一种基于混沌脆弱水印的可逆双层图像认证方案

董 峰,金 俭
(黄河科技学院,河南 郑州 450063)

摘 要:针对多媒体数字图像易遭攻击的安全性问题,文中提出了一种基于混沌脆弱水印的可逆双层图像认证方案。在发送端,首先通过像素关联技术产生像素级的定位水印,并将其嵌入到自身的 LSB 位。然后把图像分成大小相同的块,先后计算每块的关系水印和检测水印,并分别用可逆的方法嵌入到偏移块的左上角和自身块的右下角。在接收端,首先对图像进行分块;然后通过比较提取和重新计算的水印来确定是否有篡改发生,并可以区分是内容篡改还是水印篡改。当内容被篡改时,可通过定位水印将篡改进一步定位到具体的像素,否则可以通过认证。大量的理论分析和实验仿真结果表明,该算法具有可行性和高效性,在同时需要认证和完整恢复原始图像的多媒体应用中表现得尤为明显。

关键词:图像安全;脆弱水印;混沌迭代;无损恢复;图像认证;篡改检测定位
中图分类号:TP391 **文献标识码**:A **文章编号**:1673-629X(2016)06-0092-05
doi:10.3969/j.issn.1673-629X.2016.06.020

A Two-level Reversible Image Authentication Scheme Based on Chaotic Fragile Watermark

DONG Feng, JIN Jian
(Huanghe Science and Technology College, Zhengzhou 450063, China)

Abstract: A two-level novel reversible image authentication scheme based on chaotic fragile watermark is proposed to locate tampered pixel accurately and ensure security of image. In the embedding process, at the pixel level, by utilizing the pixel correlation technology, the location watermark of each pixel is generated and embedded to the LSB of the pixel itself. At the image block level, the image is then partitioned into blocks, then the relation and detection watermark of each block is computed and embedded into the top-left sub-block of its corresponding excursion block and the down-right sub-block of the block itself in a reversible way respectively. In the extracting process, the watermarked image is partitioned into blocks, the embedded detection and relation watermark of each block is extracted and the block is recovered, then computing the new relation watermark and detection watermarks of each recovered block and performing comparison with the extracted ones. In the proposed scheme, the tampered watermark can pass the authentication because it does not reduce the value of image to some extent. But if the image content is tampered, the further step is taken at the pixel level to locate tamper to specific pixel by comparing the re-computed location watermark with the extracted location watermark. Theoretical analysis and computer simulation also indicates that the algorithm is feasible and efficient, especially in multimedia application requiring both integrity and confidentiality of the original image.

Key words: image security; fragile watermark; chaos iteration; lossless recovery; image authentication; tamper detection and location

0 引 言

随着信息时代的到来,人们可以方便地利用计算机软件进行各种创作,如对多媒体数字产品的编辑、存储、修改和传播,更有甚者,一些强大的图像处理软件使得人们可以随意对图像和照片进行更改。这些给人们生活带来便利的工具却是一把双刃剑,比如一些未经授权的个体可以轻易获取数字产品的重要信息,从而出现机密泄露、侵犯版权、非法复制和传播等一系列问题[1-2]。另外,一些别有用心的人对图像的肆意修改,使得人们从肉眼上很难分辨出真假,这就使得合法使用和侵权使用的界限变得更加模糊,这就需要采用有效的方式对其进行辨别。

收稿日期:2015-09-17 **修回日期**:2015-12-23 **网络出版时间**:2016-05-05
基金项目:2014 河南省科技攻关重点项目(142102210641);2015 年度河南省高等学校重点科研项目(15A520085);2014 郑州市科技攻关项目(20140662)
作者简介:董 峰(1972-),男,硕士,副教授,研究方向为计算机网络;金 俭(1987-),女,硕士,研究方向为计算机技术。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20160505.0831.110.html

近年来,出现了大量的基于水印的图像认证方案,这些方案的共同目的是检测水印图像的完整性和真实性[3-5]。当原始图像的内容被篡改,或者被虚假信息取代后,就需要用脆弱水印去定位被篡改的区域。分块水印认证方案[6-7]主要是通过把宿主图像分成小块,然后将脆弱水印嵌入到各块中实现的。虽然该方法有很强的篡改检测能力,但是它仅能定位到包含篡改像素的块,而且易遭受量化攻击。单像素水印认证方案[8-9]是把宿主图像的灰度值嵌入到宿主图像本身,该方法能够精确地定位到被篡改的像素,但是很可能会漏掉某些区域。此外,大多数的图像认证方案由于嵌入水印,总会在原始图像上留下一些永久的失真。但是对于一些多媒体应用来说,这些失真是不允许的。

针对上述问题,文中提出了一种基于混沌脆弱水印的可逆双层图像认证方案。该方案不仅能够区分出是水印篡改还是内容篡改,而且能将篡改定位到具体的块,最后还能无损地恢复原始图像。该方案结合了分块算法和单像素认证算法的优点,可以同时抵抗量化攻击和 Oracle 攻击。

1　水印生成与嵌入

1.1　像素级水印的生成与嵌入

由于自然界的图像相邻像素之间存在很强的关联性,所以为了保证图像的安全,首先采用置乱对图像进行预处理,然后计算每个像素的定位水印并嵌入到该像素的 LSB 位,最后通过逆置乱把所有像素恢复到原始位置。具体操作过程如下:

1)将原始图像 I 进行猫置乱,得到置乱后的图像 I_p。

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \boldsymbol{A}\begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}N) = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}N) \tag{1}$$

其中:p 和 q 为正整数;$\det(\boldsymbol{A})=1$;(x,y) 和 (x',y') 分别为置乱前后图像像素的坐标。

参数 p、q 和置乱次数 m 为猫置乱的密钥。

2)将置乱后图像 I_p 中的每个像素的 LSB 位置 0。

3)计算每个像素的定位水印 W_{i-p}。首先将图像 I_p 中的像素两两分组,以像素对 (b_i,b_{i+1}) 为例,具体方法如下:

(1)计算像素对 (b_i,b_{i+1}) 的平均值 a。

(2)重新定义 b_i 和 b_{i+1}:

$$b_i' = \begin{cases} \dfrac{b_i}{a}, a > b_i \\ \dfrac{a}{b_i}, a \leqslant b_i \end{cases} \quad b_{i+1}' = \begin{cases} \dfrac{b_{i+1}}{a}, a > b_{i+1} \\ \dfrac{a}{b_{i+1}}, a \leqslant b_{i+1} \end{cases} \tag{2}$$

(3)将 b_i' 和 b_{i+1}' 分别作为 Logistic 混沌映射 $B_{i+1}=\mu B_i(1-B_i)$,$\mu \in [1,4]$,$i=0,1,\cdots$ 的初始值,迭代 m 次后的结果记为 b_i'' 和 b_{i+1}'',其中参数 μ 为密钥。

(4)对迭代结果进行二值化,并将其结果作为该像素的定位水印 W_{i-p}。具体二值化的过程如下:以 0.5 为阈值,当该值大于 0.5 时,对应像素的定位水印记作 1,否则记作 0。

4)计算出每个像素的定位水印后,用该定位水印替代该像素的 LSB 位。

5)逆置乱嵌入定位水印后的图像,逆置乱后的图像记为 I_p'。

1.2　块级水印的生成与嵌入

在大多数情况下,水印被篡改并不影响图像的使用;所以,为了提高图像的使用效率,如果检测到水印被篡改,那么图像仍能通过认证[10],但是如果图像内容被篡改,那么图像将不能通过认证。因此,文中提出了两级混沌水印方案:关系水印和检测水印。它们能区分是内容篡改还是水印篡改。

在该算法中,将会用到基于可变参数控制的分段线性混沌映射—PWLCM[11],定义如下:

$$X_{t+1}=F_P(X_t)= \begin{cases} X_t/P, & 0 \leqslant X_t < P \\ (X_t-P)/(0.5-P), & P \leqslant X_t < 0.5 \\ (1-X_t-P)/(0.5-P), & 0.5 \leqslant X_t < 1-P \\ (1-X_t)/P, & 1-P \leqslant X_t \leqslant 1 \end{cases} \tag{3}$$

其中,$X_t \in [0,1]$,$P \in (0,0.5)$ 分别表示迭代的初始值和当前的迭代参数。

1)把 256 × 256 大小的逆置乱后的图像分为 64 × 64 互不重叠的块。从上到下、从左到右扫描图像,将 $X \in \{0,1,\cdots,N-1\}$ 作为各块的编号,其中 $N=16$。

2)通过对混沌序列进行排序,得到块映射序列:选择初始值 X_0 和参数 P_0 作为 PWLCM 混沌迭代的密钥,将 PWLCM 迭代 $N-1$ 次得到一个混沌序列 $\{X_0,X_1,\cdots,X_{N-1}\}$,然后按照升序对该序列进行排序,得到一个新的序列 $\{\hat{X}_0,\hat{X}_1,\cdots,\hat{X}_{N-1}\}$。该序列中每个值在原始序列中的位置 i 即为原始图像块对应的偏移块的标号。

3)通过 PWLCM 迭代产生 128 位的混沌 hash 值作为每块的关系水印 W_{i-r},选择初始值 X_0 和 P_0 作为 PWLCM 算法的密钥,具体过程如下:

(1)首先把图像分成大小相同的块,然后把图像中每块的像素从上到下、从左到右进行扫描转化为一维数组 C,数组内的每个元素记为 C_i,然后通过运算线性映射到[0,1]内。

(2)对每一块中的像素进行如下的 PWLCM 迭代:

$$P_1 = (C_1 + P_0)/4 \in (0,0.5), X_1 = F_{P_1}(X_0) \in (0,1)$$

$$P_k = (C_k + X_{k-1})/4 \in (0,0.5), X_k = F_{P_k}(X_{k-1}) \in (0,1)$$

$$P_{s+1} = (C_s + X_s)/4 \in (0,0.5), X_{s+1} = F_{P_{s+1}}(X_s) \in (0,1)$$

$$P_k = (C_{2s-k+1} + X_{k-1})/4 \in (0,0.5), X_k = F_{P_k}(X_{k-1}) \in (0,1)$$

$$X_k = F_{P_{2s}}(X_{k-1}) \in (0,1) \tag{4}$$

注意:在当前初始值 X_{k-1} 和当前迭代参数 P_k 的控制下,运用 PWLCM 迭代产生下一个迭代值 X_k,如果 X_k 等于 0 或者 1,则需要进行再次迭代。

(3)将 $X_{2s}, X_{2s+1}, X_{2s+2}$ 转化为对应的二进制,然后分别提取小数点后的 40、40、48 位按照从左到右的顺序组成 128 位的 hash 值,作为当前块的关系水印 W_{i-r}。

4)将计算出的每块的关系水印嵌入到对应的偏移块的左上角 32 × 32 子块。为了使嵌入水印后的图像能够无损恢复,采用 RCM[12] 可逆水印嵌入算法。以像素对 (x,y) 为例,具体的 RCM 算法如下:

$$x' = 2x - y, y' = 2y - x \tag{5}$$

对应的逆变换如式(6)所示:

$$x = \lceil \frac{2}{3}x' + \frac{1}{3}y' \rceil, y = \lceil \frac{1}{3}x' + \frac{2}{3}y' \rceil \tag{6}$$

其中,$\lceil \cdot \rceil$ 为向上取整操作。

为了防止上溢和下溢,变换后的像素对也必须限定在 $D \subset [0,255] \times [0,255]$ 中,如式(7)所示:

$$0 \leqslant 2x - y \leqslant 255, 0 \leqslant 2y - x \leqslant 255 \tag{7}$$

为了避免解码的模糊性,那些位于 D 边缘上的同是奇数的像素对必须去除掉,这些像素对满足如下条件:$2x - y = 1, 2y - x = 1, 2x - y = 255, 2y - x = 255$。

用 D_c 表示排除这些模糊像素对的区域。水印嵌入的算法如下:首先将每块中左上角的 32 × 32 的像素子块按行两两分组,块中其他像素不变;然后把每一个像素对划归为 A、B、C 三种类型中的一种,对每一种类型执行相应的嵌入规则:

(1)如果 $(x,y) \notin D_c$,那么将其化为 C 类,把 x 的 LSB 位置 0,并且保留其原始的真值,该真值放在 128 位水印后一起嵌入图像中。

(2)如果 $(x,y) \in D_c$,且 (x,y) 同时为奇数,那么将其化为 B 类,并将 x 的 LSB 位置 0,y 的 LSB 位作为信息的嵌入位。

(3)如果 $(x,y) \in D_c$,并且 (x,y) 不同时为奇数,则将其划分为 A 类,利用式(5)对该像素对进行变换,把 x' 的 LSB 位置 1,y' 的 LSB 位作为信息的嵌入位。

从上面的分析可知,嵌入的信息位包括 128 位 hash 值和 C 类像素对中 x 的真值。通过实验结果可知,C 类像素对的数目非常少,因此需要嵌入的信息的长度也很少,而可用的嵌入空间足以容纳这些信息。

5)所有关系水印嵌入后,对每一块嵌入关系水印的图像计算其检测水印,并嵌入到自身块的右下角 32 × 32 子块。其中,检测水印的生成方法和嵌入方法与上面关系水印的产生和嵌入方法一样。

2 篡改检测和篡改定位

2.1 块级水印提取算法

把嵌入水印后的图像划分为互不重叠的 64 × 64 大小的子块。从每一块右下角的 32 × 32 子块中提取检测水印,并恢复其原始图像信息。水印的提取和恢复操作为,首先对提取区域中图像的像素进行两两分组,对每一个像素对 (x',y') 进行如下操作:

(1) 如果 x' 的 LSB 位为 1,则它属于 A 类,提取 y' 的 LSB 位,并把它放在提取出的水印序列里,将 x' 的 LSB 位置 0,通过式(6)恢复出原始的像素对 (x,y)。

(2)如果 x' 的 LSB 位为 0,把 x' 的 LSB 位置为 1 后,判断它们是否属于 D_c,如果属于则划为 B 类,提取 y' 的 LSB 位,并将其放在提取出的水印序列中,然后把 x' 的 LSB 位设置为 1,通过式(6)恢复出原始的像素对 (x,y)。

(3)如果 x' 的 LSB 位为 0,把 x' 的 LSB 位置为 1 后,它们不属于 D_c,则划为 C 类,从提出水印的真值中恢复出 x 的 LSB 位的真值,y 不变,则可得到原始的像素对 (x,y)。

提取出的前 128 位为该块的水印,而 64 × 64 图像的其他子块的值保持不变。用同样的方法从其他块的左上角的 32 × 32 子块中提取出对应偏移块的关系水印,并恢复其原始值。

对于每一个水印块 $\overline{b_i}$,提取出的关系水印和检测水印分别记做 W'_{i-r}, W'_{i-d},对提取出水印后恢复的图像块 $\overline{\overline{b_i}}$ 重新计算其关系水印和检测水印,方法同上,得出的关系水印和检测水印分别记做 W''_{i-r}, W''_{i-d}。通过比较提取出的水印和重新计算出的水印,判断该图像是否被篡改。若被篡改,则可将篡改进一步定位到具体的像素。具体过程如下:

(1)如果 $W'_{i-d} = W''_{i-d}, W'_{i-r} = W''_{i-r}$,即检测水印和关系水印都相等,说明图像块没有被篡改,该块可以通过认证。

(2)如果 $W'_{i-d} \neq W''_{i-d}, W'_{i-r} = W''_{i-r}$,即检测水印相等,但关系水印不相等,说明该块中有水印被篡改,该

块可以通过认证。

(3)如果 $W'_{i-d}=W''_{i-d}$,$W'_{i-r}\neq W''_{i-r}$,即检测水印不相等,关系水印相等,说明该块的偏移子块中的关系水印被篡改,该块可以通过认证。

(4)如果 $W'_{i-d}\neq W''_{i-d}$,$W'_{i-r}\neq W''_{i-r}$,即检测水印和关系水印都不相等,说明该块中的内容或者内容和水印均被篡改,该块不能通过认证。

为了提高图像的使用效率,一般情况下,如果水印被篡改,并不影响图像的使用,所以能通过认证,但是内容被篡改,则不能通过认证。因此要将篡改进一步定位到具体的某个像素。

2.2　像素级水印提取算法

(1)按照相同的密钥对图像进行置乱。

(2)在置乱后的图像中,提取出每个像素的定位水印 W'_{i-p}。

(3)在恢复后的图像中,重新计算每个像素定位水印 W''_{i-p}。

(4)比较 W'_{i-p} 和 W''_{i-p},若相等,说明该像素未被篡改,否则,该像素被篡改。

(5)所有像素被处理完后,去除孤立的被篡改的像素点,即得到最后的认证结果。

3　实验分析

在上述的双层嵌入算法中,有五种类型的算法密钥,包括控制猫置乱的参数 p,q 和迭代次数 M,生成像素级定位水印 W_{i-p} 的 Logistic 混沌映射的参数 μ,生成偏移块序列的 PWLCM 的初始值 X_0 和初始参数 P_0,在块级关系水印中产生关系水印 W_{i-r} 的 PWLCM 的初始值 X_0 和初始参数 P_0,在块级检测水印中产生检测水印 W_{i-d} 的 PWLCM 的初始值 X_0 和初始参数 P_0。初始条件、参数和混沌的复杂非线性特性对微小变化的极端敏感性,保证了该方案的密钥空间足够大。

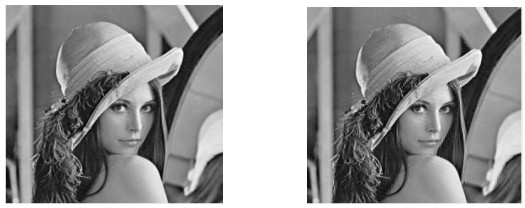
3.1　图像质量测试

文中算法采用图 1(a)所示的 Lena 图像(256 * 256 大小)作为实验的初始图像,而图 1(b)显示的则是完全嵌入水印后的图像,可以看出两幅图像基本没有太大的变化。通过 $x'+y'=x+y$ 和 $x'-y'=3(x-y)$,说明 RCM 变换只是增加了图像的对比度,并没有改变图像的平均灰度值。

峰值信噪比(PSNR)可以用来衡量嵌入水印后图像的质量。

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

其中,MSE 是原始图像和水印图像之间的均方误差。对于该实验的 Lena 图像来说,完全嵌入水印后的 PSNR 是 35.312 1,达到了峰值信噪比高于 35 dB[13] 的要求。



(a)原始 Lena 图像　　(b)完全嵌入水印的(a)图像

图 1　原始图像和水印图像

3.2　可逆容量

将嵌入的水印完全提取后,得到恢复后的图像,如图 2 所示。

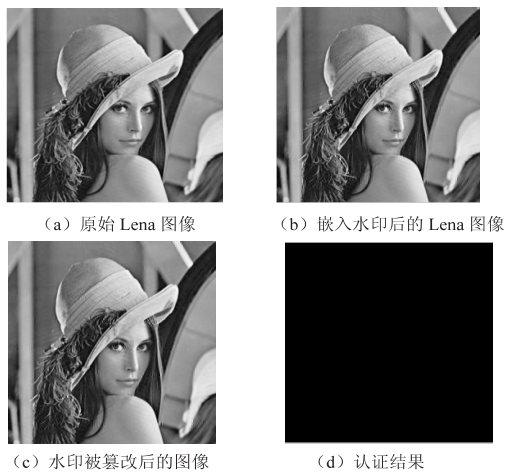
图 2　完全恢复后的图像

从图中可以看出,虽然每个块经历了关系水印和检测水印的两次提取,但是恢复后的图像中并没有留下永久的失真。

3.3　认证和定位能力

在接收端,通过比较提取的水印和重新计算的水印是否相等,从而确定该块是否被篡改。根据提出的算法,三种篡改定位能力分析如下:在认证结果图像中,通过认证的点表示为黑色,否则表示为白色。

(1)图 3(a)和图 3(b)分别表示原始的 Lena 图像和嵌入水印后的 Lena 图像。若检测水印被篡改,如图 3(c)所示,它能通过认证,结果如图 3(d)所示。在这种情况下,$W'_{i-d}\neq W''_{i-d}$,$W'_{i-r}=W''_{i-r}$,表示水印图像块 $\overline{b_i}$ 中嵌入的水印被篡改,但是恢复出的图像块 $\overline{\overline{b_i}}$ 能通过认证。



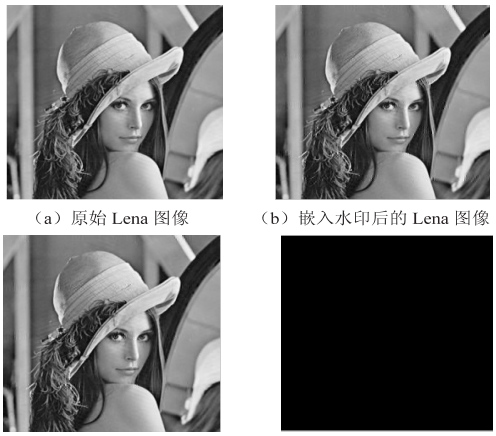
(a)原始 Lena 图像　　(b)嵌入水印后的 Lena 图像

(c)水印被篡改后的图像　　(d)认证结果

图 3　实验结果(1)

(2)图 4(a)和图 4(b)分别表示原始的 Lena 图像

和嵌入水印后的 Lena 图像。若关系水印被篡改,如图 4(c)所示,也能通过认证,结果如图 4(d)所示。在这种情况下, $W'_{i-d} = W''_{i-d}$, $W'_{i-r} \neq W''_{i-r}$,表示图像块 $\overline{b_i}$ 的偏移块中的关系水印被篡改,但是恢复出的图像块 $\overline{\overline{b_i}}$ 能通过认证。

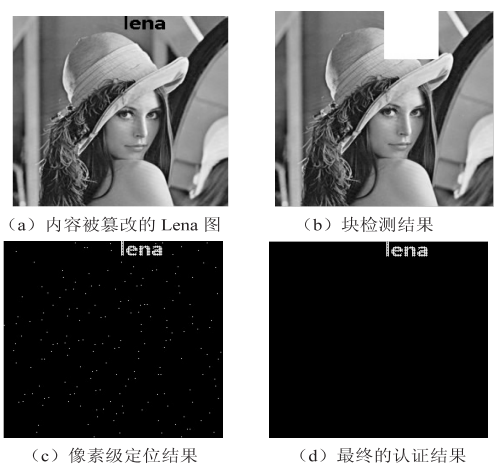


(a) 原始 Lena 图像 (b) 嵌入水印后的 Lena 图像

(c) 水印被篡改后的图像 (d) 认证结果

图 4 实验结果(2)

(3)为了测试该方案的实验效果,现在对图像内容进行修改。在嵌入水印后的 Lena 图像上加入“Lena”字样,如图 5(a)所示,在这种情况下, $W'_{i-d} \neq W''_{i-d}$, $W'_{i-r} \neq W''_{i-r}$,表明该块是可疑的。通过比较提取出的水印和重新计算出的水印,可疑块中的具体像素就能被进一步的定位,定位后的结果如图 5(c)所示。由于在像素级水印的计算过程中使用了单一的像素置乱算法,因此一些未被篡改的像素会被误认为是被篡改的,因此从认证结果图像中去除孤立的像素点,便得到了最后的认证结果,如图 5(d)所示。



(a) 内容被篡改的 Lena 图 (b) 块检测结果

(c) 像素级定位结果 (d) 最终的认证结果

图 5 实验结果(3)

3.4 安全性分析

通过 Fridrich 的观点[14],对分块算法的主要攻击为量化攻击。在提出的算法中,通过引入关系水印,使得每一个块的检测水印与它的偏移块的位置和内容是紧密相连的,当量化攻击想要替代某一块时,它将不能通过认证,因此该算法可以有效地避免量化攻击。同时,对于像素级水印来说,Oracle 攻击是最大的威胁。在提出的算法中,通过双层的水印算法来保证任何的篡改至少都能被检测到,并且定位到具体的块。

4 结束语

文中提出了一种基于混沌脆弱水印的双层图像认证方案,通过引入混沌水印,可以实现自认证和篡改定位。除此之外,在像素级的水印中,定位水印是通过 LSB 位替代实现的;在块级水印中,关系水印和检测水印是通过可逆的方式嵌入和提取,它能保证无损地恢复原始图像。理论分析和实验结果表明,该算法可以同时抵抗量化攻击和 Oracle 攻击,在需要认证和完整恢复原始图像的多媒体应用中具有可行性和高效性。

参考文献:

[1] 卢开澄. 计算机密码学:计算机网络中的数据保密与安全[M]. 北京:清华大学出版社,2003.

[2] 黄晓生. 数字图像安全技术研究进展[J]. 华东交通大学学报,2006,23(1):82-86.

[3] 王祖喜,赵湘媛. 用于图像认证的可恢复半脆弱数字水印[J]. 中国图象图形学报,2008,13(7):1258-1264.

[4] 吴金海,林福宗. 基于数字水印的图像认证技术[J]. 计算机学报,2004,27(9):1153-1161.

[5] 段贵多,赵 希,李建平,等. 一种新颖的用于图像内容认证、定位、和恢复的半脆弱数字水印算法研究[J]. 电子学报,2010,38(4):842-847.

[6] 和红杰,张家树. 基于混沌置乱的分块自嵌入水印算法[J]. 通信学报,2006,27(7):80-86.

[7] 金喜子,姜文哲. 块级篡改定位的 JPEG 图像脆弱水印[J]. 电子学报,2010,38(7):1585-1589.

[8] 谢建全,阳春华. 一种像素级的图像篡改认证算法[J]. 计算机应用,2007,27(6):1337-1338.

[9] 宋 双. 一种像素级的图像篡改定位和恢复的脆弱水印算法[D]. 长春:吉林大学,2009.

[10] 王国栋,刘粉林,刘 媛,等. 一种能区分水印或内容篡改的脆弱水印算法[J]. 电子学报,2008,36(7):1349-1354.

[11] Xiao D, Liao X F, Deng S J. One-way Hash function construction based on the chaotic map with changeable-parameter [J]. Chaos, Solitons & Fractals, 2005, 24(1): 65-71.

[12] Coltuc D, Chassery J M. Very fast watermarking by reversible contrast mapping[J]. IEEE Signal Processing Letters, 2007, 14(4): 255-258.

[13] Samuel S, Penzhorn W. Digital watermarking for copyright protection[C]//Proc of 7th AFRICON conference in Africa. [s. l.]: [s. n.], 2004: 953-957.

[14] Fridrich J. Security of fragile authentication watermarks with localization[J]. Proceeding of the SPIE, 2002, 4675: 691-700.