文章编号: 1001- 2486(2008) 04- 0059- 05

一种基于混沌的彩色图像空域半脆弱水印算法[X]

丁文霞, 卢焕章, 王 浩, 谢剑斌
(国防科技大学 电子科学与工程学院, 湖南 长沙 410073)

摘 要: 为实现对数字产品的版权保护和完整性认证, 提出了一种以最低有效位(LSB) 替换算法为核心, 以彩色图像 RGB 图层亮度分量为载体的基于混沌二值密钥随机控制的彩色图像空域有意义水印算法。实验结果表明, 算法实现简单, 实时性好, 具有良好的透明性、安全性和确定性, 可盲检测, 并能够很好地实现版权保护和篡改检测与定位, 同时算法对椒盐噪声的去除、裁剪等基本图像操作和位平面去除等恶意攻击具有一定的鲁棒性, 因而是一种性能良好的半脆弱水印算法。

关键词: 混沌; 数字水印; 半脆弱水印; 数字签名
中图分类号: TP393 文献标识码: A

A Half2fragile Space Watermarking Algorithm of Color Images Based on Chaotic System

DIAN Wen2xia, LU Huan2zhang, WANG Hao, XIE Jian2bin
(College of Electronic Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: Aimed for the copyright protection and integrality authentication, a space significant watermarking algorithm of color images controlled by chaotic binary keys which mainly use the Least Significant Bit (LSB) substitution operations and regard the lightness data of RGB layers as cover messages has been proposed in this paper. The experimental result shows that the algorithm is easy to implement and has good transparence, high security and conformity. The algorithm can also realize blind detection, copyright protection, sophistication detection and localization efficiently. At the same time, it has good robustness for hostility attacks such as pepper2salt noise wiping off, cutting and bi2plane deleting. So it is a good half2fragile watermarking algorithm.

Key words: chaos; digital watermarking; half2fragile watermarking; digital signature

近几年来, 随着网络技术的发展, 多媒体内容的完整性认证, 尤其是图像的完整性认证技术亦随之产生并发展起来, 其目前的解决方案集中在数字签名技术和脆弱水印技术两方面。基于密码学的数字签名技术的工作流程为: 信息发送者用其私钥对所传内容进行加密运算得到签名, 该签名即具有不可抵赖性, 当接受者收到信息后, 就可用发送者的公钥对数字签名的真实性进行验证。此种技术复杂性低, 易于实现, 但多媒体信息经过加密后容易引起攻击者的好奇和注意, 并且有被破解的可能, 而一旦破解其内容就完全透明了, 而且密文不允许有一点改动, 否则接受者无法恢复正确信息。脆弱数字水印技术则克服了数字签名技术的缺点。

所谓脆弱数字水印技术[1]即在保证一定视觉质量前提下, 将数字水印嵌入到多媒体数据中, 当多媒体内容受到怀疑时, 提取该水印来鉴别多媒体内容的真伪, 并指出篡改位置, 甚至攻击类型等。使用水印技术有两方面的潜在优势: (1) 水印不需存储相关的超数据(如签名) ; (2) 水印和含水印作品一起经历相同变换, 与附加签名不同, 当作品被改写时水印自身也发生变化, 因而通过水印和已知变换的比较, 不仅可以知道是否改变, 并且可以推断出何时何地发生了怎样的改变。目前, 根据识别篡改的能力, 可将脆弱水印划分为完全脆弱水印、半脆弱水印、图像可视内容鉴别和自嵌入水印四个层次[1], 其中完全脆弱水印能够检测出任何对图像像素值改变的操作或图像完整性破坏, 它不允许图像有任何改动, 而半脆弱水印比完全脆弱水印稍微鲁棒一些, 允许图像有一定的改变, 是在一定程度上的完整性检测, 同时能

X 收稿日期: 2007- 11- 17
作者简介: 丁文霞(1973)), 女, 副教授, 博士生。

够抵抗一定程度的数字信号处理, 如裁剪、加噪、JPEG 压缩、VQ 压缩等。

1 算法描述

目前, LSB 位平面替换算法仍是时空域嵌入技术的经典算法, 文献[2- 7]均以该算法为核心, 如 Tirkel 等[2- 3]采用的水印是 m 序列, 其中载体图像的每一行嵌入一个二值 m 序列。文献[4]利用 DPCM 技术对版权文件 ASCII 形式进行加密得到 8 比特水印, 将这 8 比特替换原始载体图像的 8 个像素的最低位。文献[5]的嵌入过程按行按列进行, 对于奇数行和偶数行, 分别用水印替换相应行位置的像素最低位。文献[6- 7]的嵌入过程则分块进行。考虑到最低位平面替换的鲁棒性差, 文献[8]又提出了将水印与 8 位图像的低 4 位位平面进行随机替换的多位平面替换算法, 使得算法的安全性大大提高。另外, 早期的水印嵌入算法都是针对灰度图像提出的, 用于彩色图像上的水印算法较少, 由于人眼对蓝色信息不那么敏感, Kutter 等人[9]提出通过修改每个像素的蓝色分量实现水印嵌入, Piva 等人[10]则提出基于 RGB 通道互相关的彩色图像水印算法, 文献[11]也提出了基于颜色量化技术, 即调色板设计和像素映射的彩色图像水印算法。本文在上述算法的基础上, 提出了一种用混沌二值密钥随机控制, 载体为彩色图像 RGB 各通道亮度分量的多位平面随机替换的时空域水印算法。算法的总体思路是: 将内容较不重要或容量较大的水印信号(如商标 W1)嵌入蓝色亮度分量的低 4 位位平面, 将内容较重要或容量较小的水印信号(如 ID 号 W1)分别嵌入红色亮度分量的低 2 位位平面及绿色亮度分量的低 2 位位平面, 两次嵌入的位置分别由两个独立的混沌二值密钥随机控制, 总体采用分块重复嵌入的方式, 每次重新嵌入密钥均随之更新。嵌入过程原理图如图 1 所示。需要说明的是, 为更好地实现篡改检测和定位, 本算法并不对原始水印图像进行加密处理。

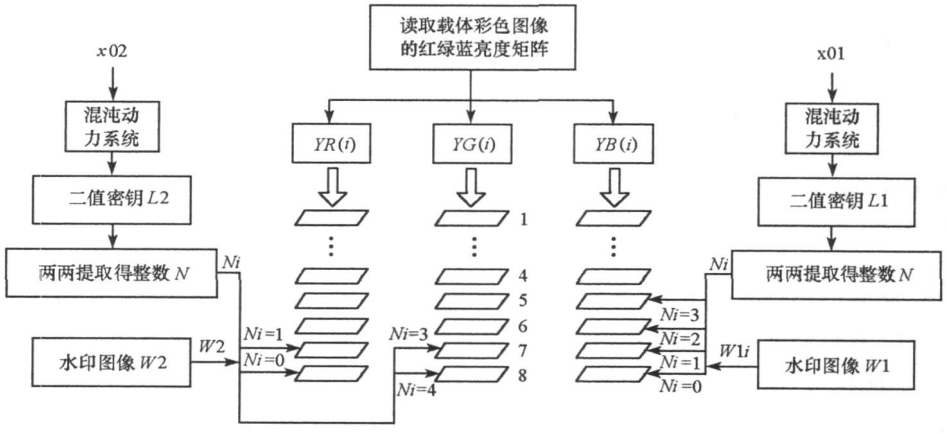

图 1 算法水印嵌入过程原理图

Fig. 1 The watermarking embedding process schematic diagram of the algorithm

具体嵌入过程实现步骤如下:

Step 1 将载体彩色图像的 RGB 亮度分量读入相应的数据矩阵 YR、YG、YB 中, 计算图像长宽值和总体大小;

Step 2 读入二值水印信号 W1 和 W2, 根据各自大小和载体图像大小, 计算需重复嵌入水印的次数, 若该次数非整数, 需将水印分块均匀嵌入载体图像中, 以避免较大的视觉差异;

Step 3 为克服单个混沌动力学系统的平凡密钥和拟平凡密钥现象, 采用 Logistic 和 Chebyshev 映射相互迭代的方式来生成混沌二值密钥, 由初值 x01 经迭代系统生成长度为 2@size(W1)的混沌二值密钥 L1, 由初值 x02 经迭代系统生成长度为 2@size(W2)的混沌二值密钥 L2; 重复嵌入时, x01 和 x02 均即时更新为: x01= [x01+ x(p)]P2; x02= [x02+ x(p)]P2; 其中 x(p)为上次混沌迭代的第 p 个实数值, p 由外部参数输入确定, 且 0< p< min(2@size(W1), 2@size(W2));

Step 4 将密钥 L1 的值两两提取并转化为 0~ 3 之间的整数 N, 依据 N 的大小将 W1 对应的值嵌入到蓝色亮度分量矩阵 YB 中, 具体嵌入方式为: N = 0 时, 将 W1(i)替换 YB(i)的第 8 位; N = 1 时, 将

W1(i) 替换 YB(i) 的第 7 位; N= 2 时, 将 W1(i) 替换 YB(i) 的第 6 位; N= 3 时, 将 W1(i) 替换 YB(i) 的第 5 位;

Step 5 将密钥 L2 的值两两提取并转化为 0~ 3 之间的整数 N, 依据 N 的大小将 W2 对应的值嵌入到红绿色亮度分量矩阵 YR、YG 中, 具体嵌入方式为: N= 0 时, 将 W2(i) 替换 YR(i) 的第 8 位; N= 1 时, 将 W2(i) 替换 YR(i) 的第 7 位; N= 2 时, 将 W2(i) 替换 YG(i) 的第 8 位; N= 3 时, 将 W2(i) 替换 YG(i) 的第 7 位;

Step 6 一轮嵌入完成后, 更新密钥, 进行重复嵌入, 直至将整幅图像处理完毕, 输出显示嵌入水印后的图像文件, 进行相应分析。

水印提取过程与嵌入过程相逆, 提取的结果仅取决于初始密钥和 p 值, 为盲提取。

2 实验结果及分析

用两个大小为 128@128 的 RGB 彩色图像(24bits true color)))) 丽娜(Lena) 和飞机(F14) 作载体图像, 如图 2(a) 、(b) 所示, 其中丽娜图像背景丰富, 颜色偏红, 飞机(F14) 主体突出, 背景平淡, 颜色偏蓝; 两个二值图像/ rose640(64@64, 图像, 类似版权商标) 和/ gfkd640(64@64, 文字, 类似版权说明) 被用作水印, 如图 2(c) 、(d) 所示。算法的各项仿真结果及攻击检测说明如下:

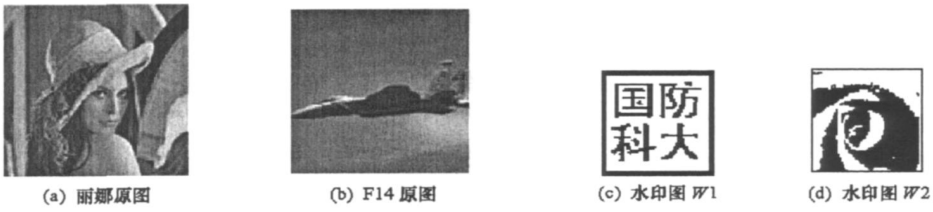

图 2 原始载体彩色图像及二值水印图像

Fig. 2 The original carrier color images and binary watermarking images

1. 水印嵌入和提取的视觉效果

在 x01= 01356487, x02= 01756849, p= 31 的外部输入参数下对两幅彩色载体图像按上述算法进行了仿真测试, 图 3 显示了水印嵌入后的图像视觉效果及密钥正确和错误(误差仅 10^{-10}) 时提取的单个或全部水印图像; 图 4 示出了丽娜图像嵌入水印前后的 RGB 三亮度分量的对应的直方图。表 1 列出了两幅含水印图像的 NAD、NMSE、PSNR、IF 和 NC 的计算结果, 这些结果均定量说明了本算法嵌入水印后的图像质量并未大幅下降, 仅有轻微损失。

图 3 嵌入水印后彩色图像及单个和整体水印提取效果

Fig. 3 The single and whole watermarking picking-up effect of the watermarking-embedded color images

2. 位平面恶意删除(0 替代) 攻击鲁棒性检测

最早的 LSB 算法很难抵抗位平面删除攻击, 即将最低位平面整体用/ 00或/ 10替代, 就可以将水印信息完全擦除。而本算法在嵌入过程中引入了一个位平面控制器, 即利用混沌伪随机序列发生器的输出随机选择位平面进行替换, 这种控制机制简单并易于实现, 但却可以有效地防止水印被自动去除, 在这种情况下, 攻击者很难从视频信号中去除水印, 除非图像质量被严重破坏, 因而算法的安全性得到了显著提高。图 5 示出了本算法对位平面替代恶意攻击的鲁棒性测试结果。

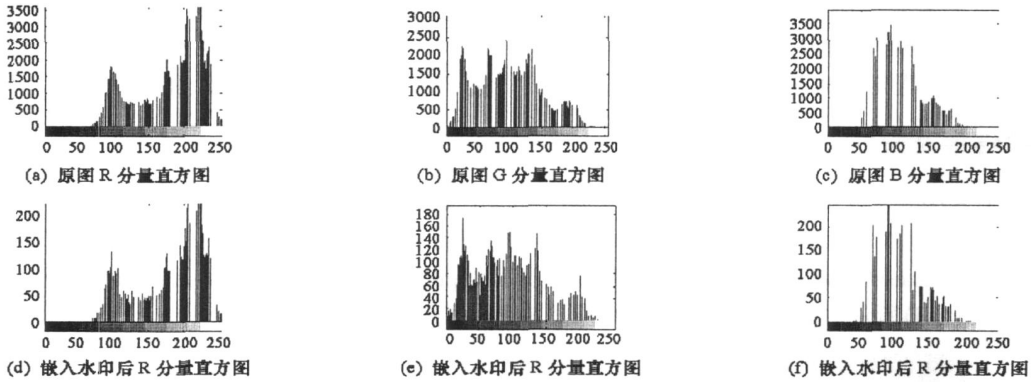

图 4 丽娜图像嵌入水印前后的 RGB 三亮度分量的直方图对比

Fig. 4 The comparison histogram of RGB lightness data of Lena original image and watermarking embedded image

表 1 部分含水印图像蓝色分量基于像素的图像质量测试值

Tab. 1 Part image quality testing values based on pixels of the blue layer of watermarking embedded image

含水印图像	基于图像像素的图像质量测试值				
	NAD	NMSE	PSNR(dB)	IF	NC
丽娜	01 0072	31 8353@10^{-4}	301 1849	01 9996	01 9873
F- 14	01 0051	11 7469@10^{-4}	401 7052	01 9998	01 9909

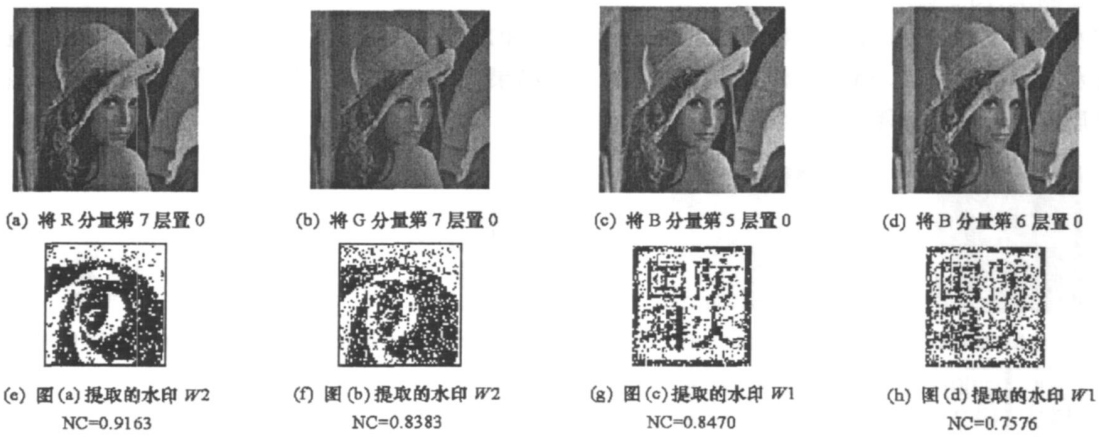

图 5 算法对位平面替代恶意攻击的鲁棒性测试

Fig. 5 Results of robustness testing for bit plane hostility substitution of the algorithm

3. 篡改检测及定位

本算法属于脆弱型数字水印算法, 根据脆弱数字水印的基本要求, 本算法应能进行篡改检测, 即当多媒体内容受到怀疑时, 可提取水印来鉴别多媒体内容的真伪, 并指出篡改位置, 甚至攻击类型等。图 6 以含水印 F14 图像为例, 给出了本算法对含水印图像进行某些篡改操作时的篡改检测仿真结果, 显示了本算法良好的篡改检测及定位功能。

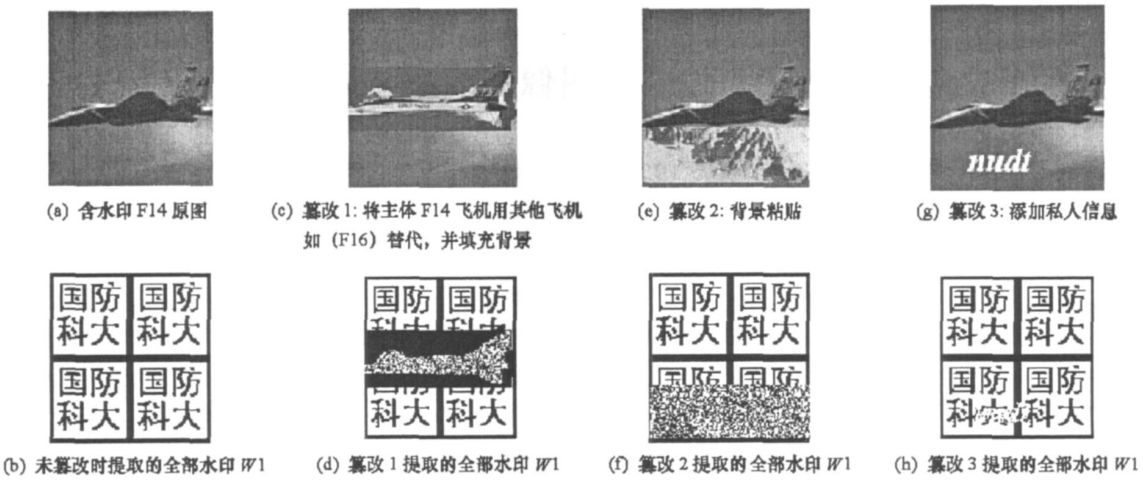

图 6 算法对篡改检测及定位鲁棒性测试(以 W1 为例)

Fig. 6 Results of robustness testing for sophistication detection and localization of the algorithm(W1 exampled)

4. 其他常见图像处理鲁棒性分析

大量实验结果表明, 本文算法对裁剪、任意涂改、加/ 椒盐0噪声等处理具有一定的鲁棒性, 而对高斯噪声、乘性噪声、滤波、增强降低亮度和对比度、平滑、锐化、JPEG 压缩、旋转等其他图像处理操作的鲁棒性很差, 几乎提取不出水印。图 7 示出了部分图像处理水印提取效果。

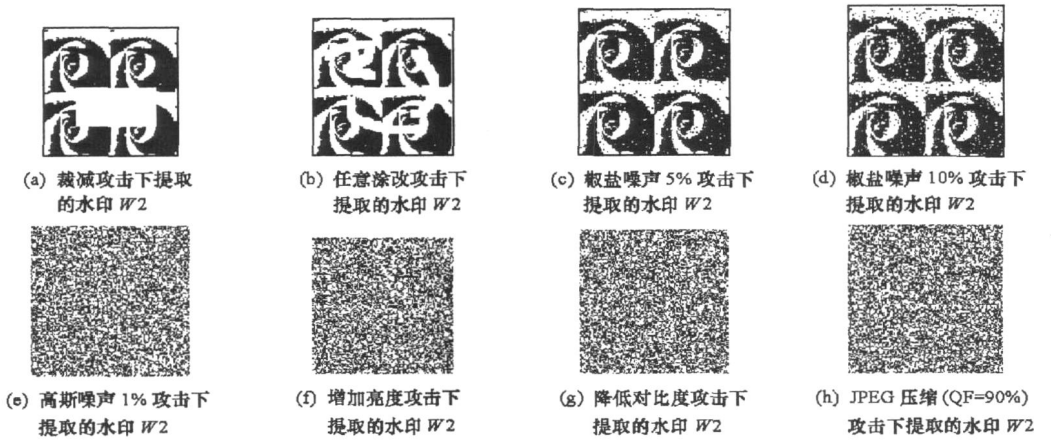

图 7 算法对一些常见图像处理鲁棒性测试结果(以 W2 为例)

Fig. 7 Results of robustness testing for some image processing of the algorithm (W2 exampled)

3 结 论

基于混沌伪随机二值序列密钥控制的 LSB 替换技术的彩色图像空域半脆弱水印算法, 密钥空间大, 安全性较高, 水印嵌入容量较大, 不但可以很好地完成图像完整性认证, 进行篡改检测和定位, 同时由于嵌入了有意义水印, 还可以实现签名认证、版权认证等功能, 且由于算法控制机制简单并易于实现, 因而水印嵌入和提取的速度较快, 嵌入和提取一幅 64 @64 大小的水印, 平均时间可小于 0115s, 因而本算法也非常适于视频流的水印嵌入与提取。

虽然数字水印技术近年来发展比较迅速, 但离实际应用尚有一段距离。目前, 水印技术的研究正朝着将时频域结合的组合水印算法、多重水印算法和以特征点为核心的第二代数字水印算法[1] 等方向发展, 数字水印技术还有很多问题值得我们进一步研究。

(下转第 102 页)

果与设计意图完全一致, 证明该轮- 腿复合式移动平台的设计方案是可行的。

参 考 文 献:

[1] Huang B, Wang P F, Sun L N. Behavior2based Control of a Hybrid Quadruped Robot[C]PPProceedings of the 6th World Congress on Intelligent Control and Automation, Dalian, China, 2006: 8997- 9001.

[2] Wang P F, Huang B, Sun L N. Walking Research on Multi2motion Mode Quadruped Bionic Robot Based on Moving ZMP[C]PPProceedings of the 2005 IEEE International Conference on Mechatronics & Automation Niagara Falls, Canada, 2005: 1935- 1940.

[3] Endo, Hirose G. Study on Roller2walker (multi2mode steering control and self2contained locomotion)[C]PPProceedings of the ICRA. 00. IEEE International Conference on Robotics and Automation. Japan: Dept. of Mechanc2aerosp. Eng., Tokyo Inst. of Technol. 2000: 2808- 2814.

[4] Adachi, Koyachi H. Development of a Leg2wheel Hybrid Mobile Robot and Its Step2passing Algorithm[C]PPProceedings. 2001 IEEEPRSL International Conference on Intelligent Robots and Systems. Tsukuba, Japan: Nat. Inst. of Adv. Ind. Sci. & Technol, 2001: 728- 733.

[5] Hashimoto, Hosobata K, Sugahara T. Realization by Biped Leg2wheeled Robot of Biped Walking and Wheel2driving Locomotion[C]PPProceeding of the 2005 IEEE International Conference on Robotics and Automation. Barcelona, Spain, 2005: 2970- 2975.

[6] Guccione S, Muscato G. The Wheeleg Robot[C]PRobotics & Automation Magazine, IEEE, Italy: Dipt. Elettrico Elettronico e Sistemistico, Universita Degli Studi di Catania, 2003: 33- 43.

[7] Eiji N, Sei N. Leg2wheel Robot: A Futuristic Mobile Platform for Forestry Industry[C]PPProceedings of the 1993 IEEEPTsukuba International Workshop on Advanced Robotics2can Robots Contribute to Preventing Environmental Deterioration, Sendai, Graduate Sch. of Inf. Sci., Tohoku Univ, 1993: 109- 112.

[8] 潘存云, 温熙森. 球齿轮行星传动结构形式与驱动机构分析[J]. 国防科技大学学报, 2004, 26(3): 93- 98.

[9] 潘存云, 温熙森. 基于渐开线球齿轮的机器人柔性手腕结构与运动分析[J]. 机械工程学报, 2005, 41(7): 141- 14.

(上接第 63 页)

参 考 文 献:

[1] 孙圣和, 陆哲明, 牛夏牧, 等. 数字水印技术及应用[M]. 北京: 科学出版社, 2004.

[2] Tirkel A Z, Rankin G A, Schyndel R. Electronic Watermark[C]PPDigital Image Computing, Technology and Applications2DICTA 93, Macquarie University, 1993: 666- 673.

[3] Van Schyndel R G, Tirkel A Z, Mee N, et al. A Digital Watermark[C]PPProceedings of IEEE International Conference on Image Processing, Austin, November 1994, 2: 86- 90.

[4] Garimella A, Satyanarayana M V V, Kumar R S, et al. VLSI Implementation of Online Digital Watermarking Technique with Difference Encoding for 8- bit Gray Scale Image[C]PP16th Internatinal Conference on VLSI Design, Jan. 4~ 8, 2003: 283- 288.

[5] Wu Q Z, Cheng H Y, Lin Y W, et al. Trust2worthy Video Enforcement for Electronic Toll Collection[C]PPDigest of technical Papers. International Conference on Consumer Electronics (ICCE. 2000), June 13~ 15, 2000: 112- 113.

[6] Wong P W. A Public Key Watermark for Image Verification and Authentication[C]PPInternational Conference on Image Processing(ICIP. 98), Oct. 4~ 7, 1998, 1: 455- 459.

[7] Byun S C, Lee I L, Shin T H, et al. A Public2key Based Watermarking for Color Image Aythentication[C]PPIEEE International Conference on Multimedia and Expo(ICME. 02), Aug. 26~ 29, 2002, 1: 593- 596.

[8] Lu Z M, Ge Q M, Niu X M. Robust Adaptive Video Watermarking in the Spatial Domain[C]PPThe 5th International Symposium on Test and Measurement(ISTM. 2003), Shenzhen, China, June 1~ 5, 2003: 1875- 1880.

[9] Kutter M, Jordan F, Bossen F. Digital Signature of Color Images Using Amplitude Modulation[C]PPI. K. Sethi, R. Jain(Eds.), Storage and Retrieval for Image and Video Databases V, SPIE, San Jose, CA, February 1997, 3022: 518- 526.

[10] Piva A, Bartonlini F, Cappellini V, et al. Exploiting the Cross2correlation of RGB2channels for Robust Watermarking of Color Image[C]PP Proceedings of the IEEE International Conference on Image Proceeding, Kobe, Japan, October, 1999, 1: 306- 310.

[11] Tsai P Y, Hu Y C, Chang C C. A Color Image Watermarking Scheme Based on Color Quantization[J]. Signal Processing, 2004, 84(1): 95- 106.