

基于小波变换的压缩感知在图像加密中的应用

张爱华,薄禄裕,盛飞,杨培

(南京邮电大学,江苏南京210003)

摘要:利用单层小波变换的压缩感知算法的特点,提出了一种基于斜帐篷映射的混沌图像加密系统的改进方法。加密时,首先应用基于单层小波变换的压缩感知算法对图像进行初始化,然后对初始化后的图像加密。解密时,首先进行加密映射的反变换解密,然后利用正交匹配追踪算法(OMP)对高频系数进行恢复,最后再进行小波反变换重构图像。仿真结果表明,该算法不仅继承了原有系统的优良密码学特性,而且在相同时间条件下,在图像较小失真的情况下大大增加图像加密的安全性。

关键词:压缩感知;图像加密;单层小波变换;斜帐篷映射;混沌序列

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2011)12-0145-03

Compressed Sensing Based on Single Layer Wavelet Transform for Image Encryption

ZHANG Ai-hua, BO Lu-yu, SHENG Fei, YANG Pei

(Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: According to compressed sensing algorithm based on the single layer wavelet transform, a new chaotic cryptosystem method based on skew tent map was proposed. For the encryption, by using the improved compressed sensing algorithm based on the single layer wavelet transform could initialize the image, then the image can be encrypted. For the decryption, decrypt the image first, then by using the orthogonal matching pursuit (OMP) algorithm, high-pass wavelet coefficients could be recovered by the measurements. Then the image could be reconstructed by the inverse wavelet transform. Compared with the original cryptosystem, the proposed cryptosystem inherited the advantages of the original one and it greatly enhances the security of image encryption with small image distortion by using the same time.

Key words: compressed sensing; image encryption; single layer wavelet transform; skew tent map; chaotic sequences

0 引言

近年来,随着计算机网络通信技术和多媒体技术的发展,通过网络传输的数据文件或作品更加容易被盗取,同时解密技术以及软硬件的发展也严重威胁着信息的安全性,因此信息安全问题受到了广泛的关注。目前混沌理论就是被广泛研究和使用的方方法之一。正是由于混沌系统具有的随机性、对初值的敏感性和类似噪声的宽带功率谱密度等优良的密码学特性^[1],使得利用混沌理论实现保密通信成为近年来最为活跃的应用研究领域之一。

而在实际中为了减少加密、解密过程时间,降低存

储、处理和传输的成本,人们常采用高速采样再压缩然后再加密的方法,这就浪费了大量的采样资源。近年来,出现了一种新的理论—compressed sensing(或CS, compressive sampling)^[2,3],即压缩感知,或压缩采样。

1 压缩感知理论概述

传统的信号获取和处理过程主要包括采样、压缩、传输和解压四个部分,在采样过程必须满足奈奎斯特采样定律, $f_s \geq 2f_{\max}$,即采样频率不能低于信号带宽的2倍。

近些年来出现了一种新的理论—compressed sensing(或CS, compressive sampling),即压缩感知,或者压缩采样。而压缩感知核心思想是将压缩与采样合并进行,其利用其他变换空间描述信号,使得在保证信息不损失的情况下,用远低于采样定理要求的速率采样信号的同时,又可完全恢复信号,即将对信号的采样转变为对信息的采样。主要包括信号的稀疏表示、编码测

收稿日期:2011-04-23;修回日期:2011-07-26

基金项目:国家自然科学基金(61070234);南京邮电大学校科研基金(NY210018)

作者简介:张爱华(1969-),女,山西广灵人,副教授,主要研究方向为非线性分析及拓扑动力系统;薄禄裕(1986-),男,硕士,研究方向为非线性分析及其应用。

量和重构算法三个方面。

信号的稀疏表示是如果长度为 N 的信号 X , 在变换域 Φ 中只有 K 个系数不为零(或者明显大于其他系数), 且 $K \ll N$, 那么可以认为信号 X 在 Φ 域中是稀疏的并可称为 K -稀疏。这是压缩感知的条件, 即信号必须可以稀疏表示。常用的稀疏表示方法有离散余弦变换基、小波变换基等。

在编码测量中, 文献[4]指出, 测量矩阵必须满足 RIP (restricted isometry property) 准则, 这个性质保证了观测矩阵不会把两个不同的 K 稀疏信号映射到同一个集合中。最后, 运用重构算法由测量值及投影矩阵重构出原始信号。信号重构过程一般转换为一个最小 l_0 范数的优化问题, 目前的求解算法有匹配追踪法、正交匹配追踪法 (OMP)^[5]、梯度投影法 (GP)、链式追踪法等。

2 基于离散斜帐篷映射的混沌加密理论

2.1 离散斜帐篷映射

帐篷映射是一种简单的混沌系统, 对初值的敏感性和迭代轨道序列的相关性以指数递减, 其轨道序列可以视为贝努利序列, 即具有很强的伪随机特性^[6], 可以直接用于对信息的加密。

斜帐篷映射是一种推广的帐篷映射, 其定义为

$$f_a(x) = \begin{cases} \frac{x}{a}, & 0 < x \leq a \\ \frac{x-1}{a-1}, & a < x \leq 1 \end{cases} \quad (1)$$

其中 $a \in (0, 1)$ 时系统处于混沌状态。

一般的混沌映射是多对一的映射, 文献[7]提出了一种对混沌映射做一一对应的离散化的一般方法, 加密和解密计算将在有限整数集合上进行, 不受精度约束, 实现更加快速。其离散化映射定义为

$$\tilde{F}_A(x) = \begin{cases} \lceil \frac{M}{A} X \rceil, & 0 < X \leq A \\ \lfloor \frac{M}{M-A} (M-X) \rfloor + 1, & A < X \leq M \end{cases} \quad (2)$$

2.2 正弦迭代映射

文中加密采用的另一个混沌系统为式(3)描述的正弦迭代映射系统:

$$x_{n+1} = \sin^2(\text{barcsin} \sqrt{x_n}) \quad (3)$$

其中 $1 < b \in R$, 系统初值 $x_0 \in R$ 且 $0 < x_0 < 1$ 。由式(3)产生的系统的 Lyapunov 指数是 $\ln b > 0$, 因而该系统是混沌的。

2.3 图像像素值替代算法

现有一幅大小为 $M \times N$ 具有 L 级灰度的图像, 设

(i, j) 坐标处的像素值为 $I(i, j)$, 其中 $1 \leq i \leq M, 1 \leq j \leq N$, 则 (i, j) 坐标处的像素值经替代操作后变为 $I'(i, j)$, 即要求设计一个映射 f 使得:

$$f: I(i, j) \rightarrow I'(i, j) \quad (4)$$

为了使替代操作后的像素值 $I'(i, j)$ 具有不可预测性, 替代操作可以由下式表示:

$$I'(i, j) = I(i, j) + \text{Key}(i, j) \bmod L \quad (5)$$

其中 $\text{Key}(i, j)$ 由式(6)的离散混沌系统产生。为了使用于加密的混沌序列对初始值更加敏感, 文中采用正弦迭代预迭代 3000 次后的值作为式(6)的初始值。 $\text{Key}(i, j)$ 具体的值由下面的公式产生:

$$\text{Key}(i, j) = \text{round}((\gamma_n \times 10^4 - \text{round}(\gamma_n \times 10^4)) \times 10^3) \quad (6)$$

其中函数 $\text{round}(x)$ 表示取与 x 最接近的整数值, 利用式(5)实现像素值的替代加密, 对所有的像素点 (i, j) 处的像素值完成替代操作后, 即完成了替代操作。

3 算法设计

常用的图像加密方法有两种: 图像置乱和图像像素值变换^[8]。文中提出的是一种混沌空间域图像加密算法, 第一步为了加快加密过程、节省加密的时间和复杂度先利用基于小波变换的压缩感知算法对图像进行初始化。第二步利用离散斜帐篷映射结合正弦迭代混沌系统对图像通过多次迭代运算实现图像加密。

3.1 图像初始化

在本算法中, 首先利用基于单层小波变换的压缩感知理论^[9,10]对图像进行初始化, 其操作如下:

步骤1 首先将 $M \times N$ 图像分解成 $N \times N$ 的子图像块, 然后对 $N \times N$ 的子图像进行单层小波分解, 得到 $\{LH_1, HL_1, HH_1, LL_1\}$ 4 个小波子带系数。

步骤2 选择合适的 M 值, 构造 $M \times N/2$ 大小的服从 $(0, 1/N)$ 高斯分布的测量矩阵 Φ 分别对 LH_1, HL_1, HH_1 进行测量, 得到相应子带的测量系数值矩阵, 保持低频 LL_1 子带系数不变。

3.2 图像像素值变换

利用 2.3 节中像素值替代法对图像的像素点进行图像像素值变换。

3.3 图像置乱

(a) 采用式(3)的正弦迭代混沌系统产生混沌序列 $\{x_1, x_2, \dots, x_M\}$, 将实值序列 $\{x_1, x_2, \dots, x_M\}$ 中的 N 个混沌值排列, 形成一个新的混沌序列 $\{x_1, x_2, \dots, x_M\}$, 那么原序列 $\{x_1, x_2, \dots, x_M\}$ 中每一个值 x_i 在新序列 $\{x'_1, x'_2, \dots, x'_M\}$ 中都有与之对应的一个位置编号, 因此获得相应的位置编号序列 $\{a_1, a_2, \dots, a_M\}$, 其中 a_i 为 $\{1, 2, \dots, M\}$ 中的一个值。

(b) 采用式(2)的离散斜帐篷混沌映射, 产生混

沌序列 $\{y_1, y_2, \dots, y_N\}$, 运用步骤(a)中的方法, 获得相应的组成位置编号序列 $\{b_1, b_2, \dots, b_N\}$, 其中 b_i 为集合 $\{1, 2, \dots, N\}$ 中的一个值。

(c) 将经过像素值替代操作后的像素点置乱到位置 (a_x, b_y) , 重复多次, 完成像素位置的置乱。

3.4 迭代加密

为了使输出的密文对明文和密钥充分敏感, 将替代设计与置换设计重复进行多轮迭代。

3.5 解密算法实现

步骤1 加密的逆过程, 输入正确的密钥后, 将加密算法逆向运算, 即可获得解密图像。

步骤2 利用 OMP 算法分别重构经过测量后的 3 个高频系数矩阵, 并结合 LL_1 子带进行小波反变换恢复图像。

4 实验分析

选择 256×256 的 lena 图像, 运用 Matlab 实现计算机仿真^[11], 将图像分解成 8×8 的子图像块^[12], 在 Matlab 下进行加密算法实验, 其仿真实验效果如图 1 所示。

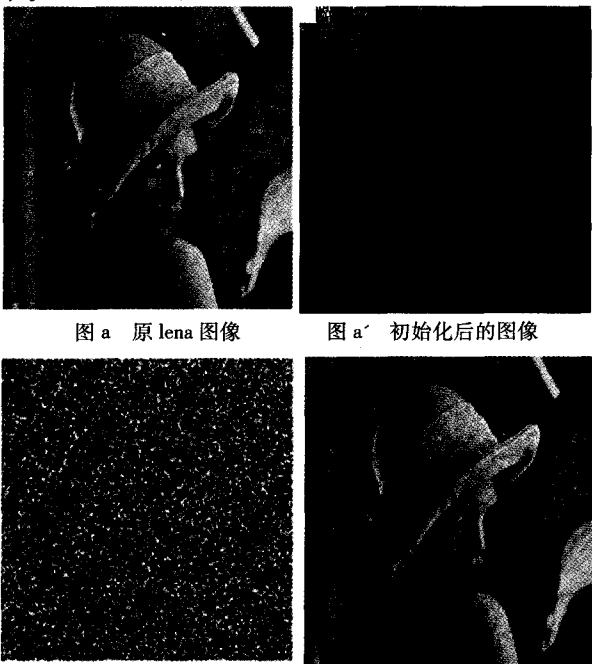


图 a 原 lena 图像 图 a' 初始化后的图像

图 b 加密图像 图 c 解密恢复后的图像

图 1 加密效果图

从明文看, 加密图像需要进行预处理, 这样不但没有增加加密/解密所需时间, 加密图像的安全性反而得到增加, 进而也增加了加密图像被攻击破译的难度。

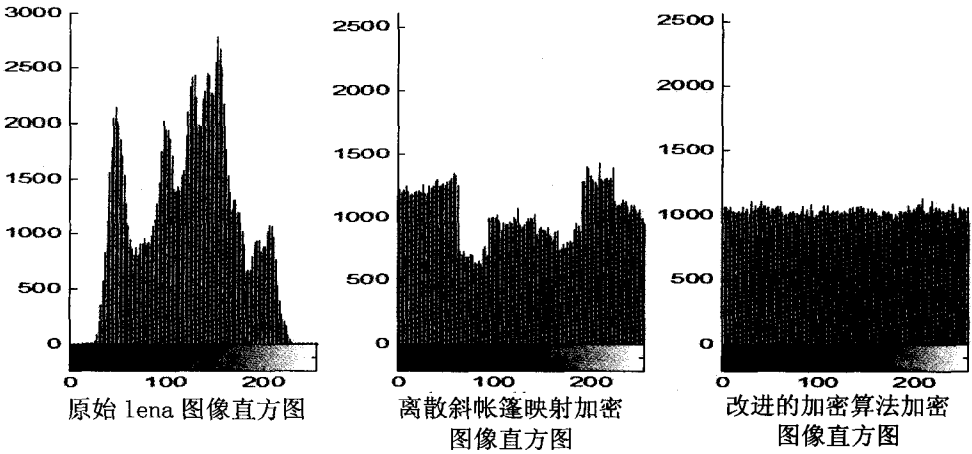


图 2 统计直方图

(2) 统计特性分析。

由图 2 可知, 原始图像的直方图变化起伏大且呈不均匀分布, 经离散斜帐篷映射算法加密后图像的直方图与原始图像的直方图相比要平坦得多, 用改进的加密算法加密后直方图则更加平坦且密文灰度值分布均匀。密文的统计特征与明文的统计特征几乎完全不同, 明文的统计特性被扩散到了密文的均匀分布中, 明文和密文的相关性大大降低。

5 结束语

文中首先简要介绍了压缩感知算法的原理, 提出了一种基于斜帐篷映射的混沌图像加密系统的改进方法—基于小波分析的压缩感知的图像加密方法。改进算法的最大特点是通过运用基于小波分析的压缩感知算法对图像初始化, 提高了加密图像的安全性。对于原有加密系统, 当需要很高的安全程度时, 相应的密钥长度也会增大, 加密、解密过程时间消耗也相应增长。文中的改进方法可以在保证一定失真和时间不增加的条件大大地增加加密图像的安全性。

参考文献:

[1] 胡向东. 应用密码学教程[M]. 北京: 电子工业出版社, 2005: 78-79.

[2] Donoho D. Compressed sensing[J]. IEEE Transactions on Information Theory, 2006, 52(4): 1289-1306.

[3] Candes E. Compressive sampling[C]//Proceedings of the International Congress of Mathematicians. Madrid, Panin: [s. n.], 2006.

[4] Candes E, Romberg J, Tao T. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency

服务是对智能处理后的信息的利用。应用层包含的应用领域较广泛,如:智能家居^[11]、智能电网、智能交通、环境监控等,因此应用层的安全问题主要来自各类新业务及应用的相关业务平台。

2.3.1 应用层面临的主要安全威胁

(1) 恶意代码以及各类软件系统自身漏洞、可能的设计缺陷,黑客,各类病毒是物联网应用系统的重要威胁。

(2) 物联网涉及范围广,目前海量数据信息处理和业务控制策略方面的技术还存在着安全性和可靠性的问题。

2.3.2 应用层的主要安全防范措施

应用层的安全从读取控制、用户认证、使用的不可抵赖性^[12]等几个方面考虑。

相应的安全措施包括:

(1) 在应用层设备中嵌入身份认证机制,对不同的用户赋予不同的权限,进而对数据进行访问控制,阻断非授权用户对资源的非法访问。

(2) 对网络层传来的数据进行过滤,以防止恶意代码、病毒等不良信息对应用层的破坏。

(3) 物联网用户在使用物联网和电脑时提高个人隐私保护意识,用户在删除重要的文件或处理废弃的电脑时,一定要对文件和电脑硬盘做不可恢复性处理^[13]。

(4) 定时进行系统安全漏洞检查,实行攻击监控、备份与恢复机制。

3 结束语

物联网安全问题制约了它的广泛应用,关于物联网的安全机制在业界也没有统一的方案,文中通过对物联网各层的不同特点与面临威胁的分析,在数据安全与隐私保护、节点安全保护与认证、信息安全通信、访问控制与系统安全保障策略等方面提出了各层的安

全防范措施。当然,物联网的安全不仅是一个技术问题,还需要有一系列与之配套的政策、法律法规和完善的的安全管理制度。

参考文献:

- [1] The Internet of Things[EB/OL]. 2009-09-06. <http://www.itu.int>.
- [2] International Telecommunication Union. The Internet of Things[R]. [s.l.]:[s.n.], 2005.
- [3] 杨庚,许建,陈伟,等. 物联网安全特征与关键技术[J]. 南京邮电大学学报(自然科学版), 2010, 30(4): 20-29.
- [4] 王志良. 物联网现在与未来[M]. 北京:机械工业出版社, 2010.
- [5] 陈柳钦. 物联网:国内外发展动态及亟待解决的关键问题[EB/OL]. 2010. www.chinavalue.net/Article/Archive/2010/8/10/192271_13.html.
- [6] 吴同. 浅析物联网的安全问题[J]. 网络安全技术与应用, 2010(8): 7-8.
- [7] 沈苏彬,范曲立,宗平,等. 物联网的体系结构与相关技术研究[J]. 南京邮电大学学报(自然科学版), 2009, 29(6): 1-10.
- [8] 李志华,许榕生. 物联网安全保卫战[J]. 计算机世界, 2010(26): 1-4.
- [9] 四大关键技术保卫物联网安全不受威胁[EB/OL]. 2010-07-19. http://miit.ccidnet.com/art/32559/20100719/2120335_1.html.
- [10] 武传坤. 物联网安全架构初探[J]. 中国科学院院刊, 2010, 25(4): 411-419.
- [11] Taylor A, Harper R, Swan L, et al. Homes that make us smart[J]. Personal and Ubiquitous Computing, 2007, 11(5): 383-393.
- [12] 叶青. 物联网安全问题技术分析[J]. 网络安全技术与应用, 2010(10): 32-33.
- [13] 聂学武,张永胜,骆琴,等. 物联网安全问题及其对策研究[J]. 计算机安全, 2010(11): 4-6.

(上接第147页)

- information[J]. IEEE Transactions on Information Theory, 2006, 52(4): 489-509.
- [5] Tropp J, Gilbert A C. Signal recovery from random measurements via orthogonal matching pursuit[J]. IEEE Transactions on Information Theory, 2007, 53(12): 4655-4666.
- [6] Masudo N, Aihara K. Cryptosystems based on space discretization of chaotic maps[J]. IEEE Trans on Circuits and Systems-I, 2002, 49(1): 28-40.
- [7] Chen Y, Liao X F, Wong K W. Chosen plaintext attack on a cryptosystem with discretized skew tent map[J]. IEEE Trans on Circuits and Systems-II, 2006, 53(7): 527-529.
- [8] 邓绍江,李传东. 混沌理论及其在密码学中的应用[J]. 重庆建筑大学学报, 2003(5): 82-83.
- [9] 岑翼刚,陈晓方,岑丽辉,等. 基于单层小波变换的压缩感知图像处理[J]. 通信学报, 2010, 31(8A): 52-55.
- [10] 张锐. 基于压缩感知理论的图像压缩初步研究[J]. 电脑与技术, 2010, 6(4): 58-59.
- [11] 罗军辉. MATLAB7.0在图像处理中的应用[M]. 北京:机械工业出版社, 2005.
- [12] 李传目,洪联系,万春. 基于混沌序列的图像分块加密方法[J]. 计算机技术与应用, 2007, 17(8): 51-54.