

混沌压缩感知算法的设计与实现

专业：信息安全 班级：2013211627 学生姓名：赵秋涵

指导老师：彭海朋 职称：副教授

摘要

混沌压缩感知是压缩感知的重要发展方向。它基于混沌系统的良好特性，由混沌序列构建混沌观测矩阵完成压缩感知过程。

本文围绕混沌压缩感知算法的核心问题——混沌观测矩阵展开，给出不同混沌观测矩阵等距约束性(Restricted Isometry Property, RIP)的证明，用统计学方法确定了低计算复杂度下的最优采样步长，通过分析提出了混沌观测矩阵的优化构建方法，对混沌观测矩阵的安全性进行评估。仿真结果表明，混沌观测矩阵能抵抗惟密文攻击，优化后的构建方法在算法速度、存储空间及重构效果方面均有改善。

关键词 压缩感知 混沌 malab 仿真 密码学

ABSTRACT

Chaos compressive sensing is an important development direction of compression sensing. It is based on the good characteristics of the chaotic system, and the chaos observation matrix is constructed by the chaotic sequence to complete the compression sensing process.

In this article, the chaotic observation matrix is developed based on the chaotic observation matrix, and the proof of the chaotic observation matrix (RIP) is given. The optimal solution under the low computational complexity is determined by statistical method. So are the sampling step and the optimal construction method of chaotic observation matrix. The security of chaotic observation matrix is evaluated. The experimental results show that the chaotic observation matrix can resist the ciphertext-only attack, and the optimized construction method has improved the algorithm speed, storage space and reconstruction effect.

KEY WORDS Compressive Sensing Chaos Matlab Simulation Cryptography

0 引言-选题背景与意义

压缩感知理论充分利用信号的可稀疏性，将采样与压缩合为一个过程，以欠 Nyquist 采样频率进行采样，通过求解非线性算法重构原信号^[1]。根据以往研究经历，压缩感知的主要问题为：信号的稀疏分解^[2]，观测矩阵的构建^[3]和重构算法^[4]。

混沌系统是一个有着复杂运动的非线性动力学系统，由于其极度的初值敏感性和良好的伪随机特点，被应用诸多领域，例如密码学与通信领域。

结合混沌系统的压缩感知理论受到各界的研究与关注，利用混沌系统构造新的观测

矩阵不仅易于解码端硬件低复杂度实现，同时也被证实有安全性好、数据量小等突出优点。在大数据时代背景下，是极具工程应用价值的重要前沿领域。

本文在第一节对压缩感知作简要介绍，第二节对混沌观测矩阵的构建方法、分析和仿真进行详细阐述，第三节进行后续研究展望。

1 压缩感知

设维度为 n 的一维信号 x ，记作 $x(n), x \in [1, 2, 3 \dots N]$ 。则可以通过一组基 $\Psi^T = [\Psi_1, \Psi_2, \dots \Psi_N]$ 的线性组合表示出信号 x ：

$$x = \sum_{k=1}^N \Psi_k a_k \quad (1)$$

当向量 a 仅有 k 个非零系数时($k \ll N$)， Ψ 称为原信号 x 的稀疏基，称系数 a 向量为 k -sparse 稀疏系数。记测量矩阵为 $\Phi = [\phi_1, \phi_2 \dots \phi_M]$ ，测量值为 y 。则有：

$$y = \Phi x \quad (2)$$

式中， y 是 $M \times 1$ 矩阵， Φ 是 $M \times N$ 矩阵。将式(2)代入(1)中：

$$y = \Phi x = \Phi \Psi a = \Theta a \quad (3)$$

由于满足 $M \ll N$ ，直接求解式(1)为“病态”问题。但由于式(3)中稀疏系数 a 是 k -sparse 并满足关系 $k < M \ll N$ ，根据文献^[2]，可通过先求解式(3)再带入式(1)得到原信号。

其中，观测矩阵 Φ 必须满足约束等距条件^[6](restricted isometry property, RIP)，RIP 条件是能否高概率高准确性求解式(3)的充要条件。

式(3)求解得到的稀疏系数 a 越稀疏越好，则压缩感知理论的数学模型有如下表示：

$$\begin{aligned} \min \quad & \|a\|_{l_0} \\ \text{s.t.} \quad & y = \Phi \Psi a \end{aligned} \quad (4)$$

如果采用 l_0 范数优化，对于长度为 N 的稀疏系数 a ，将稀疏度 k 循环遍历，则对于每个 k 有 C_N^k 种排列非零值位置的方式，使用贪婪算法策略的计算复杂度为 $\sum_{k=1}^N C_N^k \rightarrow O(2^N)$ ，属于 NP 问题。Tao 等人^[2]证明求解 l_1 范数优化可以取得逼近 l_0 范数优化的结果：

$$\begin{aligned} \min \quad & \|a\|_{l_1} \\ \text{s.t.} \quad & y = \Phi \Psi a \end{aligned} \quad (5)$$

式(5)为凸优化问题，常用求解算法为匹配追踪法(MP)和正交匹配追踪法(OMP)^[10]。

2 混沌压缩感知

混沌压缩感知的核心问题便是使用混沌序列构建观测矩阵。混沌序列的伪随机性和有界性改善了随机方式带来的稳定性和可控性问题；混沌系统对初值及其依赖，保证了将初值作为密钥的唯一性和抗惟密文攻击。

一维混沌系统和高维混沌应用于构建观测矩阵并无本质的区别。为方便讨论我们以一维 Logistic 混沌系统为例进行讨论：

$$x_{n+1} = ux_n(1 - x_n), u = 4 \quad (6)$$

2.1 构建方法

对于一维的 Logistic 系统产生的序列记为 $x(u, k, x_0)$ 。经如下映射得到序列 $v(d, k, v_0)$:

$$v_k = 1 - 2x_{n+kd} \quad k = 0, 1, 2 \dots \quad (7)$$

上式中, d 是采样间隔(步长), 为了使序列不相关性更高、统计意义上的独立同分布^[8]。按照如下方式构建观测矩阵 $\Phi \in R^{M \times N}$:

$$\Phi = \sqrt{2/M} \begin{pmatrix} v_0 & \cdots & \cdots & v_{M(N-1)} \\ v_1 & \cdots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ v_{M-1} & \cdots & \cdots & v_{MN-1} \end{pmatrix}_{M \times N} \quad (8)$$

式(3-3)中的 $\sqrt{2/M}$ 为了归一化处理。

2.2 采样步长讨论

文献^[8]表明, 虽然 Logistic 混沌系统有着相当好的伪随机性, 但不同子序列间的不相关性却较差。我们引入采样间隔(步长) d , 从生成序列中得到采样序列, 在统计意义上采样序列能更好的满足高不相关性、独立同分布性质。

显然, 当 $d \rightarrow \infty$ 时, 由混沌序列的性质可知, 此时不相关性最好, 但不符合工程实践需要。所以我们需要进一步对采样步长 d 进行讨论, 寻求低计算复杂度下的采样步长。

我们记式(7)产生的序列为 $v_n = 1 - 2x_n$ (无采样步长情况下), 其频数统计图如图 1-a。经过采样后的序列为 $v_{k,d} = 1 - 2x_{kd}$, 通过统计的方法, 选取不同的 d , 绘制 v_n 序列和 $v_{k,d}$ 的二维频数直方图可以帮助我们直观的了解两个序列的互相关性。

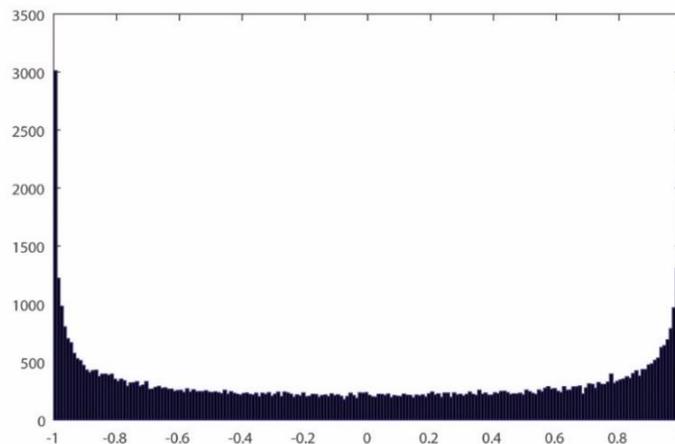


图 1-a 无采样情况下序列 v_n 的频数统计图

如图 1-b 所示, 当 $d = 5$ 时得到的采样序列 $v_{k,d}$ 和 v_n 的二维频数统计图锯齿状较多不平滑, 表明该采样间隔下的序列互相关性高, 独立性差; 当 $d = 15$ 时统计图基本平滑,

独立分布性较好。经过对 10^2 数量级以下的采样间隔的统计研究，综合考虑计算资源和重构效果情况下，我们认为当 $d = 15$ 时满足前文所说的 d “足够大”，此时的采样序列独立同分布性较好。

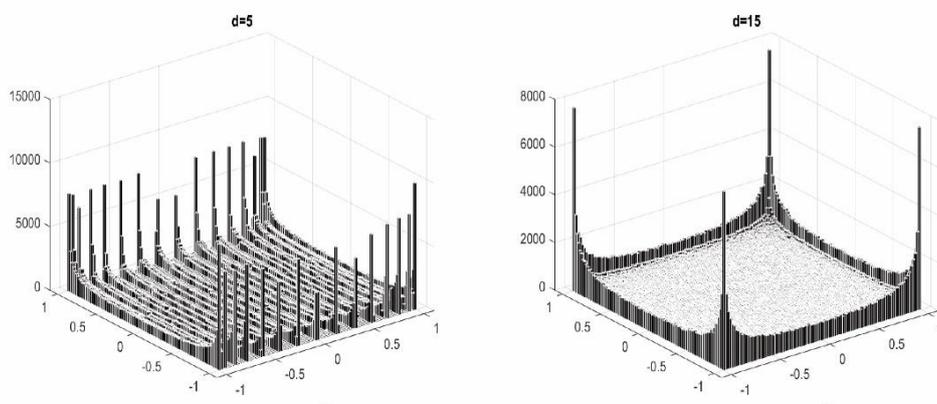


图 1-b 不同采样步长下序列 v_n 和序列 v_{k_d} 的二维频数统计图

2.3 优化构建方法

按照式(8)的排列方法，若采样步长默认为 $d = 15$ ，则需要生成序列的长度为 $M \times N \times d$ 。当压缩比为 80%情况下，则需要混沌序列迭代计算 786432 次。如果采用三维混沌系统，在 Intel Core i5/8G 电脑上需要迭代约 30 分钟。在这对于加解码方都是一个难以承受的时间和计算消耗。

Toeplitz 矩阵是一种由序列循环移位构成的矩阵，只需要确定第一行便可以得到整个矩阵，则生成序列长度可以减少为 $N \times d$ 。由图 1-a 的统计特性，对式(7)作符号映射进一步减小计算和存储压力：

$$a_k = \begin{cases} 1 & v_k \geq 0 \\ 0 & v_k < 0 \end{cases} \quad (9)$$

则观测矩阵只需要用类似稀疏矩阵的方法存储和计算：

$$\Phi = \begin{pmatrix} a_N & a_{N-1} & \cdots & \cdots & a_2 & a_1 \\ a_1 & a_N & \cdots & \cdots & \cdots & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{M-1} & a_{M-2} & \cdots & a_N & \cdots & a_M \end{pmatrix}_{M \times N} \quad (10)$$

2.4 仿真与分析

同一重构算法条件下，将 2.1 节中的混沌观测矩阵与 2.3 节中的优化观测矩阵及随机高斯矩阵的重构效果进行对比，如图 3 所示。结合仿真结果，我们可以总结改进构建方法后的主要优点，列举以下三点：

- 1) 重构性能更优。通过纵向比对，不同构建方法没有本质差异，但优化构建方法的重构效果要略优于随机高斯矩阵和 2.1 节中的构建方法。
- 2) 稳定性更好。用混沌序列构建观测矩阵的稳定性优于随机高斯矩阵，这体现在仿

真过程中同一压缩比下完成多次测量，计算出 PSNR 值趋于稳定(精确小数点后四位无变动)。

3) 相比于 2.1 节中需要大量迭代的构建方式，改进后构建方法的方式速度快、采样点少，更适合于工程实践。

采样比	30%	50%	80%
高斯随机矩阵的重构效果			
PSNR	22.8686	27.4488	31.5374
一维 Logistic 混沌系统			
PSNR	24.3024	27.5780	32.2302
改进的一维 Logistic 混沌系统			
PSNR	24.4117	27.9926	33.5710

图 2 不同测量矩阵在不同压缩比 η 下的重构效果对比

2.5 基于攻击复杂度的安全性分析

针对于混沌观测矩阵的攻击主要为惟密文攻击，敌手基于初值的估计属于穷举攻击的一种。以一维 Logistic 系统为例，默认攻击者知道控制参数 $u = 4$ 。通过仿真我们发现，当初值在小于等于 10^{-16} 阶数变动时，信号均不能被重构。而当初值在 10^{-17} 阶数变动时，攻击者已经可以通过攻击恢复得到部分密文。则一维 Logistic 系统的计算复杂度为 $O(10^{17})$ ，同理，当使用三维 Lorenz 系统或 Rossler 系统，密钥变为三个参数，在默认攻击者知道控制参数 $a = 10$ 、 $b = 8/3$ 、 $c = 28$ 的情况下，计算复杂度为 $O(10^{51})$ 。

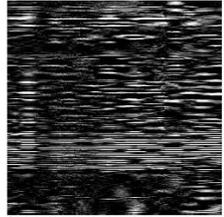
初始值	0.2	0.199999	$0.2 - 10^{-17}$
重构效果			
PSNR	33.5710	3.5214	12.0828

图 3 与真实密钥相差 10^{-6} 和 10^{-17} 的重构效果

3 展望

针对本文的不足之处，对下一步更深入的研究抛出两个主要的问题：

1) 研究更快的迭代算法。龙格库塔法在计算高阶微分方程组时速度较慢，对新的数值算法的研究也是提高构建观测矩阵速度的重要方向。

2) 研究高阶系统本身性质。由于高阶的混沌系统性质较复杂、运动轨迹更为不规律，鉴于高阶系统的应用场景更为广泛、有更高安全性特点，有必要对高阶系统本身的性质进行更为深入的研究。

参考文献

- [1] Candes E J,Wakin M B. An introduction to compressive sampling [J].Signal Processing Magazine.IEEE,2008.25(2):21-30.
- [2] Candes E J,Romberg J. Quantitative robust uncertainty principles and optimal sparse decompositions [J].Foundations of Computational Mathematics,2006,6(2):227-254.
- [3] Luo C,Wu F,Sun J,et al. Efficient measurement generation and pervasive sparsity for compressive day gathering [J].Wireless Communications,IEEE Transactions on,2010,9(12):3728-3738.
- [4] Tune P,Bhaskaran S R,Hanly S. Number of measurements in sparse signal recovery[C] Information Theory,2009. ISIT 2009. IEEE International Symposium on.IEEE,2009:16-20.
- [5] Candes E J,Romberg J,Tao T. Robust uncertainty principles:Exact signal reconstruction from highly incomplete frequency information[J]. Information Theory,IEEE Transaction on,2006,52(2):489-509.
- [6] Candes E J,Plan Y.A probabilistic and RIPless theory of compressed sensing[J].IEEE Transactions on Information Theory,2011,57(11):7235-7254.
- [7] GAN Lu.Block compressed sensing of natural images[C]//Proceedings of the International Conference on Digital Signal Processing.[S.L]:IEEE Press,2007:403-406.
- [8] A.Vlad,A.Luca,and M.Frunzete,"Computational measurements of the transient time and of the sampling distance that enables statistical independence in the logistic map,"in Proc.Int.Conf.Computational Science and Its Applications(ICCSA),Berlin,Germany,2009.pp.703-718.