第 42 卷 第 9 期 计 算 机 工 程 2016 年 9 月
Vol. 42 No. 9 Computer Engineering September 2016

·安全技术· 文章编号：1000-3428(2016)09-0121-05 文献标志码：A 中图分类号：TP309

基于分层嵌入认证与恢复的自嵌入水印算法

石亚南，李江隐，康宝生

（西北大学 信息科学与技术学院，西安 710127）

摘 要： 为提高图像的篡改定位和恢复能力，提出一种空域与频域结合的分层自嵌入水印算法。第 1 层水印嵌入把 2×2 图像块内元素的奇偶校验码、异或校验码以及图像块的灰度均值信息作为水印进行加密后都嵌入到偏移块中，将处理过的偏移块元素的奇偶认证码嵌入其自身。第 2 层水印嵌入将嵌入第 1 层水印的图像分成 8×8 大小，提取每块频域特征加密后的信息嵌入到偏移块。分 3 层对图像进行检测定位与恢复，给出基于混沌序列与 Torus 同构映射结合的偏移值选取方法，以增强密钥安全性。实验结果表明，该算法可以同时抵抗字典搜索攻击、拼贴攻击、盲攻击以及大面积的剪切攻击，能准确地定位图像的篡改位置并且图像的恢复质量较高。

关键词： 自嵌入水印；篡改定位；篡改恢复；图像认证；混沌

中文引用格式： 石亚南，李江隐，康宝生. 基于分层嵌入认证与恢复的自嵌入水印算法[J]. 计算机工程，2016，42(9)：121-125.

英文引用格式： Shi Yanan，Li Jiangyin，Kang Baosheng. Self-embedding Watermark Algorithm Based on Layered Embedded Authentication and Recovery[J]. Computer Engineering，2016，42(9)：121-125.

Self-embedding Watermark Algorithm Based on Layered Embedded Authentication and Recovery

SHI Yanan，LI Jiangyin，KANG Baosheng

（School of Information and Technology，Northwest University，Xi'an 710127，China）

【Abstract】 To improve the ability of image tamper detection and recovery，this paper proposes a layered watermark algorithm based on the combination of the spatial and frequency domain. In layer 1，one part of the watermark information authenticating a single pixel in a block with the size of 2×2 pixels is embedded into self-block，and the other part together with recovery watermark are embedded into the mapping block. In layer 2，the image processed in layer 1 is divided into blocks with the size of 8×8. The frequency information is extracted and embedded into the mapping block. Three layers are used for image detection and recovering tampered image. This paper also proposes an offset value selection scheme based on chaos sequence and Torus isomorphic mapping to improve the safety of the secret keys. Experimental results demonstrate that the proposed algorithm can not only resist dictionary search attack，collage attack，blind attack and large area cropping attack but also locates the tampered blocks precisely with high quality of the recovered image.

【Key words】 self-embedding watermark；tamper location；tamper recovery；image authentication；chaos

DOI： 10.3969/j.issn.1000-3428.2016.09.022

1 概述

随着网络技术的发展，人们很容易在网上获得许多数字图像，一些人蓄意对图像进行篡改和破坏，因此，需要图像认证机制来检验图像的完整性和真实性。基于空域[1-4]、频域[5]、空域频域结合[6]或矢量表[7]的水印嵌入和认证机制可以实现图像的篡改定位和恢复。

文献[8]提出的双水印算法容易遭受字典搜索攻击[9]、盲攻击[9]、拼贴攻击[10]。文献[11]改进的双水印算法可以抵抗字典搜索攻击。但是其认证方法不能抵抗盲攻击。文献[12]改进的水印嵌入算法由于块与块之间独立，因此也无法抵抗拼贴攻击。文献[13]的算法可以抵抗拼贴攻击，但其方法的篡

基金项目： 国家自然科学基金资助项目(61272286)；陕西省自然科学基础研究计划基金资助项目(2014JM8346)。

作者简介： 石亚南(1987－)，女，硕士研究生，主研方向为信息安全；李江隐，硕士研究生；康宝生，教授、博士后。

收稿日期： 2015-08-27 **修回日期：** 2015-11-05 **E-mail：** 373095222@qq.com

改定位只能定位到 8×8 块,定位不够精准,而且图像的恢复质量不高。

针对上述问题,本文提出空域与频域结合的分层嵌入、检测和恢复的自嵌入水印算法。该算法定位篡改到 2×2 块,同时抵抗字典搜索攻击、拼贴攻击、盲攻击以及大面积的剪切攻击。基于空域的认证水印实现对 2×2 图像块的整体认证和对块内元素的认证,利用基于频域的水印信息进行二次认证,并结合空域和频域的水印对被篡改的图像进行恢复。同时提出 Logistic 混沌序列与 Torus 同构映射相结合的方式确定水印的嵌入位置。

2 算法设计

2.1 水印的嵌入

假定原始图像 I 大小是 $M\times P$,M 与 P 都是 2 的倍数。

2.1.1 嵌入位置选取

当嵌入水印时,需要一对一的映射序列来明确图像块的水印嵌入对应的哪一块里,把水印要嵌入的块称作偏移块。只利用 Torus 同构映射确定水印嵌入为位置的方法[8]搜索空间太小,密钥安全性比较低。文献[14]提出一种基于混沌置乱的分块自嵌入算法,其问题是部分图像块的水印会全都嵌入到自身块中,导致图像块在遭受攻击时它的水印也被一起破坏。文献[12]提出用交叉混沌序列来置乱图像块的方法存在的问题是不同的图像块的水印会嵌入到相同的偏移块中,需要二次处理,且图像分块越多,这种情况就越严重。

本文提出一种基于混沌序列与 Torus 同构映射结合的方法。Torus 自同构映射一维变换公式和 Logistic 公式分别如式(1)和式(2)所示。

$$x' = (K\times x)\bmod N + 1 \tag{1}$$

$$x_{n+1} = u\times x_n(1-x_n) \tag{2}$$

本文的水印嵌入位置选取步骤如下:

步骤 1 给定作为密钥的初始值 u_0,x_0,根据式(2)得到序列 $\{x_0,x_1,\cdots,x_k,x_{k+1},\cdots,x_{k+N}\}$,截取 $\{x_{k+1},x_{k+2},\cdots,x_{k+N}\}$ 作为长度为 N 的新序列,将新序列重新记为 $\{x'_0,x'_1,\cdots,x'_{N-1}\}$。迭代步长 k 也作为密钥。

步骤 2 获取每个 $\{x'_{a_i}\}$ 的下标,得到序列 $\{a_0,a_1,\cdots,a_{N-1}\}$。依据序列 $\{a_0,a_1,\cdots,a_{N-1}\}$ 的值顺次给图像块编号,得到一张编号表。

步骤 3 选取质数 $K\in[0,N-1]$ 为密钥。对于每个块,利用编号 a_i 及式(1)获得其偏移块的编号 a'_i。

步骤 4 查询步骤 2 获得的编号表,找到 a'_i 对应的偏移块的位置。

例如图 1(a)是密钥为 $u_0=3.8$,$x_0=0.15$,迭代步长 $k=100$,根据式(2)以及步骤 1~步骤 3 得到的编号表。图 1(b)是密钥 $K=13$,根据 Torus 同构映射公式以及编号表得到的查询表。

38	46	27	20	56	15	41	10
5	0	49	61	30	34	23	59
54	18	25	36	44	13	39	8
3	47	28	32	63	21	57	52
16	42	11	6	1	50	51	62
31	2	7	12	43	35	24	17
53	58	22	33	29	60	48	4
9	40	14	55	19	26	45	37

(a)编号表

47	23	32	5	25	4	22	3
2	1	62	19	7	59	44	0
37	48	6	21	61	42	60	41
40	36	32	33	52	18	38	37
17	42	16	15	14	11	24	39
20	27	28	29	48	8	57	30
50	51	31	46	58	13	49	53
54	9	55	12	56	19	10	34

(b)查询表

图 1 编号表与查询表示例

本文方法水印嵌入位置的选取需要密钥 u_0,x_0,k,K 共同决定。由于 u_0 为(3.569 945 6,4]范围内的任意实数,x_0 为(0,1)内的任意实数,迭代步长 k 的取值无上限,因此本文提出的嵌入位置选取方法增大了密钥搜索空间,提高了密钥安全性。利用排序后的混沌序列元素的下标给图像块编号,每个图像块对应唯一不同的编号,再利用一对一的线性函数 Torus 同构映射求出偏移块的编号,Torus 映射保证不同的编号对应唯一不同的编号,因此,该方法不会出现自身块的水印嵌入到自身块的情况,也不会出现不同块的水印嵌入到同一个偏移块中的情况。

2.1.2 第 1 层水印的生成与嵌入

I 中每个像素的最低有效 3 位清零后变为 I_0,对 I_0 分块,每块 2×2 大小。

2×2 图像块水印生成步骤如下:

步骤 1 计算每个图像块 A 的均值,获取均值的最高有效 5 位,作为该块的特征信息,记为 $W=(a_7,a_6,a_5,a_4,a_3)$。

步骤 2 从 A 块里提取每个元素的最高有效 5 位,得到 20 bit 信息:

$$A_{17},A_{16},A_{15},A_{14},A_{13},A_{27},A_{26},A_{25},A_{24},A_{23}$$

$$A_{37},A_{36},A_{35},A_{34},A_{33},A_{47},A_{46},A_{45},A_{44},A_{43}$$

利用式(3)获得其奇偶校验码 p,num 是 20 bit 信息中 1 的总个数。

$$p=\begin{cases}1 & num\text{ 数是奇数}\\ 0 & num\text{ 数是偶数}\end{cases} \tag{3}$$

步骤 3　利用式(4)获得 20 bit 信息的异或校验码 v:

$$v = A_{17}\oplus A_{16}\oplus A_{15}\oplus A_{14}\oplus A_{13}\oplus\cdots \oplus A_{47}\oplus A_{46}\oplus A_{45}\oplus A_{44}\oplus A_{43} \tag{4}$$

步骤 4　C 为 A 的偏移块,q_0 为 C 元素的认证码,初始值为 0。由 $a_7,a_6,a_5,a_4,a_3,p,v,q_0$ 构成了 A 块和它的偏移块 C 块的认证水印 W_0。

步骤 5　利用式(2)产生一个长度为 7 bit 的混沌序列,若序列里的值小于 0.5,则此值被 0 替换,否则被 1 替换。W_0 里前 7 bit 的值分别与混沌序列中的对应值做异或操作,得到新的水印:

$$W=(w_1,w_2,w_3,w_4,w_5,w_6,w_7,q_0)$$

2 ×2 图像块水印的嵌入及处理步骤如下:

步骤 1　将水印 W 嵌入到每个图像块 A 的偏移块 C 的 3-LSB 和 2-LSB 中。

步骤 2　C 块嵌入水印后变为 C',利用改进的滑动函数[15]如式(5)处理 C'中每个元素的值,并得到新块 C''。

$$Y'=\begin{cases}\hat{Y} & |t|<5\\ \hat{Y}+8 & t\leqslant -5\\ \hat{Y}-8 & t\geqslant 5\end{cases} \tag{5}$$

其中,Y 是原始像素值;$\hat{Y}$ 是嵌入水印后的像素值;Y'是运用滑动函数之后得到的像素值,$t=\hat{Y}-Y$。

步骤 3　灰度图像中每个像素的颜色值有 8 bit,获取 C''块里前 3 个元素中每个元素从高到低的前 7 bit简记为 7MSBs,第 4 个元素的 6MSBs,得到关于 C''的 27 bit 信息,这 27 bit 中 1 的总数用 *sum* 表示。利用式(6)计算 C''的奇偶校验码 q_c。q_c 来替代 C''里的水印 q_0:

$$q=\begin{cases}1 & sum\ 数是奇数\\ 0 & sum\ 数是偶数\end{cases} \tag{6}$$

步骤 4　通过 2 ×2 图像块水印生成的步骤 1 ~ 步骤 5 计算 C''的水印 W'。

步骤 5　把 C''赋值给 A,W'赋值给 W,重复步骤 1 ~ 步骤 4 直到最后一个图像块 D。

步骤 6　获取 D 的水印加密后嵌入到其偏移块 A 的从低位数的第 3 个比特位,简记为 LSB-3,LSB-2 此时不需要再对 A 进行滑动函数的处理,计算 q_A 来替代 A 里的水印 q_0。

2.1.3　第 2 层水印的生成与嵌入

把经过第 1 层水印嵌入的图像均分为 4 个区,第 2 层水印的生成以及嵌入步骤如下:

步骤 1　对每一区分块,每块 8 ×8 大小。对每块进行 DCT 变换,用量化器量化处理 DCT 系数,对量化后的系数按照 *zig-zag* 顺序编码,直到满64 bit,把这 64 bit 记作 L。

步骤 2　利用式(2)产生一个长度 64 bit 范围(0,1)的 Logistic 混沌序列 S,当序列里的值大于等于 0.5 时此值被 1 替代,否则被 0 替代。

步骤 3　L 与 S 进行异或操作得到长度为 64 bit 的水印 *Water*。把 *Water* 嵌入其对角区对应的偏移块的 1-LSB。

2.2　图像块的篡改检测与定位

将可能遭受到篡改的水印图像 I'_w分 3 层检测定位。设 2 × 2 图像块 A 的偏移块是 C,A 所在的 8 ×8 块为 $Block_1$,$Block_1$ 的偏移块为 $Block_2$。标识矩阵 $\boldsymbol{F}_1$,$\boldsymbol{F}_2$ 分别标识每个 2 ×2 块以及 8 ×8 块是否有效,有效代表没有被篡改,在初始时,矩阵 $\boldsymbol{F}_1$,$\boldsymbol{F}_2$ 对每一块的标识都有效。详细步骤如下:

第 1 层检测　(1)利用 2 ×2 图像块水印的嵌入及处理的步骤 3 计算每个 2 ×2 图像块 C 的 q'_C,若 $q_C\neq q'_C$,$\boldsymbol{F}_1$ 标识此块无效。(2)利用 2 ×2 图像块水印生成的步骤 1 ~ 步骤 3 计算 A 的 p',v',W',若 $p\neq p'$或者 $v'\neq v$ 或者 $W'_A\neq W_A$,则 $\boldsymbol{F}_1$ 标记 A 无效。

第 2 层检测　搜索 $\boldsymbol{F}_1$ 标识有效的 2 ×2 块,若其邻域块中至少有 5 处被标记为无效,则 $\boldsymbol{F}_1$ 标记此块无效。

第 3 层检测　提取每个 8 ×8 块 $Block_2$ 的水印,解密后记作 L',若 $L'=L$,则 $\boldsymbol{F}_2$ 标记 $Block_1$ 有效。若 $L'\neq L$,则检测 $Block_1$ 中是否有 2 ×2 块被 $\boldsymbol{F}_1$ 标记为无效,若存在无效的块,则 $\boldsymbol{F}_2$ 标记 $Block_1$ 有效,否则无效。

2.3　篡改图像块的恢复

第 1 层恢复　(1)对于每个 2 ×2 大小的图像块 A,若 $\boldsymbol{F}_1$ 标识其无效,则根据查找表找到 A 的偏移块 C。若 $\boldsymbol{F}_1$ 标识 C 有效,则从 C 中提取 A 的水印信息,对其解密以获得 A 的 5 bit 特征水印,若 $\boldsymbol{F}_1$ 标识 C 无效,则跳过(2)进行第 2 层恢复。(2)将特征水印后面加 3 个 0 补全成 8 bit,用其代表的数值替代 A 块中每个元素的值。$\boldsymbol{F}_1$ 重新标识 A 块有效。

第 2 层恢复　(1)经过第 1 层恢复后,对于 $\boldsymbol{F}_1$ 中仍标识无效的块 A,找到其所在 8 ×8 块 $Block_1$ 的偏移块 $Block_2$。若 $\boldsymbol{F}_1$ 标识 $Block_2$ 有效,从 $Block_2$ 提取水印信息,解密,反量化,*IDCT* 变换,得到 $Block_1$ 的 8 ×8 灰度水印块 *Water*。若 $\boldsymbol{F}_1$ 标识 $Block_2$ 无效,跳过(2)进行第 3 层恢复。(2)在 $\boldsymbol{F}_1$ *Water* 找到与 A 处于相同位置的 2 ×2 块,替换 A 块,重新标识块 A 有效。

第 3 层恢复　经过第 1 层和第 2 层恢复后,若 $\boldsymbol{F}_1$ 仍标识某些块无效,找到此无效块的 3 ×3 邻域块的有效 2 ×2 图像块,计算出这些有效块的均值替代 A 里的每个元素,$\boldsymbol{F}_1$ 标识 A 块有效。

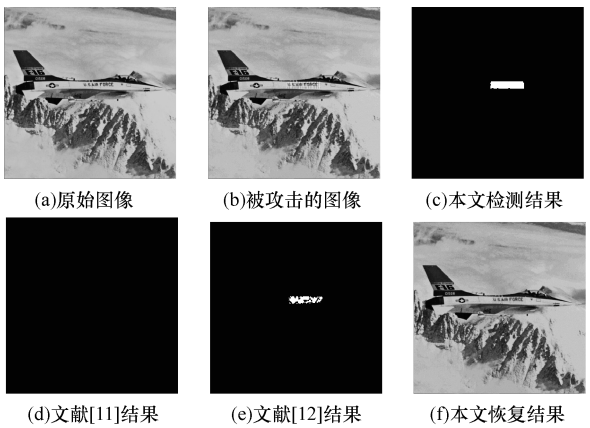
3　实验结果及分析

对本文提出的基于分层嵌入认证和恢复的自嵌入算法进行了仿真实验。本文以 jet,Barbara,Martha,

Lena 等大小为 512 像素 ×512 像素,8 bit 的灰度图像进行实验。采用篡改检测率、误检率、峰值信噪比(Peak Signal to Noise Ratio,PSNR)评估算法性能。仿真实验的测试硬件环境为 Intel(R) Core(TM)2 Duo CPU 3.00 GHz 4 GB 内存,编程环境为 Matlab2008。

3.1 盲攻击

图 2(a)是原始 jet 图像,图 2(b)jet 图像的字母处遭受盲攻击,共有 550 块 2 ×2 大小的图像块遭受攻击,图 2(c)是本文的检测结果,篡改检测率达到 97.46% 。图 2(d)是文献[11]的检测结果,篡改检测率为 0% 。图 2(e)是文献[12]的检测结果,篡改检测率为 63.45% 。图 2(f)是本文方法的恢复结果,PSNR 为 39.729 8 dB。可以看出,本文方法在针对盲攻击的检测和恢复上效果都很好。表 1 是对遭受盲攻击的 jet 图像的检测情况具体的数据描述,本文方法的篡改检测率高,误检率为 0% 。在图像遭到盲攻击时,本文方法的检测结果要优于文献[11-12]方法。



(a)原始图像 (b)被攻击的图像 (c)本文检测结果

(d)文献[11]结果 (e)文献[12]结果 (f)本文恢复结果

图 2 jet 盲攻击实验结果

表 1 盲攻击不同方法的篡改检测结果

方法	被篡改的 2 ×2 块数	检测到的块数	误检块数	篡改检测率/%
本文方法	550	537	0	97.64
文献[11]方法	550	472	0	0.00
文献[12]方法	550	349	0	63.45

3.2 拼贴攻击

图 3(a)是 Barbara 原始图像,图 3(b)是遭受拼贴攻击的嵌水印的 Barbara 图像,把 Barbara 的书柜拼贴到原书柜旁边。图 3(c)是本文的检测结果,篡改检测率是 98.36% ,误检率是 0.2% 。图 3(d)是文献[11]的检测结果,篡改检测率是 9.6% ,误检率是 6.38% 。图 3(e)是文献[12]的检测结果,篡改检测率为 0% 。图 3(f)是本文方法的恢复结果,PSNR 为 42.323 5 dB。表 2 是对遭受拼贴攻击的 Barbara 图像的检测情况具体的数据描述,本文方法的检测率远高于文献[11-12]的方法,误检率要远低于文献[11]方法。在图像遭到拼贴攻击时,本文方法的检测结果要优于文献[11-12]的方法。

(a)Barbara原始图像 (b)被篡改图像 (c)本文检测结果

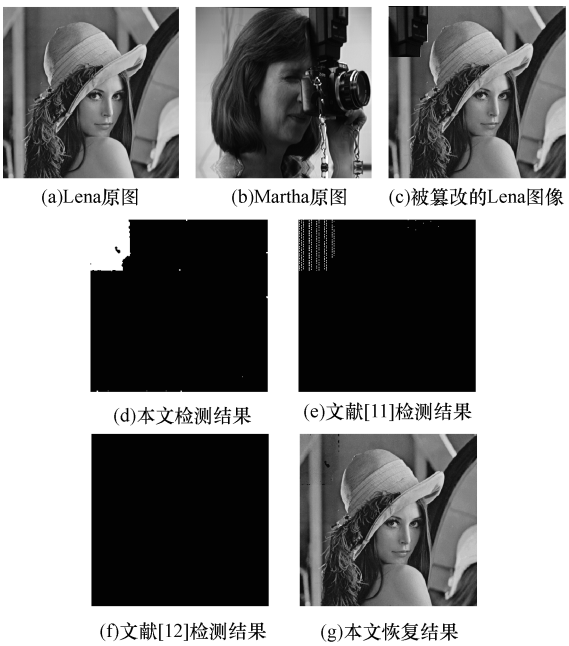
(d)文献[11]结果 (e)文献[12]结果 (f)本文恢复结果

图 3 Barbara 拼贴攻击实验结果

表 2 拼贴攻击不同方法的篡改检测结果 1

方法	被篡改的 2 ×2 块数	检测到的块数	误检块数	篡改检测率/%
本文方法	3 105	3 054	6	98.36
文献[11]方法	3 105	298	19	9.60
文献[12]方法	3 105	0	0	0.00

图 4(a)是 Lena 原始图像,图 4(b)是 Martha 原始图像,图 4(c)是遭受拼贴攻击的嵌水印的 Lena 图像,此攻击把 Martha 相机的一部分拼贴到 Lena 图像中。图 4(d)是本文的检测结果,篡改检测率是11.46% ,误检率是 0.98% 。图 4(e)是文献[11]的检测结果,篡改检测率是 9.6% ,误检率是 1.48% 。图 4(f)是文献[12]的检测结果,篡改检测率为 0% 。图 4(g)是本文方法的恢复结果,PSNR 为 37.877 7 dB。



(a)Lena原图 (b)Martha原图 (c)被篡改的Lena图像

(d)本文检测结果 (e)文献[11]检测结果

(f)文献[12]检测结果 (g)本文恢复结果

图 4 Lena 拼贴攻击实验结果

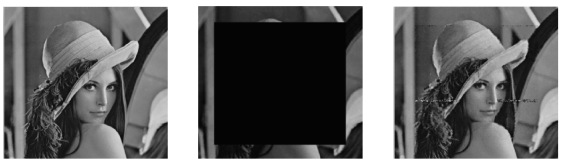
表 3是对遭受拼贴攻击的 Lena 图像的检测情况描述,本文方法的检测率远高于文献[11-12],误检率要远低于文献[11]。在图像遭到拼贴攻击时,本文方法的检测结果要优于文献[11-12]。

表 3　拼贴攻击不同方法的篡改检测结果 2

方法	被篡改的 2×2 块数	检测到的块数	误检块数	篡改检测率/%
本文方法	4 120	4 085	40	99.15
文献[11]方法	4 120	472	7	11.46
文献[12]方法	4 120	0	0	0.00

3.3　剪切攻击

图 5～图 7 是针对遭受剪切攻击的 Lena 图像的恢复效果。本文实验同时也对图像进行了上部分和左半部分的剪切,图像恢复的 PSNR 值分别是 32.700 7 dB,31.258 6 dB,因为空间有限,不再附图。实验结果表明,本文方法对各个角度的剪切攻击恢复效果都比较理想,在针对大面积的裁切攻击时的恢复效果也比较理想。



(a)Lena原图　(b)被破坏的图像　(c)恢复结果PSNR为 27.030 4 dB

图 5　Lena 中间部分剪切攻击的实验结果

(a)Lena原图　(b)被破坏的图像　(c)恢复结果PSNR为 31.420 9 dB

图 6　Lena 下半部分剪切攻击的实验结果

(a)Lena原图　(b)被破坏的图像　(c)恢复结果PSNR为 32.958 dB

图 7　Lena 右半部分剪切攻击的实验结果

4　结束语

为提高自嵌入水印抗综合攻击的能力,本文提出一种空域与频域结合的自嵌入算法。实验结果表明,该方法针对盲攻击、字典搜索攻击、拼贴攻击和剪切攻击具有很高的定位能力和恢复能力,密钥安全性高。然而,该算法对于超过 70% 的剪切攻击恢复效果并不理想,如何在保证良好的抗拼贴攻击、盲攻击的基础上对超过 70% 的篡改仍有良好的恢复效果是以后的研究方向。

参考文献

[1] Chaluvadi S B, Prasad M V N. Efficient Image Tamper Detection and Recovery Technique Using Dual Watermark[C]//Proceedings of Nature & Biologically Inspired Computing. Washington D. C., USA: IEEE Press, 2009: 993-998.

[2] 张大兴,章建芬,韩　锋. 基于混沌映射的脆弱水印算法[J]. 杭州电子科技大学学报,2013,33(6):57-61.

[3] Rawat S, Raman B. A Chaotic System Based Fragile Watermarking Scheme for Image Tamper Detection[J]. AEU——International Journal of Electronics and Communications, 2011, 65(10): 840-847.

[4] Dadkhah S, Manaf A A, Sadeghi S. Efficient Digital Image Authentication and Tamper Localization Technique Using 3Lsb Watermarking[J]. International Journal of Computer Science Issues, 2012, 9(1).

[5] 潘　蓉,田玉敏,董　萱. 一种图像内容可恢复的脆弱水印算法[J]. 华中科技大学学报,2012,40(7):67-70.

[6] 张君捧,张庆范,杨红娟. 基于块特征和混沌序列的图像篡改检测与恢复[J]. 山东大学学报,2014,44(6):63-69.

[7] Yang C W, Shen J J. Recover the Tampered Image Based on VQ Indexing[J]. Signal Process, 2010, 90(1): 331-343.

[8] Lee T Y, Lin S D. Dual Watermark for Image Tamper Detection and Recovery[J]. Pattern Recognition, 2008, 41(11): 3497-3506.

[9] Chang C, Fan Y H, Tai W L. Four-scanning Attack on Hierarchical Digital Watermarking Method for Image Tamper Detection and Recovery[J]. Pattern Recognition, 2008, 41(2): 654-661.

[10] Fridrich J, Goljan M, Memon N. Cryptanalysis of the Yeung Mintzer Fragile Watermarking Technique[J]. Journal of Electronic Imaging, 2002, 11(2): 262-274.

[11] 赵彦涛,李志全. 一种改进的图像篡改和定位恢复的分层半脆弱数字水印算法[J]. 光电子激光,2009,20(7):104-110.

[12] Tong Xiaojun, Liu Yang, Zhang Miao, et al. A Novel Chaos-based Fragile Watermarking for Image Tampering Detection and Self-recovery[J]. Signal Processing, 2013, 28(3): 301-308.

[13] Li Chunlei, Wang Yunhong, Ma Bin, et al. A Novel Self-recovery Fragile Watermarking Scheme Based on Dual-redundant-ring Structure[J]. Computer & Electrical Engineering, 2011, 37: 927-940.

[14] 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.

[15] Wang Ling, Ye Qun, Xiao Yaoqiang, et al. An Image Encryption Scheme Based on Cross Chaotic Map[C]//Proceedings of Image and Signal Processing. Washington D. C., USA: IEEE Press, 2008: 22-26.

编辑　刘　冰