Provably Secure Spread-spectrum Watermarking Schemes in the Known Message Attack Framework

Jian Cao, Jiwu Huang

School of Information Science and Technology

Sun Yat-Sun University, P.R, China,510006

phdcaojian@yahoo.cn

Outline

- Motivations
- Technical approach
- Experiment results
- Conclusion

Motivations

- Background
  - Observations: watermarked signals which are watermarked by the secret key
  - Attacks to security: gaining the knowledge about the secret key
  - Known message attack (KMA) : only own several observations
  - Watermarked Only Attack (WOA): both own several observations and corresponding embedded messages

Since compared to WOA framework, in the KMA framework the attacker still knows corresponding embedded message, secure watermarking schemes against WOA attacks are not at all necessary secure against KMA attacks.

Motivations

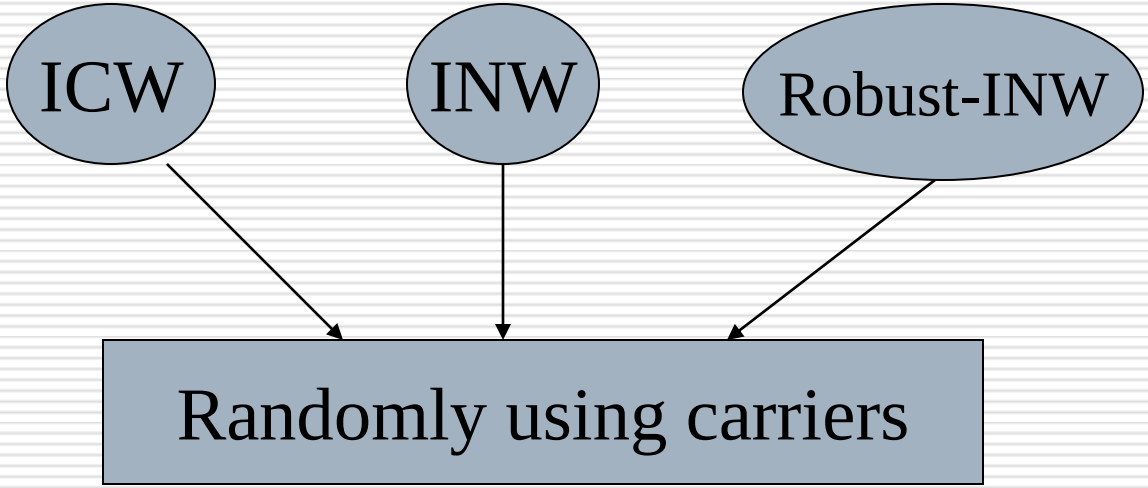
- Existing problem
  - All existing spread spectrum watermarking schemes are insecure against KMA attacks, including those watermarking schemes are secure against WOA attacks
- Assessed problem
  - Designing secure spread spectrum watermarking schemes (against KMA attacks). Specifically, in the presentation we first propose the concept of independent circular watermarking and then implement it.

Technical Approach

- Independent circular watermarking we present
  - Extension of circular watermarking [1] that the other authors presented from WOA to KMA
  - Its definition
    - For any given embedded message, the projection of watermarked signal in the embedding subspace has a conditional distribution invariant under rotations
  - It implies that it is impossible to estimate the secret carriers even given enough observations for any embedded message
  - Its three implementations
    - ICW
    - INW
    - Robust-INW

Technical Approach

The main idea behind implementing independent circular watermarking



Now, we need a method for randomly using carriers in such a way that this carriers can be estimated by the decoder for correct decoding

Technical Approach

$$\mathbf{v} = \mathbf{uQ}$$

Let **u** denote the secret carriers and **Q** the uniformly distributed orthogonal matrix, then **v** denotes the carriers used

Now, the thing we need to do is to present a method for generating this uniformly distributed orthogonal matrix, i.e., Q, in such a way that it can be estimated by the decoder. The method comes form the fact that the projection of host signal in orthogonal complement of the embedding subspace keeps invariant during embedding in the context of spread spectrum watermarking. Hence, **by organizing the projection into a matrix and then applying the Gram-Schmidt orthogonalization procedure , we can obtain the orthogonal matrix we required, namely, the matrix Q.**

Technical Approach

- First implementation of independent circular watermarking: ICW
  - Based on the well-known ISS modulation
  - Its embedding function is given by:

$$\mathbf{s} = \mathbf{x} + \sum_{i=1}^{N_c} \alpha \mathbf{m}(i) - \lambda \mathbf{x}^H \mathbf{v}_i \ \mathbf{v}_i$$

However, ICW has a disadvantage that although it is secure against carriers estimation but is insecure against embedding subspace estimation since the projection of watermarked signal in the embedding subspace has a distribution which is different from the distribution of the projection of watermarked signal in other subspace

Technical Approach

- The second implementation of independent circular watermarking: INW
  - The definition of INW
    - to keep the distribution of the projection of signal in the embedding subspace invariant during embedding for any given message
  - Its embedding function is given by:

$$\mathbf{s} = \mathbf{x} + \sum_{i=1}^{N_c} \left(\frac{1}{\sqrt{N_c}} \left\| \mathbf{x}^H \mathbf{v} \right\| \mathbf{m}(i) - \mathbf{x}^H \mathbf{v}_i \right) \mathbf{v}_i$$

The main disadvantage of INW is that its robustness is not very good since there exist a great number of watermarked signals closing to the decoding borders

Technical Approach

- The third implementation of independent circular watermarking: Robust-INW
  - In order to increase the robustness of INW, the third implementation called Robust-INW is also presented
  - Its idea is to increase the variance of the projection of watermarked signal in the embedding subspace after INW
  - Its embedding function is given by:

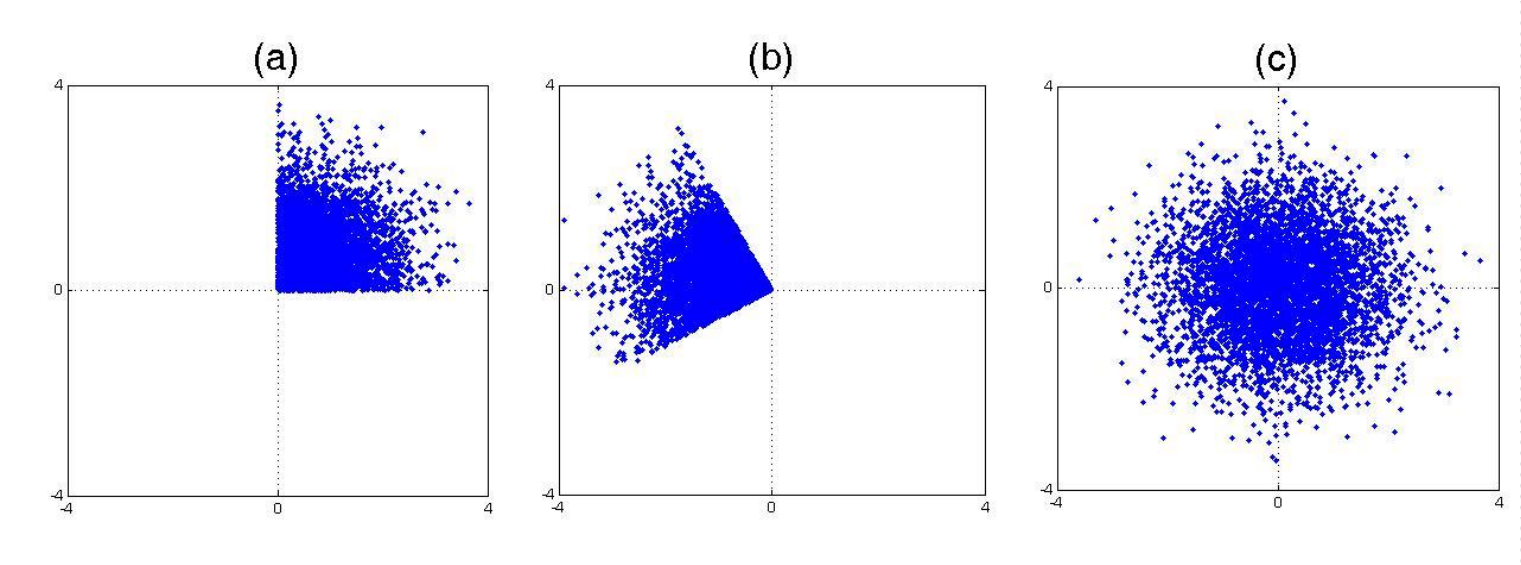
$$\mathbf{s} = \mathbf{x} + \sum_{i=1}^{N_c} \left(\frac{\lambda}{\sqrt{N_c}} \left\| \mathbf{x}^H \mathbf{v} \right\| \mathbf{m}(i) - \mathbf{x}^H \mathbf{v}_i \right) \mathbf{v}_i$$

Experiment Results

- Security
  - To assess the security of a spread spectrum watermarking scheme, we project the observations into various subspace for NW ,CW-ISS, ICW and INW. Specifically, (a) is for the embedding subspace where the orthogonal basis is the secret carriers. (b) is also for the embedding subspace but where the orthogonal basis is randomly chosen. (c) is for the randomly chosen subspace.

Experiment Results

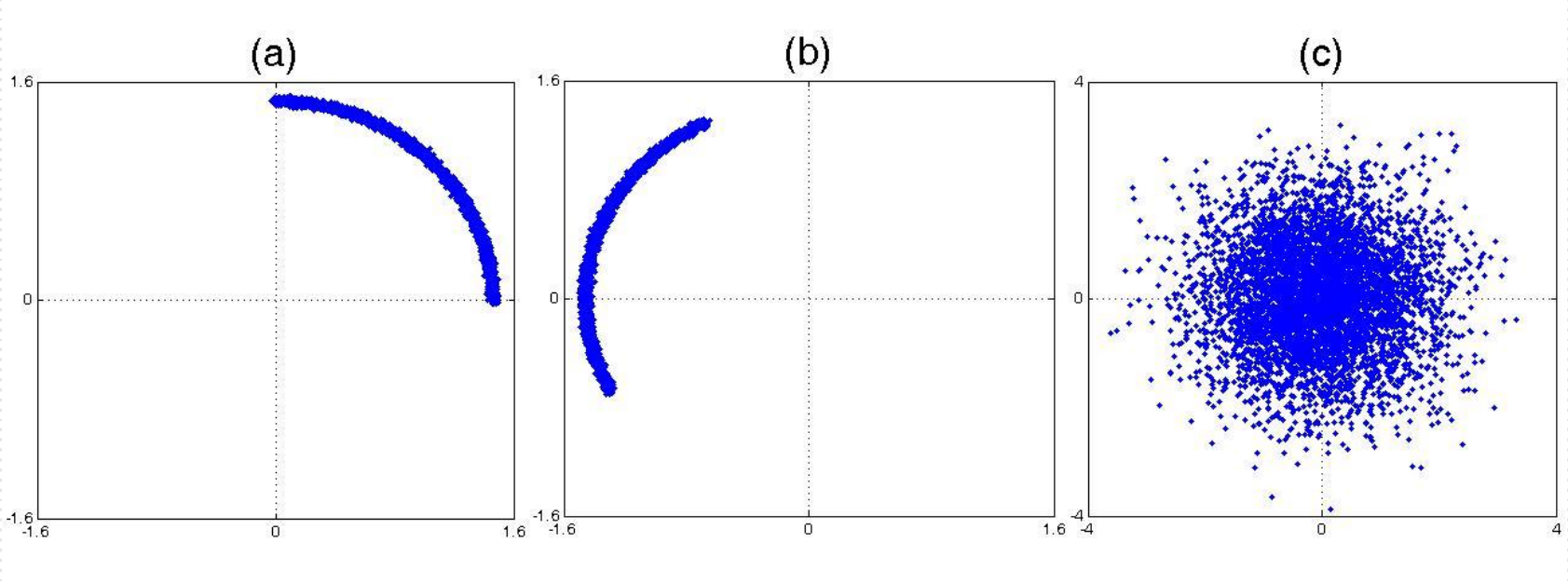
NW



Projections of observations in various subspaces

Experiment Results

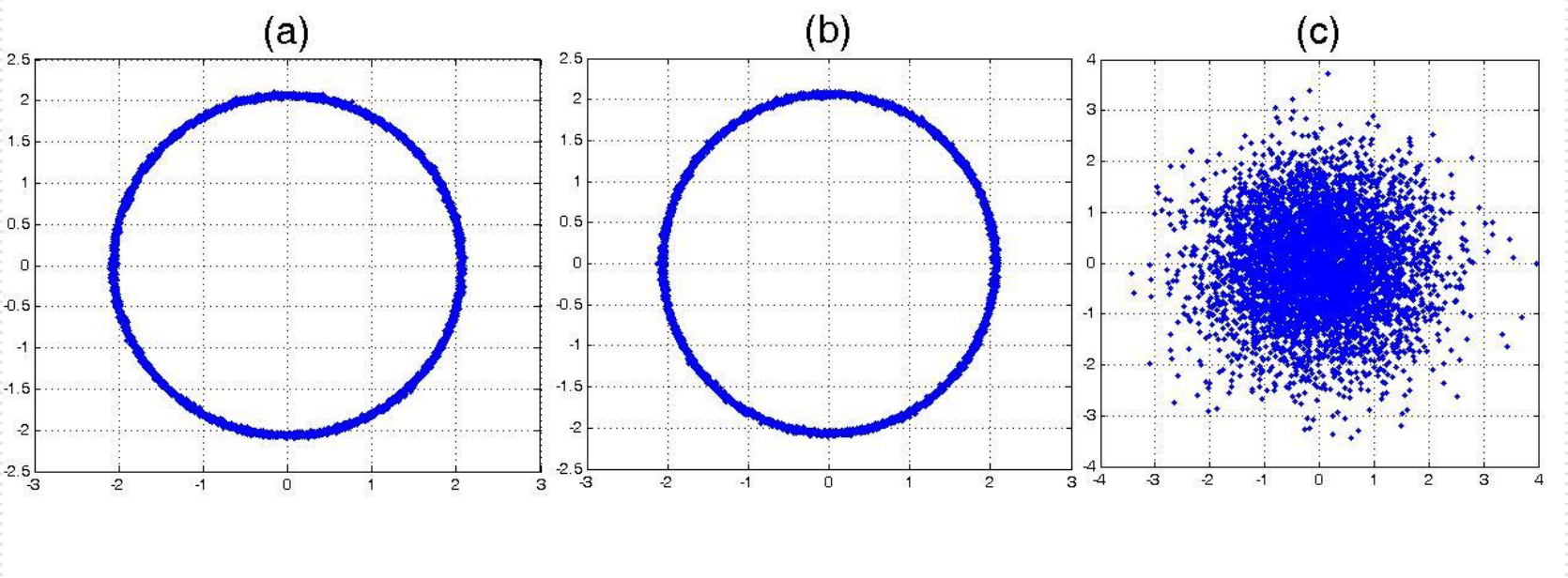
CW-ISS



Projections of observations in various subspaces

Experiment Results

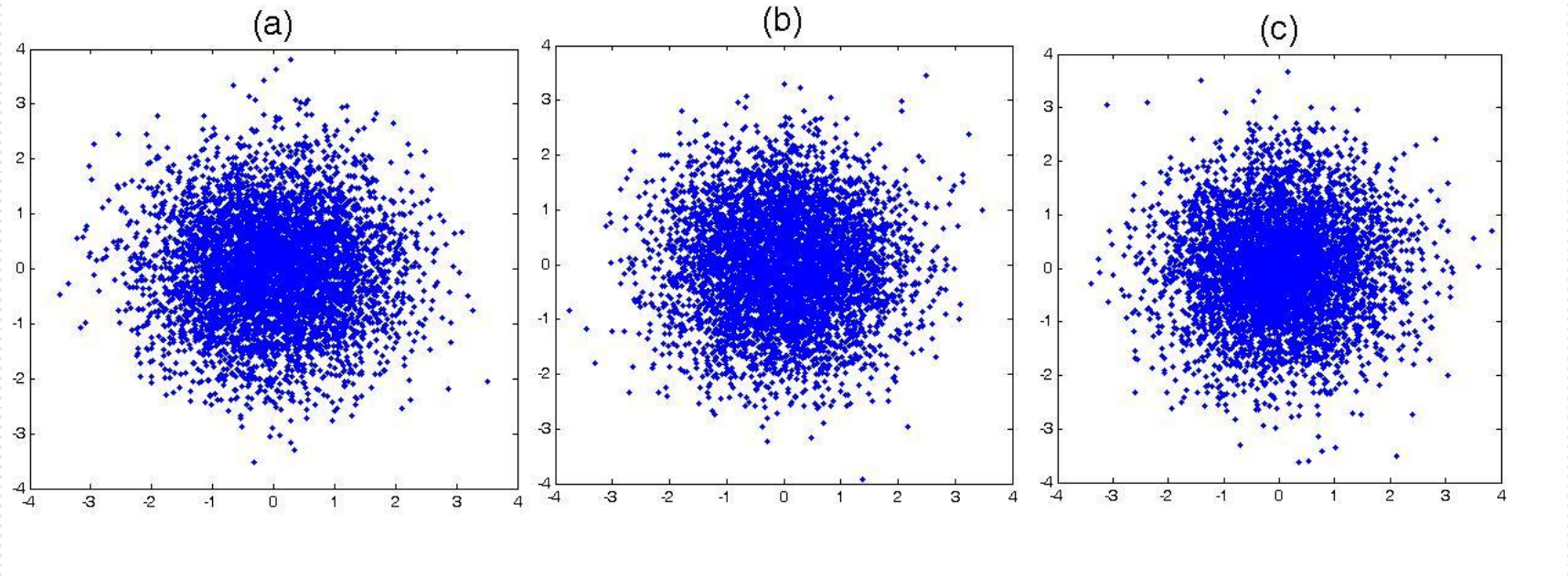
ICW



Projections of observations in various subspaces

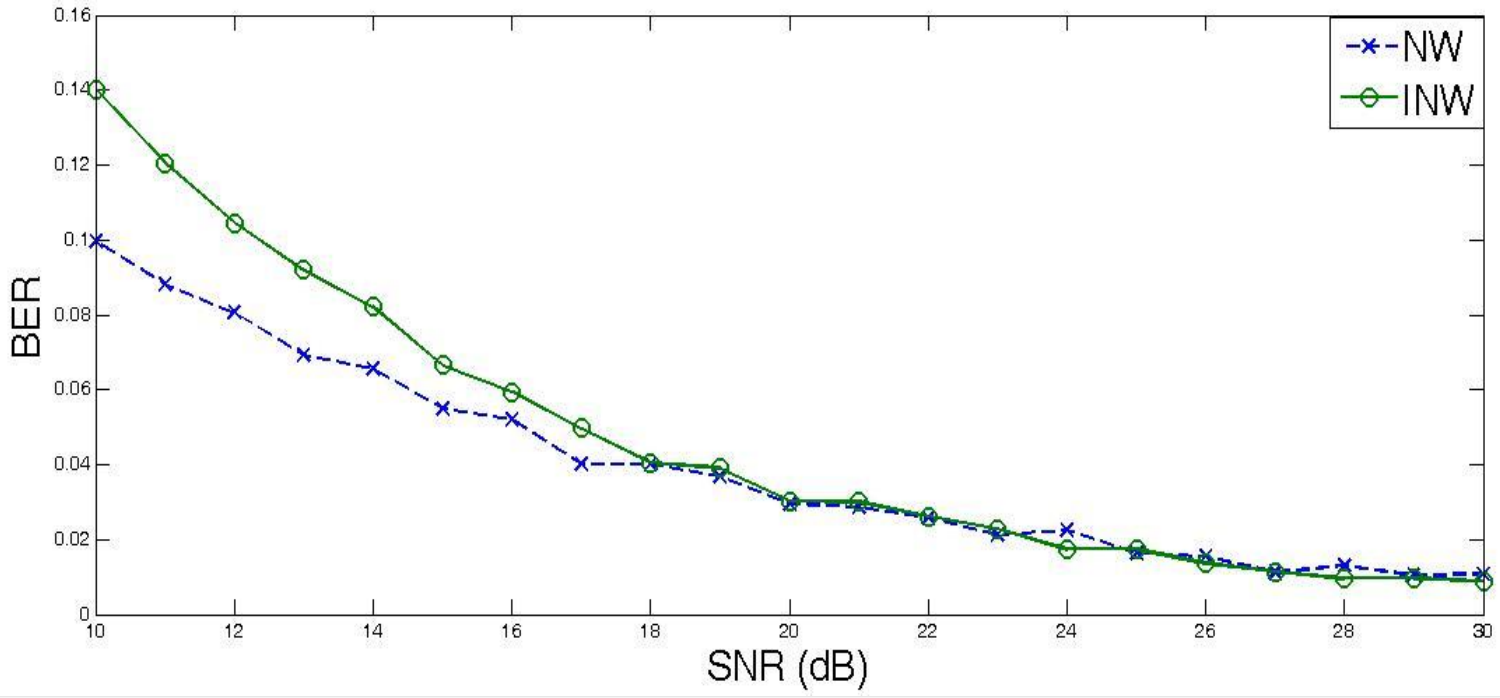
Experiment Results

INW



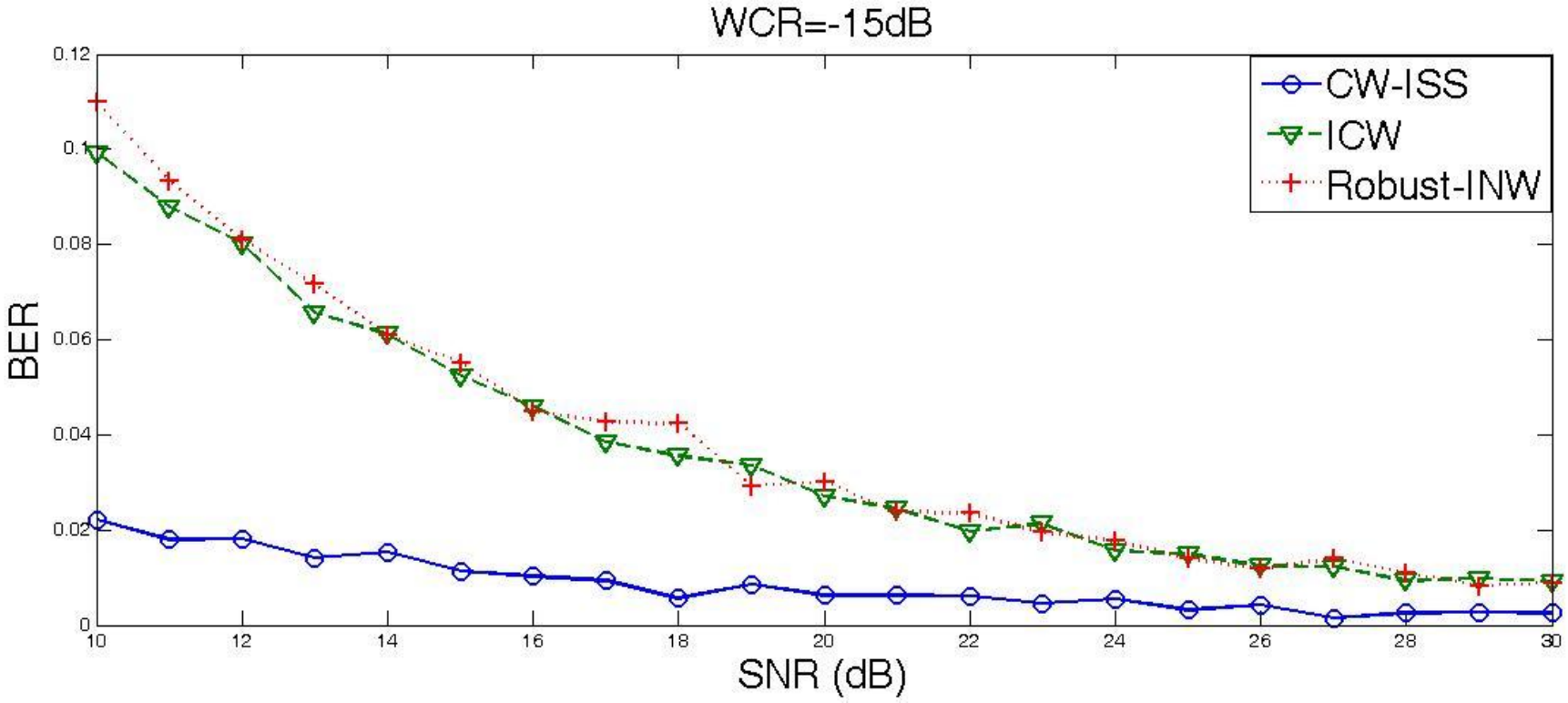
Projections of observations in various subspaces

Experiment Results



Comparison of BER for NW and INW

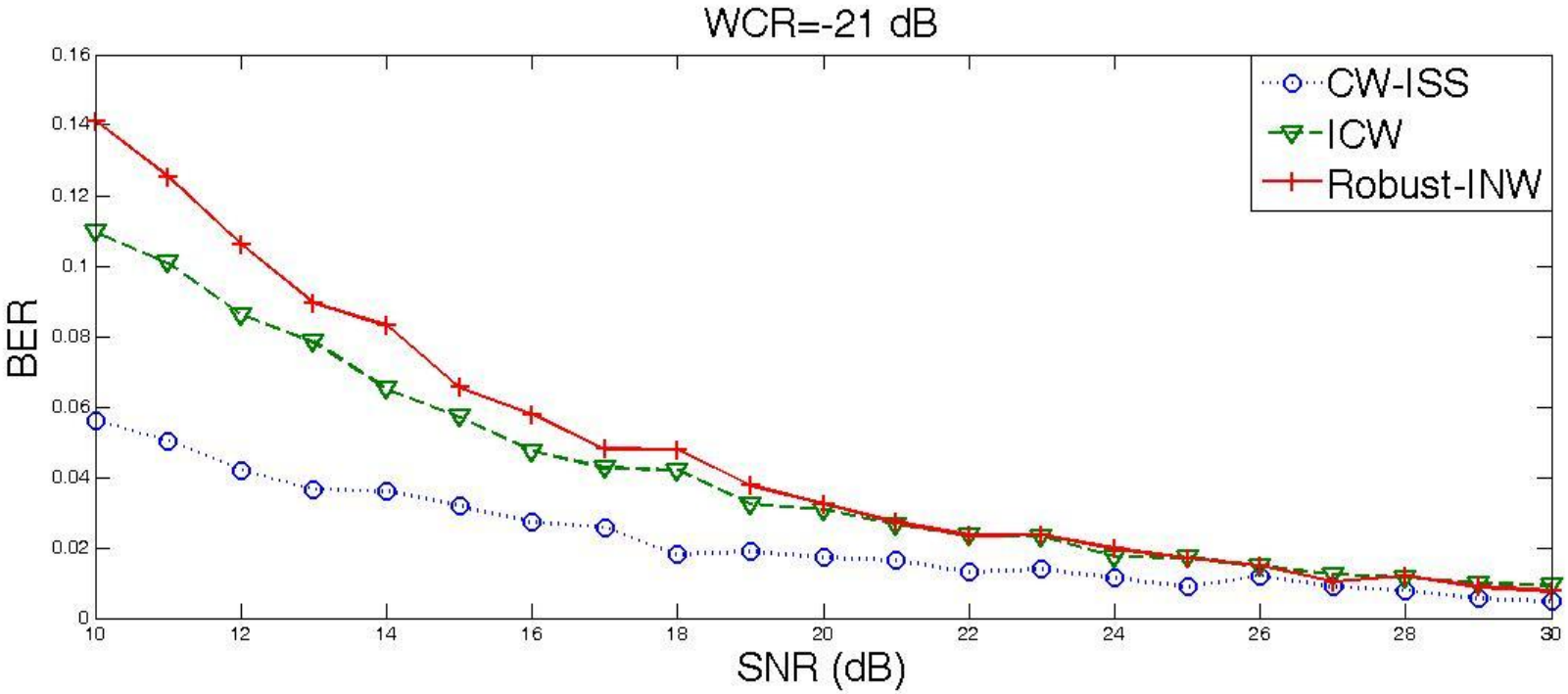
Experiment Results



Comparison of BER for CW-ISS, ICW and Robust-INW

Experiment Results

The following two figures compare the robustness of INW and NW and compare the robustness of CW-ISS, ICW and robust-INW against AWGN attack respectively. As we can see, although INW and ICW can obtain a better secure than CW-ISS and NW but come at the cost of low robustness.



Comparison of BER for CW-ISS, ICW and Robust-INW

Conclusion and further direction

- Presenting the concept of independent circular watermarking and its three implementation, namely, ICW, INW and Robust-INW
- Further direction
  - In order to improve the robustness of our three implementations of independent circular watermarking, I would like to design a new approach for transforming the projection of host signal in the orthogonal complement of the embedding subspace into a Gaussian matrix.