LOW-COMPLEXITY SECURE WATERMARK ENCRYPTION FOR COMPRESSED SENSING-BASED PRIVACY PRESERVING

Kai-Ni Hou, Ting-Sheng Chen, Hung-Chi Kuo, Tzu-Hsuan Chen and An-Yeu (Andy) Wu

Graduate Institute of Electronics Engineering, National Taiwan University, Taipei, 106, Taiwan, R.O.C.
{kanny, tim, charleykuo, jesse}@access.ee.ntu.edu.tw, andywu@ntu.edu.tw

ABSTRACT

The emerging compressed sensing (CS) technique enables new reduced-complexity designs of sensor nodes and helps to save overall transmission power in wireless sensor network. Because of the linearity of its encoding process, CS is vulnerable to Ciphertext-Only Attack (COA) and Known-Plaintext Attack (KPA). The prior works use multiple sensing matrices as the shared secret key, however, the complexity overhead of front-end sensor and synchronization issue arising from multiple keys should be well considered. In this paper, by leveraging the characteristic of CS that is sensitive to destroyed sparsity, a low-dimension watermark is randomly chosen and embedded in measurement in front-end part. Then, in back-end solver, the proposed decrypting basis can decipher the encrypted signals without synchronization. Simulation results show that the proposed scheme achieves effective protection against COA and KPA with only 5% storage overhead. It furtherly eases the encryption complexity of front-end sensor by 98.8% under our experiments.

Index Terms—compressed sensing (CS), watermark encryption, secure communications, privacy preserving

1. INTRODUCTION

The Internet of things (IoT) relies on wireless sensor network (WSN) to acquire large amounts of data locally with extremely tight resource budgets [1-2]. Data compression is necessary before transmitted to a remote node [3]. Most of all, privacy preserving in a resource-constraint environment is a great challenge. Combination of compression and cryptographic techniques is investigated but faced with a trade-off among channel bandwidth, robustness and complexity overhead [4-5].

Compressed Sensing (CS) [6-7] is an emerging signal processing technique. In the front-end sensor, the signal $\boldsymbol{x}$ is sampled by an underdetermined sensing matrix $\boldsymbol{\Phi}$ and then transformed to a compressed signal $\boldsymbol{y}$. It enables new reduced-complexity designs of sensor nodes (ADC, compression units and RF component). Afterward, the back-end solver performs reconstruction algorithm to recover the original signal $\boldsymbol{x}$. By transferring the burden from front-end sensor to back-end solver, CS helps to save overall transmission power in wireless sensor network [8-10], which is very suitable for IoT applications.

In addition to transmission power reduction, several researches show that CS can also be an encryption technique [11-14]. Without explicit sensing matrix $\boldsymbol{\Phi}$, the compressed signal $\boldsymbol{y}$ cannot be reconstructed successfully. As a result, CS can be regarded as a zero-cost encryption.

The first-two authors contributed equally.
This work was supported in part by the Ministry of Science and Technology of Taiwan (MOST 106-2221-E-002-204-MY3).

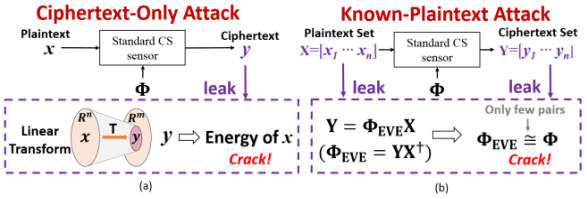

Fig. 1. Standard CS encryption under (a) Ciphertext-Only attack (COA); (b) Known-plaintext attack (KPA).

However, because of the linearity of CS encoding process, CS is vulnerable to several attacks [15-16]. As shown in Fig. 1(a), under Ciphertext-Only Attack (COA), Eve (eavesdropper) can estimate energy of $\boldsymbol{x}$ without $\boldsymbol{\Phi}$, which reveals some static information of Alice (transmitter). If Eve can furtherly collect not only $\boldsymbol{y}$ but $\boldsymbol{x}$ under the scenario of Known-Plaintext Attack (KPA), Eve can obtain the explicit sensing matrix with very few pairs as shown in Fig. 1(b). Thus, $\boldsymbol{y}$ can be easily reconstructed by Eve, threatening the privacy preserving of CS-based wireless sensor networks.

Recently, prior works have coped with the attacks by changing $\boldsymbol{\Phi}$ since sensing matrix $\boldsymbol{\Phi}$ is regarded as an encrypting key [17-20]. However, two issues should be addressed when applying prior secure model to the realistic IoT applications:

1) *High complexity of front-end sensor*: compared to single key, multiple sensing matrices require higher complexity overhead of matrix generating unit in the front-end sensor, which may not suitable for the demand of IoT applications.
2) *Synchronization issue*: Synchronization is necessary for multiple sensing matrices before reconstruction, which causes the fact that security level increases only linearly as the number of $\boldsymbol{\Phi}$ increases.

In this paper, by taking advantages that CS reconstruction is vulnerable to additive noise [21], we aim to develop a low-complexity CS-based privacy preserving framework without synchronization of key. The main contributions of this paper are as follows:

1) We proposed a novel framework for CS-based privacy preserving. In the front-end of our framework, a low-dimension watermark is randomly chosen, modulated for the target power and embedded in measurement. It can confuse the eavesdropper effectively.
2) The proposed decrypting basis in back-end solver can decipher the encoded signals without changing matrices and synchronizing watermarks, which also increases the confidential level.

The rest of this paper is organized as follows. Section 2 briefly reviews the theory of CS and prior works. Section 3 illustrates the proposed CS-based secure watermark encryption for privacy preserving. The numerical experiments and analyses are shown in Section 4. Finally, Section 5 concludes this paper.

2. PRELIMINARIES

2.1. Compressed Sensing

Compressed Sensing (CS), a technique that samples and compresses data simultaneously, is capable of transferring the complexity from front-end sensor to back-end solver. Through its linear and dimensionality-reducing transformation, CS can save transmission power in WSN. Since sparsity reflects the ability of the signal to be compressed, the processed signal needs to be sparse enough. Besides, on the proper basis, most of the natural signals are known to be sparse. Through the equation

$$\boldsymbol{x} = \sum_{i=1}^{P} \boldsymbol{\psi}_i \times \boldsymbol{s}_i = \boldsymbol{\Psi s}, \tag{1}$$

the signal $\boldsymbol{x}$ can be represented to the corresponding sparse vector $\boldsymbol{s} \in \mathbb{R}^{P\times 1}$ on the sparsifying basis $\boldsymbol{\Psi} \in \mathbb{R}^{n\times P}$.

With $\boldsymbol{\Phi} \in \mathbb{R}^{m\times n} (m \ll n)$ as the sensing matrix, the original signal $\boldsymbol{x} \in \mathbb{R}^{n\times 1}$ can lower the dimension through the equation $\boldsymbol{y} = \boldsymbol{\Phi x}$, where $\boldsymbol{y} \in \mathbb{R}^{m\times 1}$ is a transmitted measurements.

To reconstruct the original signal $\boldsymbol{x}$, measurement $\boldsymbol{y}$ and $\boldsymbol{\Theta} = \boldsymbol{\Phi\Psi}$ can solve sparse coding problem: $\min\|\boldsymbol{s}\|_1$, s.t. $\boldsymbol{\Theta s} = \mathbf{y}$. Applying to reconstruction algorithm such as Basis Pursuit (BP) [22], we obtain the recovered sparse signal $\hat{\boldsymbol{s}}$ and then the recovered signal $\hat{\boldsymbol{x}}$ according to (1).

2.2. Security Scenarios and Attack Models

Standard CS model can be regarded as a private key cryptosystem, where the plaintext $\boldsymbol{x}$ is mapped to the ciphertext $\boldsymbol{y}$ by private key $\boldsymbol{\Phi}$ [16]. In the CS-based encrypting setting, Alice encrypts $\boldsymbol{x}$ to $\boldsymbol{y}$ by using $\boldsymbol{\Phi}$, then sending $\boldsymbol{y}$ to Bob. Bob can decrypt $\boldsymbol{y}$ if he is provided with private information which can regenerate $\boldsymbol{\Phi}$. In the following, we discuss two attack situations.

Ciphertext Only Attack (COA) means that the eavesdropper, Eve, is only capable of collecting $\boldsymbol{y}$. Based on [15], $\boldsymbol{y}$ merely discloses the energy of $\boldsymbol{x}$. However, Eve can still utilize energy of $\boldsymbol{x}$ to distinguish some information such as classifying motion or static state of Alice.

Known-Plaintext Attack (KPA) means that Eve is able to access some pairs of $(\boldsymbol{x}, \boldsymbol{y})$ which is denoted as $(\boldsymbol{x}_{set}, \boldsymbol{y}_{set})$ [16]. Applying $(\boldsymbol{x}_{set}, \boldsymbol{y}_{set})$, Eve solve the private key $(\boldsymbol{\Phi}_{Eve})$ by performing inverse operation of CS transformation: $\boldsymbol{\Phi}_{\mathbf{Eve}} = \boldsymbol{y}_{set}\boldsymbol{x}_{set}^{\dagger}$. Therefore, Eve can recover $\boldsymbol{x}$ with $\boldsymbol{\Phi}_{Eve}$.

2.3. Prior Works

For standard CS model, $\boldsymbol{\Phi}$ is acted as a shared secret key to encode $\boldsymbol{x}$ and decode $\boldsymbol{y}$. To enhance security level, most existing works utilize the method of changing $\boldsymbol{\Phi}$ during a constant time period [17-20].

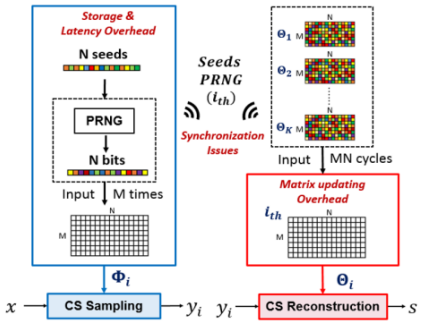

Fig. 2. Front-end sensor and back-end solver in prior model.

However, to change $\boldsymbol{\Phi}$, pseudo random number generator (PRNG) is updated for refreshing buffers of sensing $\boldsymbol{\Phi}$ as shown in Fig.2. Compared to single key, multiple sensing matrices require more complicated PRNG to generate multiple $\boldsymbol{\Phi}$, which violate the purpose of CS to reduce sensor burden. Furthermore, the solver must share and synchronize the same secret key with communication node, which increases the risk of being cracked.

3. PROPOSED FRAMEWORK

3.1. Overview of Proposed CS-based Privacy Preserving

To cope with COA and KPA, we need to confuse Eve's estimation. Therefore, under COA, our goal is to make $\boldsymbol{y}$ unable to leak explicit information of the original signal. While under KPA, we aim to increase the number of the collected $(\boldsymbol{x}, \boldsymbol{y})$ pair for recoverable estimation performed by Eve.

Since CS reconstruction is sensitive to destroyed sparsity, the quality of reconstruction drops drastically as the noise is embedded in the transmitted signal [21]. By leveraging this characteristic, we present a novel framework to introduce additional watermark to destroy the sparsity. Unlike standard CS model, the proposed encoding equation is

$$\boldsymbol{y} = \boldsymbol{\Phi}(\boldsymbol{x} + \boldsymbol{w}) = \boldsymbol{\Phi x} + \boldsymbol{W}. \tag{2}$$

For the eavesdropper who is not authenticated to receive particular key, watermark is regarded as irremovable noise so that it can degrade the reconstruction quality.

Our framework is divided into two stages as shown in Fig. 3. In off-line stage, we store multiple watermarks in the sensor and corresponding decrypting matrix in the solver. While in on-line stage, the transmitted data is encrypted with watermark by front-end sensor and decrypted by back-end solver. Noted that there is a breakable time period therefore we execute off-line stage during every period for updating multiple watermarks, i.e., generating new keys.

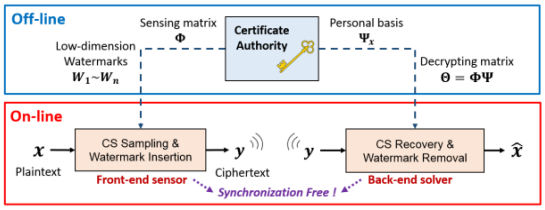

Fig. 3. The framework of the proposed algorithm.

3.2. Off-line Stage

In the front-end sensor, it only store dimensionality-reducing of multiple watermarks $\boldsymbol{W_{1\sim n} = \Phi w_{1\sim n}}$. Compared to the single watermark, multiple watermarks can confuse Eve effectively thus enhancing the security level.

Dictionary Learning (DL) is a technique to find sparse representation of signal by making the projection of training data on a pre-trained dictionary [23]. In [24], authors proposed a solution for solving dictionary-based basis optimization problem. We follow above approach to obtain dictionary-based trained basis.

In the off-line stage, we collect training signals and construct personal basis $\boldsymbol{\Psi_x}$ by applying DL. We utilize the distribution of the sparse training data set and design the customized watermarks $\boldsymbol{w_{1\sim n}}$ to confuse Eve. After constructing watermark basis $\boldsymbol{\Psi_w}$ by applying DL again, we combine $\boldsymbol{\Psi_x}$ and $\boldsymbol{\Psi_w}$ to form the merged basis $\boldsymbol{\Psi}$ as shown in Fig. 4(a). Finally, we store the decrypting matrix $\boldsymbol{\Theta = \Phi\Psi}$ in the back-end solvers. Noted that the watermark basis $\boldsymbol{\Psi_w}$ should be designed with low coherent to $\boldsymbol{\Psi_x}$ for robust reconstruction quality.

3.3. On-line Stage

In on-line stage of front-end sensor, we sample and compress the data simultaneously, and a low-dimension watermark is randomly chosen from multiple watermarks to insert the measurement. When performing the watermark insertion, we firstly set the energy goal of encrypted signal ***Goal***. After CS sampling, we obtain measurement $\boldsymbol{y}$ and randomly choose a watermark $\boldsymbol{W}$ from pre-designed multiple watermarks. To align energy (***Goal***), we utilize adaptive disturbing factor to modulate the power of $\boldsymbol{W}$ then embed $\boldsymbol{W}$ in $\boldsymbol{y}$ by applying (2).

Compared to changing the sensing matrices operated at Nyquist rate, this encryption method only embed watermark at *every N data sample*, resulting in less than 1% of energy overhead at the front-end sensor (evaluated from SPICE simulation with TSMC 40nm CMOS technology node). Furthermore, the multiple sensing matrices require much more complicated PRNG to generate multiple $\boldsymbol{\Phi}$, while single matrix and multiple watermarks have simpler hardware design.

After transmission, we apply Basic Pursuit (BP) to simultaneously recover and decrypt the data in back-end solver. The approach of removing the watermark in back-end solver is shown in Fig. 4(b). Noted that corresponding to $\boldsymbol{\Theta = \Phi[\Psi_x\Psi_w]}$, CS reconstruction finds the nonzero entries in $\hat{\boldsymbol{s}}$, which are sparse coefficients of $\boldsymbol{x + w}$. Since $\boldsymbol{\Psi_x}$ and $\boldsymbol{\Psi_w}$ is low coherent, $\hat{\boldsymbol{s}}$ can be easily separated into two regions, the sparse data of plaintext $\boldsymbol{s_x}$ and watermark $\boldsymbol{s_w}$. To successfully recover $\boldsymbol{x}$, we adapt and extend (1) as

$$\boldsymbol{x + w} = [\boldsymbol{\Psi_x\Psi_w}]\begin{bmatrix}\mathbf{s}_x \\ \mathbf{s}_w\end{bmatrix}. \tag{3}$$

By ignoring the output of $\mathbf{s}_w$, we retrieve $\hat{\boldsymbol{x}} = \boldsymbol{\Psi_x}\mathbf{s}_x$. Most importantly, since $\boldsymbol{\Psi_w}$ can decrypt any pre-defined watermarks, the proposed approach can free from synchronization of multiple watermarks. Hence, the back-end solver just needs to store the location corresponding to the region of $\boldsymbol{\Psi_w}$ rather than encrypting watermark, which also lowers the risk of leakage.

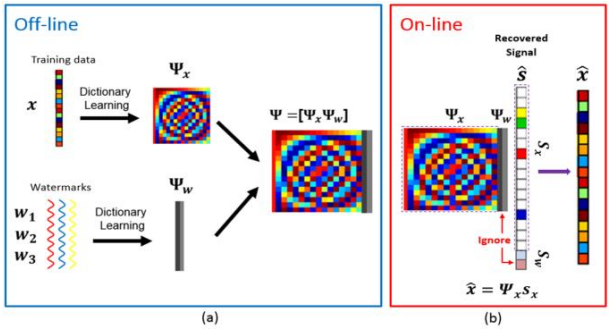

Fig. 4. (a) Decrypting basis design in off-line stage; (b) watermark removal in on-line stage.

4. SIMULATION RESULTS

4.1. ECG Database and Simulation Settings

In this section, we present experiments under different attack models. To evaluate security level, the number of watermarks in proposed framework and sensing matrices in prior model are both set to be 8. We sample the ECG signals provided by National Taiwan University Hospital at $f_s = 512$ Hz and use Bernoulli random matrix as sensing matrix in prior and proposed model. The simulation setup is summarized in Table I.

TABLE I. SIMULATION PARAMETERS

Off-line stage	
Dimension of training vectors	512
Number of training vectors	2500
Number of columns in Ψ_x	504
Number of columns in Ψ_w	8
On-line stage	
Dimension of testing vectors (*N*)	512
Dimension of measurement vectors (*M*)	128
Number of testing vectors	1500

4.2. Under Ciphertext Only Attack (COA)

COA means that Eve is able to access $\boldsymbol{y}$, whose energy discloses some information [15]. We collect the ECG signals of Atrial fibrillation (AF) and Non-AF condition from a person, both of which are sampled through standard CS model with an arbitrary Bernoulli random matrix. In Fig. 5(a), we observe that norm($\boldsymbol{x}$) and norm($\boldsymbol{y}$) have *positive correlations*. Owing to disease characteristics, the energy of signals have a distinct gap between AF and Non-AF condition. In a word, Eve can easily acquire some information of patients under COA scenario.

In Fig. 5(b), we demonstrate 15 of sampled data from the person with either AF or Non-AF condition. It is obvious that the prior model that changes sensing matrices cannot preserve the privacy, i.e., they leak the status of the patient. Conversely, the proposed framework shows that even if Eve get $\boldsymbol{y}$, the energy of $\boldsymbol{x}$ would not be estimated correctly.

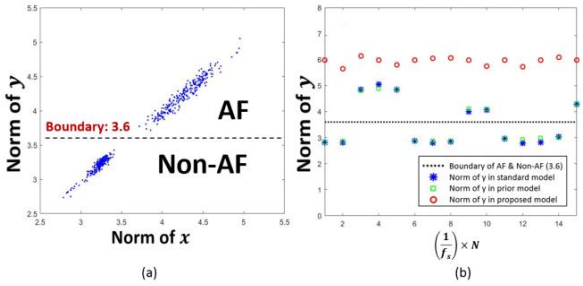

Fig. 5. (a) Energy distribution of AF and Non-AF; (b) Energy of y in the standard CS, prior and proposed model under COA.

4.3. Under Known Plaintext Attack (KPA)

Under KPA scenario, Eve can access some pairs of $(\boldsymbol{x}, \boldsymbol{y})$, which results in leaking the information of $\boldsymbol{\Phi}$. To estimate $\boldsymbol{\Phi}$, Eve performs inverse operation of CS transformation: $\boldsymbol{\Phi}_{\mathbf{Eve}} = \boldsymbol{y}_{\boldsymbol{set}}\boldsymbol{x}_{\boldsymbol{set}}^{\dagger}$, where $\boldsymbol{x}_{\boldsymbol{set}}$ and $\boldsymbol{y}_{\boldsymbol{set}}$ mean the set of $\boldsymbol{x}$ and $\boldsymbol{y}$ Eve collected. Noted that as shown in Fig. 6, in prior model, Eve can estimate several $\boldsymbol{\Phi}$ in order after classification; in proposed framework, we assume that Eve knows the existence of the watermark and considers the average of training vector is equal to zero. Regarding $\boldsymbol{W}$ as $\bar{\boldsymbol{y}}$, Eve rewrite (2) as $\boldsymbol{y} - \bar{\boldsymbol{y}} = \boldsymbol{\Phi x}$ to crack the sensing matrix and watermarks.

In the following, we perform the experiments using multiple $\boldsymbol{\Phi}$, single watermark and multiple watermarks from 1,000 to 100,000 pairs of $(\boldsymbol{x}, \boldsymbol{y})$ under KPA. To evaluate the error between the real and the estimated sensing matrix, $\boldsymbol{\Phi}$ and $\boldsymbol{\Phi}_{\mathbf{Eve}}$, we adopt the *perturbation metric* (ε), which is defined as $\|\boldsymbol{\Phi}_{\boldsymbol{O}} - \boldsymbol{\Phi}_{\boldsymbol{E}}\|_2 / \|\boldsymbol{\Phi}_{\boldsymbol{O}}\|_2$, where $\boldsymbol{\Phi}_{\boldsymbol{O}}$ is the original sensing matrix and $\boldsymbol{\Phi}_{\boldsymbol{E}}$ is the estimated sensing matrix by Eve. According to [25], we regard the recoverable estimation as $\varepsilon < 0.01$.

As shown in Fig. 7, it can be observed that the single watermark encryption model is not secure enough. The prior model are cracked as the number of the pair reaches 4,000, since the multiple matrices only increase the pairs linearly with synchronization. On the other hand, the proposed multiple-watermark encryption model can't be cracked in spite of 100,000 pairs.

We present the further experiment of recovery quality with estimated $\boldsymbol{\Phi}$ as KPA pair is 100,000, as shown in Fig. 8. We measure the *reconstruction signal-to-noise ratio* $(RSNR) = 20\log(\|\boldsymbol{x}\|_2 / \|\hat{\boldsymbol{x}} - \boldsymbol{x}\|_2)$ to evaluate the recovery quality, where $\boldsymbol{x}$ and $\hat{\boldsymbol{x}}$ are the original and reconstructed ECG signals, respectively. Fig 8(a) shows that Bob can reconstruct the signal without the interference of watermarks. Fig 8(b) depicts that Eve cannot reconstruct ECG signals with the estimated sensing

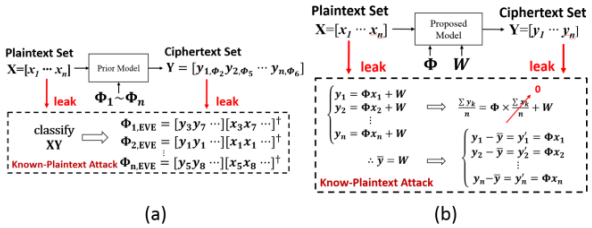

Fig. 6. Eve's estimation of $\boldsymbol{\Phi}$ in (a) prior model; (b) proposed model.

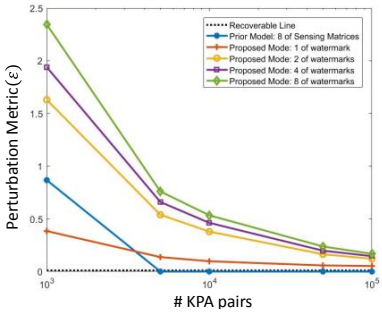

Fig. 7. Perturbation Metric of prior and proposed model.

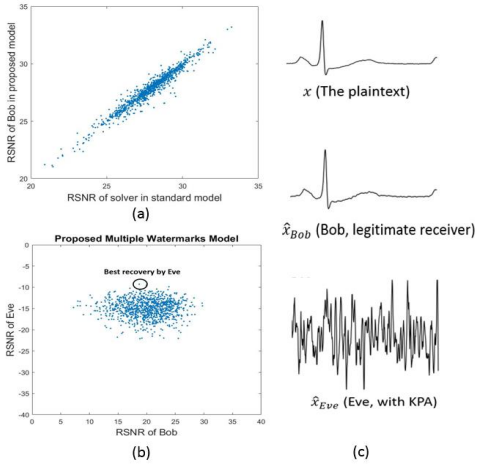

Fig. 8. Recovery quality of (a) solver in standard model and Bob in proposed model; (b) Bob and Eve in proposed model; (c) ECG signal of plaintext, reconstructed by Bob and Eve.

matrix and watermarks. The best reconstruction by Eve from the testing signals is shown in Fig. 8(c).

Lastly, we compare required bits of front-end sensor in prior and proposed model. In prior model, to generate 8 of sensing matrices, the PRNG of front-end sensor needs to have capacity of generating $(512 \times 128) \times 8 = 524288$ bits. On the other hand, in proposed model, to generate 8 of watermarks with 6-bit resolution (with fixed-point analysis), the PRNG requires the capability of generating $(128 \times 6) \times 8 = 6144$ bits with only 5% storage overhead. Therefore, our framework can release the encryption complexity of PRNG in the front-end sensor by 98.8%.

5. CONCLUSION

In this paper, we present a novel framework for CS-based privacy preserving. In contrast to using multiple sensing matrices as the shared secret, proposed watermark encryption can not only resist COA and KPA effectively but also ease the burden of device. Furthermore, combining CS reconstruction with dictionary learning can decrypt watermark without synchronization. Therefore, the proposed technique is very suitable for the emerging IoT applications that need encryption strength with very limited complexity.

6. REFERENCES

[1] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29.7 (2013): 1645-1660.

[2] Kelly, Sean Dieter Tebje, Nagender Kumar Suryadevara, and Subhas Chandra Mukhopadhyay. "Towards the implementation of IoT for environmental condition monitoring in homes." IEEE Sensors Journal 13.10 (2013): 3846-3853.

[3] Wang, Yuhao, et al. "Data-driven sampling matrix boolean optimization for energy-efficient biomedical signal acquisition by compressive sensing." IEEE transactions on biomedical circuits and systems 11.2 (2017): 255-266.

[4] Kung, Sun-Yuan. "Compressive Privacy: From Information\/Estimation Theory to Machine Learning [Lecture Notes]." IEEE Signal Processing Magazine 34.1 (2017): 94-112.

[5] Kung, Sun-Yuan, et al. "Collaborative PCA/DCA learning methods for compressive privacy." ACM Transactions on Embedded Computing Systems (TECS) 16.3 (2017): 76.

[6] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol.52, no. 4, pp. 1289–1306, Apr. 2006.

[7] E. J. Candes and M. B. Wakin, "An Introduction to Compressive Sampling," IEEE Signal Processing Magazine, vol. 25, no. 2, pp.21-30, Mar. 2008.

[8] H. Mamaghanian, N. Khaled, D. Atienza, and P. Vandergheynst, "Design and exploration of low-power analog to information conversion based on compressed sensing," IEEE J. Emerging Sel. Topics Circuits Syst., vol. 2, no. 3, pp. 493–501, Sep. 2012.

[9] R. Braojos et al., "Ultra-low power design of wearable cardiac monitoring systems," 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, 2014, pp. 1-6.

[10] Ravelomanantsoa, Andrianiaina, Hassan Rabah, and Amar Rouane. "Simple and efficient compressed sensing encoder for wireless body area network." IEEE Transactions on Instrumentation and Measurement 63.12 (2014): 2973-2982.

[11] Agrawal, Shweta, and Sriram Vishwanath. "Secrecy using compressive sensing." Information Theory Workshop (ITW), 2011 IEEE. IEEE, 2011.

[12] Rachlin, Yaron, and Dror Baron. "The secrecy of compressed sensing measurements." Communication, Control, and Computing, 2008 46th Annual Allerton Conference on. IEEE, 2008.

[13] Abdulghani, Amir M., and Esther Rodriguez-Villegas. "Compressive sensing: from "compressing while sampling" to "compressing and securing while sampling"." Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE. IEEE, 2010.

[14] Orsdemir, Adem, et al. "On the security and robustness of encryption via compressed sensing." Military Communications Conference, 2008. MILCOM 2008. IEEE. IEEE, 2008.

[15] T. Bianchi, V. Bioglio and E. Magli, "Analysis of One-Time Random Projections for Privacy Preserving Compressed Sensing," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 313-327, Feb. 2016.

[16] Cambareri, Valerio, et al. "On known-plaintext attacks to a compressed sensing-based encryption: A quantitative analysis." IEEE Transactions on Information Forensics and Security 10.10 (2015): 2182-2195.

[17] V. Cambareri, J. Haboba, F. Pareschi, H. R. Rovatti, G. Setti and K. w. Wong, "A two-class information concealing system based on compressed sensing," in Proc. ISCAS, 2013 May, pp. 1356-1359.

[18] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-complexity multiclass encryption by compressed sensing," IEEE Trans. Sig. Proc. (TSP), vol. 63, no. 9, pp. 2183-2195, May 2015.

[19] Dautov, Ruslan, and Gill R. Tsouri. "Securing while sampling in wireless body area networks with application to electrocardiography." IEEE journal of biomedical and health informatics 20.1 (2016): 135-142.

[20] Fay, Robin, and Christoph Ruland. "Compressive Sensing encryption modes and their security." Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for. IEEE, 2016.

[21] Y. M. Lin, Y. Chen, N. S. Huang and A. Y. Wu, "Low-Complexity Stochastic Gradient Pursuit Algorithm and Architecture for Robust Compressive Sensing Reconstruction," in IEEE Transactions on Signal Processing, vol. 65, no. 3, pp. 638-650, Feb.1, 1 2017.

[22] S. Chen, D. L. Donoho, and M. A. Saunders, "Atomic decomposition by basis pursuit," SIAM J. Sci Comp., vol. 43, no. 1, pp. 129–159, Feb. 2001.

[23] R. Rubinstein, A. M. Bruckstein and M. Elad, "Dictionaries for Sparse Representation Modeling," in Proceedings of the IEEE, vol. 98, no. 6, pp. 1045-1057, June 2010.

[24] J. Mairal, F. Bach, J. Ponce, and G. Sapiro, "Online dictionary learning for sparse coding," in Proc. International Conference on Machine Learning (ICML). Jun. 2009, pp. 689-696.

[25] M. A. Herman and T. Strohmer, "General Deviants: An Analysis of Perturbations in Compressed Sensing," IEEE Journal of Selected Topics in Signal Processing, vol. 4, no. 2, pp. 342-349, April 2010.