文章编号: 1001-0920(2004)07-0827-04

基于图像库的图像和视频安全传输方案

廉士国, 孙金生, 王执铨
(南京理工大学 自动化系, 江苏 南京 210094)

摘 要: 基于量化编码、分形编码、图像马赛克编码的发展和成熟, 提出一种基于图像库编码的图像和视频安全传输方案, 通过隐藏图像库、置乱图像库和加密编码码流实现不同的安全保密等级. 同时, 图像库由收发方事先保存, 传输的数据量较少, 容易实现高效快速传输. 理论分析和实验结果表明, 此方案具有较高的安全性. 因此适用于安全性和实时性要求高的图像或视频传输中.

关键词: 图像加密; 图像编码; 图像传输
中图分类号: TP309.7 **文献标识码**: A

A secure image or video transmission scheme based on image library

LIAN Shi-guo, SUN Jin-sheng, WANG Zhi-quan
(Department of Automation, Nanjing University of Science and Technology, Nanjing 210094, China. Correspondent: LIAN Shi-guo, E-mail: sg_lian@163.com)

Abstract: According to the development and wide application of vector quantization encoding, fractal encoding and image mosaic encoding, a secure transmission scheme based on image library for image or video is proposed. The scheme can realize different security levels by hiding image library, confusing image library or encrypting encoded data stream. For the image library is stored by the sender and receiver before hand, the data to be transmitted is less and it is easier to gain high transmission speed. Theoretical analyses and experiment results show that the algorithm is of high security. Thus, it is suitable for image or video transmission with requirements of high security and high speed.

Key words: image encryption; image encoding; image transmission

1 引 言

随着网络和多媒体技术的发展, 图像、视频等多媒体数据在现实生活中的应用越来越广泛, 同时对多媒体数据安全性提出了要求. 数据加密是实现安全传输的有效方法, 但传统的数据加密算法(DES, RSA, IDEA 等)不能适应多媒体数据的数据量大、实时性等特点. 将加密过程与编码过程相结合的算法, 因为能够满足实时性要求而得到广泛研究. 文献[1]给出一种基于量化编码的图像加密算法; 文献[2]给出一种基于小波零树编码的图像加密方法; 与MPEG 编码相结合的视频加密算法也得到广泛研究[3,4]. 这些算法部分加密编码数据, 保持编码格式不变, 同时满足实时性要求.

考虑到向量量化编码、分形编码、图像马赛克编码等基于图像库编码方法[5~10]的逐步成熟, 给出一种基于图像库编码的图像、视频加密方案, 分析了它

收稿日期: 2003-07-17; **修回日期**: 2003-09-26.
基金项目: 国家自然科学基金资助项目(60174005); 博士点基金资助项目(20020288025); 江苏省自然科学基金资助项目(BK2001054).
作者简介: 廉士国(1978—), 男, 江苏徐州人, 博士生, 从事混沌加密、多媒体信息加密的研究; 王执铨(1939—), 男, 湖北武汉人, 教授, 博士生导师, 从事大系统的理论与应用、信息安全等研究.

的安全性, 以分形编码为例验证了它的可行性

2 安全传输方案

图像或视频数据具有数据量大、实时性要求高等特点, 使用基于图像库的编码方法, 可以降低数据量, 获得较高的压缩比, 这也为数据的安全保密工作提供了方便. 将基于图像库编码方法用于图像和视频的安全传输, 具体方案如图 1 所示

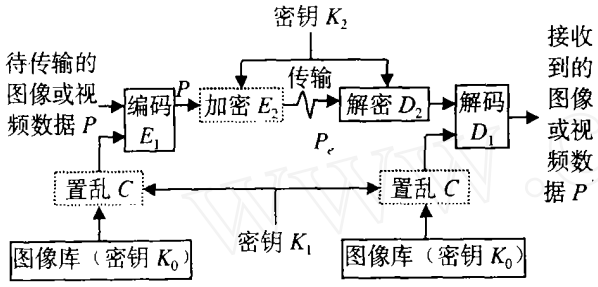


图 1 图像视频安全传输方案

可见, 整个编码过程通过密钥 K_0, K_1 和 K_2 控制. 其中: K_0 是用于编码的图像库, K_1 是图像库置乱密钥, K_2 是码流加密密钥. 其中, 图像库置乱过程和码流加密过程可以根据安全性和实时性要求进行选择

首先, 最简单的编解码过程如下: 待传输的图像或视频数据 P, 根据图像库 K_0 进行基于图像库的编码, 获得编码后的数据 P', 传输过程传送的是编码后的数据 P', 接收方收到 P' 后, 对其进行基于图像库 K_0 的数据解码操作, 得到的解码数据 P'' 即为接收方恢复的图像或视频数据. 即编码和解码操作可表示为

$$E_1(P, K_0) = P', \tag{1}$$

$$D_1(P', K_0) = P''. \tag{2}$$

其中 E_1 和 D_1 分别是基于图像库的编解码过程, 原始数据 P 和解码后的数据 P'' 的一致性由编解码算法自身来保证, 对于常用的向量量化编码、分形编码, 这一条件是可以满足的. 由式(1) 和式(2) 可见, 将图像库 K_0 作为密钥, 则编码过程和解码过程分别可以看作是加密和解密过程, 此加密系统的安全性完全由密钥 K_0 决定

其次, 图 1 中给出了进一步增加安全性的方法, 即在编码或解码前, 先用密钥 K_1 对图像库 K_0 进行置乱, 这种传输方案适用于图像库公开的场合, 此时的安全通信过程可描述为

$$E_1(P, C(K_0, K_1)) = P', \tag{3}$$

$$D_1(P', C(K_0, K_1)) = P''. \tag{4}$$

其中 $C(A, X)$ 表示以 X 为密钥对数据集合 A 进行置乱操作, 此处指对图像库进行置乱操作. 将编解码过程看作加解密过程, 则系统密钥为 $C(K_0, K_1)$, 系统安全性完全由 $C(K_0, K_1)$ 决定. 当图像库 K_0 公开时, 系统安全性由 K_1 决定. 并且, 在密钥 K_0 和 K_1 均正确的情况下, 正确解密的结果 P'' 与原始图像或视频数据相一致, 如式(3) 和式(4) 所示

另外, 加密编码码流可进一步增加系统安全性. 如图 1 所示, 使用密钥 K_2 对编码的数据流加密. 此时的安全通信过程可描述为

$$E_2(E_1(P, C(K_0, K_1)), K_2) = E_2(P', K_2) = P_e, \tag{5}$$

$$D_1(D_2(P_e, K_2), C(K_0, K_1)) = D_1(P', C(K_0, K_1)) = P''. \tag{6}$$

其中 E_2 和 D_2 分别是码流的加解密过程. 加解密过程是无损过程, 即在密钥正确情况下, 解密结果 $D_2(P_e, K_2)$ 与原数据 P' 相同. 因此, 在密钥 K_0, K_1 和 K_2 均正确的情况下, 正确解密的结果 P'' 与原始图像或视频数据相一致, 如式(5) 和式(6) 所示

3 基于图像库的图像和视频编码方法

此处讨论的图像和视频编码方法与电报中的文本编码方式相似, 只是图像和视频编码的码本为一个索引图像库. 应用于图像和视频编码的索引图像库一般通过实验方法产生, 并具有一定通用性, 以保证图像或视频的编码质量. 适用于这类图像或视频编码的方法有量化编码、分形编码和图像马赛克编码等. 其中, 向量量化方法[5], 采用合适的分块或分段方法, 搜索向量量化表, 仅仅存储数据块索引. 适用于向量量化编码的图像库通常由小的图像块组成. 分形编码[6] 以分形理论为基础, 通过存储反映自相关性的变换参数实现图像压缩. 其图像库通常由小的图像块组成. 图像马赛克编码方法[7], 在图像库中搜索与每一分块最相似的图像, 用此搜索到的图像代替相应的图像块, 并进行颜色、形状、角度等的校正, 常用于广告设计等. 其图像库通常由大量的图像组成

向量量化编码、分形编码、马赛克编码也分别被扩展, 并用于视频编码[8~10]. 即通过这些图像编码方法对单帧图像编码, 以降低空间冗余度; 通过运动预测和运动补偿方法进行帧间编码, 以降低时间冗余度. 采用帧间编码的图像, 在解码时需要依赖单独编码的图像, 因此, 加密单独编码的图像, 就破坏了帧间编码图像的正确解码. 可见, 图 1 所示的安全传输方案同样适用于视频数据

4　安全性分析

在图 1 所示的安全传输系统中, 3 种密钥可以实现不同的安全性要求. 从通信的角度看, 编码图像库 K_0 和图像库置乱密钥 K_1 可以认为是信源加密密钥, 码流加密密钥 K_2 是信道加密密钥. 从应用的角度来看, 编码图像库 K_0 是终端密钥, 即每个参与通信的端点均可拥有; 图像库置乱密钥 K_1 是用户密钥, 即每个参与通信的端点可能有多个用户, 其中每个用户拥有不同的密钥; 码流加密密钥 K_2 是通话密钥, 即每个用户在每次通信中可以采用不同的密钥. 这种安全性分级机制能够满足不同的应用要求, 而图像库置乱过程和码流加密过程也可根据实际应用情况决定是否选择. 总之, 同时选择 3 项加密操作, 具有最高的安全性, 适合多个用户、多类型通讯的场合; 不选择码流加密过程, 节省了加密操作时间, 能够保持较高的速度; 仅保留编码图像库 K_0, 而不使用图像库置乱和码流加密过程, 具有相对最快的速度, 但同时要保证图像库的拥有者都有权获取该信息. 通常情况下, 很难保证图像库不泄漏, 因此考虑到安全性, 至少要采用图像库置乱操作.

以上安全传输方案中的图像库 K_0、图像库置乱和码流加密, 对只知密文、已知明文和选择明文等攻击, 具有不同的安全性. 以下将对这 3 种加密过程的安全性分别予以分析.

4.1　隐藏图像库

与电报通信中的码本类似, 在本方案中, 图像库相当于图像或视频传输的码本. 因为码本的尺寸巨大, 穷举攻击是困难的, 而图像库较文本库更为冗长, 对图像库的穷举攻击很困难. 对于已知明文和选择明文攻击, 攻击者可通过选择足够多的合适的明文, 通过差分和统计的方法破译, 在此情况下, 仅仅隐藏图像库是不安全的.

4.2　置乱图像库

对于未知图像库的攻击者, 穷举攻击、已知明文和选择明文攻击的难度等于隐藏图象库时的攻击难度. 对于已知图像库的攻击者, 穷举攻击的工作量就是穷举空间的大小. 如果令图像库大小为 N, 则穷举空间为

$$K(N) = N! \tag{7}$$

其中 $N!$ 表示 N 的阶乘, 如若 $N = 100$, 则 $K(100) = 9.33 \times 10^{157}$. 类似地, 当 $N = 500$ 和 $N = 1\,000$ 时, $K(500) = 1.22 \times 10^{1\,134}$, $K(1\,000) = 4.02 \times 10^{2\,567}$. 事实上, 穷举过程要进行反复的解码操作, 如此大的穷举空间可保证足够的安全性.

4.3　加密编码码流

加密编码码流时, 可采用传统的高强度密码 DES, RSA, IDEA 和 AES 等, 由于它们针对已知明文和选择明文攻击具有较高安全性, 对于未知图像库和图像库置乱密钥的攻击者, 穷举攻击、已知明文和选择明文攻击都是困难的. 对于只知图像库而不知道置乱密钥的攻击者, 穷举空间为

$$K(N) = K_c(N) \cdot K_E. \tag{8}$$

其中: $K_c(N)$ 为式(7) 所示的图像库置乱空间; K_E 为码流加密的加密空间, 一般由所使用的算法决定, 而与图像库无关, 如对于 DES 和 IDEA 算法, K_E 分别为 2^{56} 和 2^{128}. 对于同时拥有正确的图像库和置乱密钥的攻击者, 穷举空间为

$$K(N) = K_E, \tag{9}$$

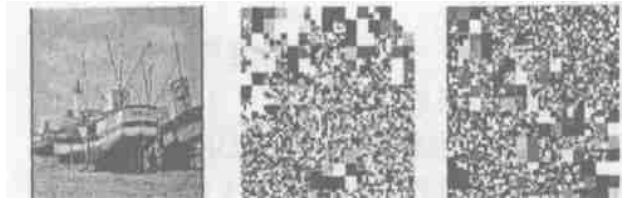
即为所使用的加密算法的密钥空间.

5　实验结果

5.1　加密结果

采用分形编码方法, 选择从动物、风景、人物图像库中截取的 2 000 个 8 × 8 的图像块构成编码图像库. 对多幅图像加密, 解码后的图像完全不可理解. 下面给出对 256 × 256 的图像 Lena 和 512 × 512 的图像 Boats 的实验结果, 如图 2 所示. 可见, 本方案具有很好的加密效果.

(a)　原始图像　　(b)　置乱图像库　　(c)　加密码流



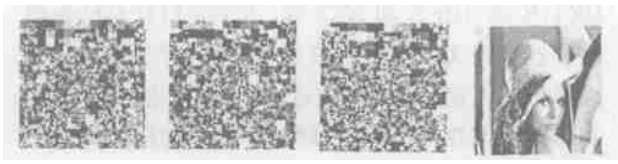
(d)　原始图像　　(c)　置乱图像库　　(f)　加密码流

图 2　图像加密结果

5.2　密钥敏感性

选择与实验 1 中相同的图像库, 采用 3 种加密过程对多种图像加密测试, 表明均具有较高的密钥敏感性. 此处给出, 在只进行图像库置乱、不进行码流加密的情况下加密系统的密钥敏感性, 如图 3 所示. 其中, 图 3(a) 是加密密钥为 1 000 的加密结果, 图 3(b), (c) 和(d) 分别是解密密钥为 1 001, 999 和

1 000 时的解密结果. 可见, 解密密钥相差 1 时, 解密结果就完全不可理解, 因此具有较高的密钥敏感性.



(a) 加密 (b) 解密 (c) 解密 (d) 解密

图 3 密钥敏感性实验

6 结 论

文中提出一种以向量量化编码、分形编码和图像马赛克编码等基于图像库的编码方法为基础的图像和视频的安全传输方案. 理论分析表明, 它具有较高安全性, 并且其多级安全性的特点使其适合多种应用场合. 实验结果表明, 加密方案具有较好加密效果和较高的密钥敏感性. 本文中图像库的选择采用随机抽取的方法, 为了适合更广泛的应用, 可通过统计方法来产生, 这有待继续研究.

参考文献(References):

[1] Chen Tung-shou, Chang Chin-chen, Hwang Min-shiang. A virtual image cryptosystem based upon vector quantization [J]. *IEEE Trans on Image Processing*, 1998, 7(10): 1485-1488.

[2] Cheng Howard, Li Xiaobo. Partial encryption of compressed images and videos [J]. *IEEE Trans on Signal Processing*, 2000, 48(8): 2439-2451.

[3] Tang L. Methods for encrypting and decrypting MPEG video data efficiently[A]. *Proc of the Fourth ACM Int Multimedia Conf (ACM Multimedia '96)* [C]. Boston, 1996. 219-230.

[4] Yen Jiu-cheng, Guo Jiu-in. A new MPEG encryption system and its VLSI architecture[A]. *IEEE Workshop on Signal Processing Systems* [C]. Taipei, 1999. 430-437.

[5] Qiu G, Varley M R, Terrell T J. Image coding based on visual vector quantization[A]. *IEE Conf Publication* [C]. Edinburgh, 1995. 301-305.

[6] Jacquin A. Image coding based on a fractal theory of iterated contractive image transformations [J]. *IEEE Trans Image Processing*, 1992, 1(1): 18-30.

[7] Finkelstein A, Range M. Image mosaics[A]. *Proc of the EP '98 and RIDT '98 Conf* [C]. St Malo, 1998. 11-22.

[8] Lin Ken K, Gray Robert M. Vector quantization of video with two codebooks[A]. *Data Compression Conf Proc*[C]. Snowbrid, 1999. 537.

[9] Lazar M S, Bruton L T. Fractal block coding of digital video [J]. *IEEE Trans on Circuits & Systems for Video Technology*, 1994, 4(3), 297-308.

[10] Litwinowicz P. Processing images and video for an impressionist effect[A]. *Proc of the ACM SIGGRAPH Conf on Computer Graphics*[C]. California, 1997. 407-414.

(上接第 826 页)

4 结 论

本文设计了一种当系统的未建模动态可表示为加性不确定性时的系统辨识最优输入信号设计方法. 取实际输出与根据实际模型设计的理想控制器下输出间误差的平方均值最小作为性能指标. 用正交基函数表示辨识模型, 结合最小二乘法和小增益定理, 给出辨识实验输入信号设计方法. 仿真结果证明了方法的有效性.

参考文献(References):

[1] Gevers M, Ljung L. Optimal experiment designs with respect to the intended model application[J]. *Automatica*, 1986, 22(5): 543-554.

[2] Ljung L. *System Identification: Theory for the User* [M]. 2nd ed. Englewood Cliffs: Prentice-Hall, 1999.

[3] Yucai Zhu, F Butoyi. Case studies on closed-loop identification for MPC [J]. *Control Engineering Practice*, 2002, 10(4): 403-417.

[4] Forssell U, Ljung L. Some results on optimal experiment design[J]. *Automatica*, 2000, 36(5): 749-756.

[5] Cooley B L, Lee J H. Control-relevant experiment design for multivariable systems described by expansions in orthonormal bases[J]. *Automatica*, 2001, 37(2): 273-281.

[6] Van den Hof, Heuberger O M J, Boker P S C. System identification with generalized orthonormal basis functions[J]. *Automatic*, 1995, 31(12): 1821-1834.

[7] 方崇智, 萧德云. 过程辨识[M]. 北京: 清华大学出版, 1998.