

一种基于混沌映射和奇异值分解的数字图像水印算法

焦 问 丁文霞

(国防科技大学电子科学与工程学院, 湖南 长沙 410073)

摘 要: 为了保证数字图像水印的安全性、透明性和鲁棒性, 本文提出了一种基于混沌映射和奇异值分解的数字图像水印算法。混沌映射具有初值敏感性, 以映射初值为私钥, 利用混沌映射将二值水印图像进行双混沌置乱, 这样可以提高水印嵌入的安全性。利用奇异值分解特性来嵌入水印, 把 U 矩阵中第一列系数作为研究对象, 采用保持相邻系数之间差值关系的方法来表示嵌入的水印比特, 这种系数差值关系在经过信号处理后能够得到保持。通过仿真实验, 表明嵌入水印后的图像具有良好的透明性, 同时还具有抵抗图像信号处理的鲁棒性。此外, 当含水印图像的内容遭到篡改时, 提取出的水印仍易于辨认, 并且能对篡改进行检测和定位。

关键词: 混沌映射; 奇异值分解; 数字水印

中图分类号: TN911 **文献标识码:** A **文章编号:** 1003-0530(2011)08-1219-05

A Digital Image Watermarking Scheme Based on Chaotic Mapping and Singular Value Decomposition

JIAO Wen DING Wen-xia

(College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China)

Abstract: In order to guarantee the security, transparency and robustness of digital image watermark, a scheme based on chaotic mapping and singular value decomposition (SVD) is proposed. Since chaotic mapping is sensitive to initial values; two chaotic maps are employed to scramble the rows and columns of the watermark image, which can enhance the security of the watermark. Initial values of the chaotic mapping are used as private key in the scheme. To utilize the characteristic of the SVD domain for embedding a watermark, the coefficients in the first column of U component are examined. The magnitude difference between the neighboring coefficients is taken as the relationship to embed the watermark. The relationship could be preserved when general image processing is performed. Experimental results demonstrate that the quality of the watermarked image is good and there is strong resistance against general image processing. Furthermore, the scheme can accurately detect and locate the place being tampered in the watermarked image, and the extracted watermark can still be easily identified.

Key words: chaotic mapping; singular value decomposition; digital watermarking

1 引言

数字水印技术已成为当今信息科学前沿领域一个新颖且具有广泛应用前景的研究热点, 尤其是在图像领域, 通常用于图像的数字水印应当具备以下三个基本要求^[1]: 安全性、透明性和鲁棒性。混沌映射具有对初值敏感性高、安全性强、密钥空间大且非周期的特性, 基于混沌映射来提高数字水印算法的性能, 主要有以下几种方法: 用混沌映射产生的序列作为水印信号^[2], 实现水印的随机嵌入^[3], 将水印信号进行置乱处理^[4]等。常用的图像置乱方法包括基于 Magic 变换、Arnold 变换, 它们都能实现对图像加密, 但密钥空间较小, 置乱矩阵是有周期的, 置乱后的图像再继续经过多次同样变换后会恢复到原图像。当算法公开时, 攻击

者容易破解恢复图像水印。而采用单一混沌映射进行图像置乱, 会构成置换群, 安全性能不高。本文采用 Arnold 变换与 Logistic 混沌映射进行组合对有意义的二值图像水印进行置乱处理, 通过增大密钥空间和克服置换群效应来提高水印置乱的安全性。为了兼顾数字图像水印的透明性和鲁棒性, 目前主要采用在图像变换域系数中嵌入水印, 大多数变换域水印算法是基于 DCT 和 DWT 实现的。而奇异值分解^[5]作为数值线性代数分析的一种重要工具, 在统计分析、信号与图像处理中被广泛应用。一些基于奇异值分解的数字水印算法把分解得到的奇异值矩阵 D 作为研究对象, 将水印嵌入到最大的奇异值中^[6]。这种方法利用了最大奇异值在图像信号处理中的相对稳定性, 但对最大奇异值的修改会使重构图像的质量受到较大影响。本文提

出一种调整奇异值分解 U 矩阵中第一列系数的水印嵌入方法,利用系数之间相对关系具有抗图像信号处理的稳健特性,使得修改后的系数间差值达到预先给定的门限,从而实现水印的嵌入,利用系数之间的相对稳定性,可提高水印抗噪声攻击的鲁棒性。

2 二值图像水印的双混沌置乱

从理论上讲,定义在连续域上的混沌映射的周期点的测度为零,也就是说,一个周期轨道的任意小的邻域内都会存在非周期轨道。而目前混沌系统的应用大多是在计算机系统上实现的,基于计算机离散混沌的计算是在有限精度下进行的,这就给混沌系统的性能带来很大负面影响^[7],从而产生动力学退化等现象。文献[8]已从理论角度证明了定长混沌二值序列集合对异或运算构成群,所以当用混沌二值序列作为密钥对数据流进行简单的异或加密时,使用多重加密将是无效的。并且所有 $N \times N$ 二维混沌置乱矩阵组成的集合对置换操作构成置换群,且为有限群,其阶为 $(N \times N)!$ 。本文提出一种 Arnold 变换与 Logistic 映射相组合的置乱算法,可以克服离散混沌系统中动力学退化问题、平凡密钥现象及单个混沌迭代轨迹暴露等问题,提高置乱算法的安全性。具体来说,采用 Arnold 变换与 Logistic 映射组合进行水印置乱的意义有以下三点:第一,用 Logistic 映射进行行列置乱改变了像素点间的空间位置,可以有效避免 Arnold 变换的短周期性;第二,尽管 Logistic 行列矩阵置乱变换构成了一个置换群,但由于 Arnold 变换的实质是先对原图像进行线性拉伸,再通过取模运算进行折叠,因而 Logistic 置换与 Arnold 结合以后很好的克服了单一系列矩阵置换的群效应;第三,进行整行整列置乱是为了减少密钥存储空间,同时加快算法的运行速度。

二维 Arnold 映射原始定义如下:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{1}, A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \quad (1)$$

由于 $\det A = 1$, 所以上述映射是保面积的一一映射,其 Lyapunov 指数为:

$$\lambda_1 = \ln\left(\frac{3}{2} + \frac{\sqrt{5}}{2}\right) > 0, \lambda_2 = \ln\left(\frac{3}{2} - \frac{\sqrt{5}}{2}\right) < 0 \quad (2)$$

其中 $\lambda_1 > 0$, 所以二维 Arnold 映射为混沌映射。通过引入参数 a 、 b 并扩展到 $N \times N$, 同时离散化, 可得到:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} ab+1 & a \\ b & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N}, \quad (3)$$

$x_0, y_0 \in \{0, 1, \dots, N-1\}$

在有限字长的计算机中直接利用混沌系统产生混沌伪随机数,使得原来没有周期的混沌序列将出现周期,且周期长度是随机的。目前对该周期长度的分析尚无理论结果,数值模拟表明周期长度和计算精度与初值选取有关^[9]。如取 $a=40$, $b=8$, $N=124$ 时,用式

(3)式对图像像素位置进行置乱,仅仅经过5轮迭代,图像即恢复原样。由于二维 Arnold 映射数字化时具有周期性现象,则对于其置乱的图像只要知道置乱算法,按照置乱空间的任意一个状态来进行迭代,都可以通过有限步恢复出原图。为增强嵌入水印的安全性,产生两个 Logistic 混沌序列分别置乱二维 Arnold 变换后的水印图像的行和列,这样一方面避免了 Arnold 变换的短周期性,另一方面使 Arnold 变换和 Logistic 映射这两种结构不同的混沌系统相结合,克服了单一混沌置乱的群效应。Logistic 混沌映射的基本定义如下:

$$x_{n+1} = \mu x_n (1 - x_n), n \in \mathbb{Z}, \mu \in [0, 4], x_n \in (0, 1) \quad (4)$$

图1显示了该映射的 Lyapunov 指数 (LE) 随分支参数 μ 在区间 $3.4 \leq \mu \leq 4$ 的变化图。

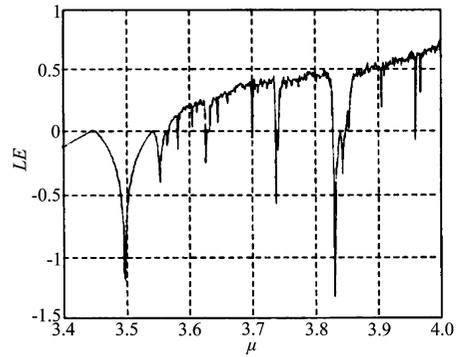


图1 一维 Logistic 映射的 LE 随分支参数 μ 的变化图

Fig. 1 The relationship between LE and μ for one-dimensional Logistic mapping

文献[10]在介绍 Lyapunov 指数计算方法中说明了当 $LE > 0$ 时,系统处于混沌状态,且 LE 越大,系统的混沌性越强,即对初值变化越敏感。当 $3.5699456 < \mu \leq 4$ 时,Logistic 映射工作于混沌状态。为保证系统混沌性达到最强,文中选取 $\mu=4$ 。

对一幅 $N \times N$ 的二值水印图像,可用矩阵表示为 $W(m, n)$, ($1 \leq m \leq N$, $1 \leq n \leq N$, $m, n \in \mathbb{Z}$)。下面给出对水印图像的置乱步骤:

①将参数 a 、 b 及迭代轮数 L 作为 Arnold 变换的密钥以增大密钥空间,采用(3)式对 $W(m, n)$ 进行空间置乱,得到 $W^A(m, n)$,再选取 key_1 和 key_2 ($0 < key_1, key_2 < 1$) 作为矩阵行、列置乱的两个密钥,即 Logistic 映射的迭代初始值;

②令迭代初值 $x_0 = key_1$, 利用(4)式中 logistic 映射进行迭代,从迭代数据中(舍弃初始段数据)随机选取 N 个互不相同的值,记为数组 $\{y_i\}$ ($i=1, 2, \dots, N$), 将 $\{y_i\}$ 按照由大到小的顺序进行排序,得到 $\{z_j\}$ ($j=1, 2, \dots, N$);

③初始化 $W^R(m, n) = 0$, 找出 $\{y_i\}$ 与 $\{z_j\}$ 中元素的对应关系,即从 $i=1, 2, \dots, N$, 如果 $y_i = z_j$, 则将矩阵 $W^A(m, n)$ 第 i 行中的所有元素放入矩阵 $W^R(m, n)$ 的第 j 行中,直到放满 $W^R(m, n)$ 为止;

④在行置乱的基础上,初始化矩阵 $W^*(m, n) = 0$, 令

迭代初值 $x_0 = key_2$, 按照步骤②、③中的方法将矩阵 $W^R(m,n)$ 中的各列所有元素放入矩阵 $W^*(m,n)$ 的对应列中, 这样就得到了最终待嵌入的水印图像 $W^*(m,n)$ 。

3 基于奇异值分解的数字水印算法

图像的奇异值分解是将一个图像像素矩阵分解为三个矩阵的乘积, 其中两个是酉矩阵, 一个是奇异值组成的对角矩阵。奇异值分解可表示为:

$$I = U \times S \times V^H \quad (5)$$

其中 I 为水印载体图像, U 和 V 为酉矩阵, V^H 为 V 的共轭转置, S 为奇异值对角阵。Sun 等人在文献[6]中提出了对奇异值矩阵 S 中的最大奇异值 S_{max} 进行量化来嵌入水印的方法, 最大奇异值 S_{max} 的稳定性使得这种方法具有抵抗一定强度图像信号处理的能力。除了在最大奇异值中嵌入水印以外, 经研究发现奇异值分解后的 U 矩阵中第一列系数之间的相对关系在图像信号处理后能够得到保持, 可以对系数进行修改, 使其相对关系满足预先设定的门限来实现水印的有效嵌入^[11]。将修改后的 U 矩阵进行逆 SVD 运算得到含水印的重构图像, 虽然在提取水印时进行 SVD 变换得到的 U 矩阵与嵌入水印时进行修改的 U 矩阵并不相同, 但是 U 矩阵第一列中系数之间的相对关系仍能够得到保持^[12]。本文选择保持相邻两个系数之间的绝对值之差来实现水印的嵌入。具体嵌入过程如下:

①以 4×4 大小对灰度载体图像进行分块, 对每块进行奇异值分解;

②将前面完成置乱的水印图像按照对应的行列顺序嵌入到每一个图像分块中, 这里选择分块奇异值分解中的 U 矩阵第一列第 2、3 个系数的相对值来嵌入水印, 如果待嵌入的比特为 1, 则要求 $|u_{2,1}| - |u_{3,1}| > T$, 如果待嵌入的比特为 0, 则要求 $|u_{3,1}| - |u_{2,1}| > T$, 其中门限值 $T > 0$, 大的门限值将降低含水印图像的峰值信噪比, 但同时也提高了水印的鲁棒性;

③如果 U 矩阵中的系数不满足要求, 则将 $u_{2,1}$ 、 $u_{3,1}$ 修改为 $u_{2,1}^*$ 、 $u_{3,1}^*$, 如果嵌入比特为 1, 令 $r = |u_{2,1}| - |u_{3,1}|$:

当 $u_{2,1} > 0$ 时, $u_{2,1}^* = u_{2,1} + (T-r)/2$; 当 $u_{2,1} < 0$ 时, $u_{2,1}^* = u_{2,1} - (T-r)/2$;

当 $u_{3,1} > 0$ 时, $u_{3,1}^* = u_{3,1} - (T-r)/2$; 当 $u_{3,1} < 0$ 时, $u_{3,1}^* = u_{3,1} + (T-r)/2$;

如果嵌入比特为 0, 令 $r = |u_{3,1}| - |u_{2,1}|$:

当 $u_{2,1} > 0$ 时, $u_{2,1}^* = u_{2,1} - (T-r)/2$; 当 $u_{2,1} < 0$ 时, $u_{2,1}^* = u_{2,1} + (T-r)/2$;

当 $u_{3,1} > 0$ 时, $u_{3,1}^* = u_{3,1} + (T-r)/2$; 当 $u_{3,1} < 0$ 时, $u_{3,1}^* = u_{3,1} - (T-r)/2$ 。

④将各块中修改后的矩阵 U 同矩阵 D 、 V 一起进行奇异值反变换, 得到含水印的图像。

篡改检测及水印的提取过程如下:

①对待检测图像进行 4×4 大小分块, 并对每块进行奇异值分解;

②检查每个子块奇异值分解对应 U 矩阵第一列第 2、3 个系数之间的相对关系:

若 $|u_{2,1}| - |u_{3,1}| > 0$, 提取出的比特为 1; 若 $|u_{3,1}| - |u_{2,1}| > 0$, 则提取的比特为 0。

③将提取的每个比特与嵌入比特进行对比, 标记出不一致比特对应的 4×4 嵌入块, 认为这些块遭到篡改;

④从所有分块中提取出来的比特形成一个二值矩阵, 根据水印置乱的逆过程, 以 Logistic 映射的初值 key_1 、 key_2 和 Arnold 变换参数 a 、 b 、 L 为解密密钥即可实现置乱水印的提取。

4 仿真分析

选取一幅 64×64 的有意义二值图像作为原始水印, 以 256×256 的 LENA.TIF 灰度图像作为水印的嵌入载体。此时, 式(3)中 $N = 64$, 选取参数 $a = 40$, $b = 8$, $L = 11$ 作为 Arnold 变换的密钥, 为保证系统的混沌特性达到最强, 式(4)中参数 $\mu = 4$, 选取迭代初始值 $key_1 = 0.123456$, $key_2 = 0.876543$ 作为 Logistic 映射的密钥。图 2 中 (a)、(b) 分别表示原二值水印图像和经双混沌置乱后的二值水印图像。

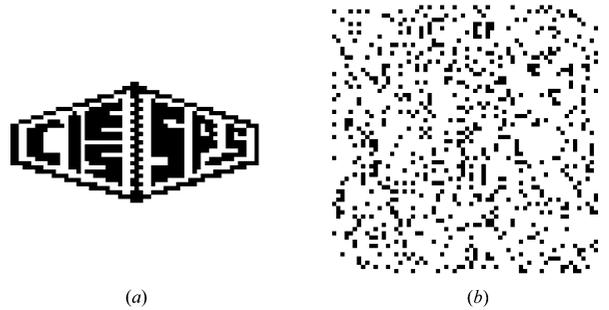


图 2 二值水印图像; (a)置乱前; (b)置乱后
Fig. 2 Two Binary Image; (a) before chaotic mapping; (b) after chaotic mapping

图 3 所示为以 $T = 0.012$ 嵌入水印时图像与原图的对比及提取出的水印, 嵌入水印后的图像质量没有明显变化, 同时水印也能实现完全正确地提取。图 4 给出了门限 T 从 0.001 到 0.025 时与嵌入水印图像峰值信噪比 (PSNR) 之间的关系。

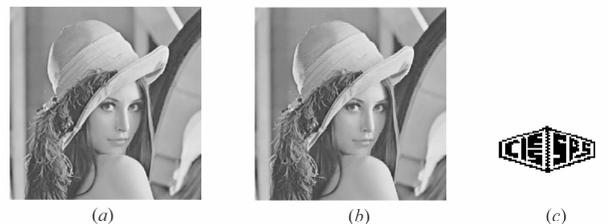
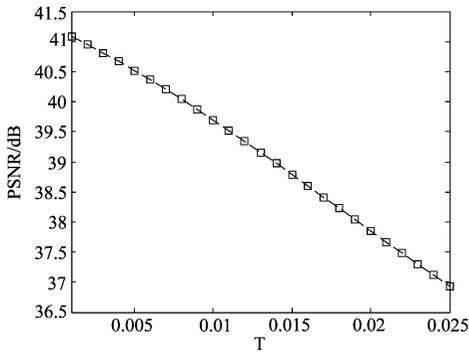


图 3 水印嵌入前后对比; (a)原始图像; (b)加载水印后的图像 ($T = 0.012$); (c)提取水印
Fig. 3 The comparison of watermark embedding; (a) original image; (b) watermarked image; (c) extracted watermark

图4 门限 T 与 PSNR 的关系Fig. 4 The relationship between T and PSNR

文献[13]中也提出了一种改进的 SVD 水印算法, 水印通过一个固定的嵌入强度嵌入到 SVD 的整个奇异值矩阵上, 与本文方法不同。下面将两种方法进行比较, 选择文献[13]中 $\alpha=0.011$, 本文中 $T=0.012$, 使得两种方法得到的嵌入水印图像 PSNR 分别为 39.895dB 和 39.901dB, 这样即可在保证嵌入水印图像透明性一致的前提下, 对两种水印算法的鲁棒性进行测试。图 5~8 分别为两种算法在 75% JPEG 压缩、方差为 0.001 的零均值高斯随机噪声、方差为 0.06 的零均值椒盐噪声及 25% 裁剪下所提取出来的水印结果。

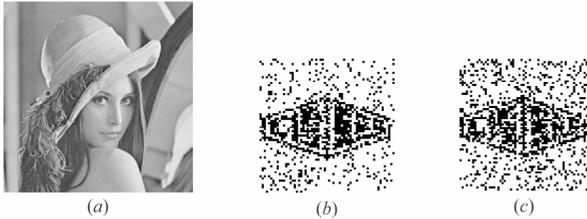


图5 JPEG 压缩实验:(a)被压缩的含水印图像,(b)用文献[13]中方法得到的水印图像,(c)用本文方法得到的水印图像

Fig. 5 JPEG compression for both methods: (a) noisy watermarked image, (b) extracted watermark by the method in [13], (c) extracted watermark image by the proposed method

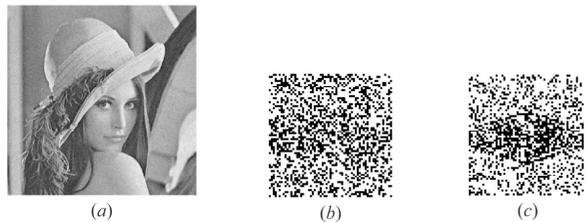


图6 添加高斯随机噪声实验:(a)添加噪声的含水印图像,(b)用文献[13]中方法得到的水印图像,(c)用本文方法得到的水印图像

Fig. 6 Addition of Gaussian noise for both methods: (a) noisy watermarked image, (b) extracted watermark by the method in [13], (c) extracted watermark image by the proposed method

表 1 列出了上述实验采用文献[13]中的方法与本文方法所提取出来水印的误比特率。可以看出, 文献[13]中的方法具有较好的抗 JPEG 压缩特性, 而本文方法在抗高斯噪声和椒盐噪声方面具有较好的性能, 两种

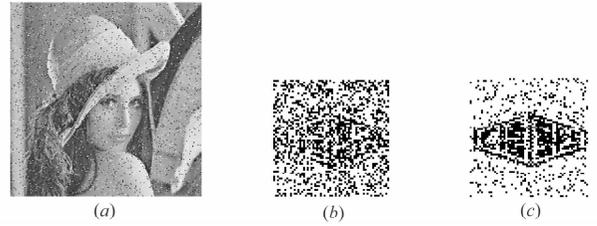


图7 椒盐噪声攻击实验:(a)受攻击的含水印图像,(b)用文献[13]中方法得到的水印图像,(c)用本文方法得到的水印图像

Fig. 7 Salt and pepper attack for both methods: (a) noisy watermarked image, (b) extracted watermark by the method in [13], (c) extracted watermark image by the proposed method

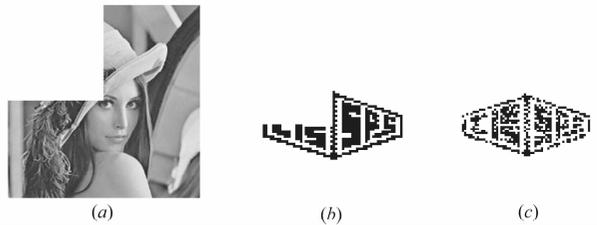


图8 图像裁剪实验:(a)被裁剪的含水印图像,(b)用文献[13]中方法得到的水印图像,(c)用本文方法得到的水印图像

Fig. 8 Cropping attack for both methods: (a) noisy watermarked image, (b) extracted watermark by the method in [13], (c) extracted watermark image by the proposed method

方法对于图像裁剪攻击误比特率相当, 由于本文方法在水印嵌入之前进行了置乱操作, 使得从受攻击图像中提取出来水印的错误比特具有杂散的空间分布, 这样便于在整体上识别提取水印的轮廓。在计算复杂度方面, 设待嵌入的水印为 $N \times N$ 的二值方阵, 两种方法在水印嵌入时的计算复杂度相当, 均为 $O(N^2)$; 本文方法在水印嵌入之前增加了置乱操作, 复杂性也相应地增加了, 但与此同时水印的安全性得到了有效提高, 这在文章第 2 部分中已详细论述; 对于水印的提取, 文献[13]中需要用到原始载体图像, 而本文方法为一种盲水印算法, 在水印提取过程中不需要用到原始图像信息。

表 1 当 $T=0.012$, $\alpha=0.011$ 时四种攻击下的误比特率Tab. 1 Error rates under four attacks with $T=0.012$ and $\alpha=0.011$

攻击类型 水印算法	JPEG 压缩 (品质 75%)	零均值高斯噪声 (方差 0.001)	零均值椒盐噪声 (方差 0.06)	图像裁剪 (大小 25%)
文献[13]算法	0.1292	0.3738	0.3049	0.0413
本文算法	0.2620	0.2485	0.1885	0.0413

最后, 用本文提出的方法对含水印图像进行篡改检测实验。当含水印的图像分块没有遭到篡改时, 其嵌入的水印比特能够正确地检测出来, 故检测虚警概率为 0; 当含水印的图像分块遭到篡改时, 嵌入水印比特的检测取决于篡改内容是否破坏了分块奇异值分解 U 矩阵中相应系数的相对关系。这里, 定义漏检概率为:

$$P_M = N_M / N_S \quad (6)$$

其中 N_M 表示未被检测出来的篡改分块个数, N_S 表示图

像分块总数。图 9 表示当门限 $T=0.012$ 时,本文算法对图像篡改的定位能力和提取出来的水印图像。子图 (a) 表示遭篡改后的含水印图像, (b) 表示篡改定位图像, (c) 表示从 (a) 中提取出的水印,此时 $P_M=0.0129$ 。

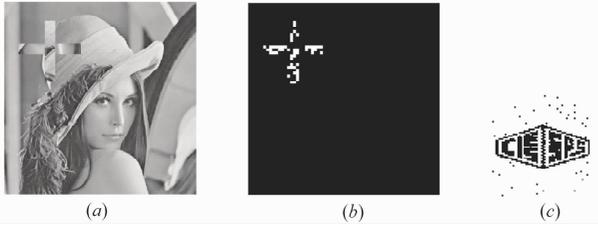


图 9 (a) 遭篡改的图像; (b) 定位图像; (c) 提取的水印

Fig.9 (a) tampered image; (b) localized image; (c) extracted watermark

5 结论

本文提出了一种基于混沌映射和奇异值分解的数字图像水印算法。通过水印置乱方法中的理论分析,采用 Arnold 变换及双重混沌映射对有意义二值水印图像进行置乱,可以提高嵌入水印的安全性。在水印嵌入与提取过程中,采用了修改图像块奇异值分解 U 矩阵中第一列系数的方法来实现水印嵌入,研究了水印透明性与嵌入门限值 T 之间的关系,在保证透明性一致的前提下将本文方法与文献[13]中的方法进行了比较,本文方法在抗图像噪声攻击方面具有更好的性能,并能够实现图像版权保护和篡改定位的功能。

参考文献

- [1] Lu W, Lu H T, Chung F L. Feature Based Watermarking Using Watermark Template Match[J]. Applied Mathematics and Computation, 2006, 177(1): 377-386.
- [2] Xiang H, Wang L D, Lin H, Shi J Y. Digital Watermarking System with Chaotic Sequences[C]. Proceedings of SPIE Conference on Security and Watermarking of Multimedia Contents, 1999: 449-457.
- [3] 高飞, 张辉. 一种基于混沌序列定位的跳频盲水印算法[J]. 北京理工大学学报, 2007, 27(8): 709-712.
Gao F, Zhang H. A Frequency-hopping Blind Watermarking Algorithm Based on Chaotic Sequence Locating[J]. Transactions of Beijing Institute of Technology, 2007, 27(8): 709-712. (in Chinese)
- [4] 范延军, 孙燮华, 阎晓东, 郑林涛. 一种基于混合混沌序列的图像置乱加密算法[J]. 中国图象图形学报, 2006, 11(3): 387-393.
Fan Y J, Sun X H, Yan X D, Zheng L T. An Image-scrambling Algorithm Based on Mixed Chaotic Sequences [J]. Journal of Image and Graphics, 2006, 11(3): 387-393. (in Chinese)

- [5] 吴翊, 李超, 罗建书, 戴清平. 应用数学基础[M]. 北京: 高等教育出版社, 2005: 167-172.
Wu Y, Li C, Luo J S, Dai Q P. Fundamentals of Applied Mathematics[M]. Beijing: High Education Press, 2005: 167-172. (in Chinese)
- [6] Sun R, Sun H, Yao T R. A SVD And Quantization Based Semi-fragile Watermarking Technique for Image Authentication[C]. IEEE Conference on Signal Processing, 2002, 2: 1592-1595.
- [7] Schmitz R. Use of Chaotic Dynamical Systems in Cryptography[J]. Journal of the Franklin Institute, 2001: 429-441.
- [8] 丁文霞, 王浩, 卢焕章. 二维混沌置乱矩阵构成置换群的理论和实验证明[J]. 国防科技大学学报, 2009, 31(2): 94-98.
Ding W X, Wang H, Lu H Z. Theoretical and Experimental Proof That 2D Chaotic Arrays are Permutation Groups [J]. Journal of National University of Defense Technology, 2009, 31(2): 94-98. (in Chinese)
- [9] 胡汉平, 刘双红, 王祖喜, 吴晓刚. 一种混沌密钥流产生方法[J]. 计算机学报, 2004, 27(3): 408-412.
Hu H P, Liu S H, Wang Z X, Wu X G. A Method for Generating Chaotic Key Stream [J]. Chinese Journal of Computers, 2004, 27(3): 408-412. (in Chinese)
- [10] Matthews R. On The Derivation of A Chaotic Encryption Algorithm[J]. Cryptologia, 1989, 8(1): 29-41.
- [11] Chung K L, Shen C H, Chang L C. A Novel SVD And VQ Based Image Hiding Scheme[J]. Pattern Recognition Letters, 2001, 22(9): 1051-1058.
- [12] Chung K L, Yang W N, Huang Y H, Wu S T, Hsu Y C. On SVD-based Watermarking Algorithm [J]. Applied Mathematics and Computation, 2007, 188(1): 54-57.
- [13] Ahmad A M, Ali A, Sameer S. An Improved SVD-based Watermarking Scheme for Protecting Rightful Ownership [J]. Signal Processing, 2008, 88(9): 2158-2180.

作者简介



焦 问(1986-),女,四川广汉人,国防科技大学电子科学与工程学院硕士研究生,主要研究方向为计算机视觉与智能信息处理。

E-mail:chenxia_gfkd@sina.com



丁文霞(1973-),女,湖南长沙人,国防科技大学电子科学与工程学院博士、副教授,主要研究方向为数字视频技术,信号与信息处理,电路与系统。

E-mail:dwx2004@sina.com