A New Spread Spectrum Watermarking Scheme to Achieve a Tradeoff Between Robustness and Security

Jian Cao, Jiwu Huang and Jiangqun Ni
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
  - Watermarked Only Attack (WOA) attacks:
    - Those attacks whose goal is to gain the knowledge about

    The secret carriers only from the observations
  - Traditional spread spectrum watermarking schemes has been proven to be insecure against carriers estimation
  - The concept of circular watermarking and natural watermarking [1]
    - **Circular watermarking: the projection of watermarked signal in the embedding subspace has a distribution invariant under rotations**
    - **Natural watermarking: the distribution of the projection keeps invariant during embedding**
    - **Circular watermarking are secure against carriers estimation and natural watermarking are secure both against carriers estimation and embedding subspace estimation**

Motivations

- What is the problem
  - Existing implementations, namely, NW and CW-ISS were designed for two extreme situations.
    - NW is designed for the situation where the watermark removal is considered as a very harmful attack and the attacker can gather enough observations, while CW-ISS is designed for the situation where the watermark removal is not considered as a harmful attack or the attacker can only gather seldom observations.

Motivations

- Research objectives
  - Our motivation is to design a spread spectrum watermarking scheme which is applicable to more situations
    - it is secure against carriers estimation for freely chosen embedding parameters
    - there exists a embedding parameters setting such that it is secure against the embedding subspace estimation
    - there exists a embedding parameters setting such that it can achieve roughly the same robustness as CW-ISS.

Technical approach

- Normalized-CW: we first present a new circular watermarking
  - The embedding function is give by:

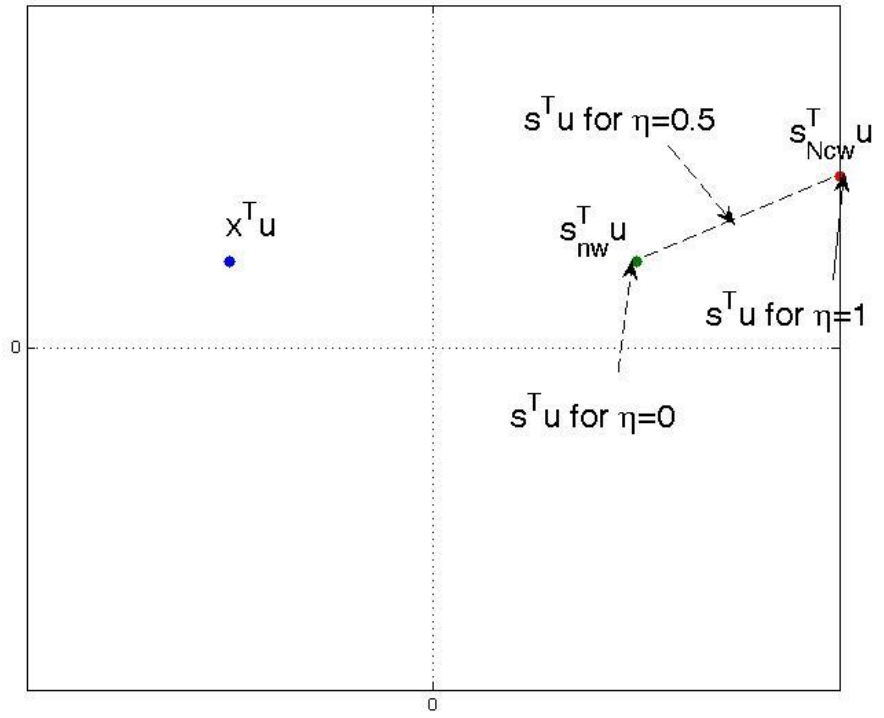
$$\mathbf{s} = \mathbf{x} + \sum_{i=1}^{N_c} \left(\alpha \mathbf{m}(i) \frac{\text{sign}\ \mathbf{x}^T \mathbf{u}_i\ \ \mathbf{x}^T \mathbf{u}_i}{\left\| \mathbf{x}^T \mathbf{u}_i \right\|} - \mathbf{x}^T \mathbf{u}_i \right) \mathbf{u}_i$$

- Normalized-CW is the key to design our trade-off watermarking because of the following two properties
  - Normalized-CW can achieve roughly the same robustness as CW-ISS
  - Normalized-CW keeps the watermarked signal's projection (in the embedding subspace) in the same orientation as NW

Technical approach

Tradeoff Watermarking:

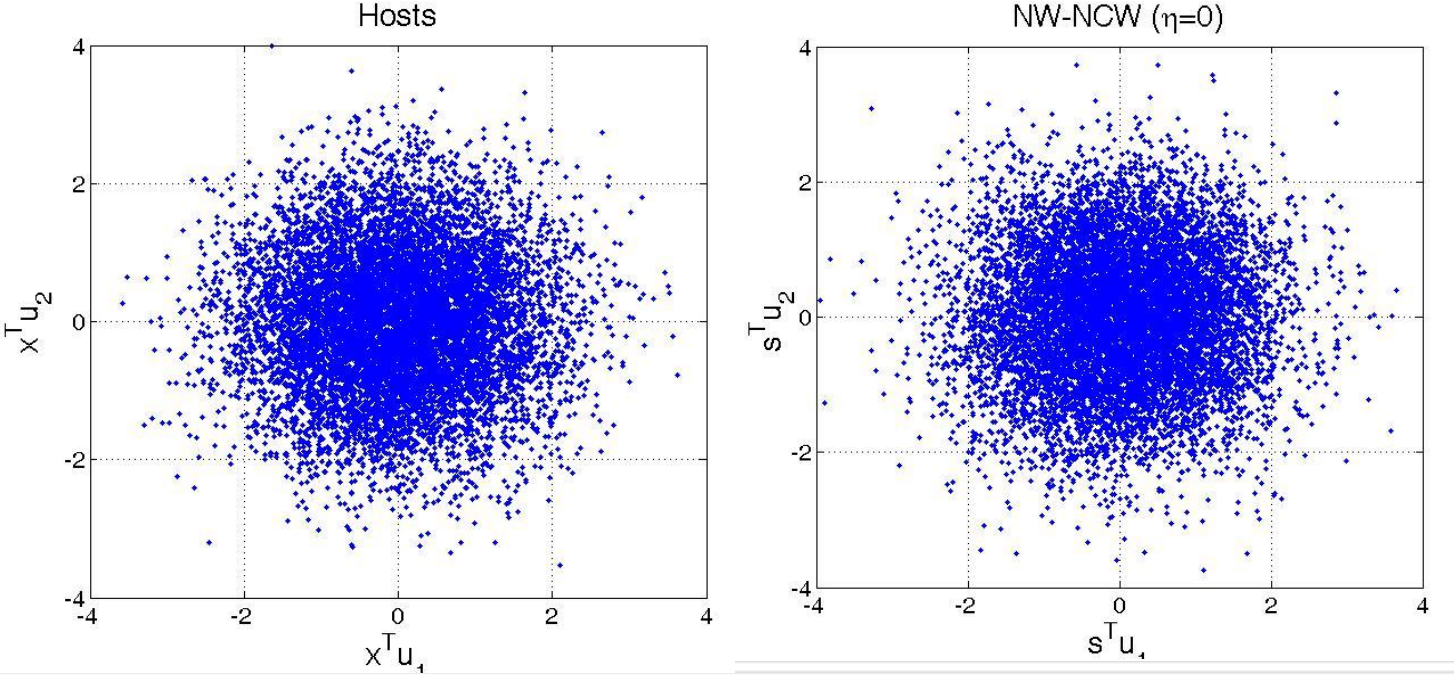
The tradeoff is achieved by taking an convex combination of the projection of watermarked signal after NW and that after Normalized-CW.



$$\mathbf{s}^T\mathbf{u} = (1-\eta)\mathbf{s}_{NW}^T\mathbf{u} + \eta\mathbf{s}_{NCW}^T\mathbf{u}$$

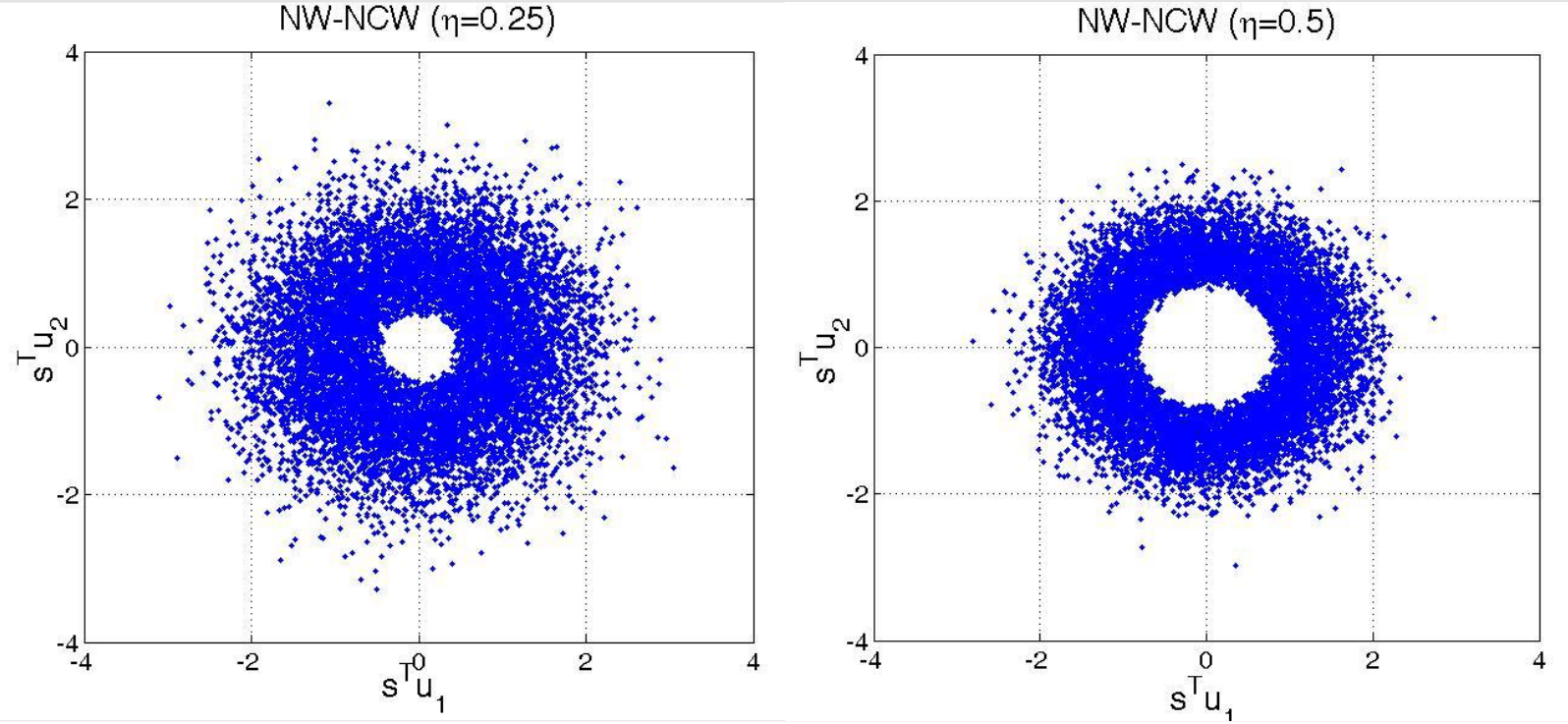
Experiment results (security)

Following figures depict the distributions of the projections of watermarked signal in the embedding subspace for various η



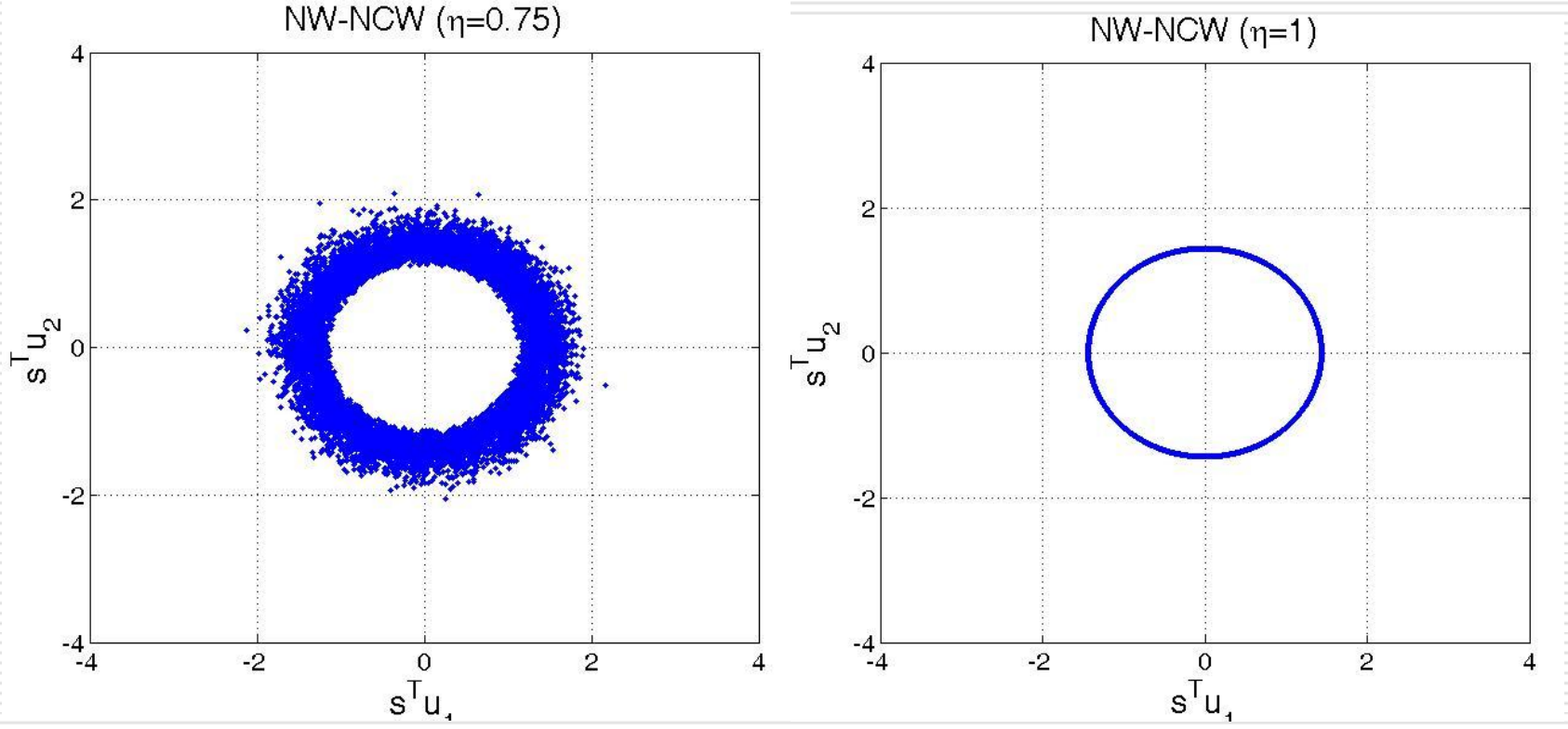
Projections of observations in the embedding subspace

Experiment results (security)



Projections of observations in the embedding subspace

Experiment results (security)

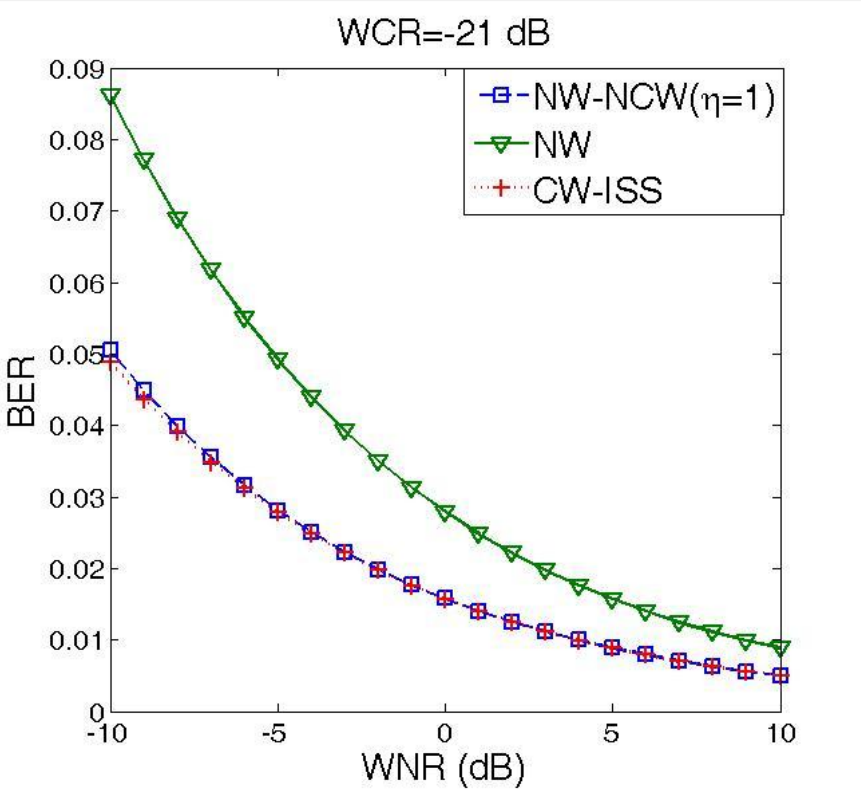


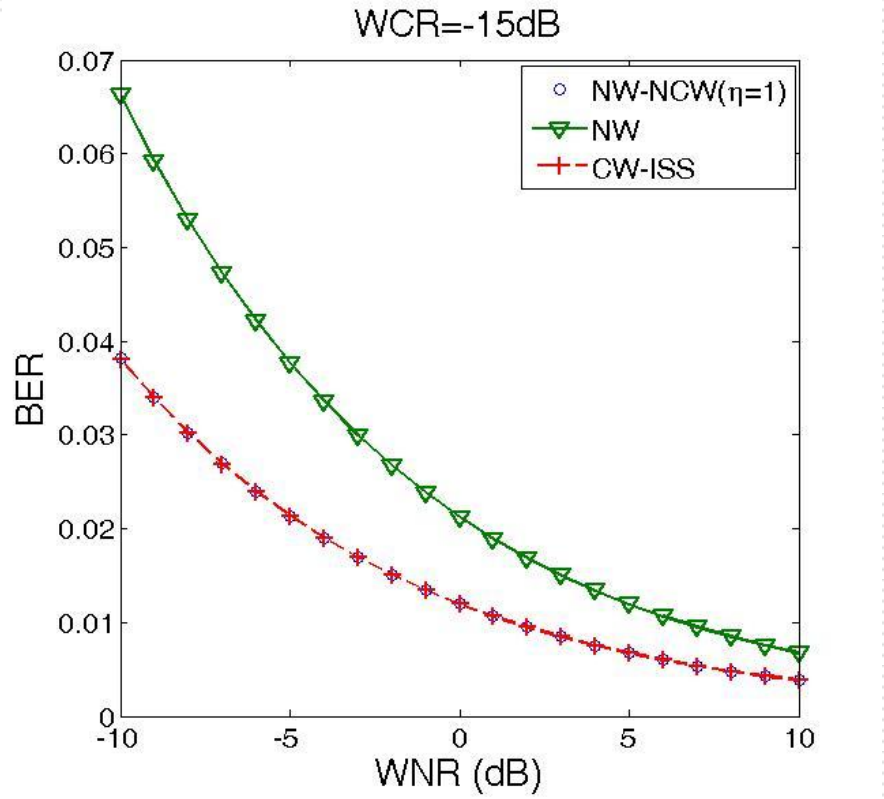
Projections of observations in the embedding subspace

Experiment results (security)

- Conclusion about the security of our tradeoff watermarking
  - As we expected, for any given the embedding parameter, the projection of watermarked signal has a distribution invariant under rotations. Besides, in the case when $\eta = 0$, host signal keeps invariant during embedding. These experiments show that for any given the embedding parameter, NW-NCW is secure against carriers estimation and when $\eta = 0$, NW-NCW is secure against the embedding subspace estimation.

Experiment results (Robustness)





Comparsion of BER for NW, CW-ISS and NW-NCW

Experiment results (Robustness)

- Conclusion about the robustness of our tradeoff watermarking
  - As we can see, NW-NCW can achieve roughly the same robustness as CW-ISS when the parameter $\eta = 0$

Conclusion

- Presenting a spread spectrum watermarking scheme which can provide a trade-off between robustness and security. Its three properties:
  - It is circular watermarking for freely chosen embedding parameters.
  - There exists a embedding parameters setting such that it is secure against the embedding space estimation.
  - There exists a embedding parameters setting such that it can achieve roughly the same robustness as circular extension of ISS