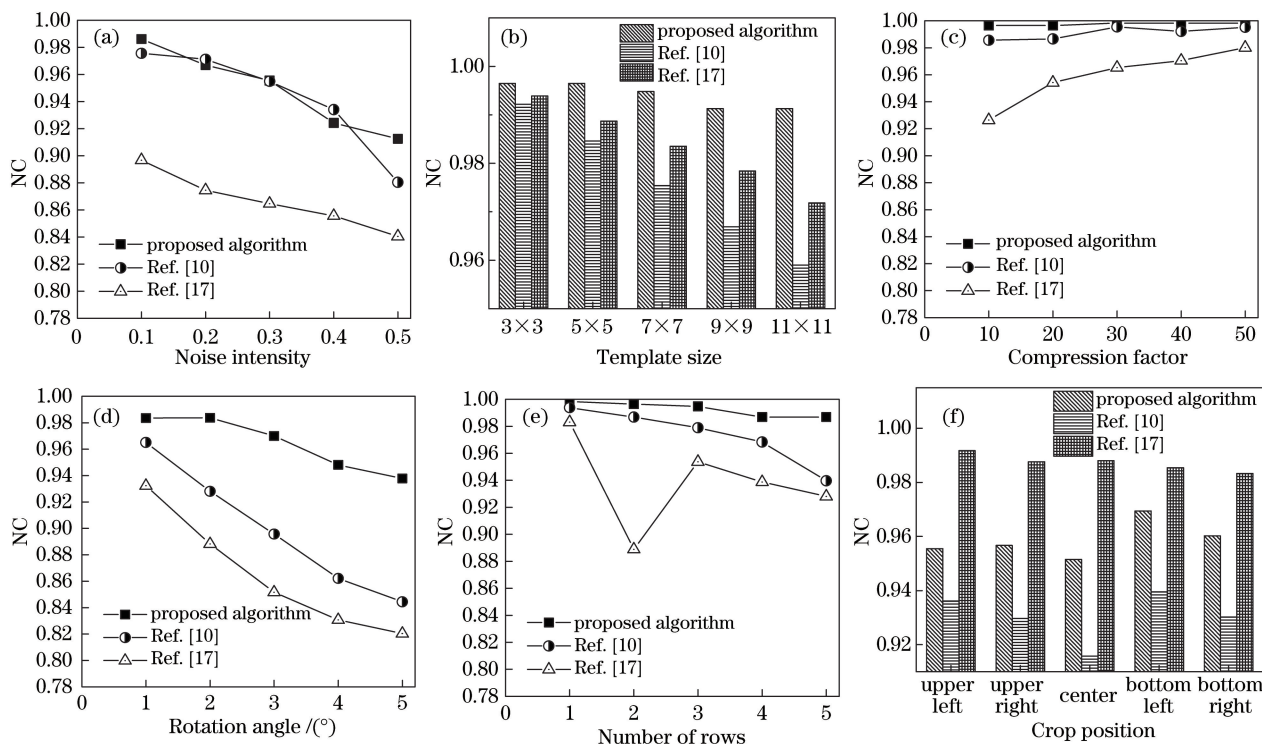


图 7 不同算法对比结果。(a)高斯噪声;(b)中值滤波;(c)JPEG 压缩;(d)旋转攻击;(e)行列偏移;(f)剪切攻击
 Fig. 7 Comparison results of different algorithms. (a) Gaussian noise; (b) median filter; (c) JPEG compression; (d) rotation attack; (e) row and column offset; (f) crop position

鲁棒性分析:本文算法与文献[10]、文献[17]算法相比,在抵抗非几何攻击性能上具有大幅度的提升,最大提升性能约为 12%,尤其在滤波攻击方面,对于两个不同强度的攻击得到的 NC 值几乎为 1.0000,主要由于本文结合 Curvelet 变换和 DWT 的滤波器中,Curvelet 变换对于图像的曲线奇异特性具有很好的表现性能,同时在滤波和去噪方面具有较好的性能,本文得到的特征矩阵为载体图像原始特征信息。而文献[17]算法仅使用每个子块的关系构造特征,虽然 DCT 在抵抗小范围的噪声和滤波攻击方面具有很好的鲁棒性,但当攻击的强度较大时,DCT 变化较快,进而导致构造的特征稳定性较差,无法提取清晰的版权图像。文献[10]算法采用图像子块的空间关系构造零水印,这种关系基于图像的空间稳定性,在非几何攻击上可以得到很好的抵抗性能。但在几何攻击上,这种关系的平衡性容易被打破,进而导致图像空间关系

的改变,因此,得到的 NC 值较低。在抵抗几何攻击上,文献[17]算法使用的传统的奇异值分解,因此在受到旋转攻击时,最大奇异值的最高位较为敏感,容易发生变化。由于本文算法使用改进奇异值的方法,克服了传统奇异值分解中最大奇异值最高位敏感问题,同时,在构造特征矩阵时,本文算法直接使用每子块的最大奇异值作为载体图像的特征,能构造直接反映载体图像的变化,因此,载体图像即使受到几何攻击,奇异值的变化都比较小,因此本文算法的鲁棒性优于文献[10]和文献[17]算法。

安全性分析:本文算法提出一种子块映射的方法,通过将每 2×2 子块的二值信息表示成一个十进制的符号信息,同时本文生成的零水印为十进制符号的零水印信息,异或运算在二进制位上进行,即使得到零水印信息也无法获取有效的版权图像,因为提取的信息需要经过子块映射逆操作才完成提取过程,相比于传统的二值零水印方法,其安全性更好。

5 结 论

本文算法在现有数字图像水印技术的基础上,通过分析水印分块和奇异值分解的特点,提出一种基于改进奇异值和子块映射的新型零水印技术,通过理论分析和实验表明,算法能够很好地抵抗常见的大强度的几何攻击、非几何攻击以及组合攻击,可以得到清晰的版权图像,且最低 NC 值可以在 0.9200 以上。改进的奇异分解能够很好地解决子块奇异值的最高位在几何攻击下的敏感性问题,有效地提高算法抵抗攻击的性能。子块映射机制能够减少版权水印与载体图像直接接触的面积,有利于提高版权水印的清晰度,同时这种映射机制能够进一步增强版权信息的安全性。本文算法生成的零水印为十进制的零水印,与传统的二值零水印相比,安全性更高,同时,当零水印的低 4 位发生改变时,零水印的整体信息变化比较小。与相似的图像零水印算法相比,在几何攻击上其安全性得到了很好的提升,表明本文算法能够适应更复杂的网络环境。

在实际应用中,版权图像的维度以及分块的方式等问题会影响版权的清晰度,未来的研究中,将重点对版权图像的维度及分块方式进行研究,以优化算法的性能。

参 考 文 献

- [1] Yin X, Huang W Q. Research on color QR code watermarking technology based on chaos theory[J]. Journal on Communications, 2018, 39(7): 50-58.
印曦, 黄伟庆. 基于混沌理论的彩色 QR 编码水印技术研究[J]. 通信学报, 2018, 39(7): 50-58.
- [2] Xie Q K, Jiang Y R, Zhang W F, et al. Information encryption technology based on digital watermarking and iteration algorithm [J]. Acta Optica Sinica, 2016, 36(6): 0607001.
解青坤, 姜艳茹, 张文飞, 等. 基于数字水印和迭代算法的信息加密技术[J]. 光学学报, 2016, 36(6): 0607001.
- [3] Jiao S M, Zhou C Y, Shi Y S, et al. Review on optical image hiding and watermarking techniques[J]. Optics & Laser Technology, 2019, 109: 370-380.
- [4] Jane O, Elbaşı E, İlk H G. Hybrid non-blind watermarking based on DWT and SVD[J]. Journal of Applied Research and Technology, 2014, 12(4): 750-761.
- [5] Thanki R, Kothari A, Trivedi D. Hybrid and blind watermarking scheme in DCuT-RDWT domain [J]. Journal of Information Security and Applications, 2019, 46: 231-249.
- [6] Wen Q, Sun T F, Wang S X. Concept and application of zero-watermark [J]. Acta Electronica Sinica, 2003, 31(2): 214-216.
温泉, 孙铁锋, 王树勋. 零水印的概念与应用[J]. 电子学报, 2003, 31(2): 214-216.
- [7] Li L L, Sun J G. A watermarking algorithm for remote sensing image based on contourlet domain and SIFT feature region[J]. Signal Processing, 2012, 28(9): 1254-1261.
李丽丽, 孙劲光. SIFT 特征区域 Contourlet 域遥感图像水印算法[J]. 信号处理, 2012, 28(9): 1254-1261.
- [8] Roy S, Pal A K. A blind DCT based color watermarking algorithm for embedding multiple watermarks[J]. AEU-International Journal of Electronics and Communications, 2017, 72: 149-161.
- [9] Ghadi M, Laouamer L, Nana L, et al. A novel zero-watermarking approach of medical images based on Jacobian matrix model[J]. Security and Communication Networks, 2016, 9(18): 5203-5218.
- [10] Xiong X G. A zero watermarking scheme with strong robustness in spatial domain[J]. Acta Automatica Sinica, 2018, 44(1): 160-175.
熊祥光. 空域强鲁棒零水印方案[J]. 自动化学报, 2018, 44(1): 160-175.
- [11] Qu C B, Wu D Y, Xiao C L, et al. Color zero watermarking algorithm in RGB spatial [J]. Journal of Frontiers of Computer Science and Technology, 2019, 13(4): 666-680.
曲长波, 吴德阳, 肖成龙, 等. RGB 空间彩色零水印算法[J]. 计算机科学与探索, 2019, 13(4): 666-680.
- [12] Meng X, Liu L, Jiang S, et al. Detection and revision of interference spectral signals based on wavelet transforms [J]. Acta Optica Sinica, 2019, 39(9): 0930007.
孟鑫, 刘磊, 江升, 等. 基于小波变换的干涉光谱信号检测与校正方法[J]. 光学学报, 2019, 39(9): 0930007.
- [13] Thanki R, Borra S, Dwivedi V, et al. An efficient medical image watermarking scheme based on FDCuT-DCT [J]. Engineering Science and Technology, an International Journal, 2017, 20(4): 1366-1379.
- [14] Ansari I A, Pant M. Multipurpose image watermarking in the domain of DWT based on SVD and ABC [J]. Pattern Recognition Letters, 2017, 94: 228-236.
- [15] Rani A, Bhullar A K, Dangwal D, et al. A zero-watermarking scheme using discrete wavelet transform [J]. Procedia Computer Science, 2015, 70: 603-609.
- [16] Waleed J, Jun H D, Saadon S, et al. An immune secret QR-code sharing based on a twofold zero-watermarking scheme [J]. International Journal of

-
- Multimedia and Ubiquitous Engineering, 2015, 10(4): 399-412.
- [17] Thanh T M, Tanaka K. An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information[J]. Multimedia Tools and Applications, 2017, 76(11): 13455-13471.
- [18] Moosazadeh M, Ekbatanifard G. An improved robust image watermarking method using DCT and YCoCg-R color space[J]. Optik, 2017, 140: 975-988.
- [19] Ernawan F, Kabir M N. A robust image watermarking technique with an optimal DCT-psychovisual threshold[J]. IEEE Access, 2018, 6: 20464-20480.