

基于自毁式数字水印的信息隐藏通信技术

王勇¹, 孙刘杰¹, 武凡静², 元朴康¹, 徐逸¹

(1.上海理工大学, 上海 200125; 2.江苏科技大学, 镇江 212003)

摘要: **目的** 为了提高信息隐藏通信技术的安全性, 提出一种自毁式数字水印隐藏通信技术, 即使非法者截获信息的载体也无法获得信息内容。**方法** 将生成的含水印信息的图像分切成图像碎片以此破坏内嵌的水印信息, 使水印信息无法从单个的图像碎片中提取, 必须经过图像碎片拼接算法合成原始含水印图像后才能提取水印信息。**结果** 通过实验仿真分析, 对于大小为 32×32 像素的 8×8 个图像碎片, 复原的含水印图像无任何图像碎片拼接错位, 拼接平均耗时为 1.59 s, 因此能实现实时在线拼接复原并顺利提取出水印信息。**结论** 从信息的嵌入到最后信息的提取都能顺利地隐藏信息的内容和信息的存在, 信息传递过程中信息的安全性能好, 因此, 自毁式数字水印信息隐藏通信技术是一种可行性极高的信息隐藏通信技术。

关键词: 信息隐藏通信; 数字水印; 图像拼接; 离散余弦变换

中图分类号: TP309 **文献标识码:** A **文章编号:** 1001-3563(2017)01-0180-05

Information Hiding Communication Technology Based on Self-destruction Type Digital Watermarking

WANG Yong¹, SUN Liu-jie¹, WU Fan-jing², YUAN Pu-kang¹, XU Yi¹

(1.University of Shanghai for Science and Technology, Shanghai 200125, China;

2.Jiangsu University of Science and Technology, Zhenjiang 212003, China)

ABSTRACT: The work aims to improve the security of information hiding communication technology and propose a self-destruction type digital watermark hiding communication technology. With this technology, even if someone illegally intercepts information carrier, he cannot get the information content. The image that contained watermark information was segmented into fragments to destroy watermark information inside, so that watermark could not be extracted from a single image fragment. To extract the watermark information is required to synthesize the original watermark image through the image fragment splicing algorithm. Through the experimental simulation analysis, for 8×8 image fragments with pixel size of 32×32 , there was no mosaic mismatch of any restored image fragment with watermark image, and the average time of stitching is 1.59 s. Therefore, the algorithm could achieve real-time online mosaic restoration and smooth watermark extraction. The content and existence of information can be hidden successfully from the embedment to the extraction of the watermark through the algorithm. The security of information is higher in the process of the information transmission. Therefore, the information hiding communication technology based on self-destruction type digital watermarking is a technology of high feasibility.

KEY WORDS: information hiding communication; digital watermarking; image mosaic; discrete cosine transform

信息隐藏通信技术是指将信息隐藏在某种载体介质中, 以隐藏信息存在为目的来进行通信的技术, 该技术的应用范围很广, 如: 战争年代, 军事情报的

秘密传输; 职场上, 商业机密的隐藏通信等。信息隐藏通信一般包括信息嵌入载体、信息传输、信息提取等过程。其中信息嵌入载体的过程是信息隐藏通信的

收稿日期: 2016-03-15

作者简介: 王勇 (1991—), 男, 上海理工大学硕士生, 主攻数字图像处理、数字水印、印刷防伪技术。

通讯作者: 孙刘杰 (1965—), 男, 博士, 上海理工大学教授, 主要研究方向为光学信息技术、数字水印技术和印刷防伪技术。

关键环节，嵌入算法的优劣直接决定了信息被非法者截获后能否提取内嵌信息，因此找到一种优良的嵌入算法显得尤为重要。

目前，按照载体介质的不同可以将信息隐藏通信技术分为文本隐藏通信技术^[1-2]、图像隐藏通信技术^[3-6]、音频隐藏通信技术^[7-11]、视频隐藏通信技术^[12]、网络层隐藏通信技术^[13-17]等。文中研究的数字水印隐藏通信技术正是属于图像隐藏通信技术中安全性能较高的一种，该技术通过载体图像内嵌水印信息来进行隐藏通信。在文中，除了利用含水印图像本身的安全性能外，还结合图像碎片拼接技术，将含水印图像分切成碎片，破坏内嵌水印信息，使非法者即使破译水印提取算法也无法从图像碎片中提取水印信息，以此提高信息隐藏通信的安全性能。

1 自毁式数字水印隐藏通信技术

1.1 基于 DCT 变化域的数字水印算法

从信号处理的角度来看，数字水印技术相当于在一个强背景（载体图像）上叠加一个视觉上不敏感的弱信号（水印信息），由于人眼的视觉系统分辨率有限，只要叠加的水印信号不高于视觉对比度阈值，人眼视觉系统就观察不到水印信息存在，因此，可以利用含水印图像中水印信息的不可见性来进行信息隐藏通信。

1.1.1 水印的嵌入

设 X 是像素大小为 $M \times N$ 的载体图像， W 是像素大小为 $P \times Q$ 的水印图像，其中 $M=2K_1P$ ， $N=2K_2Q$ ； K_1, K_2 为正整数。把水印 W 嵌入到载体图像中，算法的步骤如下：

1) 将载体图像 X 分解成大小为 8×8 像素的像素块，得到 $(M/8) \times (N/8)$ 个像素块 $B_X(m, n)$ ，同时，将 W 也分解为 $(M/8) \times (N/8)$ 个像素块 $B_W(m, n)$ ，每个块大小为 $(8 \times P/M) \times (8 \times Q/N)$ 像素。

2) 对所有的 $B_X(m, n)$ 都进行 DCT 变换，得到变换域系数矩阵 $D_{BX}(u, v)$ ，二维离散余弦变换公式见式 (1)。

$$D_{BX}(u, v) = \frac{2}{N} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} B_X(m, n) \cdot \cos \frac{(2x+1)u\pi}{2m} \cos \frac{(2y+1)v\pi}{2n} \quad (1)$$

式中： $x=0, 1, 2, \dots, m-1, y=0, 1, 2, \dots, n-1, m=8 \times P/M, n=8 \times Q/N$ 。

3) 对所有的 $D_{BX}(u, v)$ 和 $B_W(m, n)$ ， S_i 为从 $D_{BX}(u, v)$ 的中频系数中选出的水印嵌入位置坐标， t_i 为水印 $B_W(m, n)$ 的位置坐标。

$$D_{BX}'(u, v)(S_i) = \alpha \times B_W(m, n)(t_i) \quad (2)$$

式中： α 为加权系数，用 $D_{BX}'(u, v)(S_i)$ 来代替 $D_{BX}(u, v)(S_i)$ 得到嵌入水印后的图像。最后对 $D_{BX}'(u, v)(S_i)$ 进行 DCT 反变换后，将整合成含水印图像 X' 。

1.1.2 水印的提取

要将水印信息从水印图像 X' 中提取出来，其过程是水印嵌入过程的逆过程：将 X' 分解为 8×8 的 $(M/8) \times (N/8)$ 个像素块 $B'_X(m, n)$ 。对所有的 $B'_X(m, n)$ 进行二维 DCT 反变换： $B_X(m, n) = \text{IDCT}(B'_X(m, n))$ ，其中 IDCT 为 DCT 的逆变换。对于所有 $B_X(m, n)$ ，按照式 $B_W(m, n)(t_i) = \frac{1}{\alpha} \times B_X(m, n)(S_i)$ 得到 $B_W(m, n)$ 。将所有的 $B_W(m, n)$ 合并成水印信息 W 。

1.2 基于 HSV 颜色空间的彩色图像碎片拼接算法

首先将彩色图像碎片的颜色空间从 RGB 颜色空间转换为 HSV 颜色空间，这样就可以获得彩色图像碎片的 H (色相) 通道图像。然后提取每张碎片 H 通道图像边缘的灰度值构成特征向量，最后运用式 (2) 计算图像碎片之间特征向量的相似程度自动搜索对应的匹配向量。在数理统计中，相关系数的定义式为：

$$R_{XY} = \frac{\sum XY - \frac{\sum X \sum Y}{N}}{\sqrt{(\sum X^2 - \frac{(\sum X)^2}{N})(\sum Y^2 - \frac{(\sum Y)^2}{N})}} \quad (3)$$

式中： R_{XY} 为向量 X 与向量 Y 的相关系数； N 为向量 X 、向量 Y 的维数。

1.2.1 彩色图像复原

若图像碎片的数目为 $K \times K$ ，碎片的像素大小为 $m \times n$ 。人工干预找出原图像左上角的碎片命名为 1，其他碎片从数字 2 开始随机编号，直到将所有碎片编完为止。提取所有图像碎片的单色分量 H (色相)、 S (饱和度)、 V (明度) 按编码顺序依此存储在 3 个细胞组中。

1) 寻找位于原图像最左边的全部图像碎片。将 1 号碎片的最后一行像素 $H_1(m, 1:n)$ 与第 i 号碎片的第 1 行像素 $H_i(m, 1:n)$ 求相关系数 $R(1, i)$ ，其中 $i=2, 3, 4, \dots, K \times K$ 。 $R(1, i^*) = \max(R(1, i))$ ， i^* 为第 i^* 张碎片是第 1 张碎片的纵向方向的匹配碎片。根据第 i^* 张碎片，对其再进行上述操作，就可以得到第 i^* 张碎片纵向方向的匹配碎片 j^* ，以此类推，就可以找到位于原图像最左边的全部图像碎片。

2) 根据最左边的图像碎片拼接好每一行的图像碎片。(以第 k 行为例) 根据步骤一已经得到了第 k 行最左边的碎片，设为 H_k 。将 $H_k(1:m, n)$ 与第 l 号碎片的第一列像素 $H_l(1:m, 1)$ 求相关系数 $R(k, l)$ 。其中

$I=1,2,3,4\dots K \times K$ 。 $R(k,I^*)=\max(R(1,I))$, I^* 为第 I^* 张碎片是第 k 行最左边的碎片的横向方向的匹配碎片。根据第 I^* 张碎片,对其再进行上述操作,就可以得到第 I^* 张碎片横向方向的匹配碎片 J^* ,以此类推,就可以找到位于第 k 行的全部图像碎片, $k=2,3,4\dots K$ 。

3) 合成原图。根据 1) 和 2) 找到的所以碎片在原彩色图像中的位置,将原始 RGB 碎片按照 H (色相) 拼接顺序进行拼接。以上过程是按 H (色相) 的拼接顺序拼接,此外,也可以按 S (饱和度)、 V (明度) 拼接顺序,对原彩色图像进行拼接,其过程同上。拼接步骤见图 1。

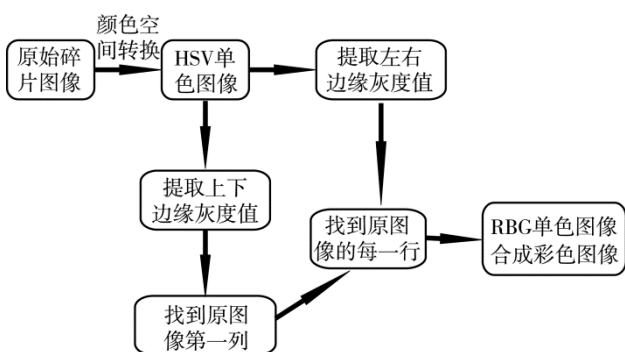


图 1 拼接步骤
Fig.1 Splicing step graph

2 仿真和实验结果分析

2.1 水印的嵌入

载体图像 Lena 的像素大小为 256×256 , 水印图像像素大小为 32×32 , 水印信息嵌入到载体图像的蓝通道中, 给定的水印嵌入强度 $\alpha=0.03$, 其载体图像、水印图像、含水印图像见图 2。

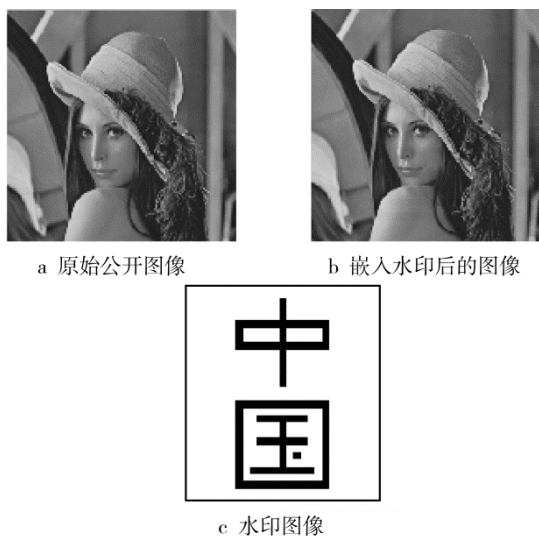


图 2 载体图像、水印图像、含水印图像
Fig.2 Carrier image, watermark image and watermark image

水印信息的嵌入过程见图 2, 此过程代表用户 A

将要发送的信息嵌入到载体图像中, 随后用户 A 将含水印图像分切为图像碎片并随机置乱碎片, 并将置乱后的碎片发送给合法用户 B。

2.2 图像碎片的拼接

通过基于 HSV 颜色空间的彩色图像碎片拼接算法将含水印图像拼接复原, 拼接算法平均耗时 1.59 s, 拼接好的图像无碎片错位。拼接结果见图 3—4。彩色图像拼接过程, 即合法用户 B 将获取的图像碎片拼接成完整的含水印图像, 见图 3—4。

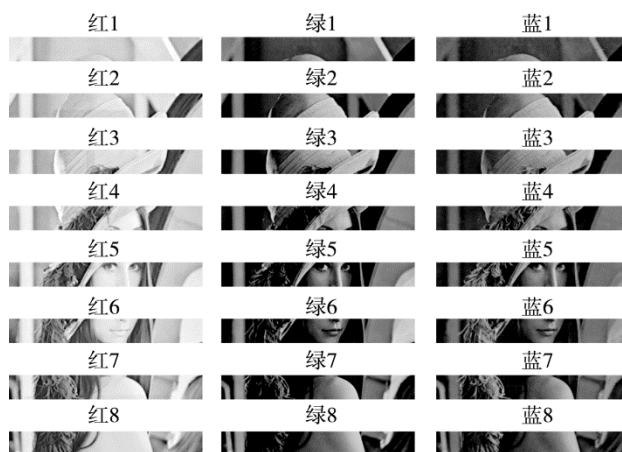


图 3 拼接好的各单色碎片行拼接
Fig.3 Mosaic of a good mosaic of each single piece of mosaic



图 4 拼接好的单色图和彩色复原
Fig.4 Mosaic of a good monochrome and color recovery map

2.3 水印的提取

对于合成的含水印图像, 为检验能否从中顺利地提取出水印信息, 利用水印提取算法进行验证, 结果见图 5。

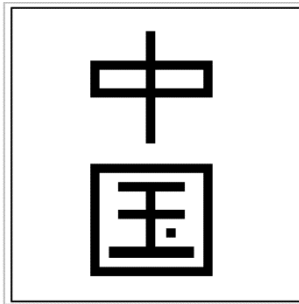


图 5 提取的水印图像
Fig.5 Extracted watermark image

水印提取过程见图 5, 即合法用户 B 从拼接好的含水印图像中提取出水印信息。仿真全过程可以看成是一个实际的应用过程, 该过程中用户 A 要将秘密信息发送给合法用户 B, 为了提高通信的安全性能, A 对信息做了双重保护(利用数字水印技术中水印的不可见性, 利用图像分切-碎片置乱技术提高其安全性)才发送给合法用户 B, 合法用户 B 接收到图像碎片后要先通过彩色图像拼接算法合成含水印图像, 然后再通过水印提取算法获得隐藏的信息。

3 结语

提出了一种基于自毁式数字水印的信息隐藏通信技术, 不仅利用了含水印图像本身隐藏信息的特性, 还结合了彩色图像拼接技术, 提高信息的隐藏性能, 相当于给要传递的信息双层加密, 这种隐藏通信技术不仅隐藏了信息的内容, 还隐藏了信息内容的存在性。此外, 拼接算法的拼接效率极高, 对于大小为 32×32 像素的 8×8 个图像碎片, 平均耗时 1.59 s, 可以实现在线实时拼接, 同时拼接复原的图像无任何图像碎片错位, 因此该彩色图像碎片的拼接算法可行性好, 用于信息隐藏通信领域能够极大地提高信息的隐藏性能。提出的信息隐藏通信技术, 通过将含水印图像分切成图像碎片, 破坏水印信息, 以此隐藏信息的存在, 只有合法用户才能通过彩色图像拼接算法复原含水印图像, 非法者即使获得图像碎片也无法提取内嵌信息, 以此提高信息传递过程中的安全性能, 达到信息隐藏通信的目的。

参考文献:

- [1] YANG Jie. Algorithm of XML Document Information Hiding Based on Equal Element[C]// Computer Science and Information Technology(ICCSIT), 3rd IEEE International, Chengdu, 2010: 250—253.
- [2] RAFAT K F. Enhanced Text Steganography in SMS [C]// Computer, Control and Communication, 2009 2nd International Conference, Karachi, 2009: 1—6.
- [3] WANG W J, HUANG Cheng-ta, WANG S J. VQ Applications in Steganographic Data Hiding Upon Multimedia Images[J]. IEEE Systems Journal, 2011, 5(4): 528—537.
- [4] 郭凌华, 邢铁豆, 刘国栋, 等. 半色调加网信息隐藏技术显隐效果研究[J]. 包装工程, 2015, 36(15): 135—137. GUO Ling-hua, XING Tie-dou, LIU Guo-dong, et al. Appearing Effect of Information Hiding Technology Based on Halftone Screening[J]. Packaging Engineering, 2015, 36(15): 135—137.
- [5] ARJUN S, RAO N. An Approach to Reversible Information Hiding for Images[C]//TENCON 2008-2008 IEEE Region 10 Conference. Hyderabad, 2008: 1—6.
- [6] MAHJABIN T, HOSSAIN S M, HAQUE M S. A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method[C]// Computer and Information Technology (ICCIT), 2012 15th International Conference, Chittagong, 2012: 168—172.
- [7] 商静静, 孙刘杰, 王文举, 等. 基于离散余弦变换的三维点云模型全息盲水印[J]. 包装工程, 2015, 36(13): 111—114. SHANG Jing-jing, SUN Liu-jie, WANG Wen-ju. Holographic Digital Blind Watermark Algorithm for 3D Point Cloud Model Based on Discrete Cosine Transform[J]. Packaging Engineering, 2015, 36(13): 111—114.
- [8] LI Jiang, LYU Rui, YANG Zhan-xin, et al. The Research on the Digital Short Radio Covert Communication Based on Audio Signal Information Hiding Technology[C]// Management and Service Science, MASS '09 International Conference on, Wuhan, 2009: 1—4.
- [9] CHEN Yun-feng, LI Tao, HU Xiao-qin, et al. A Secure Mobile Communication Approach Based on Information Hiding[C]// Mobile Technology, Applications and Systems, 2005 2nd International Conference on, Guangzhou, 2005: 1—5.
- [10] SPIER W, ARNOLD C, LU Jun, et al. Integrating Language Information With a Hidden Markov Model to Improve Communication Rate in the P300 Speller [J]. IEEE Transactions on Neural Systems and Rehabilitation Engineering, 2014, 22(3): 678—684.
- [11] 丁群, 王佳楠. 混沌键控数字保密通信研究新进展[J]. 黑龙江大学工程学报, 2010, 1(1): 84—90. DING Qun, WANG Jia-nan. Recent Advances in Chaos Shift Keying Digital Secret Communication Research [J]. Journal of Engineering of Heilongjiang University, 2010, 1(1): 84—90.
- [12] VAN L P, PRAETER J D, WALLENDIAEL G V, et al. Out-of-the-loop Information Hiding for HEVC video

- [C]// Image Processing (ICIP), 2015 IEEE International Conference, Quebec City, 2015: 3610—3614.
- [13] NAZARI B, JAMALIPOUR A. Contract Design for Relay-based Cooperative Communication with Hidden Channel State Information[C]// Communications in China (ICCC), 2012 1st IEEE International Conference, Beijing, 2012: 798—803.
- [14] ALEKPEROVA I. Some Approaches to the Development of Information Influence and Hidden Communications Detection Systems in Wiki-Environment[C]// Problems of Cybernetics and Informatics (PCI), 2012 IV International Conference, Baku, 2012: 1—2.
- [15] BOBADE S, GOUDAR R. Secure Data Communication Using Protocol Steganography in IPv6[C]// Computing Communication Control and Automation (ICCUBEA), 2015 International Conference, Pune, 2015: 275—279.
- [16] 谭庆丰, 方滨兴, 时金桥, 等. StegoP2P: 一种基于P2P网络的隐蔽通信方法[J]. 计算机研究与发展, 2014, 51(8): 1695—1703.
- TAN Qing-feng, FANG Bin-xing, SHI Jin-qiao, et al. StegoP2P: A Hidden Communication Approach in P2P Networks[J]. Journal of Computer Research and Development, 2014, 51(8): 1695—1703.
- [17] 包观笑, 孙刘杰, 周中原. 抗几何形变全息水印防伪技术[J]. 包装工程, 2014, 35(23): 115—119.
- BAO Guan-xiao, SUN Liu-jie, ZHOU Zhong-yuan. Anti-geometric Distortion Holographic Counterfeiting Watermark Technology[J]. Packaging Engineering, 2014, 35(23): 115—119.