基于混沌序列和 DCT 变换的图像零隐藏算法研究*

吴建斌 费潇潇 王年丰
(华中师范大学 物理科学与技术学院 武汉 430079)

摘 要：为提高信息隐藏技术的抗隐写分析能力，对基于图像的零隐藏技术理论模型进行推导，分析了零隐藏技术实现信息隐藏时鲁棒性和预处理的要求，考虑到离散余弦变换(DCT)和混沌序列的各自优势，提出了基于 DCT 变换和混沌序列的图像零隐藏算法。该算法利用混沌序列对隐秘信息进行预处理加密，建立载体图像 DCT 变换域直流系数与已加密隐秘信息之间的关系文档，而不是将隐秘信息嵌入到载体图像中。在 MATLAB 环境下对该算法进行性能测试，结果表明具有嵌入容量大、鲁棒性强以及抗隐写分析能力好的优点。

关键词：零隐藏算法；离散余弦变换；混沌序列；隐写分析
中图分类号：TP309.2；TN918.1 **文献标识码**：A **国家标准学科分类代码**：510.40

Zero-steganography algorithm research based on chaotic sequences and image DCT transform

Wu Jianbin Fei Xiaoxiao Wang Nianfeng
(School of physical science and technology, Central China Normal University, Wuhan 430079, China)

Abstract: In view of steganography and anti steganalysis ability requirements, the zero-steganography techniques to hide information is proposed, and the theoretical model based on the sample type zero-steganography is derived. In addition, the robustness and pretreatment of the steganography is analyzed, considering the discrete cosine transform (DCT) and chaotic sequence of their respective advantages, the zero-steganography algorithm of pictures based on PCT trans form and chaotic sequence is put forward. The method hides the payload based on relationship between the cover image dct dc coefficient and the payload preprocessing encryption, instead of directly embedding payload into the cover image. The results under MATLAB environment show that the proposed algorithm has a large embedding capacity, strong robustness, and great ability to resist steganalysis analysis.

Keywords: zero-steganography algorithm; discrete cosine transform; chaotic sequence; steganographic analysis

1 引 言

零隐藏技术是信息隐藏技术的一个重要分支，其重要特点是不修改图像载体的任何特征，通过建立载体图像的某个特征与隐秘信息之间的联系来达到信息隐藏的目的，其能掩盖秘密通信的存在，避免攻击者对通信内容进行攻击和破坏，具有非常高的安全性。其来源于早期用于数字水印中的零水印技术(zero-watermaking)，该技术在嵌入水印过程中不修改图像特征，具有非常好的鲁棒性[1-2]，而文献[3-4]考虑到零水印技术的鲁棒性特点，提出将零的思想引入到数字隐写中，实现了基于图像的零隐藏算法。

近几年来，国内外对图像信息隐藏的研究得到了迅猛发展，从各个不同角度提出了利用载体图像不同特征实现信息隐藏的不同算法，一般来说，隐藏技术可以分为空间域隐藏和变换域隐藏。基于空间域的隐藏算法一般是将秘密信息直接嵌入到图像的冗余部分，其中最具代表性的是 LSB 算法[5-6]，该类算法大多具有较好的嵌入容量，但是鲁棒性较差，使得接收方不能很好地恢复出原来的信息。基于变换域隐藏是根据人眼的视觉特性将隐秘信息嵌入到变换域频率系数中鲁棒性和不可感知性较高的区域，如离散余弦变换(DCT)、离散小波变换(DWT)和扩频[7-9]，其中应用最广泛的是基于 DCT 变换的隐藏方法，然而基于变换域的隐藏方法大多存在着容量不足的问题。并且，以上信息隐藏方法都改变了载体图像的像素值，而隐写分析技术可能会根据这些修改检测出图片中是否存在隐秘信息[10-11]，一旦隐秘信息的存在性被检测出来，纵然无法解密，也可对

收稿日期：2016-10
* 基金项目：华中师范大学中央高校基本科研业务研究基金(CCNU15A02040)资助项目

载体图片进行破坏,使得双方的隐秘通信失败,且传统隐藏技术没有过多的关注隐秘信息之间的相关性,在对隐秘信息的预处理时只是简单的加解密,没有很好的去除相关性,而这很容易被隐写分析技术分析出隐秘信息,将降低传输过程中的安全性。

为解决在隐藏过程中图像像素的变化带来的不安全因素,本文考虑到零隐藏技术在信息隐藏过程中不修改图像的特性,提出以零隐藏技术为基础的隐藏思路。在建立特征映射关系时考虑到鲁棒性的要求,选取了 DCT 变换的直流特征,在对隐秘信息预处理阶段考虑到去相关的要求,选取了伪随机性良好的 Logistic 混沌序列[12],最终实现了一种基于 Logistic 混沌序列和 DCT 变换的零隐藏算法。该算法先利用 Logistic 混沌序列的伪随机特性对隐秘信息进行置乱加密预处理,再生成已加密隐秘信息与 DCT 变换系数直流系数之间的关联文档,最终将该关联文档和相关的密钥发送给接收方。该算法在 MATLAB 环境下经过了一系列的性能测试,实验结果表明,本文提出算法具有很好的容量、鲁棒性、抗隐写分析能力和安全性,具有非常好的实用价值。

2 图像的 DCT 变换和混沌映射

2.1 图像的 DCT 变换

图像 DCT 变换的原理是将图像分割为不相互重叠的 8×8 子块,然后对每一个子块单独进行 DCT 变换,每一个子块得到一个由 1 个直流成分系数 DC 和 63 个交流成分系数 AC 组成的子块 DCT 变换系数矩阵。由于变换系数的直流成分有着图像的绝大部分能量,具有非常好的鲁棒性,因此本文选取该变换矩阵中的直流成分系数组成新的矩阵,该新矩阵将作为图像的特征与待传输的秘密信息构造关联文档。

2.2 Logistic 混沌映射

混沌序列由混沌系统产生,混沌系统是一种复杂的非线性动力学系统,该系统在一定的初始条件下可以产生具有遍历性、非周期性、伪随机性以及参数敏感性的混沌序列,因此,混沌序列被广泛应用到安全领域。

Logistic 混沌映射是典型的能产生一维混沌序列的混沌系统,具有结构简单、初始敏感性、伪随机性性良好的特性,其公式定义如下:

$$x_{k+1} = \mu x_k(1 - x_k) \tag{1}$$

式中:μ 为系统参数,k 为迭代次数,$0 < \mu \leqslant 4$,$x_k \in (0, 1)$。μ 选取不同的值该系统出现不同的混沌序列特性,当 $\mu < 1$ 时最终的迭代结果 xk 为 0,当 $\mu = 1.8$ 时迭代结果 x_k 趋于稳定,当 $\mu = 2.5$ 时迭代结果 x_k 出现震荡且最终达到平衡状态,当 $\mu = 3.1$ 时迭代结果 x_k 只有两个值交替出现,当 $\mu = 3.5$ 时迭代结果 x_k 只有 4 个值交替出现,当 $\mu = 3.55$ 时迭代结果 x_k 只有 8 个值交替出现,当 $3.569 \leqslant \mu \leqslant 4$ 时,系统迭代结果不再反复交替出现,此时,Logistic 映射处于混沌状态,不同的初始条件 μ 和 k 会产生完全不同的的混沌序列。本文针对上述的迭代特性,为了产生随机性较好的混沌序列来进一步提高安全性,在发送方和接收方选取 $3.569 \leqslant \mu \leqslant 4$ 区间的相同的 μ 值来产生混沌序列。

3 基于 DCT 变换和混沌序列的零隐藏算法

传统的隐藏算法有很多优点,或容量大,或鲁棒性强,然而这些算法都是将信息直接嵌入到空间域或变换域,在嵌入的过程中都对图片进行了或多或少的修改,这种修改人眼系统纵然无法察觉,但是一些隐写分析技术却可能检测出来,甚至破解出信息。而本文提出的隐藏方法不对图片作任何人为修改,这可以完全杜绝隐写分析技术带来的隐患,并且能够保证很好的容量和鲁棒性。图 1 所示为本方法的流程,发送方首先将隐秘信息与混沌序列异或产生新序列,然后提取载体图像的特征,该载体图像可选取网上的热门图片,之后建立特征与新序列之间的映射关系从而得到一个关联文档,最终发送发只需发送载体图片,关联文档及产生混沌序列的参数。接收方在接收到这些参数之后先提取载体图片的对应特征,再根据关联文档和由参数产生的混沌序列即可解密出原信息。该系统发送与接收的全过程中没有对载体做任何修改,并且在一定程度上对序列的长度没有限制,选取的是抗压缩性好的 DCT 变换中能量高的 *DC* 分量,因此,该方法具有非常好的不可检测性,很好的抗压缩性及较高的容量,同时载体图片选取的是网络上热门事件的图像,在发送与接收的过程中不容易引起攻击者的怀疑,可大大提高通信过程的安全性。

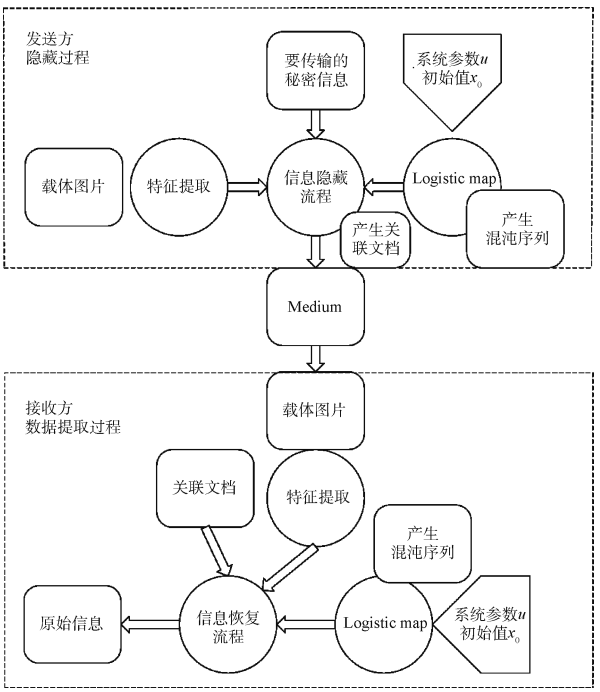

图 1 数据隐藏与接收算法流程

3.1　数据隐藏过程

如图 1 所示，隐藏过程分为 3 个部分，分别是源信息随机化，载体图像特征提取、建立关联文档。

1)发送方按照式(1)选取一个在 3.569～4 之间的 Logistic 系统参数 μ 和一个在 0～1 之间的初始值 x_0 产生一个与隐秘信息 P 等长的混沌序列 L，使 P 按照式(2)与之进行异或操作产生一个新的序列 PP，三个序列的长度均为 n。

$$PP(n) = L(n) \oplus P(n) \tag{2}$$

2)发送方对载体图片进行分块 DCT 变换(以尺寸 512×512 的图片为例)，先将尺寸为 512×512 的图片矩阵分为 64×64 个 8×8 小块的小矩阵，按照式(3)对每一个 8×8 小矩阵求分块 DCT 变换系数矩阵，该系数矩阵由 1 个直流分量 DC 和 63 个交流分量 AC 组成，取其中的直流分量重新组成新的 64×64 的新矩阵 DC。

$$F(u,v) = c(u)c(v)\frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left(\frac{2x+1}{2N}u\pi\right)\cos\left(\frac{2y+1}{2N}v\pi\right) \tag{3}$$

式中：$f(x,y)$ 为二维图像信号矩阵，N 为矩阵的维数，当 $u=v=0$ 时 $c(u)=c(v)=1/\sqrt{2}$，当 $u\neq 0, v\neq 0$ 时 $c(u)=c(v)=1$。

3)发送方任取 4 个 1～64 之间的随机数 a,b,c,d，两两组成一队 (a,b)，(c,d) 代表两个坐标，这两个坐标值取自 DC 矩阵，比较 $DC(a,b)$ 和 $DC(c,d)$ 的模值，若 $DC(a,b)$ 与 $DC(c,d)$ 的模值相等则重取 4 个值，否则令 $abs(DC(a,b))-abs(DC(c,d))=dif$，若 $dif>0$ 并且此时 PP 中的比特值为 1 则将这 4 个随机数按 $abcd$ 的顺序存入到关联文档中；若 $dif>0$ 且 PP 中此时的比特值为 0 则将这 4 个随机数按 $cdab$ 的顺序存入到关联文档中；若 $dif<0$ 并且 PP 中此时的比特值为 0 则将这 4 个随机数按 $abcd$ 的顺序存入到关联文档中；若 $dif<0$ 并且 PP 中此时的比特值为 1 则将这 4 个随机数按 $cdab$ 的顺序存入到关联文档中。如此将步骤 3)循环 n 次，依次将随机数存入到关联文档中，直到 PP 中的比特位全部与特征矩阵建立关联，形成最终的关联文档。

最后发送方通过网络环境传递给接收方的只有关联文档，载体图片，Logistic 系统的 μ 和初始值 x_0，此时的载体图片未做任何修改，因此也不会被检测出隐秘信息的存在，关联文档以及 Logistic 的两个参数先进行加密然后通过秘密途径传送过去，亦不会引起怀疑。

3.2　数据提取过程

如图 1 所示，数据提取过程也分为 3 个部分，第 1 个部分产生混沌序列，第 2 个部分提取载体图片特征，第 3 个步骤根据接收到的关联文档和混沌序列解密出源信息。

1)接收方接收到的系统参数 μ 和初始值 x_0，再按照式(1)产生一个与发送方相同的混沌序列 L。

2)接收方提取直流分量特征的方法跟发送方完全一致，接收方对载体图片进行分块 DCT 变换(以尺寸 512×512 的图片为例)，先将尺寸为 512×512 的图片矩阵分为 64×64 个 8×8 小块的小矩阵，按照公式(3)对每一个 8×8 小矩阵求 DCT 变换系数矩阵，该系数矩阵由 1 个直流分量 DC 和 63 个交流分量 AC 组成，取其中的直流分量重新组成新的 64×64 的新矩阵 DC。

3)接收方接收到关联文档从头每次取 4 个数，依次组成两队 (a,b)，(c,d) 这两队对应于 DC 矩阵两个坐标，比较 $DC(a,b)$ 和 $DC(c,d)$ 的模，若 $abs(DC(a,b))-abs(DC(c,d))$ 大于 0 则表示 PP 此时比特位的值为 1，若小于 0 则表示 PP 此时比特位的值为 0，依次解码最终得到 PP 序列，再根据式(4)对 PP 序列与(3)产生的混沌序列 L 进行异或操作得到原始信息。

$$P(n) = PP(n) \oplus L(n) \tag{4}$$

4　性能测试结果

容量、不可检测性和鲁棒性是信息隐藏中很重要的性能指标，其中容量和不可检测性是信息隐藏技术中最重要的部分，对于评价算法的实用性具有非常重要的意义，而鲁棒性在信息隐藏中不是最重要的部分，但对于评价信息隐藏算法的健壮性却有很重要的意义。

4.1　容量与不可检测性

本文提出的算法实现过程中，选取的是尺寸为 512×512 的图片，特征矩阵的尺寸为 64×64，建立关联文档时的 4 个数是随机的，这 4 个数理论上有 64×64×64×64 种组合，然关联文档在建立过程中允许有相同的 4 个数出现，故本文的算法的容量跟图片的大小无关。表 1 给出了本文提出的算法与其他一些信息隐藏算法之间容量的对比表。传统信息隐藏算法的容量与不可检测性之间存在着直接的联系，在最大容量范围内容量的增加必然会导致不可检测性的降低，表 1 中算法容量的对比是根据容量与不可检测性之间的权衡进行的，而这种权衡方法来自于文献[13]，表中所有的信息隐藏算法都经过了盲隐写分析技术对隐秘信息存在性的检测，评估指标定义为检测可靠性 p，$p=0$ 表示隐藏信息完全不会被检测出来，$p=1$ 表示隐藏信息完全会被检测出来。

表 1　本文算法和文献[4]中算法基于容量和不可感知性权衡的容量对比(U 表示不可实现的容量)

Capacity	F5	OG	PQ	CBZS	本文算法
0.05	0.241	0.879	～0	0	0
0.1	0.539	0.993	0.048	0	0
0.2	0.956	0.991	0.098	U	0
0.4	1.000	U	0.174	U	0
0.6	1.000	U	U	U	0
0.8	1.000	U	U	U	0

表 1 中进行容量对比的算法分别是文献[4]中的 CBZS (chaos based zero-steganography)算法、OG 算法、PQ 算法和 F5 算法,其中 F5、OG、PQ 等传统传统信息隐藏的容量测量指标为 bpc(bits per non-zero DCT coefficient),而 CBZS 与本文提出算法的容量测量指标为 bpp(bit per pixel),从表 1 可以看出,就隐藏容量而言,传统信息隐藏的算法较 CBZS 具有一定优势,但却要小于本文提出的算法;且在检测可靠性上,CBZS 算法和本文算法有明显的优势。并且,随着容量的增加传统信息隐藏算法的不可检测性大幅度降低,而 CBZS 算法和本文提出的算法的不可检测性不随容量的增加而降低,因此,本文算法在抵抗隐写分析方面具有非常好的安全性。

4.2 鲁棒性

为了评估本文提出的算法的鲁棒性,本文在 MATLAB 环境下分别测试了算法抵抗 JPEG 压缩攻击、noise 攻击和低通滤波器攻击的能力。本文所选用的衡量标准为误码率,定义为:

$$BER = \frac{Bc}{Bt} \tag{5}$$

式中:B_c 是接收方提取出来错误的总比特数,B_t 是发送方发送的总比特数。

文中选取了 8 张尺寸为 512×512 的图片作为载体图片,随机产生了 80 Kbyte 的二进制数作为负载信息,并且测试环境是 MATLAB2010a。测试过程分为 3 个部分,第 1 部分是分别产生每张载体图片的关联文档和相关密钥;第 2 部分是对每张图片进行攻击;第 3 部分是从已攻击的载体照片中提取出负载信息,并计算 *BER*。由于本文算法的关联文档中每组 4 个数是随机产生的,为了消除偶然性因素的影响,每张载体图片都经过了多次的上述 3 个部分的测试,之后对 *BER* 取平均值,再对所有的图片在同一条件下求 *BER* 平均值,该值为本文的算法在该种条件下的 *BER* 平均值。

4.2.1 抗 JPEG 压缩攻击

在采用 JPEG 压缩算法攻击时载体图片会发生一定程度的破坏,因此本文需要对该算法的抗 JPEG 压缩攻击能力进行测试。考虑到实际情况,本文选取的 JPEG 压缩算法的 quality 范围从 1～90 以 10 为间隔,每个点的 *BER* 值均为 8 张图片各自 *BER* 的平均值。在选取的范围中 quality 等于 1 代表最低的图片压缩质量,quanlity 等于 90 代表最高的图片压缩质量。图 2 展示了本文算法在 JPEG 压缩攻击下误码率的曲线,本文的算法在最小的 quality 下的误码率为 16%,随着 quality 的增加,误码率逐渐减小,最后在最大的 quality 下的误码率接近于 0。表 2 提供了 CBZS 算法[4],(chaos based DCT steganography,CBD)算法[13]和本文算法抗 JPEG 压缩攻击能力的比较,结果显示,在相同的 quality 值下,本文算法的 BER 明显低于另外两种算法。

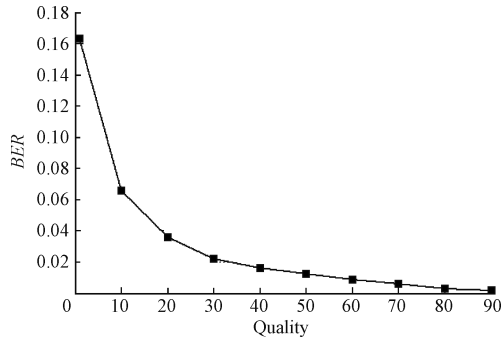

图 2 JPEG 压缩攻击

表 2 CBZS[4],CBD[13]和本文提出的算法之间抗 JPEG 压缩攻击能力的比较

Quality	CBD	CBZS	本文算法
90	0.022	0.048	0.002
70	0.038	0.080	0.009
50	0.151	0.098	0.017

4.2.2 抗噪声攻击

本文选取的噪声攻击是比较常见的高斯白噪声和椒盐噪声攻击。高斯白噪声有两个参数,分别是均值和方差,均值为 0,方差为归一化的 0～1(下同),方差为 1 代表了提供最大程度的噪声。在本文的测试中,考虑到实际情况,方差选取的是 0.1～1 以 0.1 的涨幅递增,测试结果如图 3 所示,在方差为 0.1 时 *BER* 最小,约为 14%方差为 1 时 *BER* 最大,约为 32%,方差取中间值时,*BER* 依次递增。表 3 展示了 CBZS 算法和本文提出的算法之间抗高斯白噪声攻击

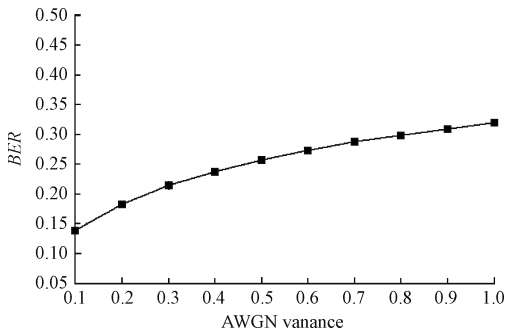

图 3 高斯噪声攻击

表 3 CBZS[4]和本文提出的算法之间抗高斯白噪声攻击能力的比较

噪声方差	CBZS	本文算法
0.1	0.18	0.14
0.4	0.21	0.24
0.7	0.22	0.29
1.0	0.22	0.32

能力的比较，由表可知，在方差较低时本文算法较于 CBZS 算法要低，但是随着方差的增加，本文算法的误码率要高于 CBZS 算法。然而在实际应用过程中高斯噪声的归一化方差不会高达 1，因此本文算法的抗高斯噪声攻击能力在实际应用过程中是可行的。

考虑到实际情况，本文选取的椒盐噪声的强度从 0.01～0.1 以 0.01 的涨幅递增，测试结果如图 4 所示，在噪声强度为 0.01 时 *BER* 最小，约为 2.7%，噪声强度为 0.1 时 *BER* 最大，约为 9.3%，方差取中间值时，*BER* 依次递增。表 4 提供了 CBD、CBZS 和本文算法抗 JPEG 压缩攻击能力的比较，结果显示，在相同的噪声强度下本文算法的 *BER* 要低于另外两种算法。

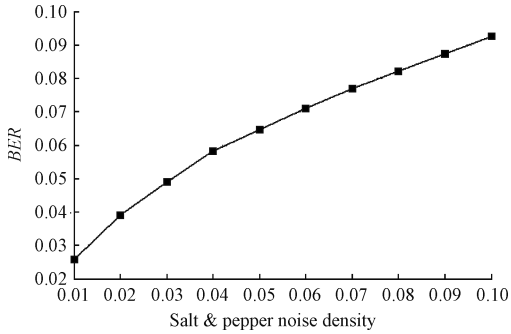

图 4　椒盐噪声攻击

表 4　CBZS[4]，CBD[13] 和本文提出的算法之间抗椒盐噪声攻击能力的比较

Noise density	CBD	CBZS	本文算法
0.01	0.071	0.062	0.026
0.1	0.128	0.098	0.093

4.2.3　抗低通滤波器攻击

本文选取的低通滤波器攻击为高斯低通滤波器攻击和均值滤波器攻击。高斯低通滤波器有参数和方差两个参数，考虑到实际情况，实验中选取的尺寸为默认尺寸，方差为 0.1～1 以 0.1 的涨幅递增，实验结果如图 5 所示，方差为 0.1 时 *BER* 最小，约为 0，方差为 1 时 *BER* 最大，约为 1.5%，取中间值时，*BER* 依次递增。表 5 给出了 CBD，CBZS 和本文算法抗 JPEG 压缩攻击能力的比较，结果显示，在相同的高斯方差下本文算法的 *BER* 要低于另外两种算法。

均值滤波器有尺寸一个参数，实验结果如图 6 所示，尺寸为 1×1 到 9×9 以 2×2 的涨幅递增。实验结果如图 6 所示，尺寸为 1×1 时 *BER* 最小，约为 0，尺寸为 9×9 时 *BER* 最大，约为 6.8%，取中间值时，*BER* 依次递增。表 6 给出了 CBZS 和本文算法抗 JPEG 压缩攻击能力的比较，结果显示，在相同的高斯方差下本文算法的 *BER* 要低于 CBZS 算法。

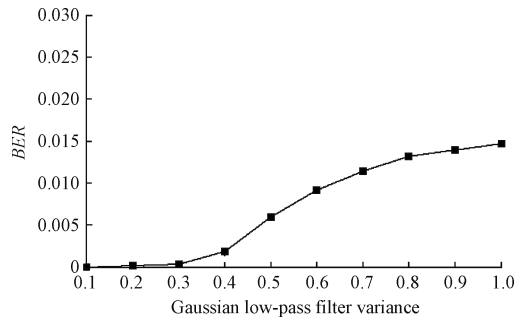

图 5　高斯低通滤波器攻击

表 5　CBZS[4]，CBD[13] 和本文提出的算法之间抗高斯低通滤波器攻击能力的比较

Gaussian variance	CBD	CBZS	本文算法
0.5	0.031	0.023	0.007
1.0	0.088	0.050	0.015

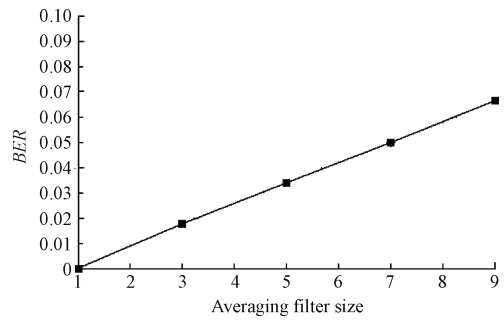

图 6　均值滤波器攻击

表 6　CBZS[4] 和本文提出的算法之间抗均值滤波器攻击能力的比较

Size	CBZS	本文算法
3×3	0.07	0.02
5×5	0.10	0.035
7×7	0.125	0.051
9×9	0.14	0.068

5　结　论

为提高信息隐藏技术的隐藏性能，实现隐秘通信，本文在分析传统信息隐藏技术的基础上，考虑到零隐藏技术的优势，借鉴了 DCT 变化和 Logistic 混沌序列在信息隐藏技术上所具有的优点，提出并实现了一种基于 Logistic 混沌序列和 DCT 变换的零隐藏算法，该种方法未修改载体图像的任何特征，通过建立载体图像 DCT 变换系数的直流成分与经 Logistic 混沌序列随机化的隐秘信息之间的关联文档，实现信息隐藏。经测试，该种方法在保证较大的容量的同时具有非常好的鲁棒性、安全性和抗隐写分析能力，达到了提高隐藏特性的要求，具有很强的实用价值。

参考文献

[1] JIANG D Y, KIM J W. A Zero-Watermarking Scheme Based on Spread Spectrum and Holography[M]. Advances in Computer Science and Ubiquitous Computing, Singapore: Springer, 2015: 375-381.

[2] 安虎,李怡璇,徐力,等. 基于曲波变换的彩色图像零水印研究[J]. 电子测量技术, 2010 (2): 45-48.

[3] ISHIZUKA H, ECHIZEN I, IWAMURA K, et al. A zero-watermarking-like steganography and potential applications[C]. Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), IEEE, 2014: 459-462.

[4] BILAB M, IMTIAZ S, ABDUI W, et al. Chaos based zero-steganography algorithm[J]. Multimedia Tools and Applications, 2014, 72(2): 1073-1092.

[5] ZHANG X. Reversible data hiding in encrypted image[J]. IEEE Signal Processing Letters, 2011, 18(4): 255-258.

[6] HONG W, CHEN T S, WU H Y. An improved reversible data hiding in encrypted images using side match[J]. IEEE Signal Processing Letters, 2012, 19(4): 199-202.

[7] 杨乾星,栗风永,张新鹏, 等. 基于 DCT 系数修改的自适应稳健可逆信息隐藏[J]. 上海大学学报:自然科学版, 2014, 20(5): 605-611.

[8] 刘金安, 金聪. 基于离散小波变换的双重水印方案[J]. 电子测量技术, 2012, 35(11): 45-48,66.

[9] SATISH K, JAYAKAR T, TOBIN C, et al. Chaos based spread spectrum image steganography[J]. IEEE Transactions on Consumer Electronics, 2004, 50(2): 587-590.

[10] 王丽娜, 王旻杰, 章鑫, 等. 针对图像空域随机 LSB 信息隐藏的提取攻击策略[J]. 武汉大学学报: 理学版, 2015 (1): 41-50.

[11] 朱婷婷, 王丽娜, 胡东辉, 等. 基于不确定性推理的 JPEG 图像通用隐藏信息检测技术[J]. 电子学报, 2013, 41(2): 233-238.

[12] 刘昕浩, 郭腾, 谢德辉, 等. 基于 Logistic 混沌映射的图像加密通信系统研究[J]. 湖南理工学院学报:自然科学版, 2015(4): 009.

[13] SINGH S, SIDDIQUI T J. A security enhanced robust steganography algorithm for data hiding[J]. International Journal of Computer Science Issues, 2012, 9(1): 131-139.

作者简介

吴建斌,1972 年出生,工学博士,副教授,硕士生导师主要研究方向为信息隐藏、探地雷达信号处理等。

费潇潇,1992 年出生,工学硕士,主要研究方向为信息隐藏。

E-mail:xiaoxiaofei@mails.ccnu.edu.cn

王年丰,1989 年出生,工学硕士,主要研究方向为信息隐藏。