第 33 卷 第 8 期 计 算 机 工 程 2007 年 4 月
Vol.33 No.8 Computer Engineering April 2007
·安全技术· 文章编号：1000—3428(2007)08—0157—03 文献标识码：A 中图分类号：TP391

基于视觉特性及低位替换优化的信息隐藏方法

刘建东[1]，陈桂强[2]，余有明[1]，田 野[1]
(1. 北京石油化工学院信息工程学院，北京 102617；2. 河北北方学院物理系，张家口 075000)

摘 要：提出了一种在图像载体中进行信息隐藏的新方法。该方法利用图像的视觉特性，通过硬 *c* 均值聚类分析进行秘密信息嵌入。通过对简单低位替换的优化调整，在图像的隐藏量和图像质量上都有很大的改进。另外，采用基于时空混沌映射置乱技术对载体图像进行置换及反向置换，对秘密信息提供了有效的安全防护手段。实验结果表明，该方法在改善图像质量及视觉隐蔽性上都取得了较好的结果。
关键词：信息隐藏；LSB 替换；视觉特性

Information Hiding Algorithm Based on Visual Perception and Optimal LSBs Substitution

LIU Jiandong[1], CHEN Guiqiang[2], YU Youming[1], TIAN Ye[1]
(1. School of Information Engineering, Beijing Institute of Petro-chemical Technology, Beijing 102617;
2. Department of Physics, Heibei North University, Zhangjiakou 075000)

【Abstract】This paper presents a method of information hiding algorithm based on optimal LSBs substitution and image visual perception. In this method, according to the characteristics of human vision sensitivity, the hard *c*-means cluster is used to identify the complexity of the cover-image. To improve the quality of embedding result, an optimal pixel adjustment process is applied to the stego-image. The scrambling technology based on spatiotemporal chaos mapping can be used to solve the problem that the hiding algorithm can not provide the way of protecting the secret information. The initial parameters of the spatiotemporal chaos mapping can act as the private keys, which can provide larger key space. Experimental results show the proposed algorithm can make a great improvement in both the imperceptibility and the quality of the cover-image.
【Key words】Information hiding; LSB substitution; Visual perception

近年来，在图像载体中进行信息隐藏逐渐成为研究热点[1]。人眼对图像平滑区的噪声较敏感，而对较复杂的纹理区的噪声不敏感。为了使嵌入信息的图像不引起人的注意，就要将数据嵌入过程与图像的复杂程度联系起来。当隐藏的数据量增加时，载体图像的质量可能降低很多，因此还须研究在增加嵌入量的同时又不使图像质量降低太多的算法[2]。

本文提出一个基于低位优化替换的自适应图像隐藏算法。该算法通过对载体图像聚类分析，根据图像视觉特性自适应地调整载体图像像素中嵌入秘密信息的位数，并对嵌入了信息的像素位进行优化调整，提高了图像隐藏的质量。另外，通过采用时空混沌置乱技术，使隐藏到载体图像中的数据有非常好的伪随机特征，具有很高的安全性。

1 载体图像中信息嵌入深度的确定

在载体图像中用于进行图像复杂性分析的像素是不能嵌入秘密信息的，否则，因像素值修改，提取信息时图像复杂性的分析结果就会和嵌入信息时的分析结果不同，从而使信息提取产生错误。为此，将载体图像像素分为 2 类，一类用于嵌入信息，称为可嵌信息像素；而另一类用于进行图像的复杂性分析，称为不可嵌像素。与每个可嵌信息像素相邻的 8 个像素为不可嵌像素，一个可嵌信息像素的邻域内的 8 个像素用来确定该可嵌信息像素所能隐藏信息的位数，称其为嵌入深度。本文依据一个像素的邻域内的 8 个像素的方均根敏感值、对比度敏感值及熵敏感值 3 个指标，通过硬 *c* 均值聚类分析来确定信息嵌入深度。

将任一可嵌信息像素(i,j)相邻的 8 个像素记为 $N(i,j)$。首先由 $N(i,j)$确定每个可嵌信息像素位的 3 个特征量：

(1)方均根敏感值，决定可嵌信息像素位邻域的纹理

$$\boldsymbol{T}=[\frac{1}{8}\sum_{k=-1}^{1}\sum_{t=-1}^{1}[g_{i+k,j+t}-B]^2]^{\frac{1}{2}}$$

(B 为(i,j)相邻像素的亮度均值，k 和 t 不同时为 0)

(2)对比度敏感值，即(i,j)相邻像素的最大距离，表现为可嵌信息像素邻域的对比度。

$$C=\max(g_{N(i,j)})-\min(g_{N(i,j)})$$

(3)熵敏感值，用于对 $N(i,j)$的不确定性进行度量

$$E=-\sum_{N(i,j)}p_{i,j}\cdot\log\ p_{i,j}$$

其中$g_{i,j}$表示$N(i,j)$内的像素的亮度值，$p_{i,j}$定义如下

这样每个子块就对应了 3 个值，由它们构成了一个加权模式向量

$$p_{i,j}=g_{i,j}/\sum_{N(i,j)}g_{i,j}$$

$$x_k=(T,\alpha C,\beta E)$$

将图像的所有子块看作是三维空间中的一个元素，对其进行硬 *c* 均值聚类分析，将载体图像的像素划分为 3 类，分

基金项目：北京市优秀人才培养专项基金资助项目(20042D050050 8)；北京市教委科技发展计划基金资助项目(KM200710017007)
作者简介：刘建东(1966－)，男，硕士、副教授，主研方向：混沌密码，图像加密与信息隐藏；陈桂强，讲师、硕士生；余有明，博士、副教授；田 野，硕士、讲师
收稿日期：2006-04-27 **E-mail：**liujiandong1178@163.com

别为图像的边缘区域、纹理区域及平滑区域。这种分类是自动的，无需人为设定阈值。根据聚类结果，给每个可嵌信息像素分配一个标记 L, $3\le L\le 5$，分别对应图像的平滑区域、纹理区域及边缘区域，其它像素标记为 0，不用于嵌入数据。由标记 L 构成一个与载体图像大小相同的嵌入深度矩阵 $B(i,j)$，元素取自 $\{0, 3, 4, 5\}$，表示载体图像像素用于隐藏秘密信息的低位位数。

2 低位替换的优化调整

2.1 简单的低位替换方法

假定要把$n$bits秘密信息M隐藏到灰度载体图像C中。由C的每个像素的最低k位所形成的图像记为k-$LSBs$。简单的低位替换方法是，将$n$bits秘密信息M分解为k比特的一些单位，由这些单位组成k比特像素值的虚拟图像M_1，然后用M_1去替换C的低k位k-$LSBs$，替换后的C记为C_1，称为含密图像。

在上述简单的低位替换方法中，当k较大时，含密图像C_1的质量变化可能非常引人注意。表 1 给出在最坏的情况下，k取不同值时的载体图像与含密图像间的峰值信噪比($PSNR$)。

表 1 最坏情况下的峰值信噪比

K	1	2	3	4
$PSNR_{worst}$	48.13	38.59	31.23	24.61

一般人眼可以察觉的 $PSNR$ 为 38.0dB，这说明当 k>2 时，人眼就能感觉到载体图像与含密图像之间的差异。

2.2 像素值的优化调整

为了改善隐藏信息后图像的质量，可对含密图像的像素值进行调整[3]。设定 g_i 和 g_i' 分别表示载体图像及用简单的低位替换方法得到的含密图像的第i个像素的像素值，由于嵌入了秘密信息，第i个像素的像素值产生的误差为 $\delta_i = g_i' - g_i$。若在载体图像的像素中嵌入k位秘密信息，则产生误差的范围是

$$-2^k < \delta_i < 2^k$$

将δ_i的可能取值划分为 3 个区间：$(2^{k-1}, 2^k)$，$[-2^{k-1}, 2^{k-1}]$和$(-2^k, -2^{k-1})$。误差δ_i落在区间$(2^{k-1}, 2^k)$及$(-2^k, -2^{k-1})$内，对图像质量影响最大。这种情况可通过对载体图像像素的最高(8-k)位的值的调整，来减小对载体图像质量的影响。具体做法是：若δ_i在区间$(2^{k-1}, 2^k)$内，且 g_i' 大于或等于 2^k，则用 g_i' 减去 2^k 的值来替换原来的灰度值 g_i'，误差区间由$(2^{k-1}, 2^k)$变成$(-2^{k-1}, 0)$；若δ_i在区间$(-2^k, -2^{k-1})$内，且 g_i' 小于或等于$(255-2^k)$，则用 g_i' 加 2^k 的值来替换原来的灰度值 g_i'，误差区间由$(-2^k, -2^{k-1})$ 变成$(0, 2^{k-1})$。这种调整发生在含密图像的高(8-k)位，不改变最低k位(k-$LSBs$)的值，因此接收方提取秘密信息时，直接提取最低k位即可恢复秘密信息。像素值调整后，含密图像与载体图像的差别明显减小。

3 伪随机置乱

考虑如下的CML[4]时空混沌映射：

$$y_{n+1}(i)=(1-\varepsilon)f(y_n(i-1))+\varepsilon f(y_n(i)) \quad (1)$$

式中，i=1,2,…,L(L为格子大小)，n为离散时间坐标，ε为耦合系数，边缘条件满足$y_n(L+i)=y_n(i)$，映射子函数选用一维混沌系统Logistic：

$$f(y)=1-ay^2$$

此时，CML为L维动力系统。取空间维数L=3，耦合系数 ε=0.99。当a=1.945 68 时，系统(1)是超混沌的，且序列$y_n(1)$ 与$y_n(3)$的互相关函数呈快速衰减。利用序列$y_n(1)$及$y_n(3)$生成无碰撞伪随机置换序列，用来对载体图像进行伪随机置乱及反置乱。

时空混沌序列对初值极为敏感，即使密钥值在 14 位有效数字内取最小的变化量，产生的序列的相关性仍接近 0，可以达到密码学的要求。三维CML系统中，密钥空间的大小为 $\#(K)=2\times10^{42}\approx2^{140}$，保证了隐藏信息的安全性。

4 信息的嵌入与提取

将载体图像的复杂性分析与低位替换的优化调整相结合，可以使含密图像获得更好的视觉隐蔽性。通过对载体图像的置乱变换，更增加了信息隐藏的安全性。信息嵌入的具体过程如下：

(1)对载体图像 C 进行复杂性分析，生成嵌入深度矩阵 $B(i,j)$，计算信息嵌入空间(比特)。

(2)设定密钥($y_0(1)$，$y_0(2)$，$y_0(3)$)。其中$y_0(1)$，$y_0(2)$，$y_0(3)$为CML映射的初始值。利用式(1)的CML映射产生的时空混沌序列$y_n(1)$及$y_n(3)$ (n=0, 1, 2, …)，生成二维无碰撞伪随机置换序列，对载体图像C的像素和嵌入深度矩阵$B(i,j)$ 的元素按相同的随机顺序分别进行置乱，得到置乱的载体图像C_1和置乱的嵌入深度矩阵$B_1(i,j)$。同时，利用式(1)产生的时空混沌序列$y_n(2)$(n=0, 1,, 2, …)，生成二进制伪随机序列流$\{b_i \mid b_i\in$0、1，i=0,1,…$\}$。序列长度为载体图像信息嵌入空间的 大小。

(3)将秘密数据M嵌入到置乱的载体图像C_1中。秘密数据是一组比特流，比特流的长度应少于或等于载体图像的嵌入空间(比特)。嵌入秘密数据时，首先将秘密数据与二进制伪随机序列流$\{b_i \mid b_i\in$0、1，i=0,1,…$\}$相异或，异或结果记为M'，再将M'嵌入到C_1中。嵌入的具体做法是，按相同的顺序读取$B_1(i,j)$的元素及 C_1的像素，令读取的$B_1(i,j)$的元素的值为k，若k值为 0，则相应的C_1的像素位不嵌入数据，若k值不为 0，则依序截取M'中的k比特信息，将其嵌入 C_1的相应的像素的最低k位，并进行像素值的优化调整。

(4)将嵌入秘密数据的置乱图像C_1进行反向置换(置换的逆过程)，得到最终的含密图像。

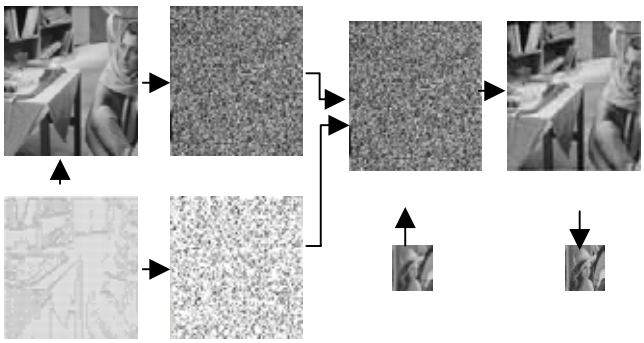
接收端提取信息时，首先要进行含密图像的复杂性分辨及含密图像与嵌入深度矩阵的置乱，然后从置乱的含密图像中提取秘密信息。基于含密图像产生的嵌入深度矩阵与基于载体图像产生的嵌入深度矩阵是相同的，这是因为每个嵌入数据的像素的 8 个相邻的像素是没有改变的。

5 实验结果

以标准测试图像$Barbara$ (120×120)为载体图像，$Lena$ (36×36)为秘密信息，置换及反向置换的密钥($y_0(1)$，$y_0(2)$，$y_0(3)$)取(0.5，0.2，0.83)。图 1 给出嵌入过程在不同阶段的表现及信息嵌入与提取的实验结果。上排左起分别是载体图像、置乱的载体图像、在置乱的载体图像中嵌入秘密信息后的图像及反向置换后得到的最终的含密图像；下排左起分别是与载体图像相对应的嵌入深度矩阵(嵌入深度矩阵元素 0、3、4、5 分别被表示为灰度级的值 255、120、60、0)、置乱的嵌入深度矩阵、预嵌入的秘密图像及接收端从含密图像中提取出的秘密图像。实验结果表明，在不知道置换密钥的情况下，从重置的载体图像和嵌入深度矩阵中提取秘密数据是非常困难的。信息隐藏具有很好的视觉不可见性，丝毫看不出图像质量的变化。

图 1 信息嵌入与提取过程

选择复杂程度不同的大小均为 120×120 的 5 幅标准测试图像 Baboon 、barbara、Sailboat、Lena 及 Airplane 作为载体



图像，以随机序列作为嵌入数据。5 幅载体图像的纹理复杂程度依次降低。

表 2 信息嵌入特性

载体图像 (120*120)	嵌入空间 (bits)	嵌入空间占载体图像的百分比	简单低位替换 PSNR(dB)	优化低位替换 PSNR(dB)	△PSNR(dB)
Baboon	13 917	12.08%	36.62	37.97	1.35
barbara	12 353	10.72%	40.54	41.73	1.19
Sailboat	12 317	10.69%	40.14	41.54	1.39
Lena	12 000	10.41%	40.47	42.06	1.59
Airplane	11 663	10.12%	41.50	43.03	1.53

表 2 给出 5 种不同的载体图像的信息嵌入空间、信息嵌入空间占载体图像的百分比，并对在各载体图像中的可嵌信息位进行简单低位替换及优化低位替换的峰值信噪比(*PSNR*)进行了比较。可以看出，纹理复杂的图像的信息嵌入空间大。优化低位替换得到的 *PSNR* 比简单低位替换得到的 *PSNR* 明显要大。

6 结论

本文结合视觉特性在图像中进行秘密信息的嵌入。图像复杂性分析采用了硬 *c* 均值聚类方法，对载体图像的分辨更细致。通过对低位替换的优化调整，使秘密信息隐藏在载体图像的复杂区域的低 5 位，也不会产生引人注意的载体图像质量的变化。与文献[5]相比，在图像的隐藏量和图像质量上都有很大的改进。采用基于时空混沌映射的空间置乱技术对载体图像进行置换及反向置换，对秘密信息提供了有效的安全防护手段。实验结果表明，本文方法在改善图像质量及视觉隐蔽性上都取得了较好的结果。

参考文献

1 Petitcolas F R P, Anderson R J. Information Hiding——A Survey[J]. Proceedings of the IEEE, 1999, 87(7): 1062-1078.

2 Wang R Z, Lin C F, Lin J C. Image Hiding by Optimal LSB Substitution and Genetic Algorithm[J]. Pattern Recognition, 2001, 34(3): 671-683.

3 Chi-Kwong Chan, Cheng L M. Hiding Data in Images by Simple LSB Substitution[J]. Pattern Recognition, 2004, 37(3): 469-474.

4 杨维明. 时空混沌和耦合映像格子[M]. 上海: 上海科学技术教育出版社, 1994.

5 Maniccam S S, Bourbakis N. Lossless Compression and Information Hiding in Images[J]. Pattern Recognition, 2004, 37(3): 475-486.

(上接第 151 页)

```
X509_REQ *req; X509_NAME*subj; int nid; X509_NAME_ENTRY *ent
struct entry{char *key="countryName";unsigned char value[1024]="CN";}
nid = OBJ_txt2nid(entry.key)//把 countryName 字段转化为对应的//NID
ent=X509_NAME_ENTRY_create_by_NID(NULL,nid,MBSTRING_ASC,entry.value,-1) //从 NID 创建 ENTRY
X509_NAME_add_entry(subj, ent, -1, 0)//把国家信息赋给 subj
X509_REQ_set_subject_name(req, subj)//向请求对象 req 中赋值
```

这样可依次把用户主体属性加入 req 中，接下来加入用户公钥（上一步生成的 pRsakey）和用户备用名。

```
X509_REQ_set_pubkey(req, pRsakey);//向证书请求中加载用户//的公钥
//加载用户备用名
X509_EXTENSION *ext;
STACK_OF(X509_EXTENSION) *extlist;
char *name = "subjectAltName";
char *value = "DNS:bupt.edu.cn";
extlist = sk_X509_EXTENSION_new_null();
ext = X509V3_EXT_conf(NULL, NULL, name, value);
sk_X509_EXTENSION_push(extlist, ext);
X509_REQ_add_extensions(req, extlist);
sk_X509_EXTENSION_pop_free(extlist,509_EXTENSION_free);
//用用户的私钥对上面的 req 进行签名。
digest = EVP_sha1();//选择签名算法
X509_REQ_sign(req, pRsakey, digest)
//把证书请求写入目标文件
PEM_write_bio_X509_REQ(bioreq, req)//要用 BIO 句柄
```

这样就生成了一份完整的证书请求，接下来要以这份证书请求为基础来生成用户证书（见图 2）。

4 结束语

作为当前网络研究和应用开发的热点，SIP 技术在 VoIP 等领域取得了很快发展，然而 SIP 协议的安全机制还不够完善。本文提出在 SIP 电话中结合使用加密和身份认证技术，提高了网络对流媒体传输的安全性；通过构建认证中心，在 Windows 系统上实现了用于 SIP 电话的认证加密系统，该系统显示了很好的语音连续性，并且语音清晰度很高，确保了通话的质量和保密性；本程序使用标准 C 编写，而 OpenSSL 也是用标准 ANSI C 编写，具有源代码级的跨平台性，只需做少量的改动，就可以把它用于 Linux 系统。

参考文献

1 Boneh D, Franklin M. Identity Based Encryption from Weil Pairing[C]//Proc. of CRYPTO'01. Berlin: Spinger Verlag, 2001: 213-229.

2 刘 刚, 侯 宾, 廖 伟, 等. IBE 构建 VoIP 系统中的私钥分发和认证方案[C]//第 20 届全国计算机安全学术交流会议论文, 西宁. 2005-08-05.

3 李新国, 葛建华, 赵春明. IBE 公钥加密系统的用户私钥分发方案[J]. 西安电子科技大学学报(自然科学版), 2004, 31(4): 569-571.

4 张浩然, 曾文萧, 蒋同海. 用 Java 和 OpenSSL 实现认证中心[J]. 计算机应用与研究, 2004, 21(5): 157-159.