

双重保护的半盲彩色数字水印算法

范馨月, 贺志恒, 周 非

(重庆邮电大学 通信与信息工程学院, 重庆 400065)

摘 要: 研究了一种基于 DWT 与 SVD 相结合的半盲彩色数字水印算法, 鉴于嵌入水印的实用性, 原始图像与水印图像采用的都是彩色图像。在置乱变换系数和半盲水印的双重保护下, 提高了水印的安全性, 奇异值分解对常见的几何失真稳健, 而小波分解可以把图像的主要能量集中到低频域中, 结合它们的优点可以更好地提高水印的抗攻击性。实验结果表明, 嵌入水印后的图像在加噪、滤波(如模糊、锐化)、缩放、旋转、剪切和有损压缩等攻击后, 其提取水印与原始水印仍有较高的相似度与峰值信噪比, 该算法具有较好的鲁棒性。

关键词: 离散小波变换; 奇异值分解; 半盲水印; 置乱变换; 鲁棒性

中图分类号: TP391; TP301.6 **文献标志码:** A **文章编号:** 1001-3695(2013)03-0917-04

doi:10.3969/j.issn.1001-3695.2013.03.071

Research on double protection of semi-blind color digital watermarking algorithm

FAN Xin-yue, HE Zhi-heng, ZHOU Fei

(College of Communication & Information Engineering, Chongqing University of Posts & Telecommunications, Chongqing 400065, China)

Abstract: This paper focused on the study of semi-blind color watermarking algorithm based on the combination DWT with SVD. In consideration of the practicality of embedding watermark, the original image and watermark image all used color pictures. In scrambling transformation and semi-blind watermarking double protection, enhanced the security of watermark. Because SVD was steady towards the common geometric distortion, and with using DWT, the main energy of image occupied the low frequency domain. It was better to improve the resistance to attack of watermark by combining with the advantages of DWT and SVD. The result demonstrates that after the watermark image subjected to the attacks of adding noise, filtering (such as obscuring and sharpening), scaling, rotating, cutting and loss compression, the extracted watermark also has high similarity and peak signal to noise ratio with the original watermark. The algorithm is robust.

Key words: discrete wavelet transform (DWT); singular value decomposition (SVD); semi-blind watermarking; scrambling transformation; robustness

近年来,随着计算机网络通信技术的蓬勃发展,数字产品在网络上的快速传播,数字产品的版权问题越来越受到重视,而数字水印技术是近几年版权保护问题中的重点研究对象。现有的数字水印技术选取的水印大多是黑白图像或者是一个随机序列,考虑到水印的实用性,水印的应用是要面向大众的、由客户提供的,水印可以是照片、身份证或是一些有意义的图像等。因此,本文选取的原始图像和水印图像都是彩色图像。

小波变换^[1]和奇异值分解^[2]是近几年水印技术中研究较多的领域。小波变换使得信号分析不仅仅只是在时域或频域单一的分析域上进行,而是在时频域的联合域上对信号进行分析,时频域局域化使小波变换在信号分析中有很大的优势,且具有易于兼容 JPEG 2000 和 MPEG-4 压缩标准等特点,已得到了普遍关注。奇异值分解具有良好的抗几何失真不变性,在经过转置、镜像、旋转、放大、平移等几何失真后,抽象化的矩阵与图像的分辨率无关。两者结合后的水印算法具有较好的稳健性。周波等人^[3]从理论上证明,图形矩阵的奇异值对结合失真具有不变性,可以用来嵌入水印,但其选用的嵌入水印是 0~1 的标准正态分布的数值,抗攻击性较差。Ganic 等人^[4]将 DWT 与 SVD 相结合,对一级小波变换后产生的四个子带分别

进行奇异值分解,并在奇异值中嵌入水印,取得了一定的效果。相对于彩色图像来说,无论是原始图像或水印图像,一级小波分解并不能使彩色图像的能量更好地集中,需要进行多级小波分解,且嵌入的水印并不是图像,而是水印的奇异值分解后的相关系数,因此在水印的提取时需要更多的数据去还原原始水印图像,加大了运算量。Sverdlov 等人^[5]对图像进行离散余弦变换后,平均分成四块进行奇异值分解,再嵌入水印,但由于 IDCT 带来的边缘丢失,且不是盲水印,应用受到限制。Bergman 等人^[6]提出了一种改变 U 矩阵中某些系数的符号位,然后重新计算,生成正交矩阵,为水印技术开辟了新的思路,但实验发现,该方法计算复杂,而且抗攻击性能并不理想。

1 算法原理

本文采用了图像置乱变换、原始图像的二级小波变换和水印图像的一级小波变换,对二级小波变换后的原始图像的低频区域进行 SVD,把小波变换后的水印图像一一对应地嵌入其中;在水印提取时,不需要原始水印图像,只需要知道嵌入水印后图像经过 SVD 后的两个正交矩阵和原始水印的奇异值,因此属于半盲水印的提取。在置乱变换系数 key 和半盲水印的

收稿日期: 2012-07-09; 修回日期: 2012-08-27

作者简介: 范馨月(1979-),女,四川犍为人,讲师,硕士,主要研究方向为图像处理、通信信号处理、雷达信号处理等(fanxy@cqupt.edu.cn); 贺志恒(1987-),男,湖南衡阳人,硕士研究生,主要研究方向为数字图像处理;周非(1977-),男,湖北浠水人,副教授,博士,主要研究方向为无线定位系统、信号检测与估计、图像处理。

双重保护下,提高了水印的安全性,基于 DWT-SVD 的水印算法,使水印具有更好的抗攻击性能。实验证明,嵌入水印的图像在加噪、滤波(如模糊、锐化)、缩放、旋转、剪切和有损压缩等攻击后,其提取水印与原始水印有较高的相似度,验证了本算法具有较好的稳健性和安全性。

1.1 SVD 几何失真不变性

从线性代数的角度看,一幅数字图像可以看成是由许多非负量组成的一个矩阵。用 $A \in \mathbb{R}^{M \times N}$ 来表示一个图像矩阵,其中 $\mathbb{R}$ 表示实数域。不失一般性, A 可以表示成

$$A = U \Sigma V^T \quad (1)$$

其中, $U \in \mathbb{R}^{M \times N}$ 和 $V \in \mathbb{R}^{M \times N}$ 都是正交阵; $\Sigma \in \mathbb{R}^{M \times N}$ 是一个非对角线上的项都是 0 的矩阵,其对角线上的元素满足

$$\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > \sigma_{r+1} = \dots = \sigma_M = 0 \quad (2)$$

其中, r 是 A 的秩,它等于非零奇异值的个数,于是有

$$\Sigma = \begin{bmatrix} \sigma_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sigma_M \end{bmatrix} \quad (3)$$

σ_i 是由该分解所唯一确定的,叫做 A 的奇异值。

矩阵奇异值具有很好的稳健性^[7,8],当矩阵 A 有微小振动时,其奇异值的改变不大,具有良好的抗几何失真不变性。几何失真包括转置、镜像、旋转、放大、平移等。

a) 转置。如果 A^T 是 A 的转置,那么

$$(A^T)(A^T)^T = A^T A \quad (4)$$

A^T 和 A 具有相同的非零奇异值,即本水印对转置失真真是稳健的。

b) 镜像。令 $P_M = \begin{bmatrix} 0 & 1 \\ \ddots & \\ 1 & 0 \end{bmatrix}_{M \times M}$, 显然它是正交对称的,故有

$P_M^{-1} = P_M^T = P_M$ 。那么 A 行镜像 A_{rm} 和列镜像 A_{cm} 可以表示为

$$A_{rm} = P_M A, A_{cm} = A P_N \quad (5)$$

所以有

$$A_{rm}^T + A_{rm} = A^T P_M^T P_M A = A^T A \quad (6)$$

$$A_{cm} + A_{cm}^T = A P_N P_N^T A^T = A A^T \quad (7)$$

因此, A_{rm} 、 A_{cm} 和 A 具有相同的非零奇异值,表明本水印对镜像失真是稳健的。

c) 旋转。假设 $A_r \in \mathbb{R}^{M \times N}$ 是图像 $A \in \mathbb{R}^{M \times N}$ 旋转任意角度后的图像,那么总是存在一个正交阵 $Q \in \mathbb{R}^{M \times N}$,使得 $A_r = QA$,因此有

$$A_r^T A_r = A^T Q^T Q A = A^T A \quad (8)$$

故 A_r 与 A 有相同的非零奇异值。综上所述,本水印具有旋转不变性。

d) 放大。设 $C \in \mathbb{R}^{M \times LN}$ 是图像 $A \in \mathbb{R}^{M \times N}$ 横向放大后的图像,它是将 A 的每一列重复 L 次得到的,即

$$C = A S_C \quad (9)$$

其中:

$$S_C = \begin{bmatrix} 1 & \dots & 1 & \dots & \dots & 0 & \dots & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & \dots & 1 & \dots & \vdots & & \vdots \\ \vdots & & \vdots & 0 & \dots & 0 & \dots & \vdots & & \vdots \\ & \dots & \dots & & \dots & & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 & \dots & 1 & \dots & 1 \end{bmatrix} \in \mathbb{R}^{N \times LN} \quad (10)$$

令

$$A^T A = \begin{bmatrix} a_{11} & \dots & a_{1N} \\ \vdots & & \vdots \\ a_{N1} & \dots & a_{NN} \end{bmatrix} \in \mathbb{R}^{N \times N} \quad (11)$$

因此

$$C^T C = S_C^T A^T A S_C = \begin{bmatrix} [a_{11}]_{L \times L} & \dots & [a_{1N}]_{L \times L} \\ \vdots & & \vdots \\ [a_{N1}]_{L \times L} & \dots & [a_{NN}]_{L \times L} \end{bmatrix} \in \mathbb{R}^{LN \times LN} \quad (12)$$

可得 C 和 A 的非零奇异值的数量相等,并且对应于 A 的每一个非零奇异值 σ ,都有 $\sigma = \sqrt{\lambda}$,且 $\sqrt{L}\sigma = \sqrt{L\lambda}$ 是 C 的一个非零奇异值。同理可得,纵向放大后的奇异值数量也相等。

综合起来,若将 A 同时纵向和横向分别放大 L_1 倍和 L_2 倍,那么对于 A 的每一个非零奇异值 σ , $\sqrt{L_1 L_2} \sigma$ 是放大后图像的一个非零奇异值,且放大前后非零奇异值的数量相同。

e) 平移。平移通常发生在四周填充了黑色像素(亮度值为 0)的延伸图像中,并且在延伸图像中进行平移等同于在延伸图像的一边填充黑色像素,同时在另一边裁剪黑色像素,因此只需研究填充(裁剪)对于奇异值的影响。

不失一般性,设 $A_e = [A \ 0]^{M \times N'} \in \mathbb{R}^{M \times (N+N')}$ 是图像 $A \in \mathbb{R}^{M \times N}$ 填充的延伸图像,于是

$$A_e A_e^T = [A \ 0]^{M \times N'} \begin{bmatrix} A^T \\ [0]^{N' \times M} \end{bmatrix} = A A^T \quad (13)$$

故 A_e 和 A 具有相同的非零奇异值。根据旋转不变性,在任意一边填充或裁剪黑色像素不会改变非零奇异值。因此,本水印具有平移不变性。

1.2 DWT 算法的研究

假设 H_2 为高通滤波器, H_1 为低通滤波器,原始信号占据的总频率带为 $(0, \pi)$,则经过一级分解后,原始频率带被分为低频率带 $(0, \pi/2)$ 和高频率带 $(\pi/2, \pi)$ 。然后对低频率带又作同样的第二级分解,如此反复下去,如图 1 所示。

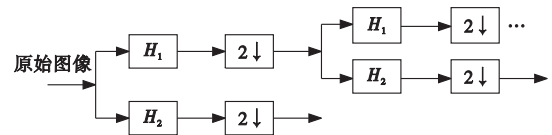


图1 频率空间分解图

基于小波分解的多分辨率分析对图像可以进行有效的时频分解,图像经过小波分解后,一级分解可以分成四个频率带,即低频、水平、垂直及对角线。第二级分解对低频率带进一步分解成以上四个频率带,如此反复。小波变换的好处是把图像的能量集中化,每一个方块都可以表示图像的基本属性,而在低频区域中,能量更为集中,能表示更多的图像信息,把水印嵌入其中,可以保证水印的稳健性,在小波重构后,水印图像被分布到图像的各个模块,有较好的不可见性。

2 算法实现

将水印嵌入到数字图像之前,一般情况下会对水印进行预处理,从而提高其安全性和隐密性,Arnold 图像置乱^[9]是当前主要的水印预处理方法。水印图像置乱通过一定置乱算法将水印图像元素原有的顺序打乱,从而实现对图像加密,目的是消除水印像素的空间相关性,提高抗剪切操作的鲁棒性。

考虑到数字图像的需要,基于位置的 Arnold 图像置乱变换可写成

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N} \quad (14)$$

其中: $x, y \in \{0, 1, 2, \dots, N-1\}$ 表示某一像素点的坐标,而 N 是

图像矩阵的阶数。由此做迭代程序,记变换中的矩阵为 A ,右端 (x, y) 为输入,左端 (x', y') 为输出。

当遭受到破坏的水印提取出来后,利用 Arnold 变换可以恢复数字水印图像,因为 Arnold 变换将会把遭到破坏的比特分散开来,减少了对人眼视觉的影响,提高了数字水印的鲁棒性。

水印的嵌入过程如下:

a) 原始图像与水印图像都是彩色图像,都要进行三色分离,分离出 R, G, B 三个分量。

b) 对水印图像 R, G, B 三个分量都要进行 Arnold 置乱,设置置乱次数 key 作为密钥。

c) 设置水印的嵌入强度 r , 三个分量的嵌入强度是不同的。基于人类视觉系统 (human visual system, HVS), 当三个嵌入强度的加权比例 $R:G:B=2:1:4$ 时^[10], 对于保证图像质量最为有利。

d) 对原始图像的 R, G, B 分量进行两级 DWT 分解, 每个分量能得到七个矩阵, 分别为 $LL_2, LH_2, HL_2, HH_2, LH_1, HL_1, HH_1$ 。对水印图像的 R, G, B 分量进行一级 DWT 分解, 每个分量能得到四个矩阵, 分别为 LL_w, LH_w, HL_w, HH_w 。

e) 然后进行一次 SVD:

$$A^k = U_A^k \Sigma_A^k V_A^{kT} \quad (15)$$

其中: $k=1, 2, 3, 4$ 分别表示 LL_2, LH_2, HL_2, HH_2 四个矩阵。按设定好的嵌入强度把水印嵌入其中, 其嵌入方式为

$$A^{*k} = \Sigma_A^k + r \times W_k \quad (16)$$

其中: W_k 分别表示 LL_w, LH_w, HL_w, HH_w 四个矩阵, 之后对 A^{*k} 再进行一次 SVD, 公式为

$$A^{*k} = U_A^{*k} \Sigma_A^{*k} V_A^{*kT} \quad (17)$$

按照第一次的 SVD 得到的相关系数重组数据为

$$A_w^k = U_A^k \Sigma_A^k V_A^{*kT} \quad (18)$$

f) 对图像的 R, G, B 三个分量分别进行小波重构, 对新得到的三个 R, G, B 分量再进行三色叠加, 得到嵌入水印后图像。

水印的提取过程如下:

a) 对嵌入水印后的图像进行三色分离。

b) 对嵌入水印后图像的 R, G, B 分量进行两级 DWT 分解, 对低频段的四个分量再进行 SVD。本文研究的是半盲提取, 因此, 对嵌入水印后图像的 DWT 分解系数进行 SVD 重构:

$$A^{*k} = U_A^{*k} \Sigma_A^{*k} V_A^{*kT} \quad (19)$$

c) 提取水印的小波系数:

$$W_k = (A^{*k} - \Sigma_A^{*k}) / r \quad (20)$$

d) 对提取的小波系数进行小波重构, 由设定好的置乱系数 key 恢复水印图像。

e) 三色叠加, 提取水印图像。

3 算法仿真数据的比较与分析

为了证明本算法与其他算法的区别, 将 DWT-SVD 算法与 DWT、SVD、SVD-DWT 算法进行对比分析, 选取的图像都是 512×512 的彩色 Lena 原始图像和 256×256 的彩色水印图像。

DWT-SVD 算法的嵌入水印与提取水印算法仿真图如图 2~5 所示。



图2 原始图像



图3 水印



图4 嵌入水印后图像



图5 提取水印

由图 2~5 可知, DWT-SVD 算法有较好的隐蔽性, 且提取水印与原始水印有较高的相似度, 且嵌入水印有很好的不可见性。分别用上述四种算法进行水印的嵌入与提取。提取水印图像的相似度 NC (normalized correlation coefficient) 和嵌入水印后图像的峰值信噪比 (peak signal to noise ratio, PSNR) 的数值如表 1 所示。

表1 四种算法的比较

比较项	DWT	SVD	SVD-DWT	DWT-SVD
嵌入时间	4.2500	58.4375	50.3438	6.1250
提取时间	9.9375	86.8594	80.3750	11.2969
PSNR	29.8318	56.7123	61.3669	51.7813
NC	0.9995	0.9999	0.9982	0.9997

从表 1 可知, DWT 算法的嵌入、提取运算速度都较快, 但是 PSNR 数值并不是很高, 一般认为 PSNR 数值在 30 以上才算得上是有好的性能, 而 NC 越接近 1 越好。SVD 算法的 PSNR 与 NC 数值都比较高, 但是运算的时间太长, 不利于实时性数字水印的实现。SVD-DWT 算法虽然在一定程度上减少了运算时间, 但是效果并不是很明显, 且对水印嵌入位置要求严格。采用本文的 DWT-SVD 算法不仅节省了运算时间, 所得到的 PSNR 和 NC 数值都比较高, 保留了原始图像的信息, 提取水印的相似度也比较高, 充分利用了 DWT 与 SVD 算法各自的优点。

为了更好地对比四种算法的优缺点, 采用以下 12 种攻击方式检查水印的抗攻击性, 并计算了 PSNR 与 NC。每一种攻击方式都采用了较大的数值, 这样能更好地区分各种算法之间的抗攻击性能差异。对水印进行各种攻击后, 提取水印图像对应的 PSNR 与 NC 如表 2 所示。

表2 水印遭受攻击后的 PSNR 与 NC

攻击方式	DWT		SVD		SVD + DWT		DWT + SVD	
	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
(a) JPEG 压缩	14.533 8	0.920 9	26.342 0	0.998 9	19.766 4	0.972 9	17.075 3	0.823 1
(b) 高斯 LPF	12.895 7	0.913 7	22.093 5	0.996 2	13.145 7	0.893 3	24.237 5	0.985 8
(c) 直方图均衡	5.249 8	0.580 3	19.141 5	0.926 1	10.841 6	0.760 7	18.960 0	0.926 4
(d) 图像变暗	1.565 4	0.056 1	17.013 2	0.846 8	2.513 5	0.153 3	16.783 3	0.845 4
(e) 增加对比度	5.653 2	0.736 2	18.609 3	0.925 2	11.532 4	0.961 9	18.039 5	0.927 3
(f) 降低对比度	5.697 7	0.624 7	9.057 0	0.600 6	5.070 5	0.491 7	9.032 1	0.602 4
(g) 加高斯噪声	6.247 6	0.705 0	15.953 7	0.9032 1	8.958 1	0.820 7	18.738 2	0.962 5
(h) 椒盐噪声	11.123 8	0.917 0	13.358 3	0.850 5	7.881 6	0.778 7	16.092 9	0.925 9
(i) 加乘性噪声	5.240 8	0.633 8	13.708 4	0.861 1	7.131 8	0.737 7	16.296 3	0.932 2
(j) 中值滤波	13.789 6	0.922 9	23.774 2	0.999 6	16.513 0	0.949 2	26.278 1	0.995 3
(k) 剪切	7.084 0	0.745 7	16.626 4	0.890 2	6.294 4	0.557 3	15.905 5	0.889 3
(l) 旋转	4.290 0	0.577 5	20.150 2	0.949 7	7.387 6	0.666 2	20.254 3	0.956 1

由表 2 可知, SVD-DWT 水印算法在没有受到攻击时, 它的 PSNR 与 NC 都比较高, 但受到攻击后, 数值变化很大, 抗攻击性很弱。SVD 与 DWT-SVD 算法的抗攻击性能比另外两种算法都要高, 但 DWT-SVD 算法运算的时间更短。

DWT-SVD 算法被攻击后的提取水印图像如图 6 所示。

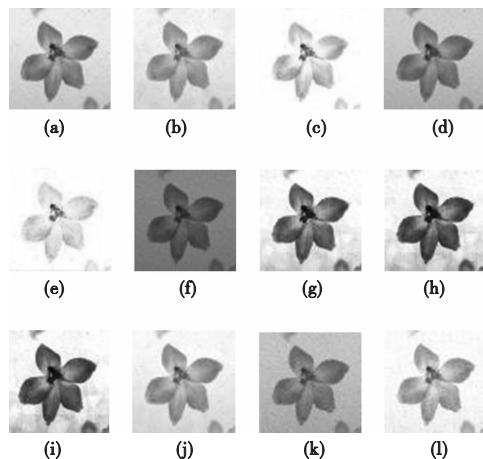


图6 攻击后的提取水印

由图 6 可知, DWT-SVD 算法在受到图 6(a) ~ (l) 这 12 种攻击之后, 其提取水印与原始水印仍有较高的峰值性噪比和相似度, 验证了本算法的优点。

4 结束语

基于 DWT-SVD 的半盲彩色图像水印算法, 对水印进行了双重保护: a) Arnold 图像置乱的系数 key; b) SVD 后的两个正交矩阵和原始水印的奇异值, 使得水印的安全级别更高, 很难被其他用户提取水印和更改水印, 因此具有很高的实用价值。

(上接第 916 页)

表 1 本文方案与其他方案的性能比较

方案	签名阶段			解密密阶段			密文长度
	P	M	E	P	M	E	
文献[4]	0(+1)	3	0	3(+1)	0	1	$2 G_1 + 2 m $
文献[5]	0(+2)	2	2	2(+2)	0	2	$ G_1 + m + q $
文献[6]	0(+1)	3	1	2(+2)	0	2	$2 G_1 + m $
文献[7]	0(+1)	3	1	3(+1)	0	1	$2 G_1 + m $
文献[8]	0(+1)	2	1	3(+1)	0	0	$2 G_1 + 2 m $
文献[9]	0(+1)	1	0	0(+1)	2	0	$ m + 2 q $
文献[10]	0(+1)	1	1	1(+0)	1	0	$ G_1 + m + q $
本文方案	0(+2)	3	2	2(+1)	0	1	$2 G_1 + m + q $

7 结束语

本文对文献[10]提出的基于身份的改进高效签密方案进行了安全性分析, 指出方案不能抵抗不可区分性选择明文攻击和不诚实接收者的一般性伪造攻击, 并提出了一种改进方案。在随机预言模型下, 证明了新方案在适应性选择密文攻击下具有不可区分性; 在适应性选择消息和身份攻击下是存在性不可伪造的。

参考文献:

- [1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Advances in Cryptology-CRYPTO'84. Berlin: Springer-Verlag,

实验证明, 本文算法对常见的攻击手段如压缩、剪切、常见的噪声干扰、几何变化等都具有良好的鲁棒性, 抗攻击性能优越。

参考文献:

- [1] 孙光民, 于瑶, 刘伟平, 等. 基于小波变换的彩色图像多分量水印嵌入算法[J]. 北京工业大学学报, 2008, 34(5): 471-475.
- [2] LIU Rui-zhen, TAN Tie-niu. An SVD-based watermarking scheme for protecting rightful ownership [J]. IEEE Trans on Multimedia, 2002, 4(1): 121-128.
- [3] 周波, 陈健. 基于奇异值分解的、抗几何失真的数字水印算法[J]. 中国图象图形学报, 2004, 9(4): 506-512.
- [4] GANIC E, ESKICIOGLU A M. Robust embedding of visual watermarks using DWT-SVD[J]. IEEE Trans on Image Processing, 2004, 4(8): 1141-1146.
- [5] SVERDLOV A, DEXTER S, ESKICIOGLU A M. Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies [C]//Proc of the 13th European Signal Processing Conference. 2005: 4-8.
- [6] BERGMAN C, DAVIDSON J. Unitary embedding for data hiding with the SVD [C]//Proc of IEEE Security, Steganography and Watermarking of Multimedia Contents V II, SPIE 5681. 2005: 619-630.
- [7] 许文丽, 李磊, 王育民. 抗噪声、几何失真和 JPEG 压缩攻击的鲁棒数字水印方案[J]. 电子与信息学报, 2008, 30(4): 933-936.
- [8] 袁大洋, 肖俊, 王颖. 数字图像水印算法抗几何攻击鲁棒性研究[J]. 电子与信息学报, 2008, 30(5): 1251-1256.
- [9] 王慧琴, 崔福明, 杜高峰. 利用 Arnold 变换和纠错编码实现盲数字水印[J]. 北京邮电大学学报, 2008, 31(1): 97-101.
- [10] 刘挺, 尤韦彦. 一种基于离散小波变换和 HVS 的彩色图像数字水印技术[J]. 计算机工程, 2003, 29(4): 115-117.

1984: 47-53.

- [2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [C]//Advances in Cryptology- CRYPTO '01, LNCS, vol 2139. Berlin: Springer-Verlag, 2001: 213-229.
- [3] ZHENG Yu-liang. Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost(encryption) [C]//Advances in Cryptology-CRYPTO'97, LNCS, vol 1294. Berlin: Springer-Verlag, 1997: 165-179.
- [4] MALONE-LEE J. Identity-based signcryption [EB/OL]. (2002-07-09). <http://eprint.iacr.org/2002/098>.
- [5] LIBERT B, QUISQUATER J. A new identity based signcryption schemes from pairings [C]//Proc of IEEE Information Theory Workshop. 2003: 155-158.
- [6] 李发根, 胡子濮, 李刚. 一个高效的基于身份的签密方案[J]. 计算机学报, 2006, 29(9): 1641-1647.
- [7] 张明武, 杨波, 周敏, 等. 两种签密方案的安全性分析及改进[J]. 电子与信息学报, 2010, 32(7): 1731-1736.
- [8] 李志敏, 徐黎, 李存华. 基于身份的公开验证签密方案[J]. 计算机应用, 2012, 32(1): 99-103.
- [9] 张串绒, 张玉清, 李发根. 适于 Ad hoc 网络安全通信的新签密算法[J]. 通信学报, 2010, 31(3): 19-24.
- [10] 肖鸿飞, 刘长江. 一种基于身份的改进高效签密方案[J]. 计算机工程, 2011, 37(24): 126-128.
- [11] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.