第 32 卷 第 7 期 计 算 机 工 程 2006 年 4 月
Vol.32 № 7 Computer Engineering April 2006
• 安全技术 • 文章编号：1000—3428(2006)07—0135—03 文献标识码：A 中图分类号：TP309.02

基于混沌加密的一种图像信息隐藏传送方法

刘年生[1]，郭东辉[2]
（1. 集美大学计算机工程学院，厦门 361021；2. 厦门大学物理系，厦门 361005）

摘 要：提出了一种新的基于混沌加密的图像信息隐藏传送方法，即将混沌序列作为一种类噪声的扩谱序列，把所要传送的敏感信号以白噪声形式的扩谱信号调制隐藏在载体图像中进行安全通信。与 LSB 和 MSB 等传统的图像信息隐藏方法相比，该新方法在信息隐藏的容量、不可觉察性、安全性和鲁棒性等性能方面有较大的提高。文章具体介绍了该方法的加密算法原理，并定义了图像信息的完整性和差异不可觉察性来分析定量分析该方法优点，最后，给出了计算机仿真验证的结果。

关键词：信息隐藏；混沌序列；加密算法；小波变换

Transmission Method of Image Information Hiding Based on Chaotic Encryption

LIU Niansheng[1], GUO Donghui[2]
（1. College of Computer Engineering, Jimei University, Xiamen 361021; 2. Department of Physics, Xiamen University, Xiamen 361005）

【Abstract】 This paper proposes a new transmission method of image information hiding scheme based on chaotic encryption. Chaotic sequence is regarded as a noise-like spread sequence, and the secret signal to be transmitted is modulated and hidden in the covert image as a white noise to implement secure communication. The new scheme is better than LSB or MSB in the imperceptibility, capacity, security and robustness of information hiding. The encryption principle of new algorithm is firstly introduced in this paper, and the merits of new scheme are quantitatively analyzed by defining integrality and imperceptibility of image information. The results of validation by computer simulation are described in the end.

【Key words】 Information hiding; Chaotic sequence; Cryptography; Wavelet transform

传统的图像信息隐藏算法如 LSB 和 MSB 等都是基于载体图像的空间域的[1,2]，因而，这些算法都存在安全性差、鲁棒性差和隐藏容量小等问题，本文提出一种新的基于混沌序列的图像信息加密隐藏算法，可将多幅机密图像分别与相应的混沌序列相乘得到一个具有伪随机噪声性质的扩频信号，把该信号以小噪声的方式添加到载体图像的变换域中，可实现高安全性大容量的网络保密通信。

在新方案中利用小波变换来进行载体图像的正变换与逆变换，小波变换是近来的一个研究热点[3]，它可以将载体图像分解为多个分量与层次，便于在不同分量或层次中进行多幅机密图像的隐藏；值得注意是当多幅机密图像隐藏在同一分量中时，则存在机密图像之间的相互干扰问题。

为了减少被隐藏在同一分量中多幅机密图像之间的相互干扰，就要求所采用的混沌序列具有 δ 函数性质，而由 Chebyshev 映射所产生的混沌序列可以较好地满足这一要求，Chebyshev 映射是一个经典的混沌系统，它所产生的混沌序列从理论上已被证明具有良好的自相关特性[4]，同时，由正交基化所得到的混沌序列矩阵比较接近于 Hadamard 矩阵，可有效较少隐藏在同一分量中多幅机密图像之间的相互干扰。

1 隐藏加密方案

基于小波变换的多幅图像信息隐藏方案如图 1 所示，它包含两部分：即信息的隐藏与提取。

（1）信息的嵌入

对于灰度图像而言，可用一个二维的矩阵来表示图像中的每个像素值，假设用矩阵 A 表示为所选择的原载体图像，当载体图像经过二维离散小波（2D-DWT）变换后产生 4 个分量，用 B 来表示，即

$$B=[cA,cH,cV,\mathrm{cD}]=dwt2(A) \quad (1)$$

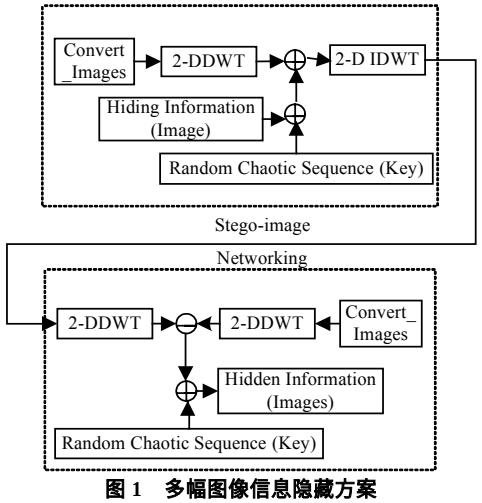


图 1 多幅图像信息隐藏方案

这里以 4 幅为例来说明，用 C_i（i=1, 2, …, n）表示所要隐藏的信息图像，用 R_i 表示混沌系统所产生的混沌随机矩阵，为了简便起见，不妨令 C_i 和 R_i 为同阶的方阵，则有

基金项目：国家自然科学基金资助项目(69886002, 60076015)；福建省自然科学基金资助项目(A0010019)

作者简介：刘年生（1967—），男，博士、副教授，主研方向：网络安全通信，人工智能；郭东辉，博士、教授、博导

收稿日期：2005-04-01 **E-mail：**nsliu163@163.com

$$D_i = C_i * R_i \tag{2}$$

D_i 就具有 R_i 的伪随机性；然后叠加到 B 中，即

$$E = [cA + K * D_1, \mathrm{cH} + K * D_2, \mathrm{cV} + K * D_3, \mathrm{cD} + K * D_4] \tag{3}$$

在式（3）中，K 为信息隐藏的加权系数。将 E 进行二维离散小波逆变换得到 F，即

$$F = idwt\ 2(E) \tag{4}$$

然后对 F 进行 8 位无符号的量化就得到灰度隐密图像 G，即

$$G = u\,\mathrm{int}8(F) \tag{5}$$

这样 C_i 就隐藏在 G 中，G 就通过公共网络系统传输给信息的接收方。一般用肉眼很难判断出它是隐密图像。

（2）信息的提取

信息的接收方在收到隐密图像 G 后先进行二维离散小波变换后得到 H，即

$$H = dwt2(G) = [cA', \mathrm{cH}', \mathrm{cV}', \mathrm{cD}'] \tag{6}$$

然后，将已存的原图像 A 进行二维离散小波变换后得到 B，即式（1），从 H 中减去 B，将其差除以加权系数 K 就得到 I，即

$$I = \begin{cases} (cA' - cA)/K \\ (cH' - cH)/K \\ (cV' - cV)/K \\ (cD' - cD)/K \end{cases} \tag{7}$$

I 与 R_i 的转置矩阵 R_i' 相乘进行相乘，得到所嵌入的信息 J_i，即

$$J_i = I * R_i' \tag{8}$$

将 J_i 以灰度图像的方式显示出来，即

$$Q_i = u\,\mathrm{int}8(J_i) \tag{9}$$

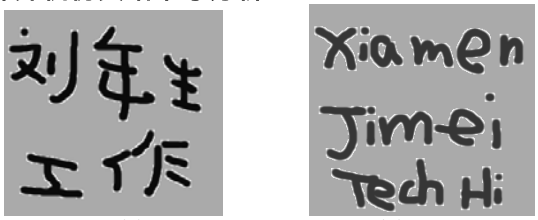
Q_i 就是对原图像 C_i 的近似恢复，即提取出所隐藏的图像；从上述算法过程可以推导出，只有当混沌序列之间满足如下条件

$$\langle R_i', R_j \rangle = \sum_j (R_j * R_i') = G^2 * \delta_{ij} \quad （G^2 为 R_i * R_i' (i=1，2，\ldots)$$

$$\delta_{ij} = \begin{cases} 1, & 当 i = j 时 \\ 0, & 当 i \neq j 时 \end{cases}$$

时，Q_i 才接近原图像 C_i。

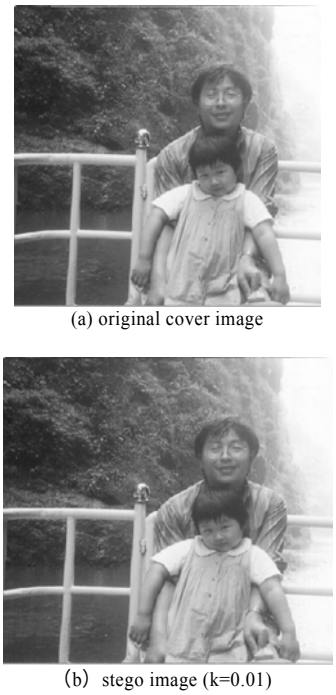
2 计算机仿真结果与分析



（a）C_1　（b）C_2　（c）C_3　（d）C_4

图 2　4 幅被隐藏的机密图像

在计算机仿真模拟过程中，4 幅被隐藏的机密图像如图 2 所示，原始载体图像和所得到的相应的隐密载体如图 3 所示，下面就仿真结果进行分析讨论。



(a) original cover image

(b) stego image (k=0.01)

图 3　原始载体图像和所得到的相应的隐密载体

2.1 不可觉察性与隐藏容量

在信息隐藏技术中不可觉察性是最重要的性能指标之一，对本算法而言，就是要求原载体图像和隐密图像之间的差异不被人眼或计算机所发现，这里用图像的相关系数 r 来定量评价这一指标。两图像之间的相关系数 r 的定义如下：

$$\gamma = \frac{\sum_m \sum_m (A_{mm} - \bar{A})(G_{mm} - \bar{G})}{\sqrt{(\sum_m \sum_m (A_{mm} - \bar{A})^2) * (\sum_m \sum_m (G_{mm} - \bar{G})^2)}} \tag{10}$$

在式（10）中，$\bar{A}$ 和 $\bar{G}$ 分别为图像 A 和 G 的平均值，对 C_i 和 Q_i(i=1,2,3,4)也有类似的定义。

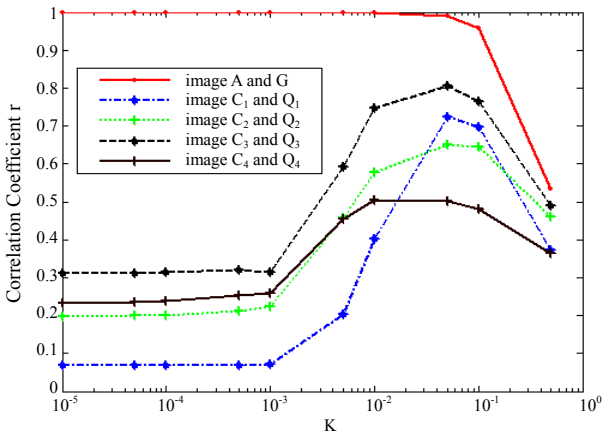
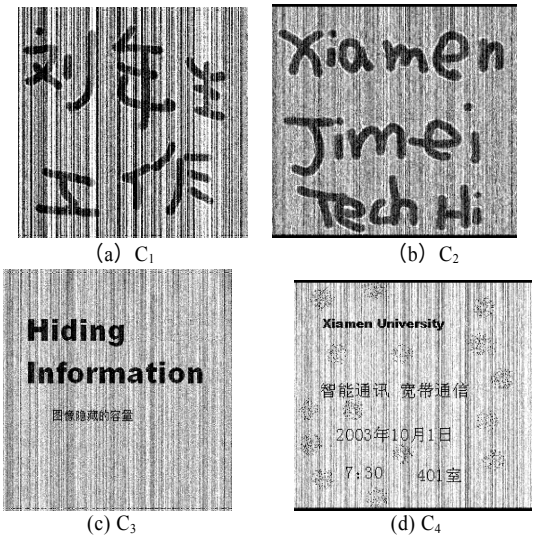


图 4　两图像之间相关系数随加权系数 K 的变化

两图像之间相关系数随加权系数 K 的变化分别如图 4 所示。在图 4 中，在加权系数 K 为 0.01 时，即使同时隐藏了 4 幅机密图像，原载体图像与隐密图像之间相关系数保持在比较高的水平，为 0.999 52，即表示所隐藏的信息具有较高的不可觉察性，人眼看不出两者间的差别；对二者间的其他图像参数统计处理，结果发现也相差甚微，相对误差均低于 0.1%，这样就增加了途中攻击者的检测难度；同时，在加权

系数 K 为 0.01 时，尽管所提取的 4 幅被隐藏图像相关系数虽然不是最高的，但是还可以看清原图像的主要内容，如图 5 所示，4 幅图像都能被提取出来，主要信息都没有任何丢失，都可以看得清楚。但是与图 2 所示原始图像相比还是存在一定的差距，这主要是由于图像的量化噪声和小波变换（正变换和逆变换不完全互逆）所引起的噪声造成的。当然，也应看到，当所提取的图像与原图像之间的相关系数达到最大时，K=0.05 左右，隐密图像与原载体图像之间的相关系数为 0.989 02，低于 0.996 的这一临界值，所得到的隐密图像出现了明显的条纹，很容易让人觉察到它是被处理过的，这样就破坏了图像信息隐藏技术所要求的不可觉察性。



(a) C_1　(b) C_2　(c) C_3　(d) C_4

图 5　被提取的图像

如果一幅载体图像的隐藏容量定义为在隐密图像与原图像之间保持良好的不可觉察性的条件下可有效提取出机密图像的最小信噪比，即

$$SNR = 10 * \log_{10}^{(S/N)} \tag{11}$$

其中，S 和 N 分别表示图像信号与噪声的功率。载体图像的噪声主要来自图像正变换和逆变换所产生的误差、图像显示量化时所造成的噪声和因隐藏机密图像所产生的噪声。而对于被提取的机密图像而言，它的噪声来源除了图像变换所产生的误差和示量化显示时所造成的噪声外，还有被隐藏机密图像之间的相互影响，使得原始机密图像和被提取后的机密图像产生差异，如果要求这二者之间相关系数 r 不能小于某一临界值 r_{min}，即让被提取后的机密图像能较好地恢复出原始的信息内容，并忽略载体图像的变换噪声和量化噪声，则可以容易地计算出一幅载体图像的隐藏容量大小。

2.2 机密图像的安全性

从机密图像的提取过程可以看到，混沌序列不仅起着扩频的作用，增加攻击者的检测难度，还起着密钥作用，对于任何第三者，只有准确地知道混沌序列，他才能提取出相应的机密图像[5]，而混沌序列是由 Chebyshev 映射的系统参数和初始状态所决定的，这些参数对外是严格保密的。在实验中用一个近似混沌序列代替实际的混沌序列，即 Chebyshev 映射的系统参数相同，但两初始状态之间的相对误差仅为 0.1%，结果提取不出所隐藏的机密图像。

一般常用的密码分析方法如差分分析和线性分析等对 Chebyshev 映射是不可行的，因为 Chebyshev 映射是个非线性的混沌系统，对系统参数和初始状态的变化是敏感的；而穷举搜寻方法在计算上是不可行的，即使是对有限精度的普通计算机而言，其计算的困难性随混沌序列的长度而呈指数方式增加。就目前情况而言，能有效分析出 Chebyshev 映射所产生的混沌序列的方法还未见相关报道，该方案的安全性是可靠的。

由于机密图像是以小噪声的形式添加在载体图像的小波变换域中，因此，在隐密图像的空间域或频域中要完全除掉机密图像是比较难的[4]，与 LSB 方法相比，新方案具有更好的信息隐藏鲁棒性。

2.3 分量图像隐藏的次序

当然，有时需要被隐藏的图像不是 4 幅，这就要分为两种情况，一种是当所需要被隐藏的图像少于 4 幅时，则应优先将其隐藏在载体图像经小波变换后的水平分量（cH）、对角线分量（cD）和垂直分量（cV）中，这是因为近似分量（cA）是代表图像信号的低频系数，而水平分量、对角线分量和垂直分量是表示图像信号的高频系数，主要刻画图像的细节部分，被隐藏的图像是以噪声的形式加入到图像中，放置高频部分对载体图像质量的影响会相对小一点，提取后的图像效果也不错。另一种情况是当所需要被隐藏的图像多于 4 幅时，就采用多尺度二维离散小波变换，把载体图像信号分解为多层，把每幅图像分别隐藏在不同层次上，这样也可以避免被隐藏图像之间的相互干扰。

3 结论

根据混沌学和小波变换理论，本文提出了一种新的图像信息隐藏方案，将多幅机密图像以小噪声的形式隐藏在载体图像的小波变换域中，引入 CDMA 多户用检测原理，让不同的合法接收者可提取相应不同的机密图像信息，提取后的机密图像能较好地保持原有图像的主要内容。所引入的混沌序列起着密钥和机密信号白噪声化双重作用；与 LSB 和 MSB 等方法相比，新方案在信息隐藏的安全性、容量和鲁棒性等技术性能方面有较大的提高，这些从计算机仿真结果中得到验证。同时，计算机的仿真结果也证实这一新方案是可行的，在今后，随着光频分复用技术的实用化，就有可能利用本算法直接在光域中进行图像的混沌加密与隐藏。

参考文献

1 Chang C C, Lin M H, Hu Y C. A Fast and Secure Image Hiding Scheme Based on LSB Substitution[J]. International Journal of Pattern Recognition and Artificial Intelligence, 2002, 16(4):399-416.

2 任智斌, 隋永心, 杨英慧等. 以图像为载体的最大意义位（MSB）信息隐藏技术的研究[J]. 光学精密工程, 2002, 10(2):182-187.

3 Weeks M, Bayoumi M. Discrete Wavelet Transform: Architecture, Design and Performance Issues[J]. The Journal of VLSI Signal Processing, 2003, 35(2):155-178.

4 Tohru K, Tsuneda A. Statistics of Chaotic Binary Sequences[J]. IEEE Transactions on Information Theory, 1997, 43(1):104-112.

5 Kim K T, Kim J H, Kim E S. Multiple Information Hiding Technique Using Random Sequence and Hadamard Matrix[J]. Optical Engineering, 2001, 40(11): 2489-2494.