Journal of Computer Applications
计算机应用,2013,33(11):3232-3234
ISSN 1001-9081
CODEN JYIIDU
2013-11-01
http://www.joca.cn

文章编号:1001-9081(2013)11-3232-03
doi:10.11772/j.issn.1001-9081.2013.11.3232

基于 CL 多小波变换和组合位平面理论的秘密信息共享算法

张 弢[1*],任 帅[2],巨永锋[1],凌 尧[1],杨照辉[1]
(1.长安大学 电子与控制工程学院,西安 710064; 2.长安大学 信息工程学院,西安 710064)
(*通信作者电子邮箱 zt904@foxmail.com)

摘 要:针对信息隐藏算法容量和不可见性与鲁棒性矛盾的特点,提出了一种新的基于 Chui-Lian(CL)多小波变换和组合位平面(CBP)理论的数字图像载体预处理算法,并将该算法用于以数字图像为载体的信息隐藏,以实现秘密通信和图像共享。其中,CL 多小波变换能够将载体图像划分为 4 个能量等级不同的最低分辨率子图像,组合位平面理论可将子图像解析为不同的位平面层次,在隐藏秘密信息时,可根据最低分辨率子图和组合位平面的能量等级由高到低分别嵌入鲁棒信息、秘密信息和脆弱信息。实验结果表明,在 25% 的嵌入率时,与基于离散余弦变换和最低有效位方法的信息隐藏算法(DCT-LSB)、基于离散小波变换和最低有效位方法的信息隐藏算法(DWT-LSB)相比,所提算法针对若干常见攻击的鲁棒性有一定程度提升,峰值信噪比(PSNR)分别提高了 37.16% 和 20.00%。

关键词:信息隐藏;秘密通信;载体预处理;CL 多小波变换;组合位平面理论
中图分类号:TP309.2; TP391.9 **文献标志码**:A

Secret information sharing algorithm based on CL multi-wavelet and combination bit plane for confidential communication

ZHANG Tao[1*], REN Shuai[2], JU Yongfeng[1], LING Yao[1], YANG Zhaohui[1]
(1. *School of Electronic and Control Engineering, Chang'an University, Xi'an Shaanxi* 710064, *China*;
2. *School of Information Engineering, Chang'an University, Xi'an Shaanxi* 710064, *China*)

Abstract: In view of the contradiction between capability, invisibility and robustness of the existing information hiding algorithms, a preprocessing algorithm for digital image based on CL (Chui-Lian) multi-wavelet transform and Combination Bit Plane (CBP) was proposed. Then the digital image preprocessed by CL multi-wavelet and CBP was taken as the cover image to embed secret information for confidential communication and image sharing. CL multi-wavelet transform could divide the cover image into four lowest resolution sub-images with different energy level. And CBP method could analyze the above four sub-images into different bit planes as the final embedding regions. During the hiding procedure, robust information, secret information and fragile information could be embedded according to the energy and robustness characteristics of the embedding regions. The experimental results show that the robustness against several common attacks described in this paper has certain enhancement compared with other two methods when the embedding rate is 25%. The Peak Signal-to-Noise Ratio (PSNR) is increased by 37.16% and 20.00% respectively compared with Discrete Cosine Transform-Least Significant Bit (DCT-LSB) and Discrete Wavelet Transform -Least Significant Bit (DWT-LSB) algorithm.

Key words: information hiding; confidential communication; carrier preprocessing; CL (Chui-Lian) multi-wavelet transform; Combination Bit Plane (CBP) theory

0 引言

在秘密通信环境下,以数字图像为载体的秘密信息共享技术主要通过修改载体与秘密信息的自身特性、或者利用两者特性使其达到最大一致性,并最终实现隐秘信息传输目的。根据不同类型的秘密信息和应用环境可选择不同的载体图像,并设计出具有不同性能的算法。而衡量一个信息隐藏算法性能的指标有:鲁棒性、不可见性、容量、抗检测性和感知篡改性等[1-2]。一个好的信息隐藏算法需要均衡地满足多个指标。文献[3]研究表明,信息隐藏算法的鲁棒性和不可见性等多个性能与载体的能量和结构特性有关,而目前的算法大多是基于运算域的,如空间域或者变换域[4-5],并未专门考虑载体特性。本文将通过对载体和欲隐藏信息的特性解析,利用 CL(Chui-Lian)多小波理论和组合位平面(Combination Bit Plane, CBP)理论[6]对其进行预处理,并充分利用载体特性来改善算法性能。

1 CL 多小波和组合位平面理论

1996 年,Chui 和 Lian[7]利用对称性给出了支集在[0,2]和[0,3]区间上的二元多尺度和多小波函数,构建了 CL 多小波变换。通常一幅图像经过多小波变换后,绝大部分能量集中于最低分辨率子图,但经过 CL 多小波变换的图像,其最低分辨率子图的绝大部分能量又进一步集中于它的第一个分量上[8-9]。在基于数字图像的多小波变换中,一幅图像经过多

收稿日期:2013-05-16;**修回日期**:2013-07-20。 **基金项目**:2013 年度长安大学中央高校基本科研业务费专项(2013G1241118);国家 863 计划项目(2012AA112312);交通运输部项目(2012-364-208-600,2012-364-208-200,201231849A70);吉林省外国专家局项目(2012-7-102-2)。

作者简介:张弢(1984-),女,山西吕梁人,讲师,博士,主要研究方向:信息安全、图像处理; 任帅(1982-),男,山西太原人,讲师,博士,CCF 会员,主要研究方向:图像信息隐藏、物联网安全; 巨永锋(1962-),男,陕西周至人,教授,博士生导师,主要研究方向:交通运输控制、模式识别。

小波变换后,能量分布会因分解的阶数和分量所在的方向而具有不同的能量分布规律[10-11],原图像的绝大部分能量都集中于最低分辨率子图像,而 CL 多小波变换的特点在于 LL_2 的高能量与 LH_2、HL_2 和 HH_2 低能量的对立分布。本文利用以上分布特性,在算法设计时选择在高能量区域中的低能量子区域实现具体的信息隐藏,在满足高能量分量子图的不可见性的前提下,使整个含密图像具有较强的鲁棒性。

图像位平面理论[12-13]是根据数字图像在计算机中的存储情况发展而来的,最典型的位平面分解是灰度图像的位平面分解,其中的每一像素的相同比特可看作表示一个二值的平面,称为位平面。而组合位平面是以位平面分解为基础,但操作对象是由任意几个颜色分量组合,分解的结果是由任意几个位平面共同生成的组合位平面。位平面中的"位"不仅仅是指 1 位,也可以是相同位置的几位的组合。位平面分解是将图像在计算机中的保存情况按同一存储位进行重新组合后表示。因此,任何颜色空间都可按照如下步骤进行位平面分解:

步骤 1　按照图像的颜色空间规则,分解出各自分量,或某几个分量的组合;

步骤 2　对各自分量进行灰度转换,统计出各个分量的表示位数;

步骤 3　按照各位对应原则,取相同位置的位数据,以空间的排列方式组成各位(或几位)位平面图。其流程如图 1 所示。

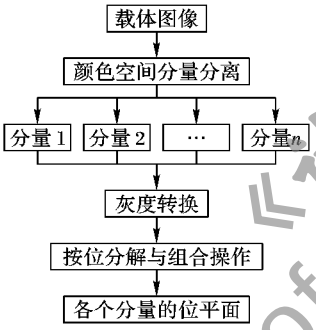


图 1　组合位平面生成步骤

2　算法设计

本文首先利用 CL 多小波变换对载体图像进行能量特性处理,生成一阶子图像,从而将载体图像的能量大多集中在 LL_2 分量上,有助于提高算法鲁棒性。再利用组合位平面分解理论对 CL 多小波变换后的各个子图像进行结构和视觉上的解析,选择子图像的特定组合位平面作为秘密信息的嵌入区域和脆弱性信息嵌入区域,可增加算法的容量,优化算法的不可见性,并进一步提升算法鲁棒性。

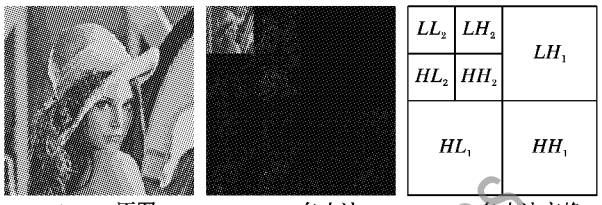
2.1　基于 CL 多小波变换的载体图像预处理

经过 CL 多小波变换后,LL_1 子图像的 4 个分量图只有 LL_2 清晰可见,占据了图像的主要能量,其余子图均难以辨识。如图 2 所示为载体图像 Lena 经过一阶 CL 多小波变换后的子图像能量分布情况。根据 CL 多小波变换后载体能量分布的这一特性,可将其应用于对鲁棒性要求较高的秘密信息共享环境中。表 1 是载体图像经过 CL 多小波一阶变换后的能量分布。

2.2　基于组合位平面方法的数字图像载体预处理

本文所采用的组合位平面方法利用各个子图像分解后所得的 8 个位平面视觉重要性的不同,将第 0 个位平面中的各像素作为秘密信息嵌入区域,将第 7 个位平面中的各像素作为参考值,而将第 3 个位平面中的各像素作为辅助校验参数用于秘密信息提取的参考。如图 3 所示,分别用 C_3 和 C_7 来表示第3位平面和第7位平面中的数据序列。若所隐藏的信息为 C_I,则根据式(1)对 C_3 进行修改,从而隐藏 C_I:

$$C_3 = C_7 \oplus C_I \tag{1}$$



(a) Lena原图　(b) CL多小波变换Lena　(c) CL多小波变换隐藏区域示意图

图 2　Lena 的一阶 CL 多小波分解图及其子区域分布图

表 1　CL 多小波变换的一阶能量分布　%

CL 多小波变换 LL_1 子图像能量占图像总能量的百分比	LL_1 子图像各个分量的能量分布			
	LL_2	LH_2	HL_2	HH_2
97.36	96.53	2.51	0.62	0.34

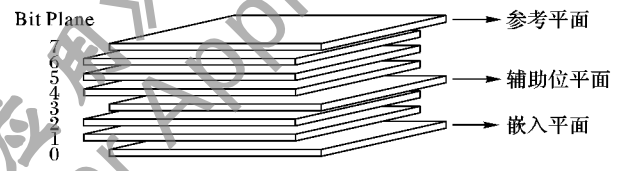


图 3　组合位平面示意图

2.3　算法实现步骤

基于 CL 多小波变换和组合位平面理论的秘密信息共享算法流程如图 4 所示,且共有 7 个步骤:

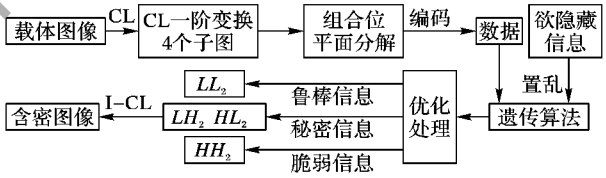


图 4　基于 CL 多小波变换和组合位平面的算法流程

步骤 1　对载体图像进行 CL 多小波变换,分解出载体图像的 LL_1 子图的 4 个分量图,分别记作 LL_2、LH_2、HL_2 和 HH_2,并将每个子图分解为位平面形式,提取出各自的第 0 个、第 3 个和第 7 个位平面。

步骤 2　对每个子图的第 0 个、第 3 个和第 7 个位平面的像素值进行骑士巡游遍历。根据式(1),第 3 个位平面的比特序列为 $C_I^{3\oplus7}$。最终隐藏到 LH_2 和 HL_2 中的秘密信息是 C:

$$C_I^{3\oplus7} = C_I^3 \oplus C_I^7 \tag{2}$$

$$C = C_2^{3\oplus7} \oplus C_3^{3\oplus7} = t_1, t_2, \cdots, t_n; \quad n = 2k \tag{3}$$

步骤 3　按照式(4),利用 Logistic 映射对需要隐藏的信息进行混沌置乱。给出参数 μ 和初始值 x_k。则经过映射后的比特序列为 C_{IN}^x,且 $C_{\mathrm{IN}}^x = b_1^x, b_2^x, \cdots b_{n-1}^x, b_n^x$:

$$x_{k+1} = \mu x_k(1 - x_k); \quad x_k \in (0,1) \tag{4}$$

步骤 4　设 C_{IN}^x 和 C 中对应比特位数值相同的比特位数为 F,利用遗传算法改变 x_k 以使得 F 最大化。基于 CL 多小波变换和组合位平面的优化模型遵循式(5)。假设 y 为最优解,将其代入 C_{IN}^x 以获得最优化的嵌入比特序列 C_{IN}^y,而 $C_{\mathrm{IN}}^y = b_1^y, b_2^y, \cdots, b_{n-1}^y, b_n^y$:

$$F(y) = \mathrm{Max}\, F(x_k) = \mathrm{Max} \sum (t_n \overline{\oplus} b_n^x) \tag{5}$$

步骤5 按照独立冗余磁盘阵列(Redundant Array of Independent Disk, RAID)技术第4种方法将 C_{IN}^{y} 嵌入 LH_2 和 HL_2 的相应位平面中即修改 LH_2 和 HL_2 相应位平面的像素值。

步骤6 LL_2 是 LL_1 中鲁棒性最强的区域,为了让接收者恢复秘密信息并判断其完整性,本算法特提供循环冗余校验码,记作 R^L,并同 y 和 μ 一起用RAID4嵌入鲁棒性区域中。

步骤7 HH_2 是 LL_1 的4个子图中最脆弱的,在其中嵌入循环冗余校验参数,记作 R^H。接收者可以对 R^H 和 R^L 进行比较,以判断含密图像是否收到攻击。

3 仿真实验

将本文提出的基于CL多小波变换和组合位平面的算法简称为CL-CBP,与基于离散余弦变换和最低有效位方法的信息隐藏算法(简称DCT-LSB)以及基于离散小波变换和最低有效位方法的信息隐藏算法(简称DWT-LSB)进行性能比较,仿真实验表明CL-CBP算法具有良好的不可见性和鲁棒性。根据峰值信噪比(Peak Signal-to-Noise Ratio, PSNR),CL-CBP与DCT-LSB和DWT-LSB相比,不可见性良好,如表2所示,当嵌入率为25%时,PSNR分别提高了37.16%和20.0%。

表2 不可见性对比(基于PSNR进行判断)

算法	PSNR/dB
CL-CBP算法	34.9482
DCT-LSB算法	25.4785
DWT-LSB算法	29.1246

图5~6和表3给出了当嵌入率为25%时的鲁棒性对比实验结果,其中 Q 表示鲁棒性检验值[14]。

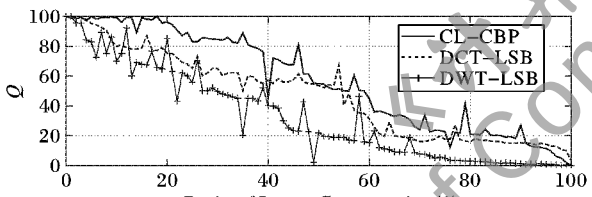


图5 压缩攻击对比实验结果

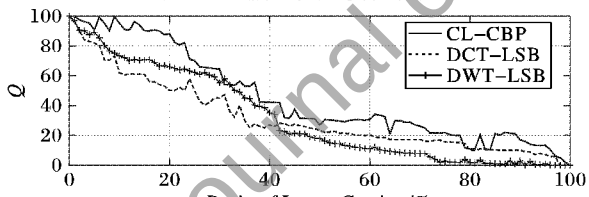


图6 剪切攻击对比实验结果

由图5可知,当JPEG2000压缩率为25%时CL-CBP的 Q 值为83.00,而DCT-LSB和DWT-LSB的鲁棒性 Q 值分别为53.08和65.10,即CL-CBP算法比DCT-LSB和DWT-LSB算法的 Q 值分别提高了56.37%和27.50%;图6表明,当剪切率为30%时,CL-CBP、DCT-LSB和DWT-LSB算法的 Q 值分别为64.53,46.12和53.23,即CL-CBP算法比DCT-LSB和DWT-LSB算法的 Q 值分别提高了39.92%和21.23%。

由表3可知,在[3,3]中值滤波攻击下,CL-CBP比DCT-LSB的 Q 值提高了16.54%;在[3,3]维娜滤波攻击下,CL-CBP比DCI-LSB的 Q 值提高了22.55%;在 $\mu=0,\sigma^2=0.003$ 的高斯加噪攻击时,CL-CBP比DCT-LSB和DWT-LSB的 Q 值分别提高了16.54%和7.70%;在 $d=0.15$ 的椒盐噪声攻击时,CL-CBP比DWT-LSB的 Q 值提高了24.88%。

表3 滤波和加噪的鲁棒性检验值对比

攻击	CL-CBP	DCT-LSB	DWT-LSB
[3,3]中值滤波	59.68	51.21	66.24
[3,3]维纳滤波	54.24	44.26	56.32
高斯加噪 $\mu=0,\sigma^2=0.003$	70.24	60.27	65.22
椒盐噪声 $d=0.15$	37.64	43.21	30.14

4 结语

本文并未如其他算法一样从运算域角度考虑,而是以载体的能量特性和结构特性为出发点,首先利用CL多小波变换对数字图像载体进行能量特性预处理,使其生成鲁棒性差异化子图;其次利用组合位平面理论对上述能量差异化子图进行空间结构预处理,使其生成具体的嵌入区域,利用置乱算法对载体和秘密信息进行置乱处理,并利用遗传优化算法使其保持比特序列上的最大一致性,这些都保证了算法良好的鲁棒性和不可见性。另外,用CL多小波变换处理载体图像计算量较小,而组合位平面理论由于其具有空域算法的优点,所以较易实现且容量较大。

参考文献:

[1] 曹玉强,龚卫国,柏森,等.基于Curvelet变换的鲁棒信息隐藏算法[J].计算机工程,2011,37(5):137-139.

[2] 徐凯平,郑洪源,丁秋林.一种基于LSB和PVD的图像信息隐藏方法研究[J].计算机应用研究,2010,27(3):1068-1071.

[3] PEVNY T, BAS P, FRIDRICH J. Steganalysis by subtractive pixel adjacency matrix [J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2):215-224.

[4] ZHANG T, MU D J, REN S. Information Hiding (IH) algorithm based on Gaussian pyramid and GHM (Geronimo Hardin Massopust) multi-wavelet transformation [J]. International Journal of Digital Content Technology and its Applications, 2011, 5(3): 210-218.

[5] ZITZMANN C, COGRANNE R, RETRAINT F, *et al*. Statistical decision methods in hidden information detection [C]// Proceedings of the 13th International Conference on Information Hiding. Berlin: Springer-Verlag, 2011: 163-177.

[6] 张弢,慕德俊,任帅.lαβ与组合位平面技术在信息隐藏算法中的应用[J].计算机工程与应用,2009,45(20):10-12.

[7] CHUI C K, LIAN J. A. A study of orthonormal multi-wavelets [J]. Applied Numerical Mathematics, 1996, 20(3): 273-298.

[8] 黄卓君,马争鸣.多小波图象变换的统计分析[J].中国图象图形学报,2001,12(6A):1198-1203.

[9] 徐涛,吴登峰,刘杰,等.多小波正交扩充算法在图像处理中的应用[J].吉林大学学报:工学版,2006,36(5):778-781.

[10] 唐笑年,王树勋,王丹.Balanced opt-rec多小波域内信息分层隐藏的分析与实现[J].电子学报,2009,37(6):1226-1231.

[11] AN Z Y, ZHAO F. Image retrieval based on the energy and entropy of multiwavelets transform [C]// ITCS'09: Proceedings of the 2009 International Conference on Information Technology and Computer Science. Washington, DC: IEEE Computer Society, 2009: 544-547.

[12] 吴晓荣,何明一,张易凡.基于多小波分解的多光谱图像矢量融合[J].电子与信息学报,2007,29(4):789-794.

[13] REINHARD E, ASHIKHMIN M, GOOCH B, *et al*. Color transfer between images [J]. IEEE Computer Graphics and Applications, 2001, 21(5):34-40.

[14] 任帅,张弢,慕德俊,等.基于GHM多小波与自适应颜色迁移的信息隐藏算法研究[J].西北工业大学学报,2010,28(2):64-269.