

## 基于公钥的可逆数字水印

李立宗<sup>1\*</sup>, 顾巧论<sup>2</sup>, 高铁杠<sup>3</sup>

(1. 天津职业技术师范大学 计算与语音中心, 天津 300222; 2. 天津职业技术师范大学 信息技术工程学院, 天津 300222;

3. 南开大学 软件学院, 天津 300071)

(\* 通信作者电子邮箱 lilizong@gmail.com)

**摘要:** 为了提高可逆数字水印的安全性和透明性, 增加嵌入容量, 提出了一种基于公钥的可逆数字水印。该方法首先对载体图像直方图中峰值点与左右两侧的零值点之间的像素点进行移位, 然后提取载体图像的特征值, 将该特征值与经过混沌系统加密的数字水印进行异或处理后, 采用公钥将其嵌入到处理后的载体图像内。图像的验证过程是嵌入过程的逆过程, 验证完成后, 根据峰值点及其与零值点之间的关系将移位的像素点复原, 即可完全复原原始图像。采用公钥系统和混沌系统充分保证了系统的安全性, 峰值点与其两侧的零值点之间的像素移位既保证了能够嵌入更多的信息和较高的峰值信噪比, 又保证了所有的像素点都能被认证。通过对大量的图像进行仿真分析, 结果显示该方法具有较高的安全性, 与同类方法相比, 能够嵌入更多的信息量, 同时具有更高的透明性。

**关键词:** 公钥系统; 可逆数字水印; 混沌系统; 直方图; 峰值

**中图分类号:** TP391.4 **文献标志码:** A

### Reversible digital watermarking based on public key system

LI Li-zong<sup>1\*</sup>, GU Qiao-lun<sup>2</sup>, GAO Tie-gang<sup>3</sup>

(1. Center of Information, Tianjin University of Technology and Education, Tianjin 300222, China;

2. School of Information Technology Engineering, Tianjin University of Technology and Education, Tianjin 300222, China;

3. College of Software, Nankai University, Tianjin 300222, China)

**Abstract:** A reversible digital watermarking based on public key system was proposed to improve the security, transparency and embedding capacity. This technique shifted the pixels between the peak and zero in the histogram, extracted the characteristics of the original image, used the Boolean exclusive OR operator between the characteristics value and the watermark image processed with chaotic system, and finally embedded the value into the image with the public key. Verification process was the inverse process of the embedding. After the verification, the shifted pixels were recovered depending on the relationships of the peak and zero in the histogram, and the image was recovered. The public key system and chaotic system guarantee the system security. The shift between the peak and zero pixels ensured more embedded information, higher peak signal-to-noise ratio, and authentication of all the pixels. The process was simulated with lots of images. The results show that the method is safer than others, can embed more information, and has more transparency.

**Key words:** public key system; reversible watermarking; chaotic system; histogram; peak value

## 0 引言

数字水印技术是指在一个载体图像内嵌入一个水印图像的技术。根据载体图像与水印图像的关系, 可以将数字水印分为信息隐藏和图像认证两类。在实现信息隐藏时, 载体图像仅仅实现隐藏水印图像的目的, 水印图像是一幅需要保护的秘密信息图像。当水印图像从载体图像内提取完成后, 载体图像的作用即失效, 可以将其丢弃。在实现图像认证时, 水印信息是和载体图像密切相关的。此时的水印图像通常是载体图像的辅助性说明信息, 例如图像的哈希函数值、版权人签名、版权信息等。由于在水印嵌入过程中不可避免地要修改载体图像, 从而对其造成一定的失真。而像医疗、军事等领域对图像质量要求较高, 甚至不允许像素级别的改变。这就要求在提取水印图像后能够完全复原载体图像, 这种技术称为可逆数字水印技术<sup>[1]</sup>。

目前主要的可逆数字水印技术<sup>[2-10]</sup>有: 位平面压缩算法、低像素层算法、基于直方图的双射圆变换算法、提升小波变换算法、差分扩展算法、基于灰度直方图的算法等。例如, Ni 等<sup>[11]</sup>提出了采用三个最大值和最小值点进行信息隐藏, 该方法能够隐藏比基本直方图算法更多的信息。但是统计分析结果表明, 该方法运算量较大, 需要记忆的嵌入提取条件相对较多, 同时可能存在溢出造成图像无法完全复原。针对上述缺点, 顾巧论等人提出了采用多个连续零值点与峰值像素匹配进行嵌入信息的算法, 仿真结果表明该算法能够嵌入更多的信息<sup>[12]</sup>。上述算法均未考虑算法实施的安全性, 为了确保嵌入信息的安全性, Lee 等<sup>[13]</sup>提出了一种基于直方图变换的公钥可逆数字水印方法, 但是该方法并未考虑水印图像的安全, 使得攻击者在获知水印的情况下, 将载体图像恶意篡改并再次应用公钥嵌入水印后, 此时的载体图像仍旧能够顺利通过认证。

**收稿日期:** 2011-10-10; **修回日期:** 2011-12-16。 **基金项目:** 国家自然科学基金资助项目(60873117); 天津市自然科学基金资助项目(11JCZDJC16000); 天津职业技术师范大学科研发展基金资助项目(KJ2009023)。

**作者简介:** 李立宗(1979-), 男, 天津宝坻人, 讲师, 硕士, CCF 会员, 主要研究方向: 图像处理、信息安全; 顾巧论(1967-), 女, 河北河间人, 教授, 博士, 主要研究方向: 信息安全、复杂系统优化与控制; 高铁杠(1966-), 男, 河北河间人, 教授, 博士, 主要研究方向: 信息安全、软件工程。

本文提出了一种基于公钥的可逆数字水印。该数字水印应用公钥系统与混沌系统确保整个过程的安全性,通过对图像直方图峰值点及其两侧零值点之间的像素点移位来保证嵌入了隐藏信息的载体图像具有较高的透明性和较大的信息嵌入量。

## 1 算法描述

### 1.1 可逆水印基本算法

为了叙述上的方便,以  $256 \times 256$  像素大小的灰度图像 clock.bmp 为例,将基于直方图的可逆数字水印基本算法描述如下。

1) 绘制载体图像直方图。读入载体图像,并绘制该图像的直方图,如图1所示。从直方图可以看出,峰值点对应的像素值为230,该峰值点的值为5230,说明在载体图像内像素值为230的像素点个数最多,共有5230个;其左端值为 $[0,31]$ 和其右端值为 $[247,255]$ 的像素值均为零,表明在载体图像中不存在这些像素值的像素点。

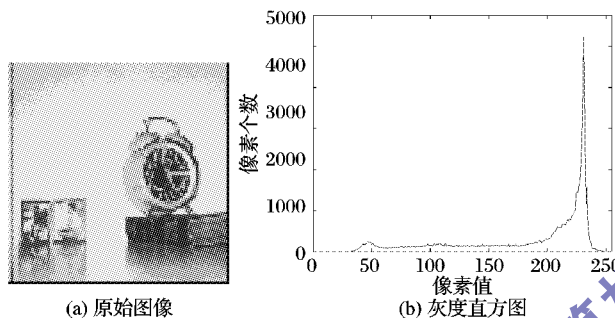


图1 示例图像及灰度直方图

2) 直方图处理。顺序扫描载体图像,当扫描到的像素点值为 $[231,246]$ 时,则将其值加上1。扫描完成后,在载体图像内不再存在像素值为231的像素点。

3) 嵌入水印。对载体图像进行再次扫描,如果扫描到的像素点其值为230,则可以在该点嵌入1位水印信息。嵌入规则为,如果待嵌入点为0,则该点保持不变;如果待嵌入点为1,则将该点像素值加1。至此,完成水印嵌入过程。

4) 提取水印。对嵌入了水印信息的图像进行顺序扫描,如果扫描到的像素点值为230,则提取一个水印信息位0;如果扫描到的像素点值为231,则提取一个水印信息位1,扫描过程完成即完成水印信息的提取。

5) 恢复载体图像。再次扫描图像,将在图像内扫描到的像素点值在 $[231,247]$ 的像素点减1,即完成载体图像的复原。

该算法的水印信息作为秘密信息嵌入到载体图像内达到信息隐藏和图像认证的目的,但水印信息和载体图像并无直接联系,因此攻击者可以轻易实现对隐藏的水印信息的篡改,从而使该算法的信息隐藏和认证失效。同时,由于在水印嵌入时,该算法只是将水印信息隐藏到对应的峰值点,嵌入完成后会在靠近该峰值点附近形成波谷,通过统计分析很容易实现水印信息的提取,因此,算法的安全性不高。为了达到对载体图像认证的目的,本文提出利用载体图像生成认证信息,将该认证信息与原有水印信息进行运算后嵌入到载体图像内。为了保证载体图像内所有像素点均能够被认证,对原始算法进行修改,将峰值点及其两侧的零值点之间的所有像素点进行移位以实现水印信息的嵌入,同时采用混沌系统对水印信息进行加密从而保证水印信息的安全性。

### 1.2 水印嵌入

认证水印信息由载体图像生成的特征值与水印信息进行运算生成。该过程将认证信息嵌入到载体图像内。

#### 1) 载体图像处理。

读取载体图像  $O$ , 绘制出其直方图, 找出该直方图的峰值点  $Max$  及其左侧的连续零值点  $L_i, i \in [0, Max)$ , 右侧连续零值点  $R_i, i \in (Max, 255]$ 。

为了确保所有像素点都能被认证, 并提高水印信息的嵌入容量和嵌入信息后图像的透明性, 针对峰值点及在直方图左右两侧的连续零值点进行匹配嵌入。单位峰值点能嵌入的水印信息位数  $En$ 、所需左右两侧连续零值点个数总和  $Sn$ 、所需左侧连续零值点个数  $Ln$ 、所需右侧连续零值点个数  $Rn$  之间的关系如表1所示。

表1 嵌入信息位数及零值点关系

位数 $En$	连续零值点个数 $Ln$ 及 $Rn$
1	$Ln + Rn = Sn, Ln \in [0, 1], Rn \in [0, 1], Sn = 1$
2	$Ln + Rn = Sn, Ln \in [0, 3], Rn \in [0, 3], Sn = 3$
3	$Ln + Rn = Sn, Ln \in [0, 7], Rn \in [0, 7], Sn = 7$
4	$Ln + Rn = Sn, Ln \in [0, 15], Rn \in [0, 15], Sn = 15$

如果峰值点左右两侧的零值点个数均大于 $\lfloor Sn/2 \rfloor$ , 则将左侧连续 $\lfloor Sn/2 \rfloor$ 个零值点作为嵌入处理位, 另一侧需要处理的连续零值点个数为 $\lceil Sn/2 \rceil$  ( $Sn = \lceil Sn/2 \rceil + \lfloor Sn/2 \rfloor$ ); 如果在峰值点两侧的某一侧中连续零值点个数  $Zn$  ( $Zn \equiv Ln$  或  $Zn \equiv Rn$ ) 小于 $\lfloor Sn/2 \rfloor$ , 则将该侧的连续零值点作为嵌入处理位, 另一侧需要匹配连续零值点个数为  $Zn'$  ( $Zn' = Sn - Zn$ )。

比如, 需要在图像  $O$  内根据单个峰值点  $Max = 230$  嵌入3位信息, 则需要连续零值点个数为  $Sn = 7$ , 其中  $Ln + Rn = Sn$ ,  $Ln \in [0, 7], Rn \in [0, 7]$ 。如果峰值点两侧的零值点个数均大于3, 则将其左侧所有像素值小于230, 并且像素值个数大于0的像素值减去3; 将其右侧所有像素值大于230, 并且像素值个数大于0的像素值加上4。这样, 在峰值点的左右两侧共空出7个零值点。如果峰值点两侧其中某一侧(假定为左侧)的零值点个数  $Ln$  小于3, 则将该侧的所有像素值小于230, 像素值个数大于0的像素值减去  $Ln$ ; 将其另外一侧(对应为右侧)所有像素值大于230, 像素值个数大于0的像素值加上  $Rn$ ,  $Rn = Sn - Ln, Ln \in [0, 3], Rn \in [0, 7], Sn = 7$ 。

经过处理后的载体图像标记为  $Od$ 。

#### 2) 水印信息生成。

RIPEMD 报文摘要算法是在欧洲 RACE 的 RIPE 项目中由研发人员开发而成的, 这些研究人员曾对 MD4 和 MD5 部分进行了攻击。该算法以一个任意长度的报文作为输入, 产生一个160位的报文摘要作为输出。RIPEMD 所产生的散列码中的每一位比特位都是输入中每一比特位的函数, 因此随机选择两个报文, 即使它们具有相似的规律性, 也很难产生相同的散列码<sup>[14]</sup>。

对原始载体图像  $O$ , 处理过的载体图像  $Od$ , 进行如下计算:

$$Hv = Hash(M, N, O, Od) \quad (1)$$

其中:  $Hash(\cdot)$  是 RIPEMD 报文摘要函数,  $M, N$  是载体图像的长和宽,  $Hv$  是经过计算得到的160位的 RIPEMD 报文摘要输出。

选择一幅二进制图像 Logo 作为载体图像的基础认证信

息图像(水印图像),例如可以是图像所有人的版权信息图像或约定的秘密信息图像等。将载体图像转换为一个长度为 $L_{sn}$ 的序列 $L_s$ 。例如载体图像Logo为 $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ ,则其转换序列 $L_s$ 为(0 0 1 1)。

计算载体图像可以嵌入的信息容量,计算公式为:

$$Len = NMax * En \quad (2)$$

其中: $NMax$ 为峰值点像素个数, $En$ 为每个峰值像素点对应的嵌入位个数, $Len$ 为载体图像可以嵌入的数据容量。

根据 $Len$ 的长度对序列 $H_v$ 和 $L_s$ 进行周期性迭代得到序列 $H_{vp}$ 和 $L_{sp}$ ,使得这两个序列的长度均为 $Len$ 。例如 $Len = 5$ , $H_v = (0 \ 1 \ 1)$ , $L_s = (1 \ 0 \ 0 \ 0)$ ,则处理后得到, $H_{vp} = (0 \ 1 \ 1 \ 0 \ 1)$ , $L_{sp} = (1 \ 0 \ 0 \ 0 \ 1)$ 。

对 $H_{vp}$ 和 $L_{sp}$ 进行异或操作,得到载体图像的水印认证信息,具体方式为:

$$W = L_{sp} \oplus H_{vp} \quad (3)$$

例如: $H_{vp} = (0 \ 1 \ 1 \ 0 \ 1)$ , $L_{sp} = (1 \ 0 \ 0 \ 0 \ 1)$ ,则所得的计算结果为 $W = (1 \ 1 \ 1 \ 0 \ 0)$ 。

3) 认证信息生成。

应用公钥加密系统对水印信息 $W$ 进行加密,具体实现为:

$$Swo = E(Ku, W) \quad (4)$$

其中:函数 $E(\cdot)$ 为公钥体系的加密函数, $Ku$ 为公钥, $Swo$ 为计算结果。

4) 认证信息加密。

为了提高认证信息的安全性,采用Logistic混沌系统对生成的信息进行加密处理,应用的混沌系统为:

$$x_{n+1} = 1 - 2x_n^2 \quad (5)$$

其中 $x_n \in [-1, 1]$ 。

应用混沌系统生成与 $Swo$ 大小相等的二值序列 $L_s$ ,然后将 $L_s$ 与 $Swo$ 进行异或操作,具体为:

$$Sw = L_s \oplus Swo \quad (6)$$

5) 认证信息的嵌入。

嵌入认证信息时,顺序扫描经过处理的载体图像 $Od$ ,如果遇到峰值点 $Max$ ,则从经过混沌置乱后的信息序列 $Sw$ 中选取 $n$ 个比特位,如果选取的 $n$ 个比特位均为0,则像素值保持不变;否则,计算选取序列的和 $Sb$ ,根据峰值点两侧零值点个数情况,将 $Max$ 与 $Sb$ 进行算术运算完成信息嵌入。

比如,载体图像 $Od$ 峰值点两侧的零值点个数均大于3,在扫描过程中遇到峰值点 $Max$ ,则从要隐藏的序列中选取3个比特位,如果选取的3个比特位均为0,则像素值保持不变;否则,计算选取序列的和 $Sb$ ,如果 $\text{mod}(Sb, 2) = 0$ ,则将峰值点减去 $Sb/2$ ;如果 $\text{mod}(Sb, 2) = 1$ ,则将峰值点加上 $\lceil Sb/2 \rceil$ 。

另一种情况下,如果峰值点某侧(以左侧为例)的零值点个数小于3,例如, $Ln = 2$ ,在扫描过程中遇到峰值点 $Max$ ,则从要隐藏的序列中选取3个比特位,如果选取的3个比特位均为0,则像素值保持不变;否则,计算选取序列的和 $Sb$ ,如果 $Sb \leq 2$ 则将峰值点减去 $Sb$ ,如果 $Sb > 2$ ,则将峰值点加上 $Sb$ 。

按照上述步骤顺序扫描图像内所有像素点,即可完成嵌入。在实际操作中,可以根据不同的图像先选取一个峰值点对应3位嵌入信息完成嵌入,嵌入完成后根据所得到的峰值信噪比和实际需要的嵌入容量对嵌入位数进行进一步的修正。

嵌入了认证信息的载体图像记为 $Odw$ 。

### 1.3 认证过程

认证过程是对图像是否发生篡改进行认证并完全复原原始图像的过程。认证时首先从要认证的图像内提取认证信息,再将认证信息与原始水印信息进行运算,完成对图像的认证,同时将载体图像复原。

1) 认证信息提取。

提取认证信息时,首先确定在信息嵌入时选取的单位峰值点能嵌入的水印信息位数 $En$ 、所需左右两侧连续零值点个数总和 $Sn$ 、左侧连续零值点个数 $Ln$ 、右侧连续零值点个数 $Rn$ 。然后,顺序扫描需要验证的载体图像 $Odw'$ ,如果遇到峰值点 $Max$ ,则提取 $En$ 个比特位0;如果遇到峰值点相关点,则根据该点具体值,将该值与 $Max$ 进行算术运算完成信息提取。

比如,在提取过程中,如果遇到像素点 $Max$ ,则提取3位秘密信息均为0;如果遇到像素点的值为 $[Max - Ln, Max + Rn]$ ,则提取信息为 $Ln$ 或 $Rn$ 。将提取的秘密信息转换为3位二进制。例如,提取到的信息为4,则将其转换为3位二进制100。

按照上述步骤顺序扫描图像内所有像素点,即可完成认证信息的提取,得到认证信息 $Swrc$ 。

应用加密过程使用的混沌系统和初始密钥,生成与 $Swrc$ 等长的序列 $L_{sn}$ ,并将它们进行异或操作,得到序列 $Swr$ ,具体为:

$$Swr = L_{sn} \oplus Swrc \quad (7)$$

2) 计算水印信息。

应用公钥系统对认证信息 $Swr$ 进行解密,具体实现为:

$$Wr = E(Kr, Sw) \quad (8)$$

其中:函数 $E(\cdot)$ 为公钥体系的解密函数, $Kr$ 为与 $Ku$ 所对应的私钥, $Wr$ 为得到的水印信息。

3) 计算报文摘要。

顺序扫描嵌入了认证信息的载体图像 $Odw$ ,将图像直方图内在像素点 $Max$ 两侧 $[Max - Ln, Max + Rn]$ 的点置为0,得到图像 $Ocr$ 。再次扫描图像 $Ocr$ ,将图像像素点 $Max$ 左侧的非零值点进行右移 $Ln$ 位,将峰值点右侧非零值点左移 $Rn$ 位,得到图像 $Or$ 。

计算图像 $Odw$ 和 $Or$ 的RIPEMD报文摘要 $Hvr$ ,具体为:

$$Hvr = \text{Hash}(Mr, Nr, Or, Ocr)$$

其中: $Mr, Nr$ 为图像 $Odw$ 的长和宽, $\text{Hash}(\cdot)$ 是RIPEMD报文摘要函数。

将报文摘要 $Hvr$ 自身进行迭代得到 $Hvrp$ 使其长度与 $Wr$ 的长度相等。例如, $Hvr = (1 \ 0 \ 1)$ , $Wr = (1 \ 1 \ 0 \ 0 \ 0)$ ,则 $Hvrp = (1 \ 0 \ 1 \ 1 \ 0)$ 。

4) 计算基本认证图像。

将水印信息 $Wr$ 和迭代后的报文摘要 $Hvrp$ 进行异或操作,得到基本认证信息 $Lspr$ ,实现方式为:

$$Lspr = Wr \oplus Hvrp \quad (10)$$

5) 认证载体图像。

将得到的基本认证信息 $Lspr$ 进行迭代得到认证信息 $Vi$ ,该信息是初始认证图像的 $n$ 次迭代。其总长度 $LVi$ 为:

$$LVi = \left\lceil \frac{\text{Length}(Lspr)}{Ls} \right\rceil * Ls \quad (11)$$

其中: $\text{Length}(\cdot)$ 是求长度函数, $Ls$ 是基本水印序列 $L_{sn}$ 的长度。

其迭代规则为:

$$Vi = \text{strcat}(Lspr, \text{mid}(Lspr, \text{mod}(Lspr, Ls) + 1, Ls)) \quad (12)$$

其中: $\text{strcat}(\cdot)$ 是字符串连接函数; $\text{mid}(s, i, j)$ 是字符串截取



函数,表示截取字符串  $s$  中  $[i,j]$  之间的子串; $\text{mod}(\cdot)$  是取余函数。

将认证信息  $V_i$  转换为  $\lceil \frac{\text{Length}(L_{\text{spr}})}{L_s} \rceil$  个矩阵  $\text{Vid}_i (i \in [1, \lceil \frac{\text{Length}(L_{\text{spr}})}{L_s} \rceil])$ , 此时每个矩阵  $\text{Vid}_i$  的大小和初始 Logo 的大小保持一致。

将转换后的矩阵  $\text{Vid}_i$  分别和原始 Logo 进行比较, 如果, 每个矩阵均与 Logo 相同, 则图像有效; 否则, 说明图像被篡改过。

例如:  $L_{\text{spr}} = (0 \ 0 \ 1 \ 1 \ 0)$ ,  $L_s = 4$ , 则  $LVi = 8$ ,  $Vi = (0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1)$ 。可以将  $Vi$  转换为 2 个和初始 Logo 大小一致的矩阵,  $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$  和  $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ 。如果原始 Logo =  $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ , 说明该图像有效, 没有被篡改过; 如果图像 Logo  $\neq \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ , 则说明图像被篡改过。

## 2 实验仿真

将本文提出的算法应用于  $512 \times 512$  大小的标准图像进行测试, 使用的部分仿真图像如图 2 所示。

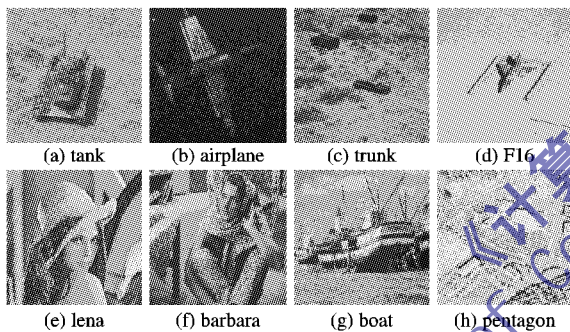


图2 仿真图像

### 2.1 水印容量

信息的嵌入容量指在载体图像内能够嵌入的秘密信息位数。在本文所提出可逆数字水印中, 应用峰值点及其两侧连续零值点之间的关系完成信息的嵌入, 可以嵌入的信息量  $S_1$  为:

$$S_1 = NMax * En \quad (13)$$

其中:  $NMax$  为峰值点像素个数,  $En$  为每个峰值像素点对应的嵌入位数。大量仿真实验表明, 当  $En$  值为 3 时, 可以取得比较好的峰值信噪比, 部分图像当  $En$  取值为 4 或 5 时, 仍旧具有较高的峰值信噪比。

可逆水印基本算法只采用了峰值点进行水印嵌入, 因此可以嵌入的水印容量  $S_2$  为:

$$S_2 = NMax \quad (14)$$

根据式(14)可以得出,  $S_2 = NMax < NMax * En = S_1$ 。

文献[12]提出的可逆水印算法在基本算法的基础上进行了改进, 可以嵌入的信息容量  $S_3$  为:

$$S_3 = NMax_1 + NMax_2 + NMax_3 \quad (15)$$

其中  $NMax_1$ 、 $NMax_2$  和  $NMax_3$  分别表示直方图中分段后的峰值点。因此,  $S_3 = NMax_1 + NMax_2 + NMax_3 < NMax_1 * 3 \leq S_1$ 。

因此, 本文提出的算法, 在嵌入容量上有较大提高, 可以嵌入更多的信息。将本文的嵌入容量与基本算法及文献[12]所提出的算法进行量化比较, 其结果如图 3 所示。

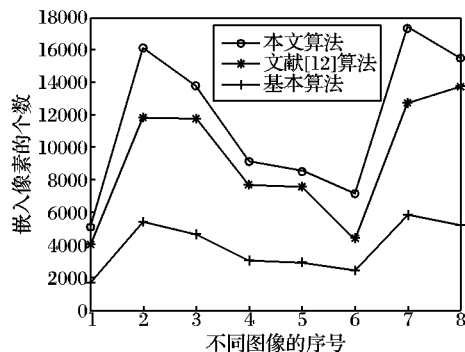


图3 嵌入容量

### 2.2 透明性

为了更客观地衡量图像的透明性, 本文采用峰值信噪比 (Peak Signal-to-Noise Ratio, PSNR) 值来对图像的透明性进行量化。峰值信噪比值具体定义如下:

$$PSNR = 10 \lg \left( \frac{255^2}{MSE} \right)$$

其中  $MSE$  (Mean Square Error) 是指像素大小为  $M \times N$  的原始图像和修改图像之间均方差, 具体定义为:

$$MSE = \frac{1}{M * N} \sum_{i=1}^M \sum_{j=1}^N (O_{ij} - Od_{ij})^2$$

其中:  $O_{ij}$  是原始图像中像素点  $(i,j)$  点的像素值,  $Od_{ij}$  是修改图像中像素点  $(i,j)$  点的像素值。

对图 1 中的图像进行仿真实验, 在峰值点嵌入 3 位信息时, 将嵌入了水印的图像与原始载体图像, 计算得到的峰值信噪比值, 与参考文献[12]对比, 结果如表 2 所示。从表 2 可以看出, 应用本文方法嵌入验证信息后, 图像具有更高的峰值信噪比值, 透明性更好。

表2 两种方法的 PSNR 比较 dB

图像	文献[12]方法	本文方法
tank	32.9166	36.7660
airplane	35.3175	37.4632
trunk	32.0308	36.4363
F16	34.4402	37.2722
lena	32.5183	36.6101
barbera	32.3944	36.5653
boat	33.4838	36.9464
pentagon	32.0296	36.4349

### 2.3 水印安全性

本文采用了混沌系统对认证信息进行加密。混沌系统对初始条件敏感依赖, 这意味着混沌系统具有长期不可预测性, 如果初始值发生微小的变化, 在短期内还可以预测但是长时间的演化后, 它的状态变得根本无法预测<sup>[15]</sup>。

三个相差为亿分之一的初值  $x_0$ , 按照式(5)迭代的情形如图 4 所示。从图中可以看出, 迭代初期, 三条曲线的相关度较大, 但是经过 30 代左右的迭代, 它们之间的关系已经不确定。例如, 在迭代的第 46 代, 初值为 0.1 与初值为 0.10000001 之间仅差了亿分之一, 但是它们的结果一个是 -0.69893504754623, 另一个为 0.60886899248229, 两者相差较大; 而此时初值为 0.10000002 的结果为 0.87383379286082, 与初值 0.10000001 的情况相差较小。可以看出, 系统呈现出长期的不可预测性。

本文应用混沌系统, 对验证信息进行加密, 仿真结果如图 5 所示。当水印图像如图 5(a) 时, 使用初始值为 0.68 的混沌

初始值计算出的加密结果如图5(b)所示,当使用与加密时对应的初始值0.68进行解密时,解密图像如图5(c)所示;当使用与加密时所对应的初始值稍有差异的初始值0.6800001解密时,解密图像如图5(d)。从仿真结果可以看出,采用混沌系统加密具有较高的安全性。

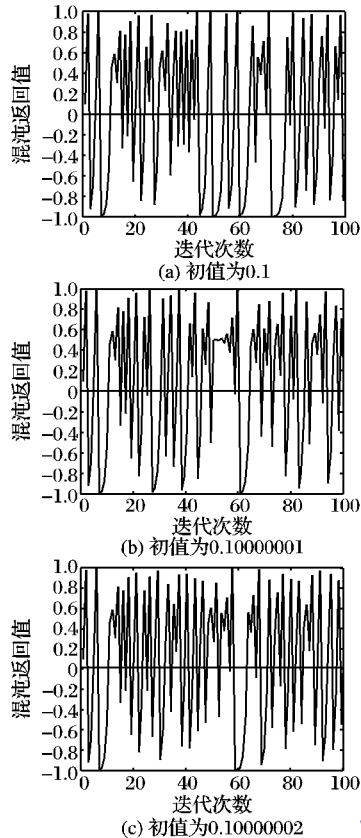


图4 不同初始值时的 Logistic 迭代曲线



图5 混沌加密

## 2.4 验证结果

应用本文提出的算法在载体图像 Lena.bmp 内嵌入水印信息如图6(a)所示,当嵌入水印信息的载体图像未被篡改时可以从中提取到如图6(b)所示的水印信息,并复原原始图像;当嵌入了水印信息的载体图像被篡改后,此时得到的水印信息如图6(c)所示,水印信息显示图像被篡改,此时载体图像虽仍旧能够被复原,但是并不可信。



图6 验证结果

## 3 结语

本文提出了一种基于公钥体系的可逆数字水印。该水印首先对载体图像的直方图进行处理,然后提取该载体图像的特征信息,将其与经过混沌系统处理的水印信息进行异或,再将其应用公钥进行加密后,嵌入到经过直方图处理后的载体

图像内。嵌入时,为了保证高透明性和较高的嵌入容量,将直方图峰值点两侧的非零值点进行移位。实验仿真结果显示,该算法的安全性高,嵌入容量大,透明性高。当图像被篡改后,验证结果能够给出有效提示。

本文提出的可逆数字水印目前只能对图像是否被篡改做出整体判断,尚无法对篡改进行准确有效的定位,下一步的工作将重点研究如何在保证原始载体能够复原的情况下,对篡改位置进行准确定位。

## 参考文献:

- [1] LIN C-C, TAI W-L, CHANG C-C. Multilevel reversible data hiding based on histogram modification of difference images[J]. Pattern Recognition, 2008, 41(12): 3582-3591.
- [2] AWRANGJEB M. An overview of reversible data hiding[C]// International Conference on Computer and Information Technology. Bangladesh: IEEE, 2003: 75-79.
- [3] CELIK M U, SHARMA G, TEKALP A M, et al. Reversible data hiding[C]// Proceedings of the IEEE International Conference on Image Processing. New York: IEEE, 2002: 157-1600.
- [4] De VLEESCHOUWER C, DELAIGLE J E, MACQ B. Circular interpretation of bijective transformation in lossless watermarking for media asset management[J]. IEEE Transactions on Multimedia, 2003, 5(1): 97-105.
- [5] YANG QUNTING, GAO TIEGANG, LI FAN. Reversible robust data hiding scheme based on histogram shifting in multi-wavelet domain[J]. International Journal of Advancements in Computing Technology, 2011, 3(5): 185-193.
- [6] COLTUC D. Low distortion transform for reversible watermarking[J]. IEEE Transactions on Image Processing, 2011, 99(7): 1057-7149.
- [7] PENG FEI, LEI YU-ZHOU, LONG MIN, et al. A reversible watermarking scheme for two-dimensional CAD engineering graphics based on improved difference expansion[J]. Computer-Aided Design, 2011, 43(8): 1018-1024.
- [8] MEMONAB N A, KHANC A, GILANID S A M, et al. Reversible watermarking method based on adaptive thresholding and companding technique[J]. International Journal of Computer Mathematics, 2011, 88(8): 1573-1594.
- [9] THAMPI S M, JACOB A J. Securing biometric images using reversible watermarking[J]. International Journal of Image Processing, 2011, 5(4): 382-389.
- [10] LUO LI-XIN, CHEN ZHEN-YONG, CHEN MING, et al. Reversible image watermarking using interpolation technique[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(1): 187-193.
- [11] NI ZHI-CHENG, SHI YUN-QING, NIRWAN A, et al. Reversible data hiding[J]. IEEE Transactions on Circuits and System for Video Technology, 2006, 16(3): 354-362.
- [12] 顾巧论, 高铁杠. 基于直方图修改的图像可逆信息隐藏算法[J]. 计算机工程与设计, 2008, 29(15): 4082-4085.
- [13] LEE S K, SUH Y H, HO Y S. Public key watermarking for reversible image authentication[C]// International Conference on Image Processing. Atlanta: IEEE IPS, 2006: 1409-1412.
- [14] 李晓航, 王宏霞, 张文芳. 认证理论及应用[M]. 北京: 清华大学出版社, 2009: 25-29.
- [15] 谭文, 王耀南. 混沌系统的模糊神经网络控制理论与方法[M]. 北京: 科学出版社, 2008: 6-8.