

基于 SVD 分解和 Hadamard 变换的图像半脆弱水印技术

王志红, 黄惠芬, 常玉红

(山东英才学院信息工程学院, 山东 济南 250014)

摘要: 针对半脆弱水印能区别正常的图像处理操作和恶意篡改的特点, 提出一种基于 Hadamard 变换和 SVD 分解相结合的半脆弱水印算法。该算法首先对载体图像进行 SVD 分解, 对所有的图像子块进行 Hadamard 变换, 利用量化的方法将水印嵌入。算法针对恶意篡改操作时反应敏感且识别篡改位置能力好, 同时对 JPEG 压缩具有较强的抵抗能力。

关键词: 半脆弱水印; 篡改; SVD 分解; Hadamard 变换

中图分类号: TP391

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00153

Semi-fragile watermarking technology based on SVD decomposition and Hadamard transform

WANG Zhi-hong, HUANG Hui-fen, CHANG Yu-hong

(School of Information Engineering, Shandong Yingcai University, Jinan 250014, China)

Abstract: The semi-fragile watermarking algorithm based on Hadamard transform and SVD decomposition was proposed to distinguish normal image processing operations from malicious tampering. Firstly, the carrier image was SVD decomposed, and Hadamard transform was performed on all image subblocks. The watermark was embedded by quantization method. The algorithm was sensitive to tampering and had good ability to recognize tampering position, and had strong resistance to JPEG compression.

Key words: semi-fragile watermarking, tamper, SVD decomposition, Hadamard transform

1 引言

数字水印技术 (digital watermarking) 作为信息隐藏学的重要分支, 得到广泛的研究和发展^[1,2], 该技术在版权保护、盗版跟踪、图像认证、票据防伪、隐蔽标识等领域得到广泛运用^[3]。

数字水印技术通过将数字、序列号、文字等信息嵌入到媒体中, 在嵌入的过程中对载体进行尽量小的修改, 以达到最强的顽健性, 当嵌入水印后的媒体受到攻击后仍然可以恢复水印或检测出水印的存在, 从而实现多媒体作品的版权保护和内容的真实性、完整性认证^[4,5]。从不同的角度

收稿日期: 2016-12-14; 修回日期: 2017-01-18。通信作者: 王志红, 4249854@qq.com

基金项目: 国家自然科学基金资助项目 (No.61402271); 山东省重点研发计划资助项目 (No.2015GGX101012, No.2016GGX101037); 山东省自然科学基金资助项目 (No.ZR2015JL023, No.ZR2015FL025, No.ZR2016FM34, No.ZR2016FQ23); 山东省社科规划基金资助项目 (No.15CXWJ08); 山东省高等学校科研计划基金资助项目 (No.J15LN54, No.J16LN55)

Foundation Items: The National Natural Science Foundation of China (No.61402271), The Key R & D Technology Development Foundation of Shandong Province (No.2015GGX101012, No.2016GGX101037), The Natural Science Foundation of Shandong Province (No.ZR2015JL023, No.ZR2015JL025, No.ZR2016FM34, No.ZR2016FQ23), The Sacral Science Planning Project of Shandong Province (No.15CXWJ08), Higher Education Research Project of Shandong Province (No.J15LN54, No.J16LN55)

可以将数字水印技术分为不同的类别，分类繁多。根据载体分类，可分为图像水印、视频水印、文档水印和音频水印；根据水印稳健性，可分为顽健性水印、半脆弱性水印和脆弱性水印^[6,7]；根据嵌入域不同可以分为空域水印技术和变换域水印技术。

随着图像编辑和处理工具的迅速发展和数字图像在生活和工作中的大量应用，修改图像内容也变得相对容易，数字图像正面临着被随意篡改和伪造的威胁，负面影响不断增多。不真实数字图像的不断出现，最终会让人失去对照片的信任。在不影响数字图像感官质量的前提下，将与图像内容提要相关或不相关的标志信息作为水印直接参与嵌入到图像内容中^[8]，当需要对图像内容进行真实和完整性认证时，可根据提取的水印信息是否被改变来判断。

在近几年的研究中，在图像中嵌入水印而形成的图像水印技术取得较大进展。文献[9]中的最低有效位 (LSB, least significant bit) 算法、文献[10]中的基于人类视觉系统的 (HVS, human visual system) 算法、文献[11]中的零水印算法等都是用来保护图像版权信息的水印算法。另外，文献[12]中的分块级水印算法、文献[13]中的像素级水印算法、文献[14]中的可恢复水印算法等可用来检测图像内容是否被篡改并找出篡改的位置继而保护图像内容。文献[15]结合小波变换和 SVD 提出一种多水印算法，在图像低频和中频区域分别嵌入水印。文献[16]对载体图像进行离散小波变换并进行 SVD 分解，将置乱处理后的水印嵌入奇异值矩阵中。文献[17]提出一种基于奇异值变换和小波包分解的自适应顽健水印算法。文献[18]提出一种基于 Hadamard 变换和 LU 分解的盲水印嵌入算法，解决了几何失真比较敏感的问题。本文主要针对半脆弱水印能区别正常的 JPEG 压缩操作和恶意篡改的特点，利用 SVD 分解对图像矩阵分块、分解后的子块对外界的操作具有较强的稳定性，同时对分解的子块进行 Hadamard 变换，利用低频系数生成水印嵌入到图像中频系数中，得到含水印图像，使图像对 JPEG 压缩具有较强抵抗能力的同时，保持对恶意篡改操作的高度敏感。

2 相关技术

2.1 图像的 Hadamard 变换

Hadamard 变换本质上是一种特殊排序的沃尔什变换，其变换矩阵也是一个方阵，只包括+1和-1这2种矩阵元素，各行或各列之间彼此是正交的，即任意两行相乘或两列相乘后的各数之和必定为零，Hadamard 变换的最大优点在于其变换矩阵具有简单的递推关系，此特点使 Hadamard 变换更容易被采用^[19]，对图像进行该变换，图像重建时误差较小。

一维的 Hadamard 变换 (HT) 式为

$$H(u) = -\frac{1}{N} \sum_{x=0}^{N-1} f(x) \sum_{i=0}^{N-1} b_i(x) b_i(u) \quad (1)$$

其中， $N = 2^n$ ； $u = 0, 1, 2, \dots, N-1$ ； $x = 0, 1, 2, \dots, N-1$ ； $b_k(z)$ 是 z 的二进制表示的第 k 位值。

最低阶 ($N = 2$) 的 Hadamard 变换为

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (2)$$

$2N$ 阶 Hadamard 矩阵 H_{2N} 与 N 阶 Hadamard 矩阵 H_N 之间的递推关系可表示为

$$H_{2N} = \begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix} \quad (3)$$

Hadamard 变换容易实现且速度快，比 DCT 和 DFT 具有更好的实时性，更能够满足实际应用的需要。

2.2 SVD 分解

数字图像在计算机内是以矩阵形式存储的，矩阵的每个元素表示图像中相应坐标像素的值。SVD 分解变换是一种将矩阵对角化的数值方法^[20]，是一种正交变换。

若一副图像用 A 表示，定义为 $A \in R^{m \times n}$ ，其中 R 表示实数域。任意一个 $m \times n$ 阶矩阵 A 的 SVD 可以表示为

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

$$U = [u_1, u_2, \dots, u_m] \in R^{m \times m} \quad (5)$$

$$V = [v_1, v_2, \dots, v_n] \in R^{n \times n} \quad (6)$$

其中， U 和 V 都是正交的，即 $UU^T = I \in R^{m \times m}$ ， $VV^T = I \in R^{n \times n}$ ，且 $\|U\| = \|V\| = 1$ 。 V^T 表示矩阵 V 的转置矩阵。 $S = \text{diag}(\sigma_1, \sigma_2, \dots, \sigma_n)$ 是 $m \times n$ 的非负

对角阵, 其主对角线元素按从大到小的顺序排列, 称为矩阵 A 的 SVD, 其中 $\sigma_1^2 \geq \sigma_2^2 \geq \dots \geq \sigma_n^2$ 是矩阵 $A^T A$ 的特征值。图像的 SVD 分解具有较强的稳定性, 当图像被施加小的篡改扰动时图像的 SVD 不会有大的改变。

3 水印的嵌入和篡改检测定位

3.1 水印的嵌入算法

假定原始图像为 $M \times N$ 的矩阵, 表示为

$$I = \{f(x, y), 0 \leq x \leq M, 0 \leq y \leq N\} \quad (7)$$

对图像矩阵 I 进行分块 SVD 分解, 图像划分为 $\frac{M}{8} \times \frac{N}{8}$ 个独立的 8×8 子块, 每个图像子块可以分别表示为

$$B(m, n) = \{f(8 \times m + i, 8 \times n + j), 0 \leq i, j \leq 7\} \quad (8)$$

其中, $0 \leq m \leq \frac{M}{8}$, $0 \leq n \leq \frac{N}{8}$, 对每个图像子块嵌入水印, 过程如下。

1) 对所有的子块进行 Hadamard 变换, $P_{ik} = HT(B_i)$, 其中 B_i 表示正进行变换的子块, k 是变换后的系数序号, 取值范围为 $[1, 64]$ 。

2) 对 8×8 的系数矩阵进行 Zig-Zag 排序, 选取中频的 12 个系数用于嵌入水印。

3) 对所有子块的 12 个低频系数进行量化处理操作, 量化后图像会对正常处理操作不敏感。

$$Cn[i] = \left\lfloor q \frac{c[i]}{q} + 0.5 \right\rfloor \quad (9)$$

其中, q 称为恒定量因子, $\lfloor \cdot + 0.5 \rfloor$ 是把 x 向下取整。取 50 幅图像作为测试样本进行实验, 图像样本表示为 $S: \{w_1, w_2, \dots, w_{50}\}$, 每个样本取 q 为 1~256 的量化步长, 利用每个量化步长生成含水图像 $W_{i,k} (i=1, 2, \dots, 50, k=1, 2, \dots, 256)$, 对生成的含水图像进行 JPEG 压缩操作 ($Quality=50$) 和图像内容篡改操作。

4) 生成水印信息: 取子块量化后的低频系数, 采用 MD5 算法生成固定的 128 bit 摘要, 取前 12 bit 生成水印信息。

5) 在密钥的作用下随机选择水印即将嵌入的子块。将 $1 \sim \frac{M}{8} \times \frac{N}{8}$ 的整数序列根据密钥 Key 进行置乱, 得到伪随机序列 P , 设该序列的第 n

个元素是 P_n , 令

$$n = k \left(\frac{M}{8} \right) + 1 \quad (10)$$

$$P_n = i \left(\frac{N}{8} \right) + j \quad (11)$$

将子块 (i, j) 生成的水印嵌入子块 (k, l) 的中频系数中。

6) 在图像子块的 12 个中频系数里嵌入水印信息。

$$P'_{i,k} = P_{i,k} + \partial \text{sign}(W_{i,k} - 0.5) \quad (12)$$

其中, $i=1, 2, \dots, w \times w$; $k=1, 2, \dots, 12$; $P_{i,k}$ 为嵌入水印前的中频系数, $P'_{i,k}$ 为水印嵌入后的中频系数, ∂ 为嵌入强度系数, $W_{i,k}$ 为水印信息位。

7) 对图像进行逆 Hadamard 变换, 重构嵌入水印后的图像, 得到含水图像。

3.2 认证算法

针对被检测的含水图像, 若想判断是否被篡改过, 可通过验证所嵌入的水印是否被改变。对要检测的图像和原含水图像进行水印对比, 若二者水印相似, 说明该图像未被篡改过。提取水印算法是嵌入水印算法的逆过程, 按照 3.1 节相同的方法对待检测图像进行分块 Hadamard 变换, 选取子块低频系数进行量化得到水印 W , 提取中频系数中所嵌入的水印 C 做比较, 计算 W 和 C 之间的相关性以判定该图像是否被篡改。计算公式如式(13)所示。

$$NC = \rho(W_{i,k}, C_{j,k}) = \sum_{k=1}^{12} W_{i,k}^2 \sum_{k=1}^{12} C_{j,k}^2 \quad i, j = 1, 2, \dots, N \quad (13)$$

其中, W 为含水图像低频量化后生成的水印信息, C 为从嵌入水印后的图像中频系数中提取的水印。本文采用如下的判定规则, 根据 NC 的值来判定若相关性, NC 值越大, 可判定低频产生的水印和图像原先嵌入中频中的水印相似度越高, 该图像未被篡改, 可信度越高, 反之, 图像就被篡改过, 可进一步判断篡改的位置实现篡改定位。

3.3 篡改检测和篡改定位

为了定量地分析图像是否被恶意篡改并对篡改进行定位, 用 D 表示原始图像 (嵌入水印) 与提取水印图像的差值图像, 如式(14)所示。

$$D = \{d(m, n) = |W(m, n) - \hat{W}(m, n)|\} \quad (14)$$

其中, $1 \leq m \leq M, 1 \leq n \leq N$ 。当对含水印图像进行正常操作时, D 上错误像素点一般都是孤立稀疏的; 当图像受到恶意攻击或篡改时, D 上的错误像素点通常是非常密集的。通过观察差值图像 D 上的错误像素点是稀疏还是密集, 便可从主观和客观上来评价算法的恶意篡改与定位能力, 还可以进一步确定篡改的区域以及篡改的强度。

D 中的密集差错像素点用 $area_{dense}$ 表示; D 中的稀疏差错像素点表示为 $area_{sparse}$; $area_{total}$: D 中差错像素点的总数, 即有 $area_{total} = area_{dense} + area_{sparse}$; $area$ 表示 D 中的总像素点。

$$\lambda = \frac{area_{total}}{area} \quad (15)$$

$$\eta = \frac{area_{dense}}{area_{total}} \quad (16)$$

定义判定规则如下。

- 1) 若 $\lambda = 0$, 则原图像 (含水印) 未做任何修改。
- 2) 若 $\lambda > 0$ 且 $\eta < \tau$, 则认为原图像 (含水印) 做的是正常处理操作。其中 τ 为预设阈值, 通常选在区间 $[0.5, 1]$ 。
- 3) 若 $\eta \geq \tau$, 则认为图像受到了恶意攻击。

4 仿真实验

4.1 水印对视觉效果的影响

原始图像、利用本文算法嵌入水印后生成的含水印图像分别如图 1 所示。实验在 Matlab 环境下进行, 用本文算法对图像嵌入水印后, 图像从视觉上观察并无差异。

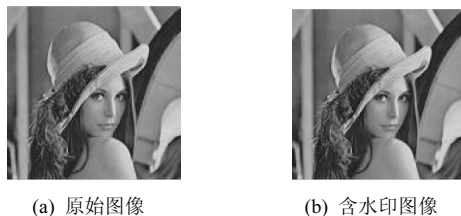


图 1 视觉效果测试比较

4.2 水印算法对常规操作的顽健性

水印对 JPEG2000 压缩操作的顽健性实验结果如表 1 所示。

由表 1 可知, 含水印图像经过 JPEG2000 压缩后, 提取的水印信息没有发生明显的改变。验证了本文算法对 JPEG2000 压缩较强的顽健性。

4.3 算法对恶意篡改的检测

1) 复制粘贴篡改实验

不同图像之间的复制粘贴篡改操作是常见的图像编辑手段, 实验结果如图 2 所示。原始图像 (如图 2(a)所示) 含水印, 经过不同图像之间复制粘贴篡改后生成图像 (如图 2(b)所示), 在未见原图的基础上, 用本文算法能够检测发现篡改并定位篡改所在位置, 如图 2(c)所示。

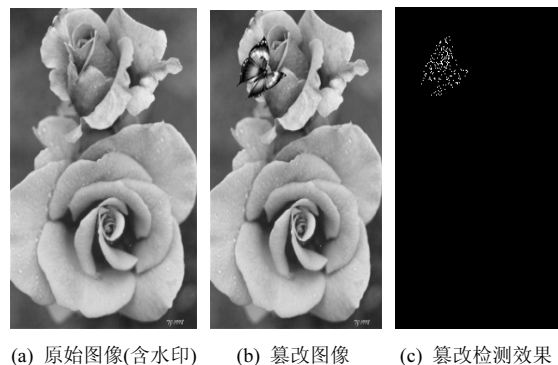


图 2 复制粘贴篡改检测

2) 纹理替换攻击实验

纹理替换可以有效地改变图像所表达的内容。采用标准 lenna 图像 (512×512) 进行实验, 结果如图 3 所示。对 lenna 原始图像 (含水印) 中帽子部分区域进行纹理替换生成图 3(b), 本文检测算法对纹理替换部分进行了很好的定位如图 3(c)所示。对含水印的原始图像图 3(d)裤子区域进行篡改, 将自然的纹理替换成图 3(e), 本文检测算法对替换部分能进行很好的篡改定位如图 3(f)所示。

表 1

水印对 JPEG2000 压缩操作的顽健性实验结果

含水印	提取的水印 (无压缩)	认证结果 (无压缩)	提取的水印 (压缩比 50%)	认证结果 (压缩比 50%)	提取的水印 (压缩比 20%)	认证结果 (压缩比 20%)
lenna						



图3 纹理攻击实验结果

5 结束语

数字水印技术发展迅速, 其应用领域越来越广, 近几年涌现了众多的水印算法并取得了理想成果, 但仍然有很多难题亟待解决, 如水印的抗攻击性和水印加密技术等问题。本文提出的基于SVD分解和Hadamard域变换的数字水印检测算法, 所嵌水印对图像外观视觉没有影响, 在针对恶意篡改操作时反应敏感且识别篡改位置能力强, 同时对JPEG压缩具有较强的抵抗能力, 所提算法可以应用于图像内容真实性认证鉴别, 用于判定图像是否被篡改过。

参考文献:

- [1] 孙圣和, 陆哲明. 数字水印技术及应用[M]. 北京: 科学出版社, 2004.
- [2] SUN S H, LU Z M. Digital watermarking technology and application[M]. Beijing: Science Press, 2004.
- [3] COX I J, MILLER M L, BLOOM J A. Digital watermarking[M]. Beijing: Publishing House of Electronics Industry, 2003.
- [4] 许文丽, 王命宇, 马君. 数字水印技术及应用[M]. 北京: 电子工业出版社, 2013.
- [5] XU W L, WANG M Y, MA J. Digital watermarking technology and application[M]. Beijing: Publishing House of Electronics Industry, 2013.
- [6] INGEMAR J, MATTHEW L, JEFFREY A, et al. Digital watermarking[M]. Beijing: Publishing House of Electronics Industry, 2003.
- [7] INGEMAR J, COX I J, MILLER M L. The first 50 years of electronic watermarking[J]. EURASIP Journal on Advances in Signal Processing, 2002(2):126-132.
- [8] 金正. 基于变换域的彩色图像水印算法研究[D]. 长沙: 中南林

业科技大学, 2009.

JIN Z. Study of digital watermarking algorithm for color image based on transform domain[D]. Changsha: Central South University of Forestry and Technology, 2009.

- [7] 聂雪莲. 面向图像版权和内容保护的数字水印技术研究[D]. 郑州: 解放军信息工程大学, 2012.
- [8] NIE X L. Study of digital watermarking technology oriente to image copyright and content protection[D]. Zhengzhou: The PLA Information Engineering University, 2012.
- [9] 王艳辉, 王相海. 用于图像认证的数字水印技术综述[J]. 计算机工程与应用, 2007, 43(2): 33-38.
- [10] WANG Y H, WANG X H. Digital watermarking technique designed to image authentication[J]. Computer Engineering and Applications, 2007, 43(2): 33-38.
- [11] KUMAR S, SINGH T. Performance improvement of simple LSB watermarking using SVD[C]//IEEE. 2014: 133-137.
- [12] YIN K X, ZHANG L J, WANG Z S, et al. Digital watermarking algorithm based on chaotic encryption and HVS[J]. Multimedia Information Networking and Security, 2009, 12: 134-137.
- [13] WEN Q, SUN T F, WANG S X. Concept and application of zero-watermark[J]. Acta Electronica Sinica, 2003, 31(2): 214-216.
- [14] QI H, ZHENG D, ZHAO J. Human visual system based adaptive digital image watermarking[J]. Signal Processing, 2007: 174-188.
- [15] HSU C T, WU J L. Hidden digital watermarks in images[J]. IEEE Transactions on Image Processing a Publication of the IEEE Signal Processing Society, 1999, 8(1): 58-68.
- [16] ZHANG X, WANG S, QIAN Z, et al. Reference sharing mechanism for watermark self-embedding[J]. IEEE Trans Image Process, 2011, 20(2): 485-495.
- [17] 薛胜男, 陈秀宏. 基于混沌加密和SVD的数字图像水印算法[J]. 计算机工程, 2012, 38(19): 107-110.
- [18] XUE S N, CHEN X H. Digital image watermarking algorithm based on chaos encryption and SVD[J]. Computer Engineering, 2012, 38(19): 107-110.
- [19] 熊祥光, 王力. 一种改进的DWT-SVD域参考水印方案[J]. 计算

机工程与应用, 2014, 50(7):75-79.

XIONG X G, WANG L. A modified DWT-SVD referenced watermark scheme[J]. Computer Engineering and Application, 2014, 50(7): 75-79.

- [17] 朱光, 张军亮. 基于 SVD 和小波包分解的自适应鲁棒水印算法[J]. 计算机应用研究, 2013, 30(4): 1230-1233.

ZHU G, ZHANG J L. Adaptive robust watermarking algorithm based on SVD and wave packet decomposition[J]. Application Research of Computers, 2013, 30(4) : 1230- 1233.

- [18] 吴捷, 马小虎. 基于 Hadamard 变换和 LU 分解的盲水印算法[J]. 计算机技术与发展, 2016, 26(2):82-85.

WU J, MA X H. blind watermarking algorithm based on Hadamard transform and LU decomposition[J]. Computer Technology and Development, 2016, 26(2): 82-85.

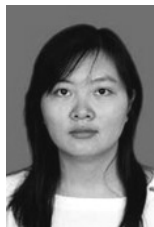
- [19] 张大兴, 李何明, 李海华. 图像 Hadamard 变换域鲁棒水印算法[J]. 计算机与应用, 2010, 46(5):76-79.

ZHANG D X, LI H M, LI H H. Image Hadamard transform robust watermarking algorithm[J]. Application Research of Computers, 2010, 46(5):76-79.

- [20] 史宝明, 李恒杰, 贺元香. 基于微遗传算法与 SVD 的鲁棒性数字水印技术研究[J]. 兰州文理学院学报 (自然科学版), 2014, 28(6): 45-49.

SHI B M, LI H J, HE Y X. Study of Robust digital watermarking technology based on micro genetic algorithm and SVD[J]. Journal of Lanzhou University of Arts and Science: Natural Science Edition, 2014, 28(6):45-49.

作者简介:



王志红 (1978-), 女, 山东泰安人, 硕士, 山东英才学院副教授, 主要研究方向为信息隐藏。



黄惠芬 (1980-), 女, 山东威海人, 博士, 山东英才学院教授, 主要研究方向为信息隐藏。



常玉红 (1977-), 女, 山东聊城人, 硕士, 山东英才学院副教授, 主要研究方向为信息隐藏。