



混沌压缩感知算法的设计与实现

网络空间安全学院

赵秋涵

Allen_zqh@bupt.edu.cn

目录

Contents

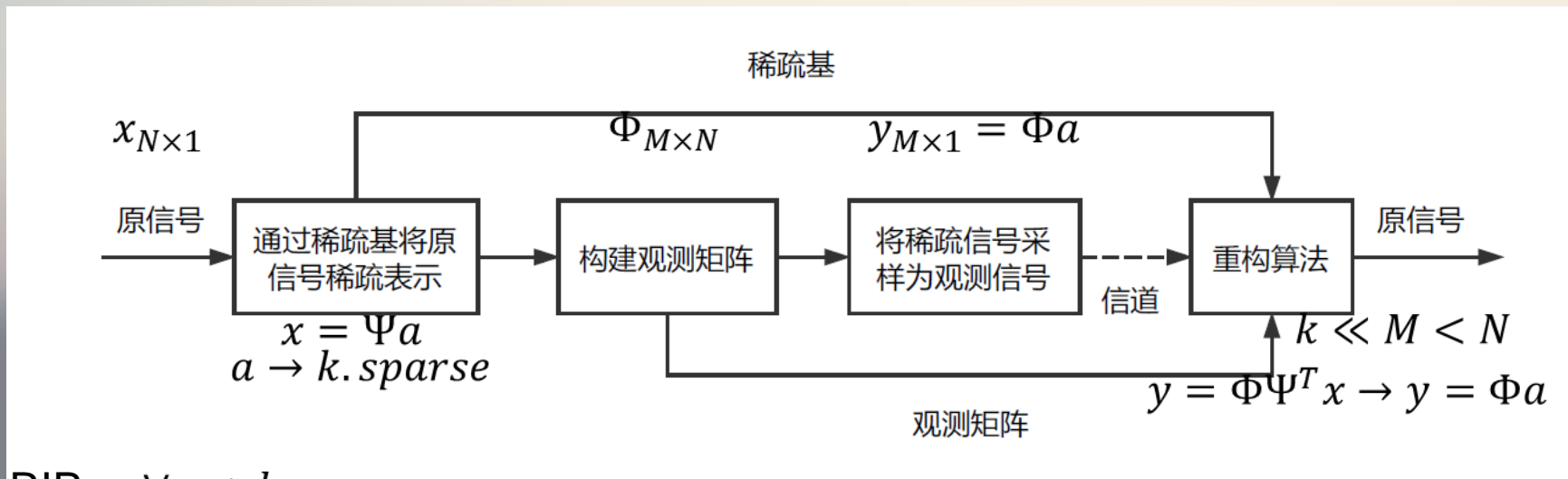
- 压缩感知与混沌系统
- 混沌压缩感知
- 结语

01

压缩感知与混沌系统

简介与仿真

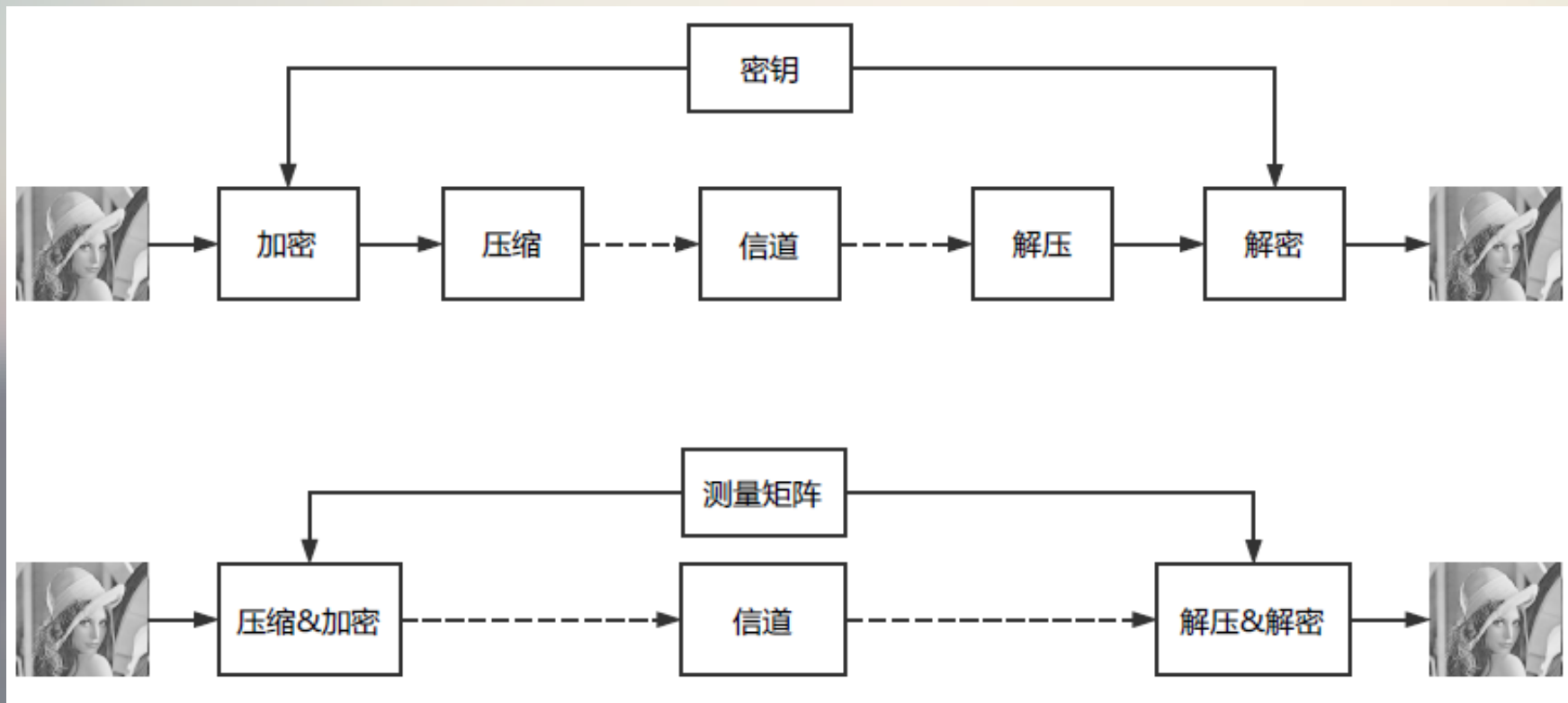
1-1 压缩感知




RIP: $\forall v \Rightarrow k.\text{sparse}$

$$s.t \exists \varepsilon \quad 1 - \varepsilon \leq \frac{\|\Phi v\|_2}{\|v\|_2} \leq 1 + \varepsilon \quad s.t \exists \varepsilon \quad 1 - \varepsilon \leq \lambda(\Phi_H) \leq 1 + \varepsilon$$

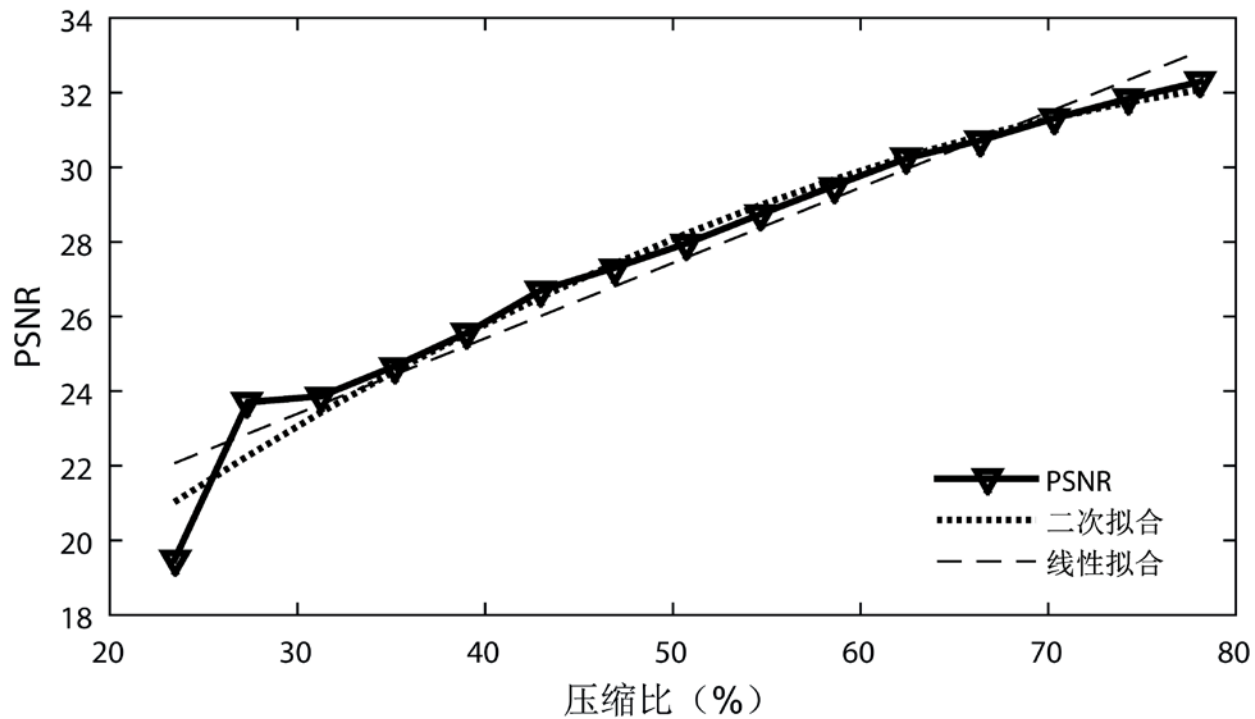
1-1 压缩感知



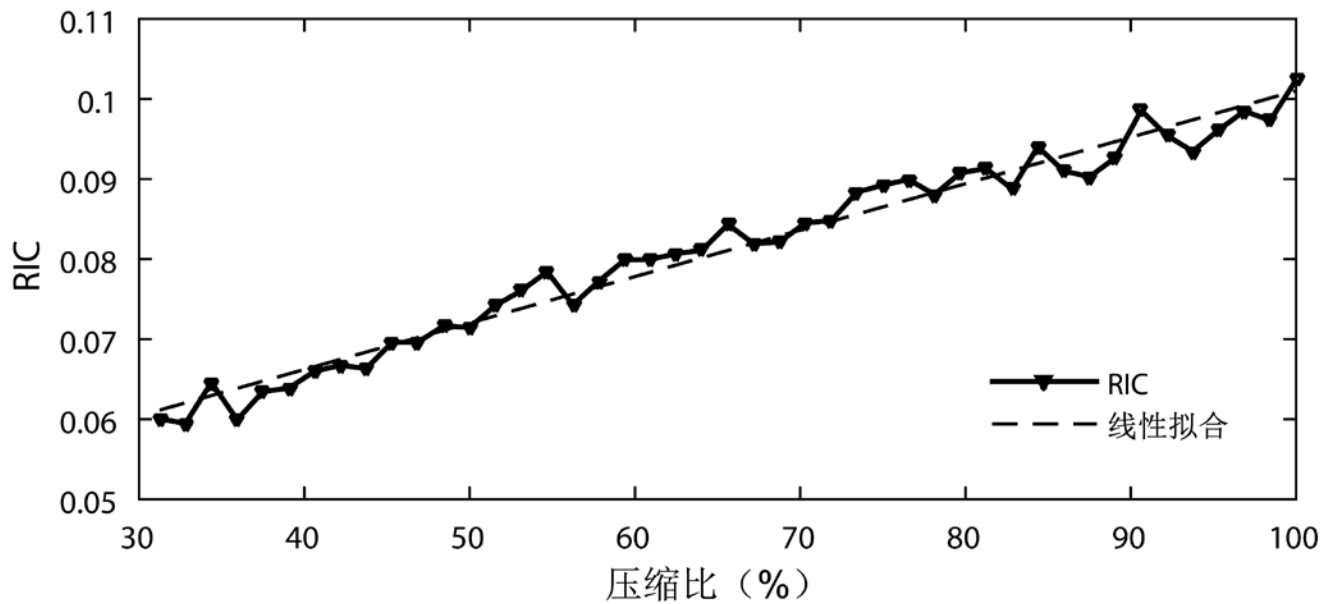
1-1 压缩感知

压缩比	30%	50%	80%
高斯 随机 矩阵 的重 构 效果			
PSNR	22.8686	27.4488	31.5374

1-1 压缩感知

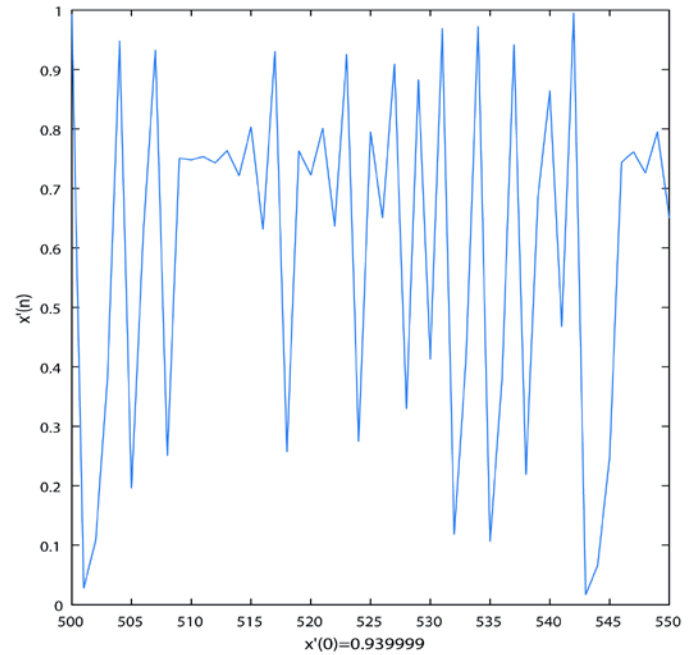
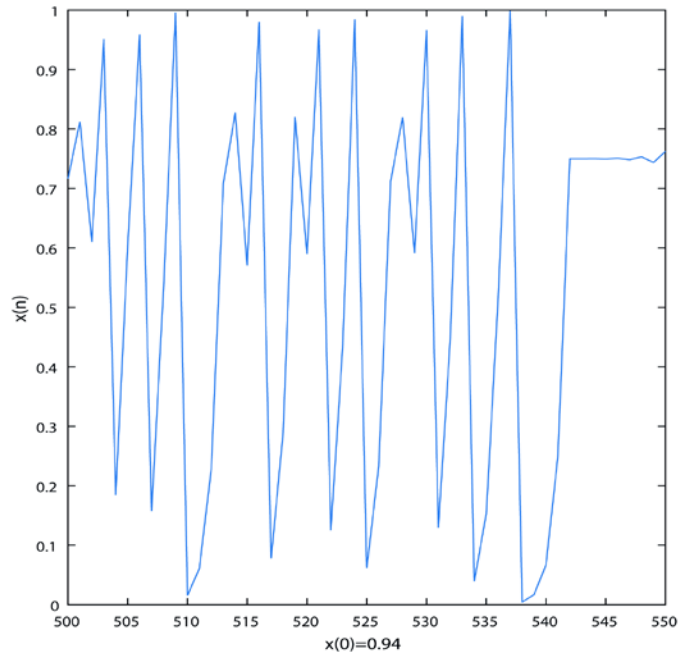


1-1 压缩感知



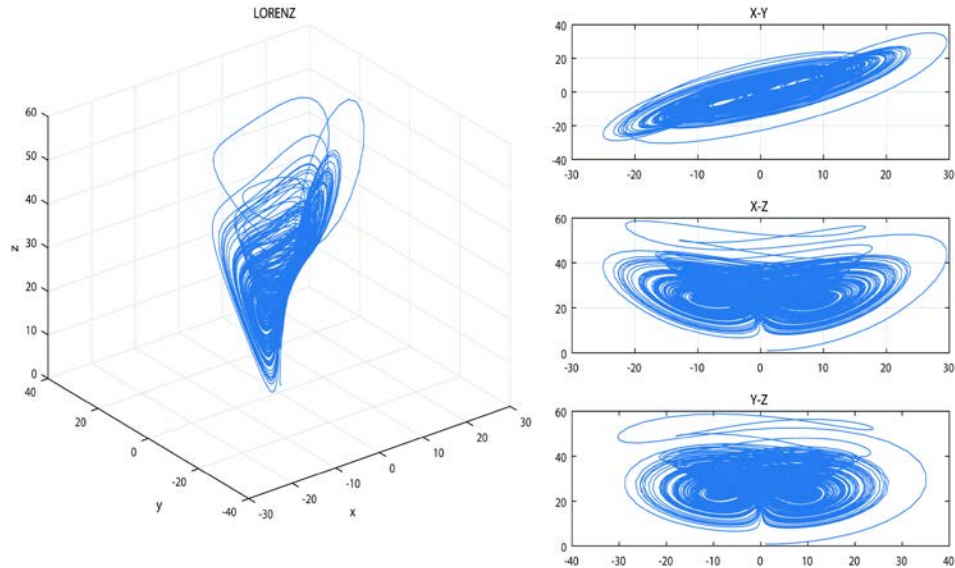
1-2 混沌系统

- 初值敏感性



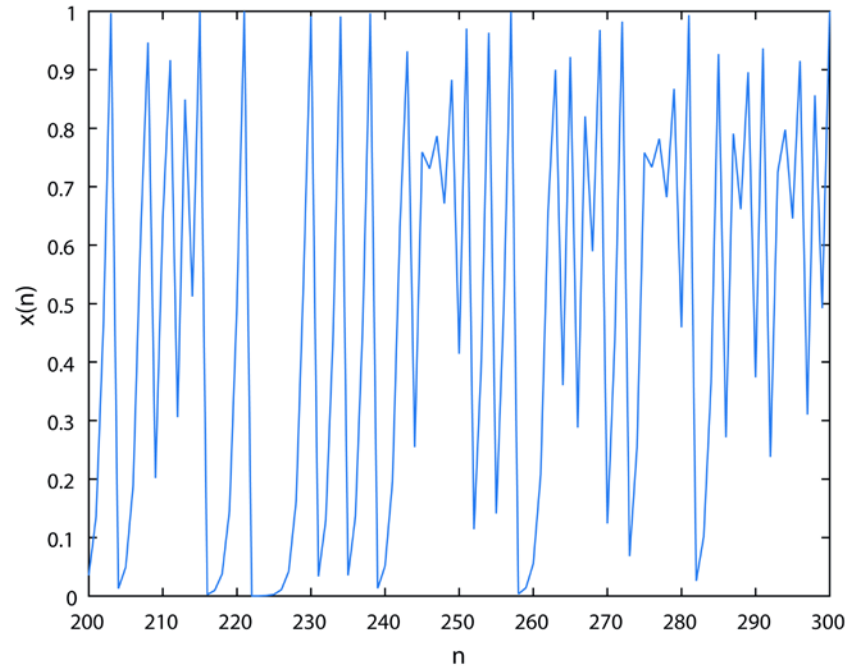
1-2 混沌系统

- 分形性



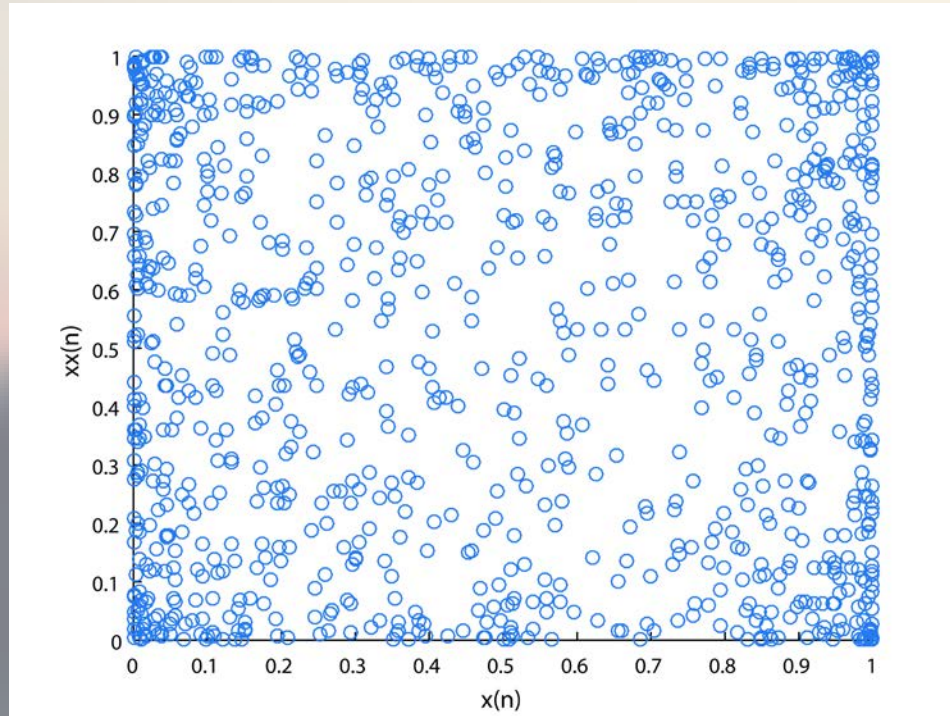
1-2 混沌系统

- 随机性与有界性



1-2 混沌系统

- 遍历性

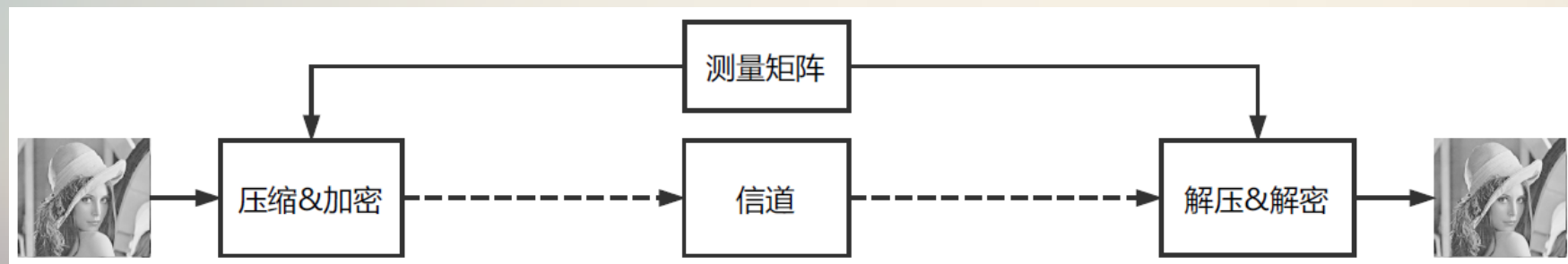


02

混沌压缩感知

观测矩阵的构建

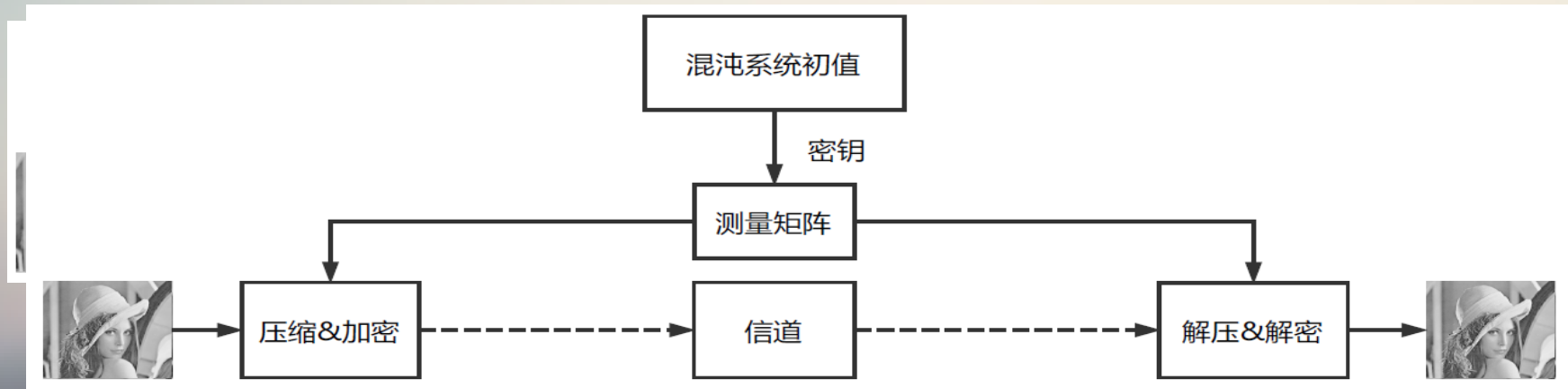
2-1 混沌压缩感知通信模型



传统CS模型中测量矩阵的缺陷:

- 测量矩阵不够可控和稳定
- 信道负载大
- 安全性不足
- 作“伪随机”和有界性
- 信道无需传输观测矩阵
- 抵抗惟密文攻击

2-1 混沌压缩感知通信模型



传统CS模型中测量矩阵的缺陷:

- 测量矩阵不够可控和稳定
- 信道负载大
- 安全性不足
- 作“伪随机”和有界性
- 信道无需传输观测矩阵
- 抵抗惟密文攻击

2-2 观测矩阵的构建

一维混沌系统Logistic为例： $x_{n+1} = ux_n(1 - x_n)$, $u = 4$

生成混沌序列，并由 $v_{k+1} = 1 - 2x_{n+kd}$, $d = 15$ 采样，得到生成序列用于构建观测矩阵；

其中，设 $n = 0$ 作简化， d 为采样步长，后续将对其进行讨论。

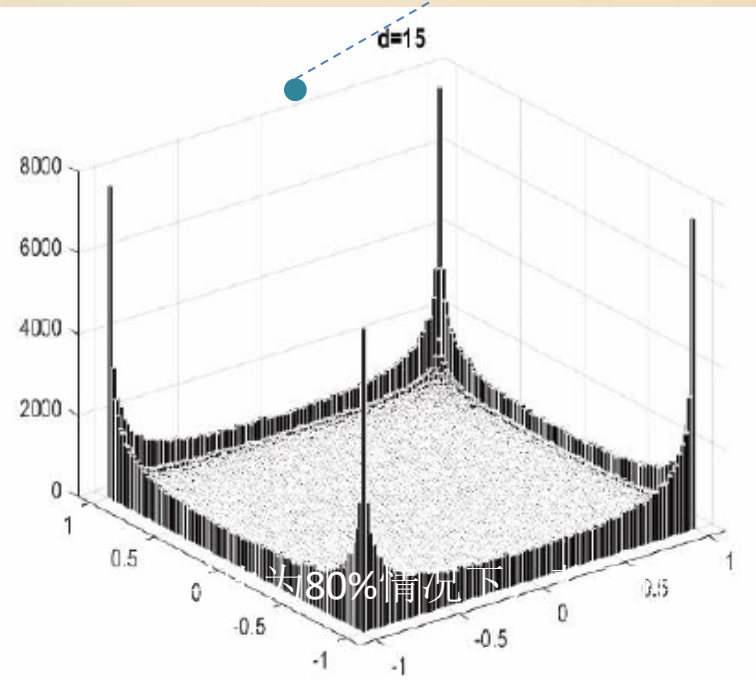
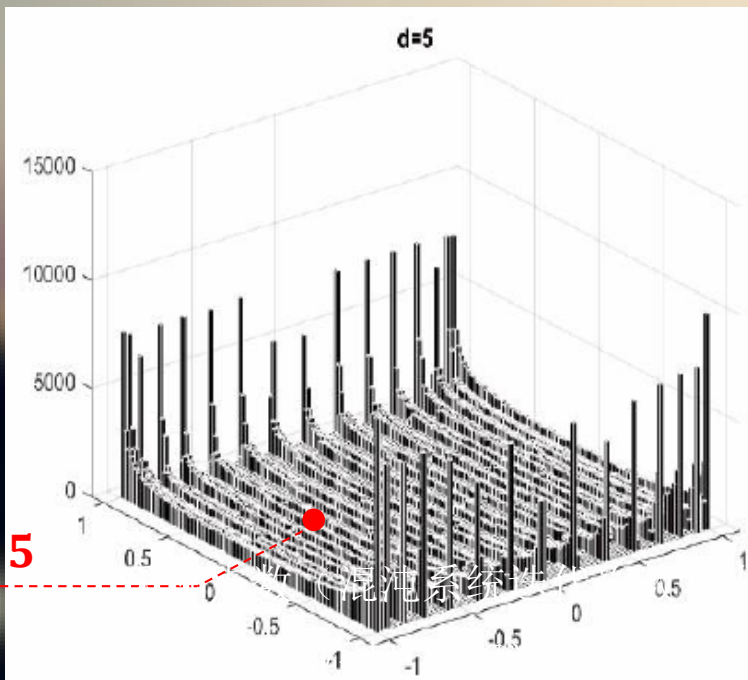
矩阵的构建方法

$$\Phi = \sqrt{\frac{2}{M}} \begin{pmatrix} v_0 & \dots & \dots & v_{M(N-1)} \\ v_1 & \dots & \dots & v_{M(N-1)+1} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ v_{M-1} & \dots & \dots & v_{MN-1} \end{pmatrix}_{M \times N}$$

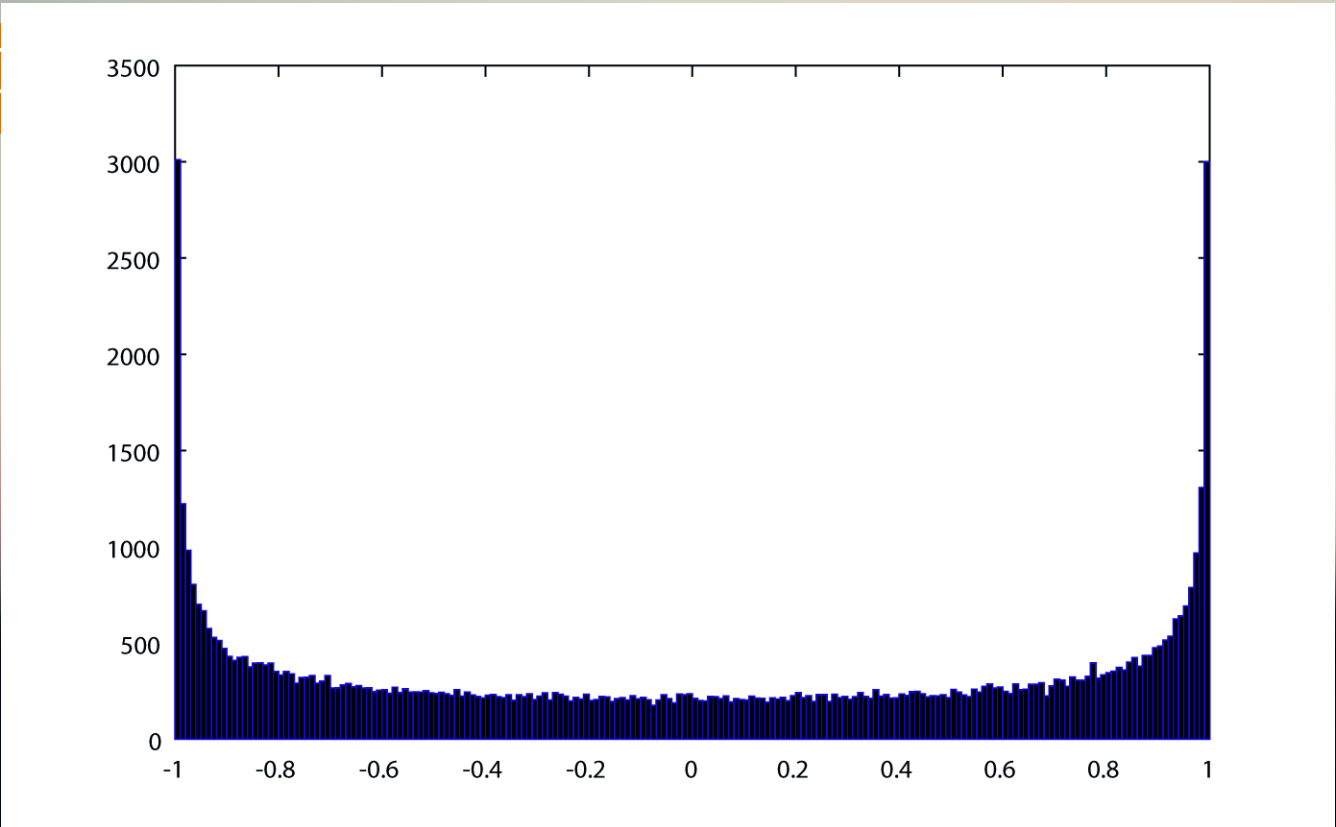
仿真效果

不同间隔的讨论

$d = 15$



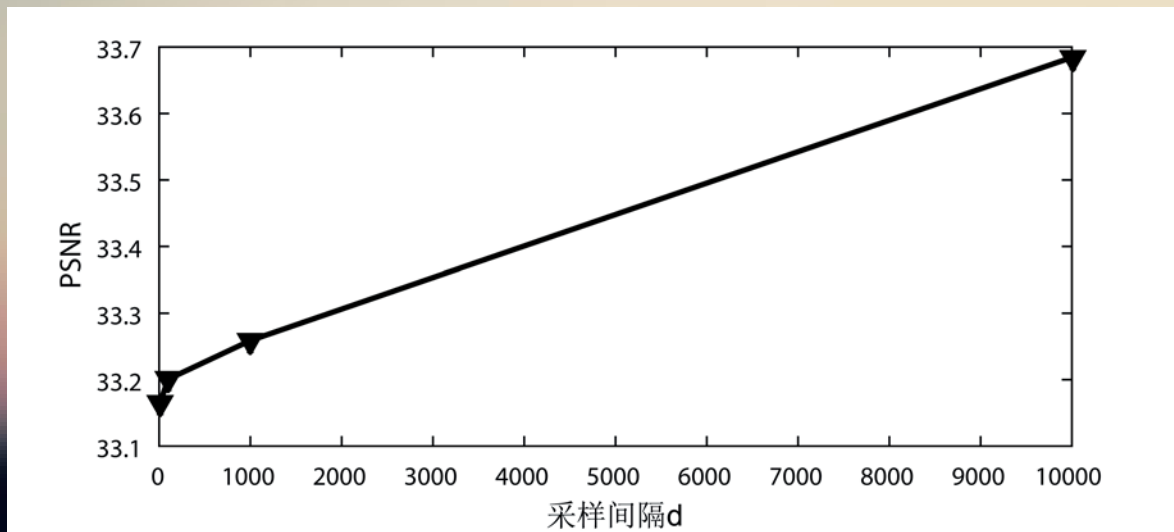
仿真效果



采样点数（混沌系统迭代次数）为 $M \times N \times d$ 。采样比为80%情况下，若采样间隔为 10^2 级别，则混沌系统迭代次数需达到 $80\% \times 256 \times 256 \times 100 = 5242880$ 。

仿真效果










不同间隔的讨论



η \ d	5	15
30%	23.6244	24.3024
50%	27.2398	27.5780
80%	31.8654	32.2302

仿真效果

不同间隔的

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
三维 Chen 混沌系统 (x轴序列)			
PSNR	23.9744	27.4155	32.1777

仿真效果 法的优化

一维混沌系统Logistic为例: $x_{n+1} = ux_n(1 - x_n)$, $u = 4$

生成混沌序列后经过采样间隔 $d = 15$ 得到采样序列, 做符号映射得到生成序列 a_k :

$$a_k = \begin{cases} 1 & v_k \geq 0 \\ 0 & v_k < 0 \end{cases}$$

矩阵的构建方法

$$\Phi = \begin{pmatrix} a_N & a_{N-1} & \dots & \dots & a_2 & a_1 \\ a_1 & a_N & a_{N-1} & \dots & \dots & a_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{M-1} & a_{M-2} & \dots & a_N & \dots & a_M \end{pmatrix}_{M \times N}$$

仿真效果 法的优化










一维混沌系统Logistic为例: x_{n+1}

生成混沌序列后经过采样间隔 $d =$

$$a_k = \begin{cases} 1 & v_k \geq 0 \\ 0 & v_k < 0 \end{cases}$$

矩阵的构建方法

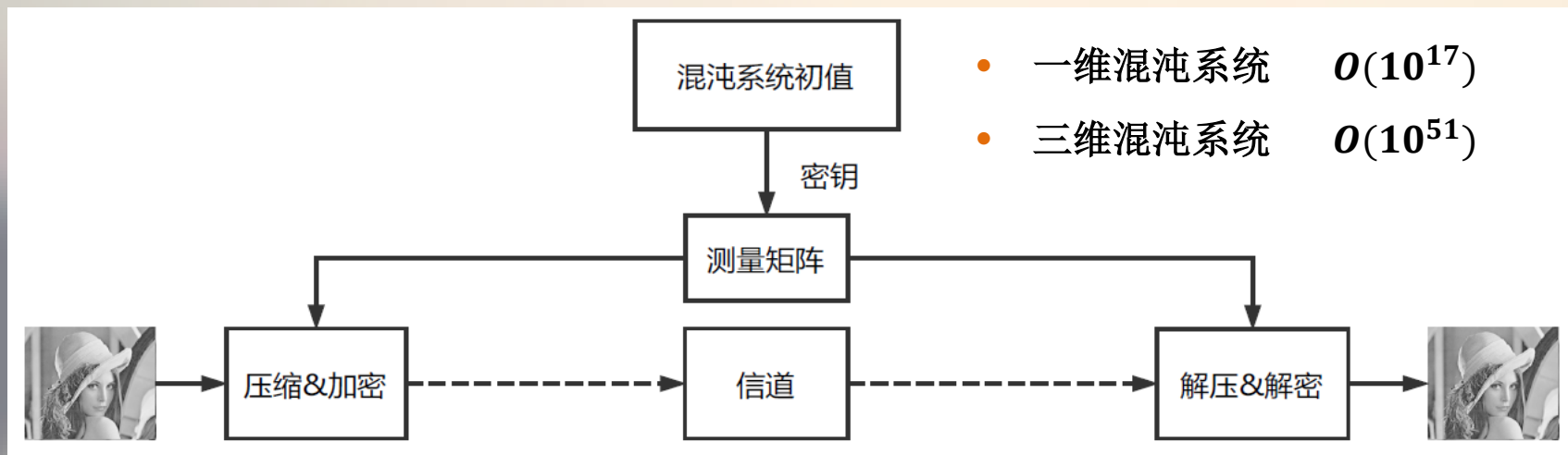
$$\Phi = \begin{pmatrix} a_N \\ a_1 \\ \dots \\ a_{M-1} \end{pmatrix}$$

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
改进后的一维Logistic混沌系统			
PSNR	24.4117	27.9926	33.5710


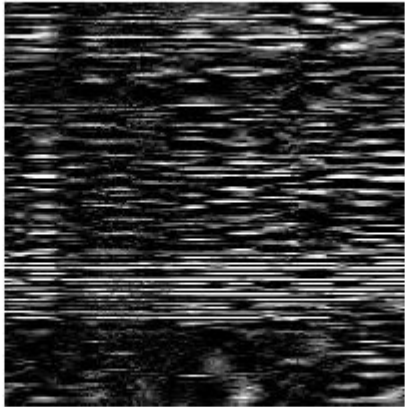

2-5 混沌压缩感知的安全性分析

惟密文攻击

在攻击者已知系统控制参数情况下：



2-5 混沌压缩感知的安全性分析

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

二维混沌系统 $U(10^{-17})$

2-5 混沌压缩感知的安全性分析

惟密文攻击


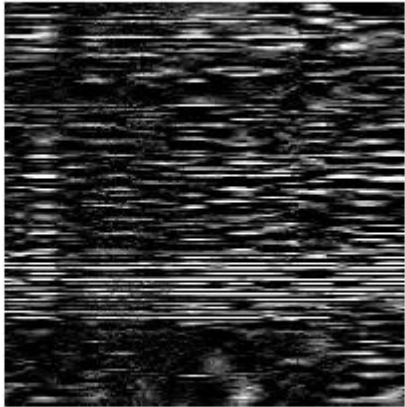



在攻击者已知系统控制参数情况下：

一维混沌系统 $O(10^{17})$

• 三维混沌系统 $O(10^{51})$

2-5 混沌压缩感知的安全性分析

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

二维混沌系统 $U(10^{-17})$

03

结语

工作总结和亮点

3-1 工作总结



通过理论和仿真相结合的方法，讨论压缩感知和混沌系统相关性质。



从理论角度对每种混沌序列构建观测矩阵的方法进行RIP性质证明，并完成仿真与分析。



使用统计学方法确定低计算复杂度下的采样步长，并仿真对比重构效果。



提出混沌压缩通信模型，并对其优点和安全性进行详细分析和仿真。

3-2 亮点



统计学方法

避开复杂的统计学和复变背景，用统计学方法直观的展示低复杂度下的最优步长。



优化构建方法

首次将采样间隔引入 Toplitz 结构，并得到了稍优的仿真结果。



通信模型

根据仿真结论，提出基于混沌压缩感知算法的安全通信模型，并对其安全性和改进点进行分析。



严格证明

全文以多学科交叉方式进行研讨，对于每种方法都先进行严格数学证明后仿真验证的方式。



感谢聆听!

混沌压缩感知算法的设计与实现

网络空间安全学院

赵秋涵

Allen_zqh@bupt.edu.cn