Hindawi
Security and Communication Networks
Volume 2018, Article ID 4740174, 1 page
https://doi.org/10.1155/2018/4740174

Editorial

Exploiting the Security Aspects of Compressive Sampling

Junxin Chen,[1] **Leo Yu Zhang**,[2] **Yushu Zhang**,[2] **Fabio Pareschi**,[3] **and Yu-Dong Yao**[4]

[1]*Sino-Dutch Biomedical and Information Engineering School, Northeastern University, Shenyang, Liaoning, China*
[2]*School of Information Technology, Deakin University, Burwood, VIC, Australia*
[3]*Department of Engineering, University of Ferrara, Ferrara, Italy*
[4]*Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, USA*

Correspondence should be addressed to Junxin Chen; chenjx@bmie.neu.edu.cn

Received 20 February 2018; Accepted 21 February 2018; Published 24 April 2018

Compressive sampling (CS) has received extensive research attention in the past decade, as it allows sampling at a rate lower than that required by the Nyquist-Shannon sampling theorem. Besides, benefiting from its intrinsic simplicity, convenience and simultaneous encryption, and compression performance, CS also shows great potential in the information security field. This special issue received 13 submissions and published 5 papers which are carefully peer-reviewed by experts in the field.

The published papers of this special issue focus on the application security of compressive sampling. R. Zhang et al. extended the usage of CS for image authentication. Specifically, the primary image is firstly (DWT) transformed and then divided into important part, that is, low frequency part, and unimportant part, that is, high frequency part. For high frequency part, it is encrypted with CS to vacate space for watermark, whereas chaotic encryption is employed to conceal the low frequency phase. The innovation is that Zhang's scheme can realize not only tamper detection and localization but also tamper recovery, in comparison with existing authentication algorithms. J. Wang et al. proposed to use CS for identifying data injection attacks in a nonlinear cyber-physical system and it can also work well in linear systems. The authors conclude that only a small fraction of the observations is supposed to be attacked at a given time instance due to the property of data injection attacks. Hence the error correction problem can be formulated as a sparse optimization primitive and consequently highly relates to CS theory. M. Li et al. proposed to combine reversible data hidden (RDH) with CS and investigated a novel method for image encryption. The key idea is that RDH is applied in CS domain, which introduces a variety of benefits in terms of image sampling, communication, and security. It is demonstrated that the watermark embedding rate is significantly higher than those of other state-of-the-art schemes. Furthermore, the computational complexity of the receiver is also reduced. Two image security papers have also been included in this special issue and are expected to be beneficial for broadening the CS security research. C. Fu et al. developed a chaos-based color image encryption scheme. Different from traditional solutions, a pixel swapping based scrambling approach is developed for permutation, whereas an efficient keystream generation strategy is employed for pixel substitution. Experimental results demonstrate the satisfactory security performance. C.-J. Ouyang et al. considered the security measure in steganography and steganalysis. The proposed security measure evaluates the similarity between two vague sets of cover images and stego images in terms of *n-order* Markov chain for capturing the interpixel correlation and has been shown to have the properties of boundedness, commutativity, and unity.

Presenting these papers together in a special issue, we wish to provide better views for general readers and researchers about the state-of-the-art development of CS security and also expect that this special issue can attract more researchers into the CS security area.

Junxin Chen
Leo Yu Zhang
Yushu Zhang
Fabio Pareschi
Yu-Dong Yao