



基于非下采样 Contourlet 变换和 Hill 编码的图像隐写

孙树亮^{1,2}

- (1. 福建师范大学福清分校电子与信息工程学院, 福建 福清 350300;
2. 福建师范大学福清分校创新信息产业研究所, 福建 福清 350300)

摘 要:在非下采样 Contourlet 变换(NSCT)和 Hill 编码的基础上,提出了一种新的隐写方法。首先把载体图像用 NSCT 进行分解,得到一幅低频和若干幅高频图像。NSCT 提供了图像多方向和多尺度的表示。选择一幅高频图像作为载体来嵌入秘密数据。在嵌入之前,用 Hill 密码对秘密数据进行编码。Hill 密码最重要的是如何找到合适的编码矩阵。编码矩阵应满足的条件是可逆,同时要与字母的个数互质。为了改善隐写图像的视觉效果,采用了 2^k 修正法进一步减小隐写图像和载体图像之间的视觉误差。实验证明,提出的方法具有更好的图像质量,因此更具有优越性。

关键词: NSCT; Hill 编码; 2^k 修正; 编码矩阵

中图分类号: TP391

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016170

Image steganography based on nonsubsampling Contourlet transform and Hill cipher

SUN Shuliang^{1,2}

1. School of Electronics and Information Engineering, Fuqing Branch of Fujian Normal University, Fuqing 350300, China
2. Innovative Information Industry Research Center, Fuqing Branch of Fujian Normal University, Fuqing 350300, China

Abstract: A novel image steganography was proposed, which was based on nonsubsampling Contourlet transform (NSCT) and Hill cipher. Firstly, cover image was decomposed with NSCT. It provided a multi-scale and multi-directional representation of an image. One of subbands was selected to embed secret data. Then Hill cipher was applied to encrypt the secret message. How to find a proper cipher matrix was important in this way. The selected matrix should be inevitable and relatively prime to the number of alphabets. The skill of 2^k correction was applied to ease the difference between cover and stego image. Experiment results show that both stego image and retrieved image have better image quality with the proposed approach than other methods.

Key words: NSCT, Hill cipher, 2^k correction, cipher matrix

收稿日期: 2015-11-26; 修回日期: 2016-06-13

基金项目: 国家自然科学基金资助项目 (No. 61473329); 福建省科技厅基金资助项目 (No. 2016J05153)

Foundation Items: The National Natural Science Foundation of China (No. 61473329), Natural Science Foundation of Fujian Province (No. 2016J05153)

1 引言

在秘密通信中,有两种常用的方法:隐写术与密码学。密码学是通过加密密钥将要传递的信息变成密文,接收端通过解密密钥恢复出要传输的消息。入侵者如果没有解密密钥,将不能有效提取秘密信息,因此可以起到保护信息的目的^[1]。由于密码学并不隐藏通信双方“正在通信”这个事实,因此任何人都能够注意到双方正在进行秘密通信,攻击者即使不能够有效破解密码,也可能对密文进行破坏,使合法的接收者也不能正确地解密出信息。隐写术起源于古希腊,它将秘密信息隐藏在文本、图像、声音、视频等数字媒体信号中进行传输^[2]。在隐写术中,非法用户根本不会怀疑看似普通的载体下隐藏有秘密消息。

现代隐写术主要分为两大类,一类基于空间域(图像域);另一类基于变换域。基于空间域的图像隐写实现简单、隐藏容量大,缺点是很容易受到图像变换(剪切、滤波、噪声、采样)的影响^[3,4]。基于变换域的隐写对基本的图像变换具有更强的顽健性,是目前隐写算法的主流。基于离散傅里叶变换(discrete Fourier transform,DFT)的算法会造成细节信息损失^[5]。基于离散小波变换(discrete wavelet transform,DWT)的增强方法只能增强有限的方向,不能很好地表示图像中的方向信息,因此细节信息的增强明显不足^[6]。多尺度几何分析(multiscale geometric analysis,MGA)理论的提出和发展弥补了小波变换的这一缺陷。2002 年 Do 和 Martin^[7]在继承小波多尺度分析思想的基础上提出了 Contourlet 变换,它能在任意尺度上实现任意方向的分解,擅长描述图像中的细节、轮廓和方向性纹理信息,很好地弥补了小波变换的不足。虽然 Contourlet 变换可以更好地利用图像的细节信息,但是它同 DFT 和 DWT 一样会产生“振铃”现象。其次,Contourlet 变换不具备平移不变性。于是,2006 年 Cunha 等人^[8]提出了无下采样的 Contourlet 变换(nonsampled Contourlet transform,NSCT),该变换是一种完全平移不变的 Contourlet 变换。NSCT 由于具有多分辨率、局部定位、多方向性、各向异性和平移不变性的特点,而且 NSCT 的冗余性较 Contourlet 变换与人眼的视觉特性(human visual system,HVS)更接近,因此非常适合应用在

信息隐藏中。NSCT 刚刚被提出不久,其理论正趋于完善,国内外相关的研究工作也刚刚开始,目前还没有专门针对 NSCT 的隐写分析工具,因此 NSCT 成为变换域算法中研究的新热点。

2 非下采样 Contourlet 变换

非下采样 Contourlet 变换的滤波器组由非下采样金字塔滤波器组(nonsampled laplacian pyramid,NSLP)和非下采样方向滤波器组(nonsampled directional filter bank,NSDFB)构成。通过非下采样金字塔滤波器组可以将载体图像分解成一个低频子带和多个高频子带,其中,高频子带的数量与多尺度分解的级数相等,且每个子带图像与原始图像尺寸相等。高频子带捕获原始图像中的奇异点,为了获取延伸在各个方向上的奇异曲线,再使用非下采样方向滤波器组对每个高频子带进行方向滤波,这样就得到了每个尺度下各个方向上的子带图像。

小波变换只能表示有限的方向,不能很好地表示图像的细节,而 NSCT 可以在任意尺度上实现任意方向的分解,能够很好地描述图像中的轮廓和细节。同时,由于 NSCT 具有各向异性的特点,改变某一高频系数的值对其他系数的影响很小,因此 NSCT 比小波变换更适合图像隐写。设 j 为多尺度分解级数, l_j 为 j 尺度下的分解方向数,则

NSCT 可以将原始图像分解成 $1 + \sum_{j=1}^J 2^{l_j}$ 个子图像。

首先把载体图像用 2 层 NSCT 进行分解,获得一个低通图像和若干个高通图像。从第 2 层分解中随机选择一个高通图像作为载体,用来嵌入秘密信息,选择的图像数作为密钥 K1。为了增强秘密信息的安全性,在嵌入之前,应对其进行编码。最后用编码后的秘密信息取代 NSCT 系数的 1 位最低有效位。

3 Hill 编码

对信息的编码,本文采用的是 Hill 编码。Hill 编码是 Hill L S^[9]在 1929 年提出的。该方法是基于矩阵的线性变换,优点是隐藏了字符的频率信息。对字母表来说,26 个字母用 0~25 的整数来表示。例如:A=0,B=1,⋯,Z=25,具体见表 1。

表 1 字母编码表(N=26)

字母	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
数字	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25



要对秘密信息进行编码,首先随机选择一个 $n \times n$ 的矩阵,该矩阵应是可逆矩阵,同时与编码长度 N 互质^[10]。然后把需要编码的信息分成长度为 n 的块,每一块乘以编码矩阵,乘积与 N 进行求模运算,即加密后的结果。进行解密时,每一块密码块乘以加密矩阵的逆矩阵,同理,矩阵的乘积与 N 进行求模运算,即恢复出原始的消息。

加密与解密的计算式为^[11]:

$$C_d = P_d \times C_m [\text{mod } N] \quad (1)$$

$$P_d = C_d \times C_m^{-1} [\text{mod } N] \quad (2)$$

其中, C_d 是编码后的数据, C_m 是编码矩阵, P_d 是原始数据, N 是编码表的长度。对于灰度图像来说, N 为 256, 即取图像的灰度级数作为密码表的长度。

4 2^k 修正法

隐藏秘密信息以后的载体图像称为载密图像。通常载密图像与原始载体图像之间会存在一定的差异,为了增强隐写图像的视觉效果,减小两者之间的差异,本文采用的是 2^k 修正法^[12]进行修正。

具体过程如下^[13]。

已知: 载体像素值(actual pixel value, APV), 隐写像素值(stego pixel value, SPV), 误差值(error value, EV), 新的隐写像素值(new stego pixel value, NSPV), k 为替换最低位的二进制位数。

if (SPV-APV > 2^{k-1}) & (SPV- $2^k \geq 0$)

NSPV = SPV - 2^k

else if (SPV-APV < - 2^{k-1}) & (SPV + $2^k \leq 255$)

NSPV = SPV + 2^k

else NSPV = SPV

经过 2^k 修正以后, 新的隐写像素值更接近原始载体像素值, 同时不会影响隐藏的秘密数据。

5 提出的算法

数据隐藏算法如图 1 所示。

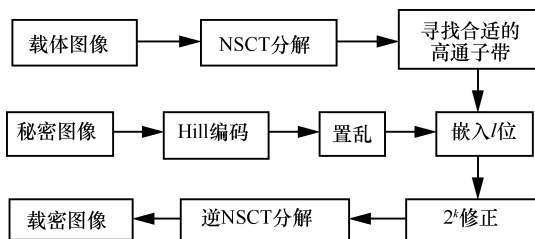


图 1 数据隐藏算法框架

嵌入算法过程如下:

- 读取载体图像和秘密图像;
- 对载体图像进行 NSCT 分解, 得到一个低通图像和若干个高通图像;
- 在第 2 层分解得到的高通图像中随机选择一幅图像 K1 作为载体来嵌入秘密信息;
- 对秘密图像进行 Hill 编码(这里应对 256 求模);
- 对编码后的信息进行置乱, 密钥为 K2;
- 高通 K1 的 NSCT 系数用 1 位秘密数据替换;
- 利用 2^k 修正法对图像进行修正;
- 对隐写图像进行逆 NSCT 分解;
- 最终获得隐写图像。

信息提取的过程是上述过程的逆过程, 这里不再详细描述。

6 实验过程和结果

本文的实验是在 Windows 7 下用 MATLAB 10 实现的。为了衡量提出的算法, 采用峰值信噪比(peak signal-to-noise ratio, PSNR)作为参数。为了计算 PSNR, 首先计算均方误差(MSE)。

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \|I(i,j) - S(i,j)\|^2 \quad (3)$$

其中, I 是载体图像, S 是隐写图像, M 和 N 分别是载体图像的长和宽。

$$PSNR = 20 \lg \left(\frac{255}{\sqrt{MSE}} \right) \quad (4)$$

相关系数 NC 用来检测原始秘密图像和恢复的秘密图像之间的相似程度。

$$NC = \frac{\sum_{i=1}^M \sum_{j=1}^N w(i,j)w'(i,j)}{\sum_{i=1}^M \sum_{j=1}^N w^2(i,j)} \quad (5)$$

其中, w 和 w' 分别是原始秘密图像和提取的秘密图像, M 和 N 分别是载体图像的长和宽。载体图像的大小是 512 dpi × 512 dpi 的灰度图像, 秘密信息是 128 dpi × 128 dpi 的灰度图像。

为了衡量本文所提出算法的优劣性, 把本文提出的方法与 Ramezani H 等人^[14]和 Karthikeyan B 等人^[15]的方法进行比较。

由表 2 可见, 本文的算法具有更大的 NC 值。由表 3 可

表 2 本文算法和参考文献[15]算法 NC 值的比较

攻击类别	噪声		剪切		旋转		压缩		滤波	
	高斯	椒盐	1/16	1/4	10°	30°	30%	80%	高斯	均值
参考文献[15]算法	0.993 0	0.986 4	0.995 6	0.976 7	0.804 2	0.781 2	0.999	0.999 7	0.999 2	0.968 3
本文算法	0.997 4	0.993 4	0.998 5	0.987 9	0.864 5	0.838 5	0.999	0.999 9	0.999 7	0.992 1

表 3 本文的方法与参考文献[11]、参考文献[14]的方法 PSNR 值的比较

载体图像	算法		
	参考文献[14]算法	参考文献[11]算法	本文算法
Baboon	50.87	48.25	52.66
Lena	51.31	48.69	53.28
Peppers	51.03	48.47	52.96

见,对于不同的载体图像,本文的算法都具有更好的 PSNR 值,因此本文所提出的算法能够获得更好的隐写质量。

从图 2 也可以看出,与其他两种方法相比,本文提出的算法所获得的隐写图像和直方图更接近原始载体图像,从而说明了本文算法的有效性。

图 3 显示了载体图像、秘密图像、载密图像、提取的秘密图像及其相应的直方图。秘密图像与用本文的方法提取

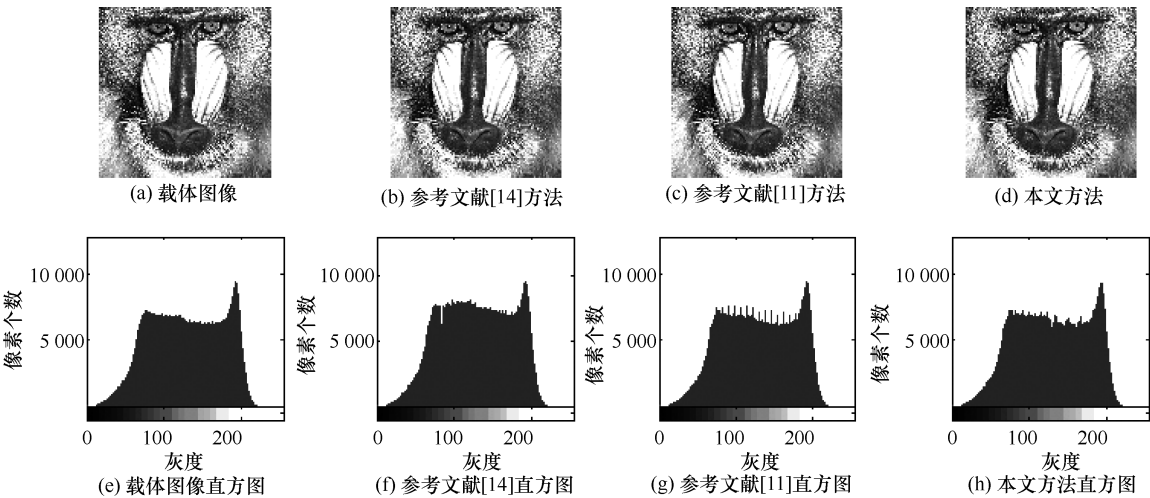


图 2 用不同方法获得的隐写图像及其相应的直方图

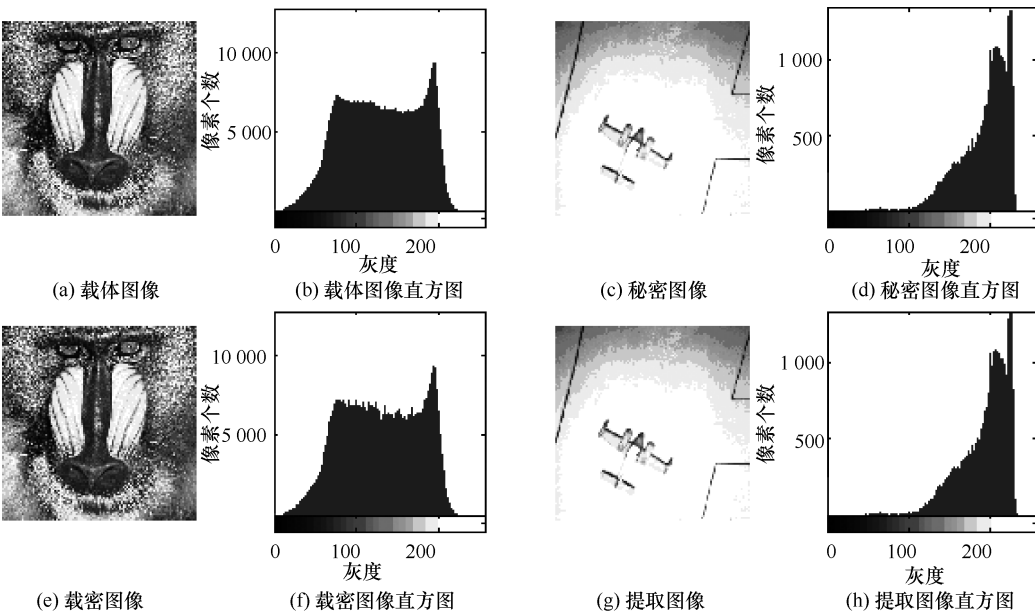


图 3 隐写图像和提取的秘密图像及其对应的直方图



的载体图像几乎完全一致,两者对应的直方图也说明了这一点。

即使载密图像被检测出来,但是由于本文使用了密钥 K1、K2 以及 2^k 修正,没有密钥也不能正确地获取秘密图像,进一步增强了秘密信息的安全性。

7 结束语

由于人类视觉对平滑区域的微小变化比对边缘区域更为敏感,因此为了尽可能减小对载体图像的影响,本文的秘密信息仅仅隐藏在载体的边缘及细节区域,即高通子带的 NSCT 系数内。为了进一步增强秘密信息的安全性,采用了 Hill 密码对秘密信息进行加密。为了获得更好的视觉效果,减少载体图像和隐写图像之间的差异,采用了 2^k 修正法对隐写图像进行修正。实验表明,本文方法具有更好的隐写效果和 PSNR 值,从而证明了本文所提出方法的有效性。

将来的工作应加强对信息隐藏能力的分析以及用不同的隐写分析方法对隐写图像的检测情况进行进一步分析。

参考文献:

- [1] 钟黔川,朱清新. Blowfish 密码系统分析 [J]. 计算机应用, 2007, 27(12): 2940-2944.
ZHONG Q C, ZHU Q X. Analysis of Blowfish cryptography[J]. Computer Applications, 2007, 27(12): 2940-2944.
- [2] CHANNALLI S, JADHAY A. Steganography-an art of hiding data [J]. International Journal on Computer Science and Engineering, 2009, 1(3): 137-141.
- [3] JUNEJA M, SANDHU P S. An improved LSB based steganography technique for RGB color images [J]. International Journal of Computer and Communication Engineering, 2013, 2(4): 513-517.
- [4] 吴霞,徐向阳,黄友荣. 抗统计分析的 BPCS 隐写算法 [J]. 计算机工程与应用, 2007, 43(7): 52-54.
WU X, XU X Y, HUANG Y R. BPCS steganography algorithm against statistical analysis [J]. Computer Engineering and Applications, 2007, 43(7): 52-54.
- [5] 李艳玲,黄红艳. 基于 DFT 域的图像信息隐藏技术 [J]. 华北水利水电学院学报, 2008, 29(4): 62-64.
LI Y L, HUANG H Y. Information hiding technology based on DFT domain [J]. Journal of North China Institute of Water Conservancy and Hydroelectric Power, 2008, 29(4): 62-64.
- [6] JAMDAR A S, SHAH A V, GAVALI D D, et al. Edge adaptive steganography using DWT [J]. International Journal of Engineering and Advanced Technology, 2013, 2(4): 648-652.
- [7] DO M N, VETTERLI M. The contourlet transform: an efficient directional multiresolution image representation [J]. IEEE Transactions on Image Processing, 2005, 14(12): 2091-2106.
- [8] CUNHA A L D, ZHOU J P, DO M. N. The nonsubsampling contourlet transform: theory, design, and applications [J]. IEEE Transactions on Image Processing, 2006, 15(10): 3089-3101.
- [9] HILL L S. Cryptography in an algebraic alphabet [J]. The American Mathematical Monthly, 1929, 36(6): 306-312.
- [10] PAVAN N, NAGARJUN G A, NIHAAR N, et al. Image steganography based on hill cipher with key hiding technique[J]. IOSR Journal of Computer Engineering, 2013, 11(5): 47-50.
- [11] KARTHIKEYAN B, CHAKRAVARTHY I, RAMASUBRAMANIAN S. Amalgamation of scanning paths and modified hill cipher for secure steganography [J]. Australian Journal of Basic and Applied Sciences, 2012, 6(7): 55-61.
- [12] KAUR A, KAUR S. Image steganography based on hybrid edge detection and 2^k correction method [J]. International Journal of Engineering and Innovative Technology, 2012, 1(2): 167-170.
- [13] SUN S L, GUO Y N. A novel image steganography based on contourlet transform and hill cipher [J]. Journal of Information Hiding and Multimedia Signal Processing, 2015, 6(5): 889-897.
- [14] RAMEZANI H, KEYNIA F, RAMEZANI F. A novel image steganography in contourlet domain using genetic algorithm[J]. International Journal of Future Computer and Communication, 2013, 2(4): 359-363.
- [15] 闫芬,王康碧,李晨,等. 一种基于 NSCT 与抖动量化的盲水印算法 [J]. 云南民族大学学报: 自然科学版, 2013, 22 (3) : 222-225.
YAN F, WANG K B, LI C, et al. A blind algorithm based on NSCT and dither quantization [J]. Journal of Yunnan Minzu University: Natural Sciences Edition, 2013, 22(3): 222-225.

[作者简介]



孙树亮(1982-),男,福建师范大学福清分校副教授,主要研究方向为信息安全与图像处理。