

面向医学图像的篡改检测双重水印算法

王苗苗¹, 吴德阳^{2,3*}, 胡森¹, 王佳炎^{2,3}, 王妍¹, 金海波¹, 曲长波¹¹辽宁工程技术大学软件学院, 辽宁 葫芦岛 125105;²燕山大学信息科学与工程学院, 河北 秦皇岛 066004;³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 针对医学图像中嵌入水印信息造成的鲁棒性与透明性的不平衡问题,提出了一种面向医学图像的篡改检测双重水印算法。首先,采用 Sine-Cubic 混沌映射加密算法将 Sine 映射与 Cubic 映射进行线性耦合,利用得到的混沌序列对版权图像进行加密。其次,对载体图像进行小波变换,并对低频子带进行安全区域划分,根据安全区域内子块熵值将医学图像划分为感兴趣区域(ROI)和非感兴趣区域(NROI)。同时,通过提取 ROI 的稳定特征与加密的版权构造鲁棒的零水印。最后,将零水印嵌入医学图像 NROI 子块 Schur 分解的上三角矩阵最大系数中,同时记录嵌入水印后的最大系数用于篡改检测。实验结果表明:所提水印算法具有不可感知性、鲁棒性和安全性,同时可以准确地定位被篡改的含水印区域;与其他水印算法相比,所提双重水印算法在鲁棒性和算法效率上均有很大的提升。

关键词 医用光学; 双重水印; 鲁棒性; Sine-Cubic 混沌映射; 医学图像水印

中图分类号 TP391 文献标志码 A

DOI: 10.3788/LOP213052

Double Watermarking Algorithm for Tamper Detection of Medical Images

Wang Miaomiao¹, Wu Deyang^{2,3*}, Hu Sen¹, Wang Jiayan^{2,3}, Wang Yan¹, Jin Haibo¹, Qu Changbo¹¹College of Software, Liaoning Technical University, Huludao 125105, Liaoning, China;²College of Information Science and Engineering, Yan Shan University, Qinhuangdao 066004, Hebei, China;³The Key Laboratory for Computer Virtual Technology and System Integration of Hebei Province, Qinhuangdao 066004, Hebei, China

Abstract A double watermarking algorithm for medical image tamper detection is proposed to address the imbalance between robustness and transparency caused by embedding watermark information in medical images. First, the Sine-Cubic chaotic map encryption algorithm is used to linearly couple the Sine map and Cubic map, and the obtained chaotic sequence is used to encrypt the copyright image. Second, the carrier image is wavelet transformed, and the low-frequency sub-band is divided into safety regions. The medical image is divided into regions of interest (ROI) and non-interest (NROI) based on the entropy value of the sub-block in the safety region. Simultaneously, a strong zero watermark is created by combining the stable features of the ROI region and the encrypted copyright. Finally, the zero watermark is embedded into the maximum coefficient of the upper triangular matrix of Schur decomposition of the NROI sub-block of the medical image, and the maximum coefficient following the watermark embedding is recorded for tamper detection. The experimental results demonstrate that the proposed watermarking algorithm is imperceptible, robust, and secure, and can accurately locate the tampered watermarked region; when compared to other watermarking algorithms, the proposed double watermarking algorithm is significantly more robust and efficient.

Key words medical optics; double watermark; robustness; Sine-Cubic chaotic map; medical image watermarking

1 引言

随着网络信息技术的不断发展,利用信息和通信

技术的远程医疗逐渐兴起,成为先进医疗基础建设不可或缺的一部分。但是远程医疗数据可视化使记录患者信息的医学图像在网络传输过程中,面临着一系列

收稿日期: 2021-11-24; 修回日期: 2021-12-16; 录用日期: 2022-01-06; 网络首发日期: 2022-01-16

基金项目: 国家自然科学基金(62173171)

通信作者: *wdy@stumail.ysu.edu.cn

的版权侵权问题,如患者信息被非法盗用,病患信息被篡改从而影响诊断结果等。因此,对医学影像的版权保护研究具有重要的意义。数字水印技术作为一种有效保护医学数据不受非法操作和访问的方法,被广泛应用在版权保护与认证领域^[1-2]。

根据嵌入方式,可将数字水印算法分为零水印、鲁棒水印、盲水印等。鲁棒水印和盲水印的区别在于是否借助额外信息提取水印,这两种类型的嵌入方式不可避免地会对载体图像产生影响。文献[3]对图像小波低频子带分块后进行奇异值分解(SVD),通过改变奇异值的奇偶性将水印信息嵌入载体图像中,由于对低频系数的修改幅度较小,因此具有良好的不可见性。文献[4]提出了两种水印方案,分别在DCT和DWT的中频系数中嵌入水印信息,由于中频系数中包含着图像的纹理和边缘信息,不容易引入视觉效果的变化,因此具有良好的不可见性。上述算法虽然表现出较好的不可见性,但对于内容完整性要求较高的医学图像,其仍难以同时兼顾不可见性和鲁棒性的要求。而文献[5]对医学图像进行整数小波变换(IWT),选择高频系数嵌入电子病历信息(EPR),由于高频系数含有较少的图像信息,嵌入水印对图像影响较小,但是无法抵抗较高强度的攻击。虽然文献[3-5]选择中高频信息作为水印信息的嵌入位置,可以获得良好的不可见性,但图像的纹理信息在常规攻击下较为敏感,因此算法的鲁棒性较差。文献[6-10]对盲水印的鲁棒性问题进行研究,通过操作载体图像的低频系数完成水印的嵌入,有效地平衡了盲水印算法中的鲁棒性和不可见性,但是含水水印图像的峰值信噪比(PSNR)仅在38 dB左右,无法满足医学图像对图像质量的要求。零水印^[11-12]的基本思想是提取载体图像的特征与版权水印进行逻辑运算生成零水印信息,并将零水印注册到版权保护中心。零水印作为水印信息与载体特征的中间产物,具有版权保护和载体特征唯一的特性,因此在发生版权纠纷时,可以利用零水印信息提取水印图像进行版权认证。文献[13]利用DWT图像变换提取低频信息,并对每一子块进行SVD获取子块最大奇异值构造特征矩阵,最后与版权水印异或生成零水印信息。文献[14-15]对眼底图像进行扇形区域划分,并计算每个扇形块的灰度值作为图像特征,最后利用视觉密码生成零水印和私有权图像,该方法能够有效区分相似图像之间提取的特征。而文献[16]则利用极复指数变换提取图像的几何特征,并与加密后的版权图像运算生成零水印,由于极复指数变换具有很强的抗几何变化性能,因此对于旋转攻击表现强的鲁棒性。文献[17]将整数阶径向谐波傅里叶矩推广到分数阶,有效缓解提取的图像矩特征数值不稳定的问题,同时提高计算精度,提升水印的鲁棒性。近些年,出现了在图像中嵌入信息后可无损恢复成原图的水印算法。文献[18-19]将水印信息嵌入极谱变换矩(PHTMs)系数

中,并计算重建图与原图的差异信息,将差异信息无损压缩后可逆嵌入图像边角区域;当图像受攻击时,可正常进行版权认证;当图像未受攻击时,可根据差异信息无损恢复原始图像,但极谱变换矩的计算量较大,算法效率下降,不适用于大量医学图像的版权保护。文献[20]对医学图像进行上采样操作,以获取更大的嵌入容量,在图像中嵌入篡改校验信息和电子病历信息,当图像未受攻击时,可无损恢复原始医学图像。该算法实现简单,运行效率较高,但在信息嵌入过程中扩大了载体图像尺寸,对于医学图像的保存和传输产生了一定的影响。由于医学图像的特殊性,难以使用单一的零水印或盲水印算法完成版权保护任务,为此许多研究学者将多种类型的水印方案进行组合,以提高版权保护认证系统的综合性能。Tarhouni等^[21]从图像中提取颜色信息和结构信息,并将其嵌入图像的DCT频域系数中,以增强嵌入水印的唯一性,实现图像的完整性保护,但载体图像嵌入信息后受到一定程度的影响,难以用于到医学图像的版权保护中。Tayachi等^[22]根据阈值将医学图像分为结构区域和背景区域,提取结构区域的中值、熵、偏度等信息作为特征构造零水印,再将零水印嵌入背景区域,以实现医学图像版权保护,该方案在医学图像的背景区域嵌入信息,不会影响医学图像的结构内容,但在分区过程中只是使用单一阈值进行简单处理,存在一定的局限性。

综上所述,现阶段单一水印或多水印的医学图像算法中,仍存在以下问题:1)在医学图像中嵌入水印信息破坏了医学图像细节信息的完整性,可能会导致诊断结果错误;2)现有的零水印方案难以区分相似图像的特征,使得利用同类型的医学图像便可以提取版权图像;3)多水印的融合可以有效解决部分单一水印的问题,但是仍存在着算法效率低、局限性高和不易存储和传输等问题。

基于上述问题,本文提出了一种面向医学图像的篡改检测的双重水印算法。提取医学图像稳定特征构造零水印,并将零水印嵌入载体图像,不需要额外的三方机构存储,降低存储成本。在嵌入水印之前,在医学图像内接圆形区域作为安全区域,减少水印信息被抹去的风险。利用子块信息熵将安全划分感兴趣区域(ROI)和非感兴趣区域(NROI),将零水印嵌入NROI很好地平衡水印算法的鲁棒性与透明性。同时所提篡改检测方案可以有效定位出被篡改的含水子块的位置,所提Sine-Cubic线性耦合混沌映射算法将两种混沌系统线性耦合,降低混沌的概率密度并提升初值敏感度,可实现更好的加密效果。

2 基本原理

2.1 子块选择理论依据

为了避免嵌入水印对远程医学诊断造成干扰,从

而导致诊疗结果出现误差,在医学图像中嵌入水印信息时,需要对医学图像的区域进行划分,将医学图像划分为 ROI 和 NROI,并将水印信息嵌入不影响医疗诊断的 NROI 中。

2.1.1 安全区域选择

由于医学图像用于诊断的区域大多位于图像中心,将水印信息嵌入背景区域可以在保证水印信息的不可见性的同时保证医学图像中用于诊断区域的完整性不被破坏。但当含水印图像受到旋转等几何攻击

时,嵌入靠近边缘区域的水印信息容易被抹去,故本研究在进行子块选择前首先找出一个安全区域。当图像受到不同角度的旋转攻击时,含水印图像的边缘会丢失,如图 1 所示。当图像旋转任一角度时,图像内接圆面积均相等,因此选定载体图像内接圆内的区域为安全区域,减少水印因受到几何攻击被抹去的可能性,如图 1(b) 所示。图 1(c)、(d) 分别为含水印图像旋转 45° 和旋转校正的图像。从图中可以看出,内接圆内的区域没有因为旋转而发生内容上的改变。

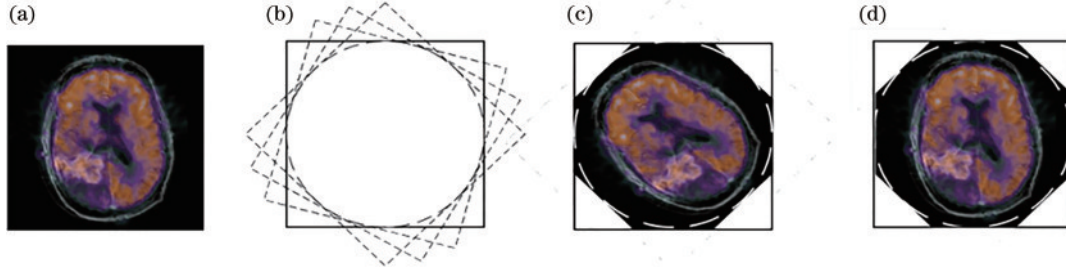


图 1 安全区域构建原理及效果。(a)原始图像;(b)安全区域构建;(c)旋转 45° ;(d)旋转校正

Fig. 1 Construction principle and effect of safety area. (a) Original image; (b) safe area construction; (c) rotation 45° ; (d) rotation correction

2.1.2 子块选择

根据图像子块的信息熵在安全区域进行子块选择,将医学图像内接圆内区域划分为 ROI 和 NROI; ROI 为信息熵值大的纹理子块,这些子块的纹理信息较为复杂,嵌入水印会影响诊断细节失真;NROI 为信息熵值较小的平滑子块,这些子块大多位于背景区域,嵌入水印信息不会影响医学诊断的结果。图像信息熵的计算公式为

$$H(\mathbf{X}) = -[P_1 \log(P_1) + P_2 \log(P_2) + \dots + P_n \log(P_n)] = -\sum_{k=1}^{255} p_k \log p_k, \quad (1)$$

式中: \mathbf{X} 表示输入的图像; p_k 表示图像中灰度值为 k 的像素所占的比例,并且 $p_k \in [0, 1]$, $\sum_{k=1}^n p_k = 1$ 。为了便于后期选择水印嵌入区域,将图像分为互不重叠的子块,每一子块的信息熵的表达式为

$$h_i(x) = -\sum_{k=1}^{255} p_k \log p_k. \quad (2)$$

为不破坏医学图像的完整性,将水印信息嵌入平滑子块中,根据图像的信息熵将图像分为纹理子块和平滑子块,并分别表示为 $B^T(x)$ 和 $B^S(x)$:

$$[h_i^{\text{value}}, h_i^{\text{index}}] = \text{sort}(h_i), \quad (3)$$

$$B_i^f = \begin{cases} f = T, & h_i > h_{1024}^{\text{value}} \\ f = S, & h_i \leq h_{1024}^{\text{value}} \end{cases}, \quad (4)$$

式中: sort 为排序函数; h_i^{value} 表示将熵值从小到大排列得到的索引序列, i 表示子块顺序; h_i^{index} 表示子块索引位置,用于作为嵌入水印子块选择的依据。选择纹理信息较少的子块,即前 1024 个信息熵值较小的子块作

为 NROI 嵌入水印信息。同时将子块选择方式形成掩码密钥,作为嵌入和提取水印的依据。掩码密钥生成的方式如下: 设置一个全零矩阵作为过渡矩阵,根据子块索引 h_i^{index} 标记 NROI 子块 $B^S(x)$ 的位置,将对应位置的数据置 1,得到一个原始图像相同尺寸的掩码密钥。

2.2 Sine-Cubic 线性耦合

Sine 函数是三角函数中正弦函数的变形,具有结构简单、便于计算的特点,常常被应用于图像混沌加密算法中,可变参数的 Sine 映射的动力系统模型为

$$z_{k+1} = S(z_k, \mu) = \mu \sin(\pi z_k), \quad (5)$$

式中: S 为 Sine 映射混沌函数; $z \in [0, 1]$; $k = 1, 2, 3, \dots$; μ 为可变参数,且 μ 的取值范围为 $[0, 1]$,但是 Sine 映射的概率密度差异较大,且仅当 $\mu = 0$ 时,才能达到满映射。

同时, Cubic 映射作为最常见的混沌映射方式,具有随机性和遍历性,结构简单易于操作,可以表示为

$$z_{k+1} = C(z_k, \mu) = \mu \times z_k(1 - z_k^2), \quad (6)$$

式中: C 为 Cubic 映射混沌函数。Cubic 映射的概率密度差异较大,且当 $\mu = 2.53$ 时,才能达到混沌状态。

为了解决上述两种混沌映射概率密度差异问题,构造线性方程将 Sine 映射与 Cubic 映射进行耦合,从而达到较好的混沌状态,且满足初值敏感的混沌要求。构建的基于 Sine-Cubic(S-C)混沌系统的线性方程为

$$z_{k+1} = G(z_k, p, q) = p \times C(z_k) + q \times S(z_k) = 2.53p \times z_k \times (1 - z_k^2) + q \times \sin(\pi z_k), \quad (7)$$

式中: G 为 S-C 混沌映射函数; p, q 为可变参数,当

$p, q \in [0, 1]$ 且 $p + q = 1$ 时, $z_k \in [0, 1], k = 1, 2, 3, \dots$ 。由于 $q = 1 - p$, 则式(7)可以改写为

$$z_{k+1} = 2.53p \times z_k \times (1 - z_k^2) + (1 - p) \times \sin(\pi z_k) = p[\sin(\pi \times z_k) - 2.53 \times z_k(1 - z_k^2)] + 2.53 \times z_k(1 - z_k^2), \quad (8)$$

式中: $p \in [0, 1]$ 。

Sine 混沌映射本质上为迭代 n 次的 Sin 型复合函数, Sin 函数是有界函数, 因此 Sin 函数的时间复杂度为 $O(1)$, 内部函数 πz_k 为 1 阶函数, 所以内部函数的复杂度为 $O(n)$, Sine 混沌映射的时间复杂度 $T_s(n) = n \cdot O(n)$ 。Cubic 函数为迭代 n 次的立方阶函数, 因此 Cubic 的算法复杂度 $T_c(n) = n \cdot O(n^3)$ 。S-C 混沌系统为 Sine 和 Cubic 的线性耦合, 因此耦合后的函数的最高阶与原始混沌映射的最高阶相等, S-C 混沌系统的算法复杂度 $T_G(n) = n \cdot O(n^3)$, 与 Cubic 映射的复杂度相等。3 个混沌系统的时间复杂度排序为 $T_s(n) < T_c(n) = T_G(n)$ 。S-C 映射混沌函数的时域如图 2 所示, 从图中可以看出, 利用 S-C 混沌系统得到的混沌序

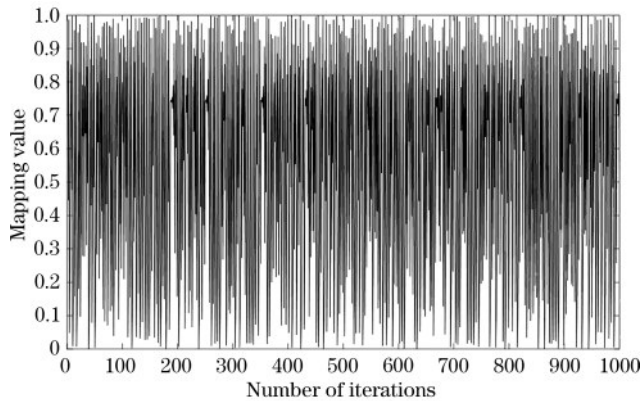


图 2 混沌时域图

Fig. 2 Chaotic time domain diagram

列具有较好的随机性, 适用于水印的版权图像加密。

2.3 载体特征稳定性分析

通过提取载体图像的稳定特征, 构造鲁棒的零水印。为提取彩色医学图像的稳定特征, 将彩色载体图像 I 转换到 YCbCr 空间, 提取亮度分量 I^Y 进行二维 DCT 变换:

$$F(u, v) = c(u)c(v) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i, j) \times \cos\left[\frac{(i+0.5)\pi}{N}u\right] \cos\left[\frac{(j+0.5)\pi}{N}v\right], \quad (9)$$

$$cc(u) = \begin{cases} \sqrt{\frac{1}{N}}, & u=0 \\ \sqrt{\frac{2}{N}}, & u \neq 0 \end{cases}, \quad (10)$$

式中: $N \times N$ 为原始图像的像素大小; $f(i, j)$ 是原始图像的像素; $F(u, v)$ 是 DCT 变换的系数; $c(u)$ 、 $c(v)$ 是可以使 DCT 变换矩阵为正交矩阵的补偿系数, 并选取 DCT 稳定系数作为零水印的载体特征。

为了测试 DCT 低频系数的稳定性, 对脑部医学图像进行不同种类的攻击, 结果如表 1 所示, 其中 A~G 分别代表无攻击、高斯噪声 0.1、椒盐噪声 0.1、JPEG 压缩 10、中值滤波 5×5 、放大 4 倍和剪切 1/8。为了方便观察和分析, 表 1 列出了低频部分前 8 个系数在不同攻击下的情况。

由表 1 可以看出: DCT 系数对不同攻击的敏感程度不同, 当受到较大强度的噪声攻击、滤波攻击和剪切攻击时, 低频系数的数值发生较大的变化; 但是对于 JPEG 压缩和缩放攻击, 低频系数的数值变化较小, 且在任一攻击下, DCT 低频系数的正负性均没有发生变化, 说明 DCT 低频系数的符号具有很强的稳定性, 因此可以利用 DCT 系数符号作为构造零水印的载体特征。

表 1 DCT 系数特征稳定性

Table 1 Characteristic stability of DCT coefficients

Image	$C(1,1)$	$C(1,2)$	$C(1,3)$	$C(1,4)$	$C(1,5)$	$C(1,6)$	$C(1,7)$	$C(1,8)$
A	2.7991	0.2099	-0.8241	-0.0947	0.0854	-0.0317	-0.0683	0.0461
B	3.4839	0.1653	-0.6004	-0.0865	0.0689	-0.0276	-0.0468	0.0430
C	3.1684	0.1891	-0.7450	-0.0833	0.0784	-0.0397	-0.0547	0.0399
D	2.7991	0.2099	-0.8241	-0.0947	0.0854	-0.0317	-0.0683	0.0461
E	2.8049	0.2114	-0.8293	-0.0966	0.0868	-0.0323	-0.0695	0.0467
F	2.7990	0.2099	-0.8241	-0.0947	0.0854	-0.0317	-0.0683	0.0461
G	2.7863	0.1923	-0.8404	-0.1089	0.0678	-0.0560	-0.0908	0.0265

3 双重水印算法

双重水印算法主要包含水印图像预处理、生成零水印、嵌入零水印和版权认证等 4 个阶段, 其中在生成零水印和嵌入零水印过程需要对图像进行预处理, 将

图像划分为 ROI 和 NROI, 分别用于生成零水印和嵌入零水印信息, 大致过程如图 3 所示。设 I 是大小为 $M \times N \times 3$ 的彩色载体图像, W 是大小为 $p \times q$ 的二值版权水印图像。

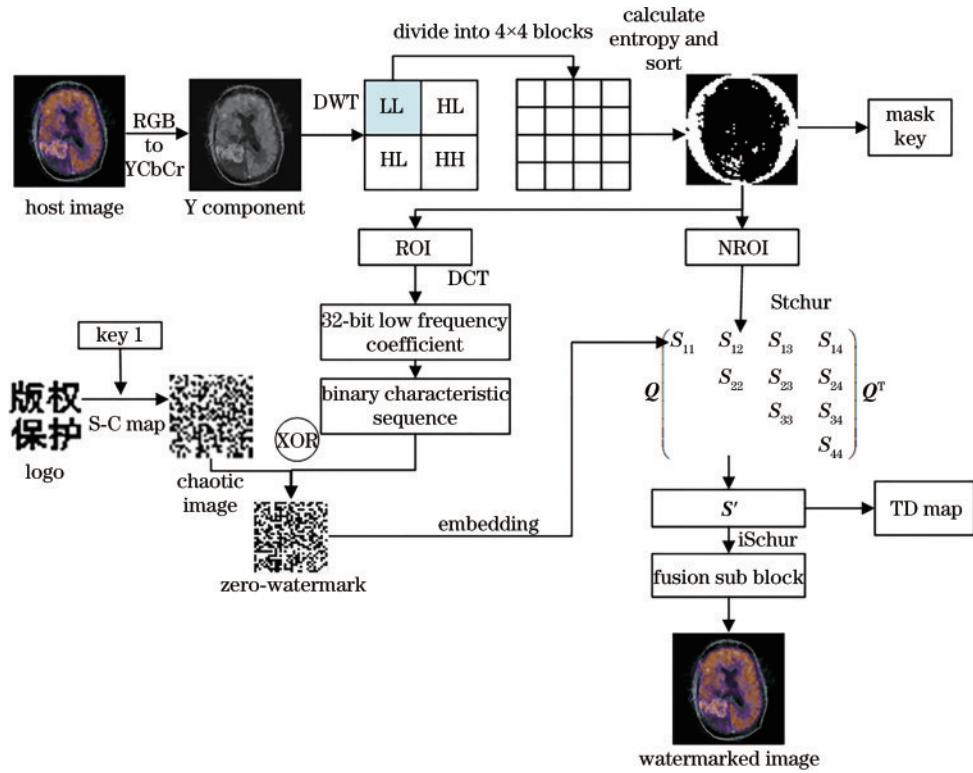


图 3 双重水印的生成过程

Fig. 3 Double watermark construction process

3.1 水印图像预处理

水印图像预处理过程利用所提 Sine-Cubic 混沌映射对大小为 $p \times q$ 的版权图像 W 进行加密, 加密过程如图 4 所示。

1) 在 $[0, 1]$ 内选出一个随机数 z_1 作为 Sine-Cubic 混沌映射的初值, 并作为加密密钥保存。将初值 z_1 代入式 (8) 生成一个长度为 $p \times q$ 的随机混沌序列 $Z, Z = \{z_1, z_2, \dots, z_{p \times q}\}$ 。

2) 将混沌序列 Z 进行升序或降序排列, 得到混沌序列的位置索引 Z_{index} , 排序方式为

$$[\sim Z_{\text{index}}] = \text{sort}(Z), \quad (11)$$

式中: Z_{index} 为排序后得到索引序列, 可用于图像的混沌映射。

3) 将图像 W 中的像素进行降维重组, 排列成一个 $1 \times (p \times q)$ 的数组, 记作 $W(1, p \times q) = \{w_1, w_2, \dots, w_{p \times q}\}$ 。

4) 利用索引对降维的图像序列 W' 中元素位置进行置乱, 得到加密序列 S_w , 置乱方式为

$$S_w(1, p \times q) = W[\mathbf{Z}_{\text{index}(1)}, \mathbf{Z}_{\text{index}(p \times q)}] \quad (12)$$

5) 对加密序列进行重组, 得到加密的图像矩阵 S'_w 。

$$S'_w(p, q) = \text{reshape}[S_w(1, p \times q)] \quad (13)$$

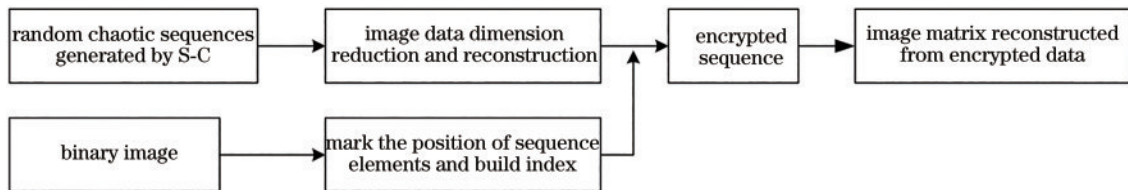


图 4 版权图像加密过程

Fig. 4 Encryption process of watermark image

3.2 零水印生成

零水印生成过程主要利用小波变换和 DCT 提取载体图像的特征矩阵与版权水印进行逻辑运算生成零水印信息, 具体步骤如下:

1) 将 RGB 彩色载体图像 I 转换到 YCbCr 颜色空间, 得到 I^Y, I^U, I^V 等 3 个颜色分量。

$$[I^Y, I^U, I^V] = \text{rgb2ycbcr}(I) \quad (14)$$

2) 选取亮度分量 I^Y 进行一级小波分解, 得到低频分量 I^Y_{LL} , 并进行 4×4 不重叠子块划分, 每个子块标记为 $B_{i,j}$, 分块方式如下:

$$[I^Y_{\text{LL}}, I^Y_{\text{LH}}, I^Y_{\text{HL}}, I^Y_{\text{HH}}] = \text{dct2}(I^Y) \quad (15)$$

$$I_{LL}^Y = \begin{bmatrix} B_{1,1} & \cdots & \cdots & B_{1,j} \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ B_{j,1} & \cdots & \cdots & B_{i,j} \end{bmatrix}, \quad (16)$$

式中: $i \in \left\{1, 2, \dots, \frac{M}{8}\right\}$; $j \in \left\{1, 2, \dots, \frac{N}{8}\right\}$; $B_{i,j}$ 为 4×4 大小的子块。

3) 根据第 2.1.1 小节的方式在 I_{LL}^Y 内接圆形区域选取安全区域, 并计算安全区域内的子块熵值, 按照熵值大小将安全区域内的子块划分为 ROI 和 NROI。选择内接圆内熵值较小的 $p \times q$ 个平滑子块嵌入水印信息, 将相对位置标记为 1; 其余的熵值较大的纹理子块用于生成零水印, 并将相应的位置标记为 0, 记作 mask key。

4) 对 ROI 子块进行重构, 并对重构的子块执行 2D-DCT, 提取前 4 行 8 列 32 位系数作为稳定的载体特征 F , 并根据 DCT 系数符号进行二值化处理:

$$F = \begin{cases} 1, & F > 0 \\ 0, & F \leq 0 \end{cases} \quad (17)$$

$$T'_{i,j}(1, 1) = \begin{cases} T_{i,j}(1, 1) - \Delta - 0.25 \times \lambda, & W_z = 1 \text{ and } \Delta \in [0, 0.25 \times \lambda) \\ T_{i,j}(1, 1) - \Delta + 0.75 \times \lambda, & W_z = 1 \text{ and } \Delta \in [0.25 \times \lambda, \lambda) \\ T_{i,j}(1, 1) - \Delta + 0.25 \times \lambda, & W_z = 0 \text{ and } \Delta \in [0, 0.75 \times \lambda) \\ T_{i,j}(1, 1) - \Delta + 1.25 \times \lambda, & W_z = 0 \text{ and } \Delta \in [0.75 \times \lambda, \lambda) \end{cases}, \quad (20)$$

式中: $\Delta = \text{mod}[T_{i,j}(1, 1), \lambda]$, mod 是取模运算; $T_{i,j}(1, 1)$ 为上三角矩阵 $T_{i,j}$ 第 1 行第 1 列元素, $T'_{i,j}$ 为嵌入水印信息的上三角矩阵; λ 为水印嵌入强度。

3) 生成一个全零矩阵作为过渡矩阵, 将嵌入水印后的 $T'_{i,j}(1, 1)$ 写入全零矩阵的对应位置, 得到一个篡改检测矩阵, 记作 M^{TD} 。并根据 M^{TD} 中非零数值的均值进行二值化处理, 得到二值化的篡改检测矩阵 M^{BTD} 。

4) 将嵌入水印信息的 $T'_{i,j}$ 进行 Schur 重构, 并进行小波变换逆操作, 得到含水印的亮度分量 I^Y 。

5) 结合 I^Y 、 I^U 、 I^V 进行 YUV 色彩空间重构, 并将 YUV 色彩空间转到 RGB 颜色空间, 得到含双重水印的图像 I' 。

3.4 版权认证过程

版权认证的过程是构造双重水印的逆过程, 包括在受到攻击的载体含水印图像中提取零水印, 并在零水印中提取版权两个阶段, 如图 5 所示。设受到攻击的含水印图像为 I'_{att} , 具体的操作步骤如下:

1) 含水印图像预处理

① 将受到攻击的彩色医学图像通过傅里叶-梅林算法进行几何校正, 恢复受到几何攻击的图像的相位信息, 得到 I''_{att} 。

② 将校正的图像 I''_{att} 按照第 3.2 小节中步骤 1)~3) 进行预处理, 利用位置密钥 mask key 得到选出嵌入水

5) 将载体特征进行冗余构造, 根据水印图像大小, 排成 $p \times q$ 大小的二值特征矩阵 F' 。

6) 将提取的 ROI 的稳定特征 F' 与第 3.1.1 小节得到的加密的版权图像 S'_w 进行异或运算, 得到鲁棒的零水印 W_z , 同时将零水印信息注册版权保护中心。

$$W_z = \text{XOR}(F', S'_w). \quad (18)$$

3.3 嵌入零水印过程

盲水印过程主要将第 3.2 小节中得到的零水印信息作为版权信息嵌入载体图像的 NROI, 用于实现双重水印, 具体步骤如下:

1) 将选择的 NROI 中的纹理子块 $B_{i,j}^S$ 进行 Schur 分解:

$$[U_{i,j}, T_{i,j}] = \text{Schur}(B_{i,j}^S), \quad (19)$$

式中: $U_{i,j}$ 为酉矩阵; $T_{i,j}$ 为上三角矩阵; i, j 为子块位置的索引, 并且满足 $i \in \left\{1, 2, \dots, \frac{M}{8}\right\}$, $j \in \left\{1, 2, \dots, \frac{N}{8}\right\}$ 。

2) 在上三角矩阵 $T_{i,j}$ 中量化嵌入得到的零水印 W_z :

印信息的 NROI 和用于构造零水印的 ROI。

2) 提取零水印信息

① 对 NROI 中的平滑子块 $B_{i,j}^S$ 依次进行 Schur 矩阵分解, 得到上三角矩阵 $T''_{i,j}$:

$$[\sim, T''_{i,j}] = \text{Schur}(B_{i,j}^S), \quad (21)$$

式中: $i \in \left\{1, 2, \dots, \frac{M}{8}\right\}$; $j \in \left\{1, 2, \dots, \frac{N}{8}\right\}$ 。

② 取上三角矩阵 $T''_{i,j}$ 第 1 行第 1 列的元素 $T''_{i,j}(1, 1)$, 将嵌入水印后的 $T''_{i,j}(1, 1)$ 写入全零矩阵的对应位置, 并将矩阵中非零数值的均值进行二值化处理, 得到二值化的篡改检测矩阵 $M^{BTD'}$ 。同时提取水印信息:

$$W_z'(i, j) = \begin{cases} 0, & \Delta' \in [0, 0.5 \times \lambda) \\ 1, & \Delta' \in (0.5 \times \lambda, \lambda) \end{cases}, \quad (22)$$

式中: $\Delta' = \text{mod}[T''_{i,j}(1, 1), \lambda]$; λ 为水印嵌入强度; W_z' 为提取得到的加密水印。

3) 提取版权水印

① 将 ROI 区域内纹理子块 $B_{i,j}^T$ 进行 2D-DCT, 提取前 4 行 8 列 32 位系数作为攻击后的图像特征, 并按照式 (17) 进行二值化处理, 得到 F'_{att} 。

② 将 F'_{att} 与从含水印图像中提取的攻击后的零水印 W_z' 进行异或运算提取版权水印信息 W_{att} 。

$$W_{att} = \text{XOR}(F'_{att}, W_z'). \quad (23)$$

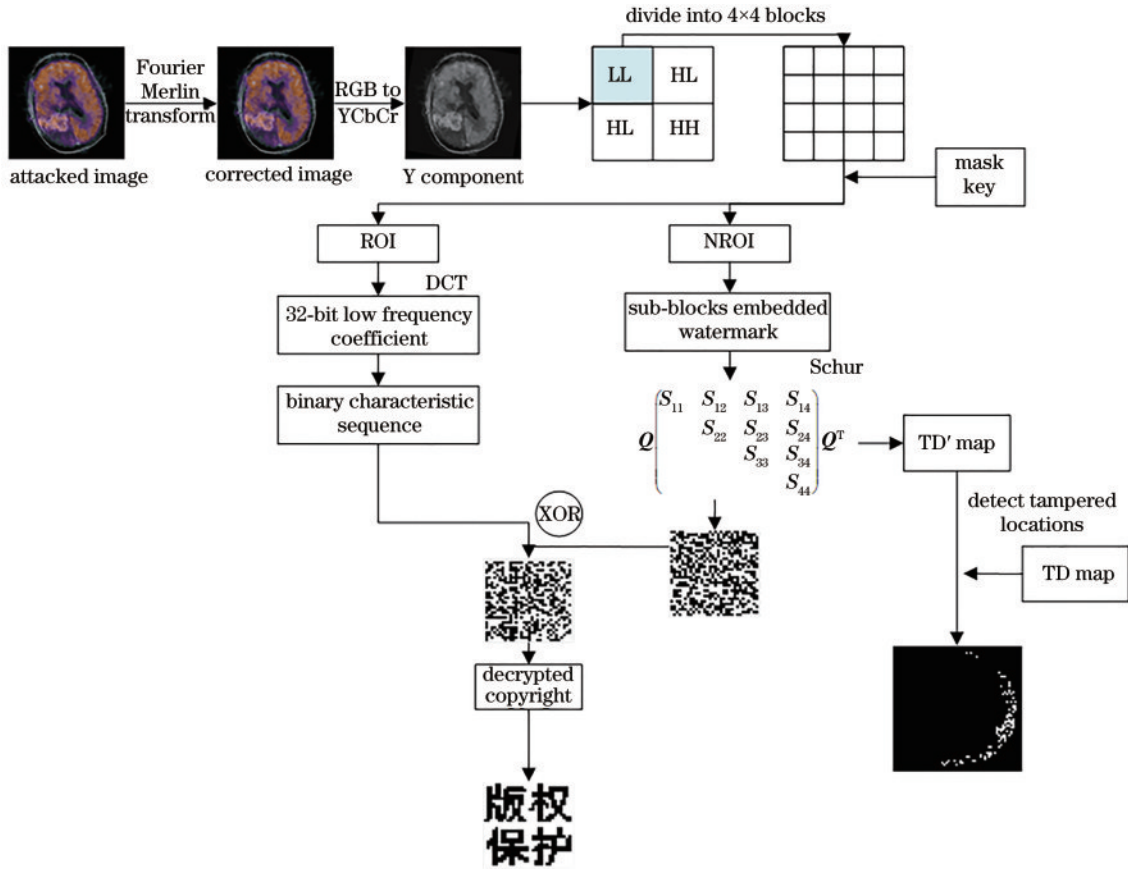


图 5 双重水印提取过程

Fig. 5 Double watermark extraction process

③利用 S-C 混沌系统初值密钥 key 1 对加密的版权水印 W_{att} 进行解密, 提取最终的版权水印 W'_{att} , 并与原始版权 W 进行对比, 确认版权归属。

④同时, 利用 M^{BTD} 和 $M^{BTD'}$ 检测受到篡改的含水印子块位置。

$$M = XOR(M^{BTD}, M^{BTD'}), \quad (24)$$

式中: 当矩阵 M 中数值为 1 时, 说明该位置的子块遭受篡改。

4 实验结果及分析

为了验证所提算法有效性, 选择大小为 $512 \times 512 \times 3$ 的标准彩色医学图像作为载体图像, 如图 6(a)~(h) 所示, 选择大小为 32×32 的二值图像作为版权水印, 如图 6(i) 所示。此外, 为了准确有效地评价所提方案的性能, 对水印图像进行多种仿真攻击实

验, 并与相似的嵌入式水印进行对比。实验采用的软件平台为 Windows 10 操作系统和 Matlab R2016a。本节从双重水印系统的鲁棒性及安全性方面进行分析, 并选用归一化相关系数 (NC) 和误码率 (BER)^[5] 作为衡量水印鲁棒性的标准。

4.1 不可感知性分析

为了平衡所提水印算法的鲁棒性和不可感知性, 选择合适的嵌入强度将零水印嵌入 NROI 中, 并利用 PSNR 作为嵌入式水印不可感知性的评价指标。通常认为, 当图像的 PSNR 大于 36 dB 时, 水印图像具有良好的不可感知性。表 2 为当嵌入强度因子 λ 为 150 时, 得到的含水印图像及与原始图像对比的 PSNR 值。

从表 2 可以看出, 嵌入零水印的彩色医学图像均具有良好的视觉效果, 且含水印的医学图像与原始图像对比, PSNR 最小为 40.7596 dB, 平均 PSNR 为

表 2 水印的不可见性

Table 2 Invisibility of watermark

Image name	Fundus 1	Fundus 2	Fundus 3	Brain map 1	Brain map 2	Brain map 3
Watermarked image						
PSNR /dB	40.7834	40.8793	40.7596	41.0008	41.1943	40.9259

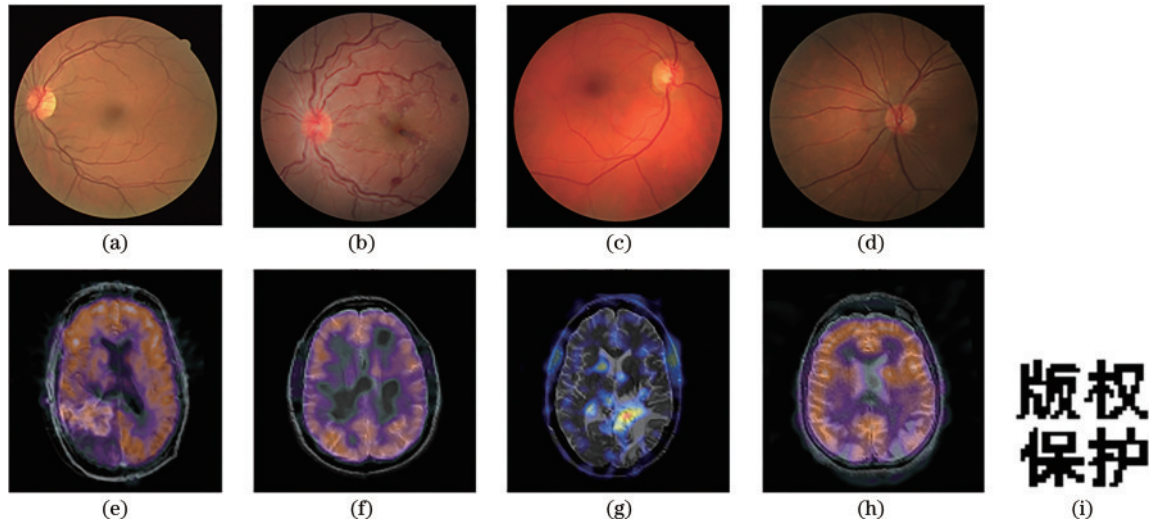


图 6 载体图像和标识图像。(a) 眼底 1; (b) 眼底 2; (c) 眼底 3; (d) 眼底 4; (e) 脑图 1; (f) 脑图 2; (g) 脑图 3; (h) 脑图 4; (i) 版权标识
Fig. 6 Host image and logo image. (a) Fundus 1; (b) fundus 2; (c) fundus 3; (d) fundus 4; (e) brain map 1; (f) brain map 2; (g) brain map 3; (h) brain map 4; (i) copyright logo

40.9239 dB。由于所提算法在医学图像的 RONI 嵌入水印信息,未破坏医学图像主体内容,同时具备良好的视觉效果,可以满足医学图像对不可感知性的要求。

4.2 篡改检测分析

为了验证所提篡改检测的有效性,可以准确定位出遭到篡改的含水印子块的位置,对含水印的脑部图像添加不同的攻击。图 7 显示了在不同攻击下的含水印图像和篡改检测的结果。

从图 7(a)可以看出,当含水印图像没有受到攻击时,嵌入水印信息的子块没有被篡改,水印信息可以完全提取;从图 7(b)可以看出,当受到较大强度的高斯

噪声攻击时,部分嵌入水印信息的子块被篡改,提取的水印图存在失真;从图 7(c)可以看出,当受到 11×11 的中值滤波攻击时,含水印图像变得模糊,影响到嵌入水印信息的子块,导致水印信息遭到破坏;图 7(d)、(e)分别为受到 50 行 50 列偏移和 75 行剪切攻击的检测情况,当含水印图像受到较大尺度的偏移和剪切时,相应位置的水印信息丢失,检测的结果与攻击的位置一致;从图 7(f)可以看出,由于水印信息嵌入载体图像内接圆内,当含水印图像受到旋转攻击时,嵌入水印信息的位置仅受到很小的干扰。一系列实验结果表明,篡改检测的结果与提取版权的结果一致,说明所提篡

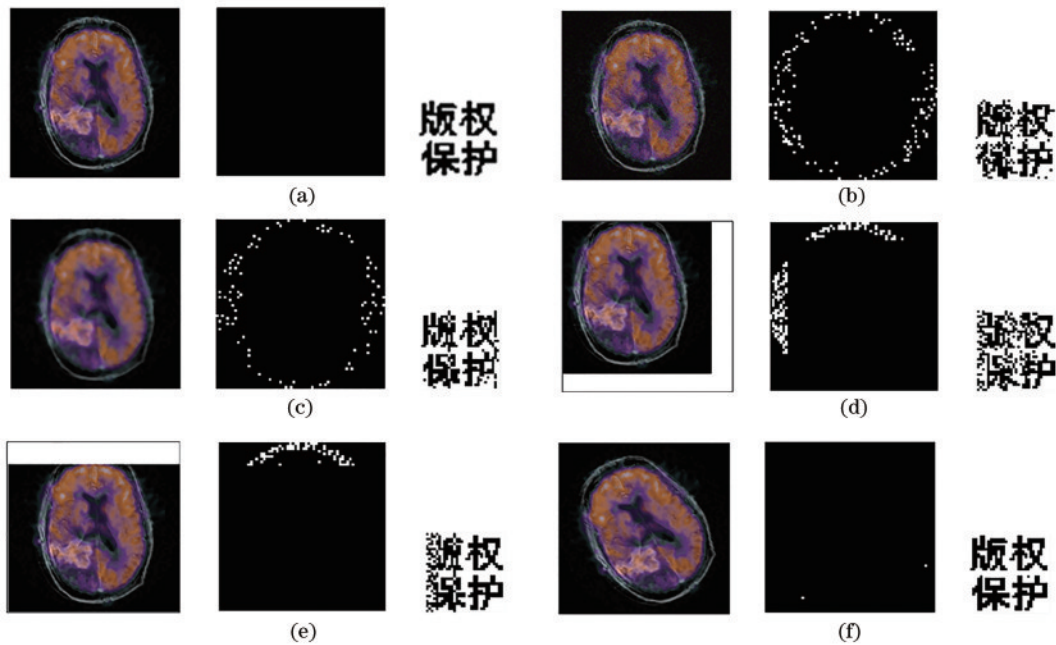


图 7 篡改检测。(a) 无攻击; (b) 高斯噪声 0.005; (c) 中值滤波 11×11 ; (d) 行列偏移 50×50 ; (e) 剪切 75 行; (f) 旋转 30°
Fig. 7 Tamper detection. (a) No attack; (b) Gaussian noise 0.005; (c) median filter 11×11 ; (d) row and column offset 50×50 ; (e) cut 75 lines; (f) rotate 30°

改检测算法可以准确定位遭到篡改的含水印子块的位置。

4.3 鲁棒性分析

为了验证双重水印系统的鲁棒性,分别对双重水印进行几何攻击和非几何攻击,并对得到的 NC 值进行分析。鲁棒测试阶段,水印的嵌入强度因子 λ 取 150。在提取版权水印阶段,对水印的嵌入位置进行选择,同时利用傅里叶-梅林算法检测含水印图像受到几何攻击的参数,并根据得到的参数对图像进行校正。

4.3.1 非几何攻击

非几何攻击将攻击信号叠加到原始图像上来改变像素值的大小。为了测试所提算法在受到非几何攻击时的鲁棒性,分别对 6 幅彩色医学图像进行非几何攻击测试,计算其提取水印的 NC 值及 BER 并分别对攻击后的版权与零水印的 NC 值进行分析,分别对 6 幅测试图像添加强度为 0.002 和 0.005 的高斯噪声、椒盐噪声和乘性噪声、滤波窗口为 3×3 、 7×7 和 11×11 的中值滤波、维纳滤波和高斯滤波及压缩因子为 20 和 30 的 JPEG 压缩,分别计算提取的零水印与原始零水印之间的相似度(分别用 BER1 和 NC1 表示)及攻击后的版权与原始版权之间的相似度(分别用 BER2 和 NC2 表示)。非几何攻击的实验结果如表 3 所示。

表 3 双重水印的非几何攻击实验结果

Table 3 Experimental results of non geometric attack on double watermark

Attack type	Parameter	BER1	NC1	BER2	NC2
Gaussian noise	0.002	0.0034	0.9966	0.0073	0.9935
	0.005	0.1130	0.8841	0.1262	0.8864
Salt & Pepper noise	0.002	0.0424	0.9582	0.0424	0.9623
	0.005	0.0916	0.9094	0.0945	0.9152
Speckle noise	0.005	0.0000	1.0000	0.0000	1.0000
	0.010	0.0000	1.0000	0.0000	1.0000
Median filtering	3×3	0.0000	1.0000	0.0078	0.9930
	7×7	0.0000	0.9996	0.0273	0.9755
	11×11	0.0505	1.0000	0.0818	0.9268
Wiener filtering	3×3	0.0000	1.0000	0.0000	1.0000
	7×7	0.0010	0.9498	0.0125	0.9889
	11×11	0.0706	1.0000	0.0876	0.9213
Gaussian filtering	3×3	0.0000	0.9991	0.0039	0.9965
	7×7	0.0000	0.9301	0.0039	0.9965
	11×11	0.0000	1.0000	0.0039	0.9965
JPEG	20	0.0000	1.0000	0.0117	0.9895
	30	0.0000	1.0000	0.0000	1.0000

从表 3 可以看出,当嵌入零水印的载体图像受到非几何攻击时均表现出较强的鲁棒性能。当受到噪声攻击时,攻击后的版权水印的 NC 值均在 0.88 以上,当受到乘性噪声时,水印的误码率为 0.0000,NC 值为 1.0000,说明水印算法在噪声攻击下具有较强的鲁棒

性。当受到滤波攻击时,提取的零水印的 NC 值均在 0.93 以上,版权认证的结果也均在 0.92 以上,说明所提算法可以抵抗较大强度的滤波攻击。当受到 JPEG 压缩且压缩因子为 30 时,提取的版权的误码率为 0.0000,可以无损地提取水印信息。

4.3.2 几何攻击

几何攻击对图像的像素位置的改变较大,载体图像受到几何攻击后,会破坏提取水印的同步性。在提取水印前,使用傅里叶-梅林变换算法对受到攻击后的图像进行相位检测,估计图像受到几何攻击的参数,用于图像的几何校正。为测试所提算法的有效性,对 6 幅载体图像分别进行旋转、缩放和剪切攻击,实验结果如表 4 所示。

表 4 几何攻击实验结果

Table 4 Experimental results of geometric attack

Attack type	Parameter	BER1	NC1	BER2	NC2
Scaling	0.25	0.0007	1.0000	0.0039	0.9965
	0.5	0.0007	1.0000	0.0000	1.0000
	2	0.0003	1.0000	0.0000	1.0000
	4	0.0160	1.0000	0.0000	1.0000
Crop	Upper left 1/8	0.0003	1.0000	0.0000	1.0000
	Upper left 1/4	0.0007	0.9723	0.0985	0.9119
	Center 1/8	0.0169	0.9981	0.1533	0.8608
	Center 1/4	0.0723	0.9927	0.1992	0.8201
Rotate	15	0.0033	0.9954	0.0085	0.9924
	30	0.0029	0.9983	0.0056	0.9950
	45	0.0091	0.9989	0.0011	0.9990
	90	0.0003	1.0000	0.0000	1.0000

由表 4 可知,对于缩放攻击,双重水印的鲁棒性能都很高,NC 值最高为 1.0000,最低为 0.9965。对于剪切攻击,整体的 NC 值均很高,但是当剪切面积过大时,位于载体图像的中心部位的 ROI 遭到破坏,导致提取的载体特征存在误差,使得版权认证结果低于提取的零水印之间的相似度,存在部分 NC 值偏低的现象,但是 NC 值仍在 0.8201 以上,表明所提算法对于剪切操作具有较好的抵抗能力。当含水印的载体图像受到旋转攻击时,由于在进行零水印提取和版权认证前使用了傅里叶-梅林算法对旋转角度进行估计,并对受攻击的含水印图像进行几何矫正,所以算法抗旋转性能良好。由于水印信息嵌入在医学图像的内接圆区域内,因此受到旋转攻击时,嵌入水印的子块不会发生信息丢失,但是在旋转矫正过程中会存在微小的误差,导致水印信息不能完全提取,但当旋转角度较大时,提取的版权的 NC 值仍在 0.99 以上。

4.4 对比实验及分析

4.4.1 鲁棒性实验对比

为了验证所提算法的优越性,选取近年来先进的

盲水印算法 [8-10] 进行实验对比, 并选取像素值为 512×512 的 6 幅彩色医学图像作为载体图像, 选取大小为 32×32 带有“版权保护”标识的二值图像作为水印图像, 将文献 [8-10] 的含水印图像与本研究水印图像的 PSNR 值均平衡在 40 左右, 分别对含水印的 6 幅

含水印医学图像进行非几何攻击和几何攻击: 非几何攻击包括噪声攻击、JPEG 压缩攻击和滤波攻击; 几何攻击包括旋转攻击、缩放攻击和剪切攻击, 并计算在每种攻击下的平均 NC 值。具体对比实验结果如表 5 所示。

表 5 实验对比结果
Table 5 Experimental comparison results

Attack type	Parameter	Reference[8]	Reference[9]	Reference[10]	NC1	NC2
Gaussian noise	0.002	0.8900	0.8226	0.7634	0.9966	0.9935
	0.005	0.8546	0.8002	0.7181	0.8841	0.8864
Salt & Pepper noise	0.002	0.9450	0.9602	0.6859	0.9582	0.9623
	0.005	0.9338	0.9580	0.6973	0.9094	0.9152
Speckle noise	0.002	0.9466	0.9826	0.6800	1.0000	1.0000
	0.005	0.9452	0.9815	0.6663	1.0000	1.0000
Median filtering	3×3	0.5019	0.9346	0.6815	1.0000	0.9930
	5×5	0.3993	0.6873	0.8127	0.9996	0.9755
Wiener filtering	3×3	0.8636	0.9662	0.8390	1.0000	1.0000
	7×7	0.8649	0.7822	0.7692	0.9498	0.9889
Gaussian filtering	3×3	0.8489	0.9522	0.8757	0.9991	0.9965
	7×7	0.8005	0.9408	0.8206	0.9301	0.9965
JPEG	20	0.4747	0.7346	0.7658	1.0000	0.9895
	30	0.6838	0.9315	0.9243	1.0000	1.0000
Scaling	2	0.9350	0.9777	0.8136	1.0000	1.0000
	4	0.9398	0.9791	0.6840	1.0000	1.0000
	0.5	0.8558	0.9544	0.8136	1.0000	1.0000
	0.25	0.4314	0.6169	0.6801	1.0000	0.9965
Crop	Upper left 1/8	0.9466	0.9823	0.6944	1.0000	1.0000
	Upper left 1/4	0.9346	0.9788	0.7067	0.9723	0.9119
	Center 1/8	0.9468	0.9693	0.6770	0.9981	0.8608
	Center 1/4	0.9468	0.9176	0.6669	0.9927	0.8201
Rotate	15	0.8381	0.9339	0.8610	0.9954	0.9924
	30	0.8517	0.9491	0.8541	0.9983	0.9950
	45	0.9246	0.9736	0.8267	0.9989	0.9990
	90	0.9468	0.9823	0.9400	1.0000	1.0000

从表 5 可以看出, 所提双重水印算法在几何攻击和非几何攻击下的鲁棒性整体高于文献 [8-10] 算法。在受到噪声攻击时, 所提水印算法的 NC 均高于文献 [8, 10] 算法, 仅在受到 0.005 的椒盐噪声时略低于文献 [9] 算法; 在受到滤波攻击时, 所提算法鲁棒性远高于文献 [8-10] 算法, 最低仍在 0.94 以上, 而文献 [8-10] 算法的 NC 值均在 0.82 以下, 最低仅为 0.39。当受到剪切攻击时, 由于所提算法将水印嵌入载体图像内接圆内, 在受到剪切攻击时, 损失的水印信息较少, NC 值均高于文献 [8-10] 算法。为了验证所提算法在旋转攻击下的鲁棒性, 在提取水印时, 均使用傅里叶-梅林算法对受到旋转攻击的图像进行几何校正, 在同样的攻击强度下,

所提算法的鲁棒性仍高于文献 [8-10] 算法, 说明在旋转攻击下所提算法更具鲁棒性。由于文献 [8-9] 算法均匀地将水印图像嵌入整个载体图像, 这不仅会影响图像的整体视觉效果, 且在常规攻击下图像的边缘信息更容易受到影响, 进而影响系统的鲁棒性。文献 [10] 算法在嵌入水印前, 对 DCT 系数进行分析, 选择 DCT 稳定的低频系数作为水印嵌入位置, 可平衡鲁棒性与不可感知性。而所提算法在嵌入水印前划分安全区域, 并利用子块熵值选择嵌入水印信息的子块, 减小了水印信息被抹去的可能性, 与文献 [8-10] 算法相比, 无论在几何攻击还是非几何攻击上, 整体鲁棒性能更优。

4.4.2 算法效率对比

对水印构造的时间和版权认证的时间进行测试,并与文献[8-10]算法进行对比。实验均在 Intel-i5-

10210U 处理器、8 GB 运行内存、Windows 10 操作系统和 Matlab R2016a 的软件平台上进行,并且进行多次实验,具体的实验结果如表 6 所示。

表 6 水印算法运行时间

Table 6 Running time of watermarking algorithm

Algorithm	Technology	Embedding time /s	Extraction time /s	Extraction time /s
Reference[8]	DCT+DFT	1.2634	0.5485	1.8092
Reference[9]	DWT+SVD	1.6563	0.8289	2.4582
Reference[10]	CT+DCT+SVD	0.7390	0.2343	0.9733
Proposed algorithm	DWT+DCT+Schur	0.5570	0.0654	0.6224

从表 6 可以看出,所提算法的运行效率远高于文献[8-10]算法。由于所提算法在水印构造过程中,对载体图像进行 DWT 后将低频子带进行分区域计算,对纹理子块执行 DCT 运算,对内接圆内的平滑子块执行 Schur 分解,在一定程度上提高了运算的速率。因此双重水印构造时间和版权认证的时间累计仅为 0.6224 s。文献[8]算法虽然是在空间域进行水印的嵌入,但是在空间域进行了两次遍历,并依次进行了 DCT 和 DHT,因此运行的时间较长,但是总运行时间仍低于 2 s。文献[9]算法进行了 3 级 DWT,并对低频系数进行 SVD,增加了计算量,因此算法的运行时间较长,效率较低。文献[10]算法结合多种频域变换和矩阵分解的方法,分别进行 CT、DCT 和 SVD,具有较高的复杂度。

4.5 安全性分析

为了验证所提 Sine-Cubic 混沌加密映射的安全

性,对初值敏感度和与随机矩阵的相似度进行测试。为测试混沌映射加密的初值敏感度,取 Sine-Cubic 映射的混沌初值为 0.312346778,将测试的初值范围选择在 $[0.312345678, 0.312345878]$,并以 1×10^{-9} 的步长增长,生成 200 个与混沌序列相等的混沌序列,其中第 101 个为正确的初值。分别计算与正确混沌初值序列相似度的 NC 值,如图 8(a)所示,只有在第 101 个正确的初值产生的混沌序列的 NC 为 1,其余均为 0.5 左右,说明所提 Sine-Cubic 混沌加密映射具有很高的初值敏感度。为测试利用 Sine-Cubic 混沌映射生成的混沌序列的唯一性,随机生成 200 个与混沌序列大小相等的二值序列,并用正确的混沌序列替换第 101 个随机序列,分别计算与正确的混沌序列的 NC 值,如图 8(b)所示,只有第 101 个正确序列的 NC 值为 1,其余的随机混沌序列的 NC 仅在 0.5 左右,说明利用 Sine-Cubic 混沌加密映射产生的序列具有唯一性。

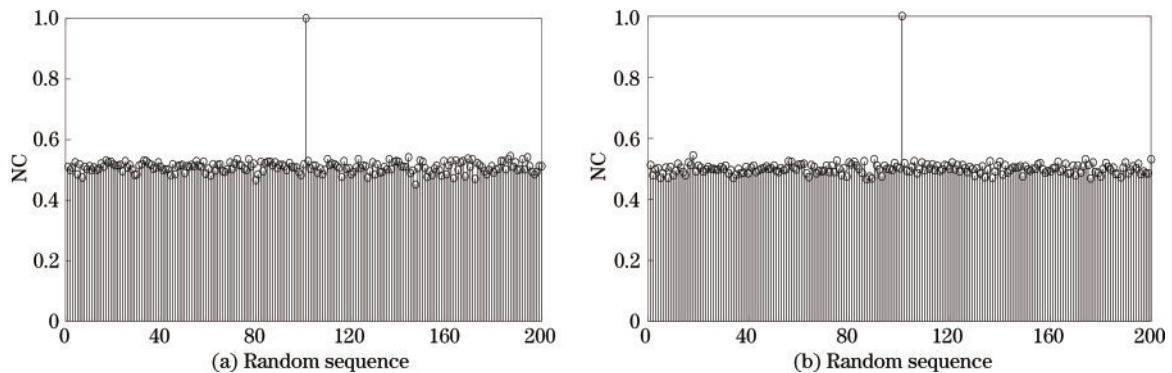


图 8 安全性实验。(a) 初值敏感性测试;(b) 混沌序列唯一性测试

Fig. 8 Security experiment. (a) Initial value sensitivity test; (b) chaotic sequence uniqueness test

实验结果表明,所提 S-C 混沌映射加密算法的初值敏感度可以精确到小数点后的第 9 位,而耦合前的 Sine 映射和 Cubic 映射的初值敏感度仅精确到小数点后的第 5 位^[23],说明所提 S-C 混沌映射具有更大的密钥空间,可以保证水印在网络中安全传输。

5 结 论

提出了一种面向医学图像的篡改检测双重水印方案。实验结果表明,所提水印方案能够有效地抵抗几何

攻击和非几何攻击。根据图像的信息熵分析载体图像的纹理特点,并将构造的鲁棒零水印嵌入 NROI 的子块,保证医疗诊断的准确性和水印的不可感知性。此外,采用所提 Sine-Cubic 混沌映射算法加密水印图像后,混沌初值密钥具有较高敏感度,且具备很好的加密效果,提升了水印算法的安全性。由于所提算法主要平衡含水印医学图像的鲁棒性与透明性,未引入编码方式对版权信息进行检错纠错,今后将尝试对载体进行多区域划分嵌入编码后的信息,以提高算法的检错纠错性能。

参 考 文 献

- [1] 吴德阳, 赵静, 汪国平, 等. 一种基于改进奇异值和子块映射的图像零水印技术[J]. 光学学报, 2020, 40(20): 2010002.
Wu D Y, Zhao J, Wang G P, et al. An image zero watermarking technology based on ameliorated singular value and subblock mapping[J]. Acta Optica Sinica, 2020, 40(20): 2010002.
- [2] 刘颖, 杨星, 朱婷鸽. 基于结构森林边缘和 SIFT 的鲁棒水印算法[J]. 激光与光电子学进展, 2021, 58(6): 0615006.
Liu Y, Yang X, Zhu T G. Robust watermarking algorithm based on structured forests edge and SIFT[J]. Laser & Optoelectronics Progress, 2021, 58(6): 0615006.
- [3] Zermi N, Khaldi A, Kafi R, et al. A DWT-SVD based robust digital watermarking for medical image security[J]. Forensic Science International, 2021, 320: 110691.
- [4] Fares K, Khaldi A, Redouane K, et al. DCT & DWT based watermarking scheme for medical information security[J]. Biomedical Signal Processing and Control, 2021, 66: 102403.
- [5] Chowdary N S D, Sivaraman R, Sridevi A, et al. Transform domain influenced variable bit-variable pixel medical image watermarking scheme[C]//2020 International Conference on Computer Communication and Informatics (ICCCI), January 22-24, 2020, Coimbatore, India. New York: IEEE Press, 2020.
- [6] Moosazadeh M, Ekbatanifard G. A new DCT-based robust image watermarking method using teaching-learning-based optimization[J]. Journal of Information Security and Applications, 2019, 47: 28-38.
- [7] 吴为民, 陈家祯. 基于双快速反应码双随机相位加密系统的多重水印方法[J]. 激光与光电子学进展, 2017, 54(12): 120901.
Wu W M, Chen J Z. Multiple watermarking method based on double random phase encryption system with double quick response code[J]. Laser & Optoelectronics Progress, 2017, 54(12): 120901.
- [8] Su Q T, Su L, Wang G, et al. A novel colour image watermarking scheme based on Schur decomposition[J]. International Journal of Embedded Systems, 2020, 12(1): 31-38.
- [9] 张琳琳, 杨亮, 高铁杠. 基于自嵌入鲁棒双水印的图像认证算法[J]. 光电子·激光, 2020, 31(2): 206-213.
Zhang L L, Yang L, Gao T G. Self-embedding robust dual watermarking scheme for image authentication[J]. Journal of Optoelectronics·Laser, 2020, 31(2): 206-213.
- [10] Tian C, Wen R H, Zou W P, et al. Robust and blind watermarking algorithm based on DCT and SVD in the contourlet domain[J]. Multimedia Tools and Applications, 2020, 79(11): 7515-7541.
- [11] 温泉, 孙铤锋, 王树勋. 零水印的概念与应用[J]. 电子学报, 2003, 31(2): 214-216.
Wen Q, Sun T F, Wang S X. Concept and application of zero-watermark[J]. Acta Electronica Sinica, 2003, 31(2): 214-216.
- [12] 胡森, 吴德阳, 仲美玉, 等. 基于 SURF 和半色调映射加密的彩色零水印算法[J]. 激光与光电子学进展, 2021, 58(20): 2010017.
Hu S, Wu D Y, Zhong M Y, et al. Color zero-watermarking algorithm based on SURF and halftone mapping encryption[J]. Laser & Optoelectronics Progress, 2021, 58(20): 2010017.
- [13] Singh A, Dutta M K. Lossless and robust digital watermarking scheme for retinal images[C]//2018 4th International Conference on Computational Intelligence & Communication Technology (CICT), February 9-10, 2018, Ghaziabad, India. New York: IEEE Press, 2018.
- [14] Liu X Y, Lou J T, Wang Y F, et al. Discriminative and robust zero-watermarking scheme based on completed local binary pattern for authentication and copyright identification of medical images[J]. Proceedings of SPIE, 2018, 10579: 105791I.
- [15] Zou B J, Du J Y, Liu X Y, et al. Distinguishable zero-watermarking scheme with similarity-based retrieval for digital rights Management of Fundus Image[J]. Multimedia Tools and Applications, 2018, 77(21): 28685-28708.
- [16] Wang W B, Li Y, Liu S L. A polar complex exponential transform-based zero-watermarking for multiple medical images with high discrimination[J]. Security and Communication Networks, 2021, 2021: 6615678.
- [17] Xia Z Q, Wang X Y, Wang C P, et al. Novel quaternion polar complex exponential transform and its application in color image zero-watermarking[J]. Digital Signal Processing, 2021, 116: 103130.
- [18] Hu R W, Xiang S J. Lossless robust image watermarking by using polar harmonic transform[J]. Signal Processing, 2021, 179: 107833.
- [19] Yap P T, Jiang X D, Kot A C. Two-dimensional polar harmonic transforms for invariant image representation [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2010, 32(7): 1259-1270.
- [20] Geetha R, Geetha S. Efficient high capacity technique to embed EPR information and to detect tampering in medical images[J]. Journal of Medical Engineering & Technology, 2020, 44(2): 55-68.
- [21] Tarhouni N, Charfeddine M, Amar C B. Novel and robust image watermarking for copyright protection and integrity control[J]. Circuits, Systems, and Signal Processing, 2020, 39(10): 5059-5103.
- [22] Tayachi M, Nana L, Benzarti F, et al. A dual watermarking approach for DICOM images[C]//2020 5th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), September 2-5, 2020, Sousse, Tunisia. New York: IEEE Press, 2020.
- [23] 赵欣. 不同一维混沌映射的优化性能比较研究[J]. 计算机应用研究, 2012, 29(3): 913-915.
Zhao X. Research on optimization performance comparison of different one-dimensional chaotic maps[J]. Application Research of Computers, 2012, 29(3): 913-915.