IJE TRANSACTIONS A: Basics Vol. 33, No. 7, (July 2020) 1214-1222

International Journal of Engineering

Journal Homepage: www.ije.ir

Optimal Singular Value Decomposition Based Pre-coding for Secret Key Extraction from Correlated Orthogonal Frequency Division Multiplexing Sub-channels

A. Aliabadian, M. R. Zahabi*, M. Mobini

Department of Electrical and Computer Engineering, Babol Noshirvani University of Technology, Babol, Iran

PAPER INFO

Paper history:
Received 07 November 2019
Received in revised form 02 June 2020
Accepted 18 June 2020

Keywords:
Orthogonal Frequency Division Multiplexing
Physical Layer Security
Secret Key
Singular Value Decomposition based Channel Decorrelation

ABSTRACT

Secret key extraction is a crucial issue in physical layer security and a less complex and, at the same time, a more robust scheme for the next generation of 5G and beyond. Unlike previous works on this topic, in which Orthogonal Frequency Division Multiplexing (OFDM) sub-channels were considered to be independent, the effect of correlation between sub-channels on the secret key rate is addressed in this paper. As an assumption, a realistic model for dependency among sub-channels is considered. Benchmarked by simulation, the result shows that the key exchange rate may decline by up to 72% due to the correlation of sub-channels. A new approach for efficient key extraction is used in this study. To do this, a Singular Value Decomposition based (SVD-based) pre-coding is utilized to alleviate the sub-channels correlation and the channel noise. The low computational complexity of our proposed approach makes it a promising candidate for developing secure and high-speed networks. Results obtained through simulation indicate that applying pre-coding on the measured correlated data resulted in a minimum gain of 9 dB. In addition, the result also depicts the advantage of SVD versus other pre-coding techniques, namely PCA, DCT, and WT.

doi: *10.5829/ije.2020.33.07a.07*

1. INTRODUCTION

Efficient secret key generation of physical layer and authentication schemes based on wireless channels are developing issues in physical layer security, especially in Orthogonal Frequency Division Multiplexing (OFDM)-based communication systems. Therefore, the channel parameter has received a lot of attention in literature as the fundamental part of key construction techniques [1-3].

Depending on the environmental conditions, the Key Generation Rate (KGR) is defined as a parameter that specifies the rate of secret key bits generated per second. Similarly, Key Disagreement Rate (KDR) is defined as the distinction rate of the key bits generated by Alice and Bob as the two ends of the communication link.

In recent studies, OFDM structures have been utilized for key generation with long sequences and increasing the rate of key generation by obtaining a key for each sub-channel in a coherence time. Since KGR and KDR oppose each other, a reasonable tradeoff should be set. This setting is configured between them by considering the demands of the system and the user interface. In literature, the key generation method is separated into four stages including the channel probing, quantization, information reconciliation and privacy amplification [4-6].

In the channel probing stage, the transmitter and the receiver use the static period of channel parameters in a coherence time interval. The extracted parameters from the channel are channel impulse response, channel frequency response, received signal strength, and channel phase.

In this stage, due to several reasons such as the channel noise, random displacements, multipath and scattering, the values measured by both ends of the communication link are not equal so some pre-processing should be done [7]. Unequal measurements of the

*Corresponding Author Email: *zahabi@nit.ac.ir* (M. R. Zahabi)

Please cite this article as: A. Aliabadian, M. R. Zahabi, M. Mobini, Optimal Singular Value Decomposition Based Pre-coding for Secret Key Extraction from Correlated Orthogonal Frequency Division Multiplexing Sub-channels, International Journal of Engineering (IJE), IJE TRANSACTIONS A: Basics Vol. 33, No. 7, (July 2020) 1214-1222

channel lead to disagreement among the keys, while a high KDR might lead to the deficiency of the key generation process [8, 9].

The quantization scheme is utilized to optimize the operation of randomness, KGR, and KDR by adjusting the level of quantization and the threshold limit [10, 11].

Another part of the information is also sent through public channels during the information reconciliation stage, which can be heard by Eve as a wire-tapper. This can potentially threaten the security of the key sequence. Privacy amplification is finally used for removing the revealed information from the agreed key sequence by legitimate users (Alice and Bob).

In the key generation, based on channel reciprocity, the secret key is made from one or more channel parameters such as channel phase, Received Signal Strength (RSS), and Channel State Information (CSI) [5, 12].

In the previous works on this topic, it is typically assumed that the sub-channels do not correlate for the sake of simplicity. In practice, there is a correlation between the sub-channels that suppresse the assumption of randomness. Thus, determining the secret key rate by considering the correlation between sub-channels and maintaining the randomness as well as increasing the KGR is essential in physical layer security. However, in this paper, the correlation between the sub-channels and its effect on the secret key rate is studied.

There is no theoretical model for the mutual correlation between the measured values due to the lack of closed form for it. Thus, the correlation can be improved by interpolation or filter configuration, which is commonly done through different experiments [8, 13]. Due to the considerable impact of noise in a slow fading channel, a Low Pass Filter (LPF*)* is needed to eliminate the high-frequency components of the noise and to enhance the correlation [14].

In [9], efficient signal pre-coding is addressed and it is demonstrated that Principal Component Analysis (PCA)-based pre-coding achieves a higher KGR than Discrete Cosine Transform (DCT) and Wavelet Transform (WT). In other words, the channel correlation can be eliminated by a signal pre-processing procedure such as PCA [15], DCT [16, 17], and WT [18, 19].

The singular value decomposition (SVD) is a factorization of a real or complex matrix by which the original matrix is expressed by/forms three matrix, namely USV*. One of the most widely used functions of SVD is noise elimination and reduction of measured correlations.

In this paper, inspired by [9], an SVD-based channel decorrelation is proposed which is more accurate than the PCA-based method, with a significant superiority from the computational complexity point of view.

The main contributions that distinguish our work from others in literature are as follows:

- In previous works, authors did not consider the correlation among sub-channels, for the sake of simplicity. However, in our study, the effect of correlation among sub-channels is evaluated by applying a new realistic model.
- An optimal SVD-based pre-coding scheme is presnted which has lower computational complexity than other works. Moreover, the Mutual Information (MI) calculation and KGR improvement are provided.
- Our proposed SVD-based method is numerically compared with some other approaches, especially with the PCA-based method as an appropriate benchmark to determine the method which is better for key extraction; to the best of our knowledge, the numerical aspect has not been yet considered in any previous literature. As a result of SVD-based pre-coding, one will be able to obtain an optimal key generation.

The remainder of this paper is organized as follows: In Section 2, the communication and adversary models are presented. The correlation of the sub-channels and its effect on the secret key rate is also derived in this section. In Section 3, our proposed SVD-based pre-coding is addressed. The comparison among SVD and other approaches are also done, and advantages of the proposed approach are further investigated. In Section 4, simulation results are expressed. Finally, Section 5 deals with conclusions.

2. OFDM SYSTEM MODEL WITH CORRELATED SUB-CHANNLE

Figure 1 shows an OFDM-based system model including three nodes in which Alice and Bob are known as legitimate users and Eve is known as the adversary or the interceptor [20]. In this model, the adversary can only initiate a passive attack. In other words, Eve can tap into the connection between legitimate users and search for the secret key based on her deductions. Therefore, she cannot affect the information between Alice and Bob [21, 22]. Alice and Bob use a half-duplex communication system. Thus, they cannot simultaneously send and receive a signal. Mathematically, Alice and Bob attempt to estimate the channel by sending signals according to the following formulas:

$$h_A = h_{BA} + z_A \quad , \quad h_B = h_{AB} + z_B \tag{1}$$

in which z_A and z_B refer to the channel noises at the locations of Alice and Bob respectively. h_{BA} and h_{AB} are the legitimate channel vectors in frequency domain.

The measured values of the channel such as CSI, RSS, and channel phase are collected by Alice and Bob. They probe the channel by sending successive time signals in each period. Due to channel reciprocity in coherence time, a high correlation exists between the measured values of Alice and Bob, and these measured

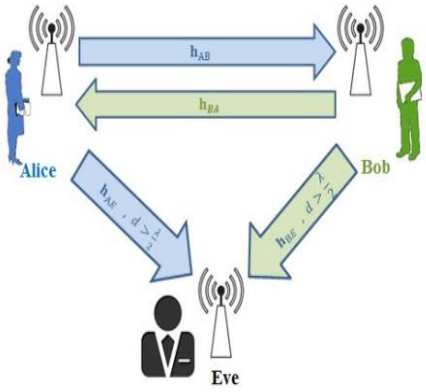

Figure 1. The communication model

values of the channel will change into a vector of bits after quantization. However, the quantized values of the channel slightly differ from each other due to the existence of noise. Because of the channel reciprocity between $\mathbf{h}_{\mathrm{BA}}$ and $\mathbf{h}_{\mathrm{AB}}$ which are the channel vectors between Alice and Bob in the frequency domain, they can be written as:

$$\begin{aligned} &\mathrm{h_{BA}} = \mathrm{h_{AB}} = \mathrm{h} = [\mathrm{h_1}, \mathrm{h_2}, \ldots \mathrm{h_N}], \\ &\mathrm{z_A} = [\mathrm{z_{A1}}, \mathrm{z_{A2}}, \ldots \mathrm{z_{AN}}] \quad , \quad \mathrm{z_B} = [\mathrm{z_{B1}}, \mathrm{z_{B2}}, \ldots \mathrm{z_{BN}}]. \end{aligned} \tag{2}$$

In Figure 1, the terms $\mathbf{h}_{\mathrm{AE}}$ and $\mathbf{h}_{\mathrm{BE}}$ show information about Eve from the channel and it is assumed that Eve is positioned at a distance greater than one half-wavelength from Alice and Bob. Therefore, $\mathbf{h}_{\mathrm{E}}$ has no correlation with $\mathbf{h}_{\mathrm{A}}$ and $\mathbf{h}_{\mathrm{B}}$. Here, it is assumed that the sub-channels h_i, $i = 1,2,3, \ldots$ N have $CN(0, \sigma_{h_i}^2)$ distribution and also $\boldsymbol{z}_{Bi}$ and $\boldsymbol{z}_{Ai}$ are independent noises with distributions $\boldsymbol{z}_{Ai} \sim CN(0, \sigma_{Z_{Ai}}^2)$, and $\boldsymbol{z}_{Bi} \sim CN(0, \sigma_{z_{Bi}}^2)$ which are also independent of h_i. Therefore, the estimated values of $\mathbf{h}_{\mathrm{A}}$ and $\mathbf{h}_{\mathrm{B}}$, and their distributions can be readily written as:

$$\mathrm{h_A} = \mathrm{h_{BA}} + \mathrm{z_A} \quad , \quad \mathrm{h_B} = \mathrm{h_{AB}} + \mathrm{z_B} \tag{3}$$

$$\mathrm{h_A} \sim \mathrm{CN}(0, \mathrm{R_A}) \quad , \quad \mathrm{h_B} \sim \mathrm{CN}(0, \mathrm{R_B}) \tag{4}$$

$$(\mathrm{h_A}, \mathrm{h_B}) \sim \mathrm{CN}(0, \mathrm{R_{AB}}) \ , \ \mathrm{R_{AB}} = \begin{bmatrix} \mathrm{R_A} & \mathrm{R_C} \\ \mathrm{R_D} & \mathrm{R_B} \end{bmatrix} \tag{5}$$

where the covariance matrices $\boldsymbol{R}_A$ and $\boldsymbol{R}_B$ are both diagonal. In literature, for the sake of simplicity, it is assumed that the sub-channels have no correlation and the secret key rate in OFDM systems based on the sub-channel state information is calculated and analyzed. To increase the key generation rate, the corresponding keys k_i are generated for each independent sub-channel h_i from N sub-channels, and the long key sequence K is then generated as:

$$K = k_1 k_2 k_3 \ldots k_N \tag{6}$$

It should be noted that there is a correlation between the sub-channels which leads to the lower randomness in the practical scenarios. Thus, calculating the secret key rate by considering the amount of correlation among sub-channels and maintaining randomness as well as increasing the KGR would be crucial. The relation of the secret key rate for $\mathbf{h}_A$ and $\mathbf{h}_B$ is given as [14]:

$$\begin{aligned} &I_m = I(\mathbf{h_A}, \mathbf{h_B} | \mathbf{h_{AE}}) = I(\mathbf{h_A}, \mathbf{h_B} | \mathbf{h_{BE}}) = I(\mathbf{h}_A, \mathbf{h}_B) \\ &= H(\mathbf{h}_A) + H(\mathbf{h}_B) - H(\mathbf{h}_A, \mathbf{h}_B) \end{aligned} \tag{7}$$

in which H(.) refers to entropy function. Therefore, by considering the correlation among sub-channels in the OFDM system, the relation for the covariance between the two sub-channels h_{iA} and h_{jA} can be written as:

$$\begin{aligned} &COV(h_{iA}, h_{jA}) = COV[(h_i + n_{Ai}), (h_j + n_{Aj})] = \\ &E[(h_i + n_{Ai})(h_j + n_{Aj})^*] \\ &= E[h_i h_j{}^* + h_i n_{Aj}{}^* + h_j{}^* n_{Ai} + n_{Ai} n_{Aj}{}^*] \\ &= \begin{cases} E(h_i h_j{}^*) & i \neq j \\ E(|h_i|^2) + E(|n_i|^2) & i = j \end{cases}, \end{aligned} \tag{8}$$

where the covariance matrices R_A and R_B are diagonal matrices defined by:

$$\mathbf{R}_A = \begin{pmatrix} \sigma_{h_1}^2 + \sigma_{n_{A_1}}^2 & E(h_1 h_2{}^*) & \cdots & E(h_1 h_N{}^*) \\ E(h_2 h_1{}^*) & \sigma_{h_2}^2 + \sigma_{n_{A_2}}^2 & \ldots & \\ \vdots & & \ddots & \vdots \\ E(h_N h_1{}^*) & \ldots & & \sigma_{h_N}^2 + \sigma_{n_{A_N}}^2 \end{pmatrix} \tag{9}$$

$$\mathbf{R}_B = \begin{pmatrix} \sigma_{h_1}^2 + \sigma_{n_{B_1}}^2 & E(h_1 h_2{}^*) & \cdots & E(h_1 h_N{}^*) \\ E(h_2 h_1{}^*) & \sigma_{h_2}^2 + \sigma_{n_{B_2}}^2 & \ldots & \\ \vdots & & \ddots & \vdots \\ E(h_N h_1{}^*) & \ldots & & \sigma_{h_N}^2 + \sigma_{n_{B_N}}^2 \end{pmatrix} \tag{10}$$

Also $\mathbf{R}_C$ and $\mathbf{R}_D$ are defined by:

$$\mathbf{R}_C = \mathbf{R}_D = \begin{pmatrix} \sigma_{h_1}^2 & E(h_1 h_2{}^*) & \cdots & E(h_1 h_N{}^*) \\ E(h_2 h_1{}^*) & \sigma_{h_2}^2 & \ldots & \\ \vdots & & \ddots & \vdots \\ E(h_N h_1{}^*) & \ldots & & \sigma_{h_N}^2 \end{pmatrix}. \tag{11}$$

Therefore, the formula for the secret key rate can be derived as follows:

$$\begin{aligned} &I(\mathbf{h}_A; \mathbf{h}_B) = log_2(|\pi e \mathbf{R}_A|) + log_2(|\pi e \mathbf{R}_B|) - \\ &log_2(|\pi e \mathbf{R}_{AB}|) = log_2\left(\frac{|\mathbf{R}_A|.|\mathbf{R}_B|}{|\mathbf{R}_A|.|\mathbf{R}_A - \mathbf{R}_D \mathbf{R}_A{}^{-1} \mathbf{R}_C|}\right). \end{aligned} \tag{12}$$

3. THE PROPOSED SVD-BASED PRE-CODING METHOD

In this section, our proposed SVD-based pre-coding method is presented. According to Equation (12), to achieve a more efficient secret key and preventing the similarity of key sequences, the correlation between sub-channels should be considered. Using Equation (12) in

which the frequency correlation of the sub-channels is considered, a more accurate model for the KGR can be presented. It is worthwhile to point out that the correlation between the measured sub-channel coefficients of data can be eliminated by a signal pre-processing procedure such as the PCA [15], DCT [16, 17] and WT [18, 19]. In [9], a new pre-coding method is addressed and it is also demonstrated that PCA-based pre-coding achieves a higher KGR than both the DCT and the WT. In this paper, the SVD is applied on the covariance matrix of the channel $\mathbf{h}_A$. The correlation matrix is defined as:

$$\mathbf{R}_{\mathrm{A}} = E\{\mathbf{h}_A \mathbf{h}_A{}^H\} = \mathbf{U}_A(\mathbf{\Lambda}_A + \sigma_n^2 \mathbf{I}_N)\mathbf{U}_A^H \quad (13)$$

where $\mathbf{U}_A = [u_A^{(1)}, u_A^{(2)}, \dots u_A^{(N)}]$ is the transform matrix and $\mathbf{\Lambda}_A$ is a diagonal matrix with sorted eigenvalues ($\lambda_1 \geq \lambda_2 \dots \geq \lambda_i \geq \lambda_N$). Our main goal is to obtain the optimal unitary matrix $\mathbf{V}^*$ through maximizing the MI which can be obtained using:

$$\mathbf{V}^* = Arg\ max_{\mathrm{V}}\ \tilde{I} \qquad s.t\ \mathbf{V}^{\mathrm{H}}\mathbf{V} = \mathbf{I}_{\mathrm{M}},\ \mathbf{M} \leq \mathbf{N}. \quad (14)$$

Ultimately, $\mathbf{V}_A^*$, $\widetilde{\mathbf{R}}_A$, $\widetilde{\mathbf{R}}_B$, $\widetilde{\mathbf{R}}_C$ and $\widetilde{\mathbf{R}}_D$ are written as:

$$\mathbf{V}_A^* = \left[v_A^{*(1)}, v_A^{*(2)}, \dots v_A^{*(M)}\right], \quad (15)$$

$$\widetilde{\mathbf{R}}_A = \mathbf{V}_A^*(\mathbf{\Lambda}_A + \sigma_n^2 \mathbf{I}_M)\mathbf{V}_A^{*\mathrm{H}}, \quad (16)$$

$$\widetilde{\mathbf{R}}_B = \mathbf{V}_B^*(\mathbf{\Lambda}_B + \sigma_n^2 \mathbf{I}_M)\mathbf{V}_B^{*\mathrm{H}}, \quad (17)$$

$$\widetilde{\mathbf{R}}_C = \mathbf{V}_C^*(\mathbf{\Lambda}_C + \sigma_n^2 \mathbf{I}_M)\mathbf{V}_C^{*\mathrm{H}}, \quad (18)$$

$$\widetilde{\mathbf{R}}_D = \mathbf{V}_D^*(\mathbf{\Lambda}_D + \sigma_n^2 \mathbf{I}_M)\mathbf{V}_D^{*\mathrm{H}}. \quad (19)$$

The optimal transform matrix $\mathbf{V}_A^*$ is provided by the eigenvectors of the channel covariance matrix corresponding to the *M* maximum eigenvalues; the proof can be found in [9].

As explained above, it is demonstrated that the optimal V_A^* consists of the maximum *M* eigenvectors of the covariance matrix. This means that the proposed method mathematically obtains the optimal solution from the secret key rate aspect. Bob's pre-coding vector can be obtained similarly. In addition, it can be concluded from Equation (12) that:

$$\tilde{I}(\mathbf{h}_A; \mathbf{h}_B) = log_2\left(\frac{|\widetilde{\mathbf{R}}_A|.|\widetilde{\mathbf{R}}_B|}{|\widetilde{\mathbf{R}}_A|.\left|\widetilde{\mathbf{R}}_A - \widetilde{\mathbf{R}}_D \widetilde{\mathbf{R}}_A{}^{-1} \widetilde{\mathbf{R}}_C\right|}\right). \quad (20)$$

The block diagram for the proposed system is shown in Figure 2.

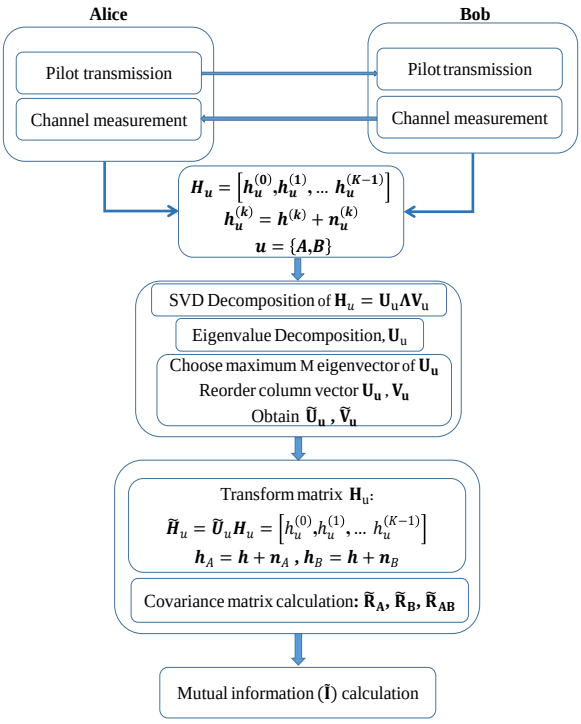

Figure 1. The block diagram for the proposed system

3. 1. Comparison between SVD and PCA In this subsection, a comparison between SVD and PCA is presented. The SVD decomposes a diagonalizable matrix into special matrices that are straightforward to handle and to analyze; however, the PCA method maps some data linearly into different properties that are not correlated with each other. Meanwhile, PCA can use various algorithms to implement the principal component analysis such as Eigenvalue Decomposition of the covariance matrix. It is faster than SVD, but less accurate. Another algorithm is Alternating Least Squares (ALS) algorithm, which uses an iterative method with a random seed. It is designed to handle missing values [23].

The PCA-based approach is used to break down $\boldsymbol{R}_A$ into $\boldsymbol{U}_A \boldsymbol{\Lambda}_A \boldsymbol{V}_A^H$, only if $\boldsymbol{R}_A$ is a square matrix. Hereby, one result can be expanded for all matrices using SVD, which indicates the numerical advantages of this approach. The matrices $\boldsymbol{R}_A \boldsymbol{R}_A^T$ and $\boldsymbol{R}_A^T \boldsymbol{R}_A$ are symmetric, square, positive semi-definite with positive eigenvalues, and both have the same rank. Since they are symmetric, it is inferred that its eigenvectors must be orthonormal. This is an essential property for symmetric matrices [24]. Therefore, using SVD, $\boldsymbol{R}_A$ does not require to be square. The eigenvectors for $\boldsymbol{R}_A \boldsymbol{R}_A^T$ are shown as u_i and $\boldsymbol{R}_A^T \boldsymbol{R}_A$ shown as v_i, and these sets of eigenvectors are called $\boldsymbol{U}_A$ and $\boldsymbol{V}_A$ *singular vectors* of $\boldsymbol{R}_A$. The square roots of these eigenvalues are called *singular values*.

Comparing to Eigen-decomposition, SVD works on non-square matrices. $\boldsymbol{U}_A$ and $\boldsymbol{V}_A$ are invertible for any matrix in SVD and they are orthonormal. Besides, singular values are numerically more stable than eigenvalues [25]. Although the PCA-based method mathematically has an optimal performance for using in channel decorrelation and key extraction systems, the numerical aspect has not been considered yet in similar research efforts.

Using SVD has some numerical advantages over the PCA. A suitable approach for calculating PCA on a computer is needed to directly implement the eigenvalue decomposition of $\boldsymbol{R}_A\boldsymbol{R}_A^T$.

It results in some computational complexity that could be decreased by adopting SVD. Let $\tilde{\sigma}_i$ be the output of an algorithm calculating singular values for R_A, and σ_i be the appropriate singular value, it can be shown that:

$$|\tilde{\sigma}_i - \sigma_i| = O(\varepsilon\|\mathbf{R}_A\|)\,, \tag{21}$$

where $\|\mathbf{R}_A\|$ is a measure of the size of $\mathbf{R}_A$. On the other hand, for an algorithm that calculates the eigenvalues λ_i of $\mathbf{R}_A{}^{\mathrm{T}}\mathbf{R}_A$, it can be shown as:

$$\left|\tilde{\lambda_i} - \lambda_i\right| = O(\varepsilon\|\mathbf{R}_A{}^{\mathrm{T}}\mathbf{R}_A\|) = O(\varepsilon\|\mathbf{R}_A\|^2) \tag{22}$$

which in terms of the singular values of $\mathbf{R}_A$, it can be written as:

$$|\tilde{\sigma}_i - \sigma_i| = O\left(\varepsilon\frac{\|\mathbf{R}_A\|^2}{\sigma_i}\right). \tag{23}$$

Ultimately, when small singular values, e.g. $\sigma_i \ll \|\mathbf{R}_A\|$ are needed, using $\mathbf{R}_A$ will result in more accurate output than using $\mathbf{R}_A{}^{\mathrm{T}}\mathbf{R}_A$.

4. SIMULATION RESULTS

In this section, we simulate some examples to evaluate the performance of our proposed method. The Monte Carlo simulation is adopted using MATLAB to model both the SVD and PCA algorithms. In all simulation examples, we assume that the OFDM symbols undergo Rayleigh fading. Moreover, channel realizations are based on statistical distributions presented in [20]. In our simulation studies, some curves are presented for both dependent and independent of frequency domains to assess the effect of the SVD. Some verifications are further done to demonstrate the optimality of the proposed SVD-based pre-coding. Meanwhile, our proposed method is compared with a PCA-based pre-coding method in both the MI and computational complexity aspects. As a case study, we focus on the de-correlation algorithms for channel measurement with frequency correlation in the OFDM model. Channel measurements are generated by the channel responses of all the sub-channels of an OFDM symbol.

4. 1. Example 1: Considering Correlated Sub-Channels in OFDM Model In this simulation example, we evaluate the secret key rate for both uncorrelated and correlated sub-channels. We assume that the variance of each sub-channel is random and normalized. The variance of sub-channels utilized in this example is listed in Table 1 for sub-channels.

Figure 3 shows the MI in terms of the SNR in outdoor conditions for constant T_m and independent sub-channels. As seen, the secret key rate is increased as the SNR becomes greater. Also, the secret key rate increases as the number of sub-channels increases. For N=8, 16, 32, the secret key rate is increased to 16.19, 27.42, 55.3 bits, respectively, where the target SNR is considered to be 8 dB. This increment in the secret key rate is due to the increase in the number of random sources as the greater number of sub-channels is utilized.

Figure 4 depicts the secret key rate for an OFDM-based system with correlated sub-channels with the above assumptions. As obviously observed, the rate in the dependent scenario is less than the independent scenario because of the correlation between sub-channels. As a result, where the target SNR is 8 dB, the secret key rate is obtained as Independent = 5.139, 8.814, 10.97, 15.17 bits, which are less than the values illustrated in Figure 3 for independent scenarios, for the same number of sub-channels.

Figure 5 illustrates the comparison of the secret key rate for both dependent and independent scenarios for an OFDM symbol including 32 sub-channels. As a result, the values of secret key rate where the target SNR is considered to be 8 dB are obtained as 15.17, 55.3 bits for correlated and independent sub-channels, respectively.

4. 2. Example 2: Evaluation of the Performance of Proposed SVD-Based Pre-coding In this sub-section, an OFDM model including 32 sub-carriers is utilized to do the simulations. Figure 6 shows the covariance matrix of $\boldsymbol{h}_{iA}, \boldsymbol{h}_{jA}$. Each element in this pattern indicates the amount of correlation between the two sub-channels. As an up-down sorting, a significant correlation is illustrated in brown, red and yellow colors, respectively. The first *M*

TABLE 1. Variance vectors for different number of sub-channels

Number of sub-channels	Variance
$N = 4$	$\delta_h^2 = [1.1819 \quad 1.0935 \quad 0.3597 \quad 0.820]$
$N = 8$	$\delta_h^2 = [1.1819 \quad 1.0935 \quad 0.7653 \quad 1.2042 \quad 2.4845 \quad 1.299 \quad 0.3597 \quad 0.820]$
$N = 16$	$\delta_h^2 = \begin{bmatrix} 1.1194 & 0.6190 & 0.3706 & 0.7079 & 1.0966 & 0.9597 & 1.0638 & 0.2884 \\ 0.4019 & 0.8906 & 1.4591 & 0.5037 & 1.4586 & 0.8723 & 1.2445 & 0.6251 \end{bmatrix}$
$N = 32$	$\delta_h^2 = \begin{bmatrix} 1.1997 & 0.9788 & 0.9412 & 0.7271 & 1.5351 & 2.0229 & 1.3886 & 1.4335 \\ 1.1822 & 0.9545 & 0.4923 & 0.9560 & 2.5430 & 0.5750 & 0.9384 & 0.3889 \\ 1.0682 & 0.3771 & 0.9178 & 0.5328 & 0.8034 & 0.4233 & 0.3446 & 0.2924 \\ 0.4517 & 0.3455 & 0.3942 & 0.7221 & 0.5543 & 0.6546 & 2.3146 & 0.7294 \end{bmatrix}$

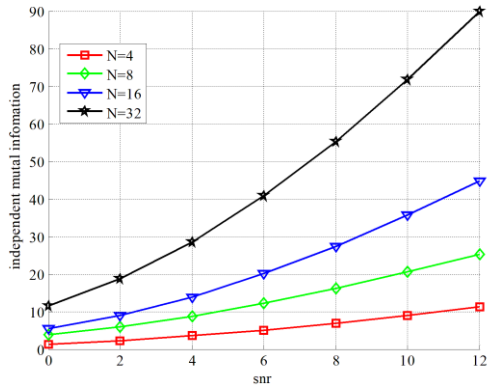

Figure 3. Secret key rate for independent sub-channels

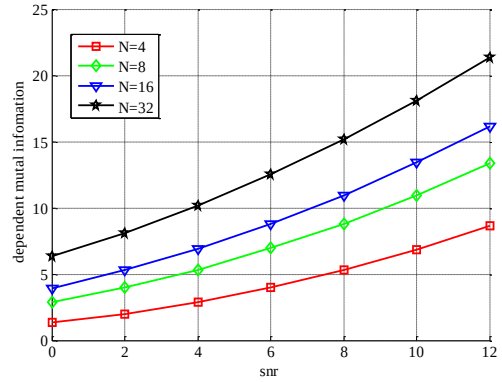

Figure 4. Secret key rate for correlated Sub-channels

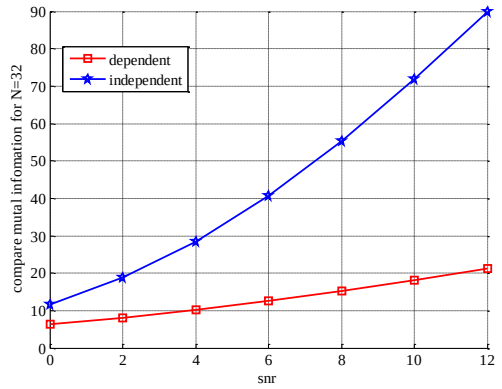

Figure 5. The comparison of the secret key rate between independent and dependent sub-channels for N = 32 and constant T_m

rows of *V* represent the signal subspace and the other rows describe the noise subspace which may be separated. The most important feature of the SVD is that the matrix *U*, which transforms the matrix of correlated sub-channels into a matrix of uncorrelated coefficients is unitary.

Figure 7 illustrates a 3D-view of the covariance matrix values. It should be noted that in our proposed approach, we try to select the elements of the matrix that are effective in the key generation process by discarding the destructive elements.

According to the PCA approach, the covariance matrix of the ideal channel $\mathbf{h}_A$ can be decomposed as $\mathbf{R}_A = \mathbf{U}_A\mathbf{\Lambda}_A\mathbf{U}_A^{\mathrm{H}}$, where $\mathbf{U}_A = \left[u_A^{(1)}, u_A^{(2)}, \ldots u_A^{(N)}\right]$ is the transform matrix and $\mathbf{\Lambda}_A$is a diagonal matrix with some sorted eigenvalues.

After transformation, matrix $\mathbf{H}_u$ is transformed into $\mathbf{Y}_u = \left[y_u^{(0)}, y_u^{(1)}, \ldots y_u^{(K-1)}\right]$ by expanding the CSI estimates with their projections on $\mathbf{Y}_u = \mathbf{U}^{\mathbf{H}}\mathbf{H}_u$. Because only a part of $\mathbf{U}$ is used for key generation, column vectors can be re-ordered and a part be choosen as a $M \times K$ matrix $\mathbf{Y}_u$ as $\mathbf{V} = [\mathbf{V}^{(1)}, \ldots, \mathbf{V}^{(M)}]$. This is an $N \times K$ matrix and satisfies $\mathbf{V}^{\mathrm{H}}\mathbf{V} = \mathbf{I}_M$, $M \leq N$. The output $M \times K$ matrix $\widetilde{\mathbf{Y}}_u$ is obtained by $\widetilde{\mathbf{Y}}_u = \mathbf{V}^{\mathrm{H}}\mathbf{H}_u$, where $\widetilde{\mathbf{Y}}_u$ is the result of the pre-coding procedure. Figure 7 shows the values of the new covariance matrix as long as we consider the equivalent channel. Figures 8 and 9 show the values of the covariance matrix of R_B after applying SVD and PCA pre-coding. As seen, the proposed algorithm will eliminate the peaks of the covariance matrix in Figure 9 and the smoother values are well selected.

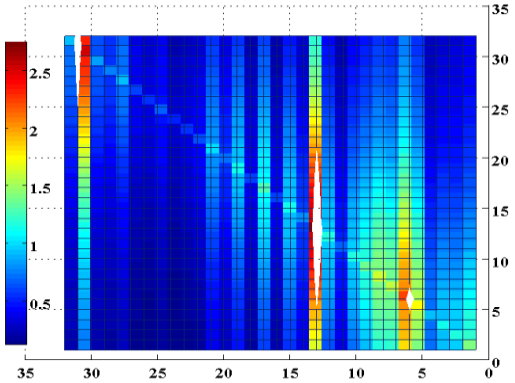

Figure 6. Covariance matrix of original channel. Each element indicates the correlation between two sub-channels $\boldsymbol{h}_{iA}$,$\boldsymbol{h}_{jA}$

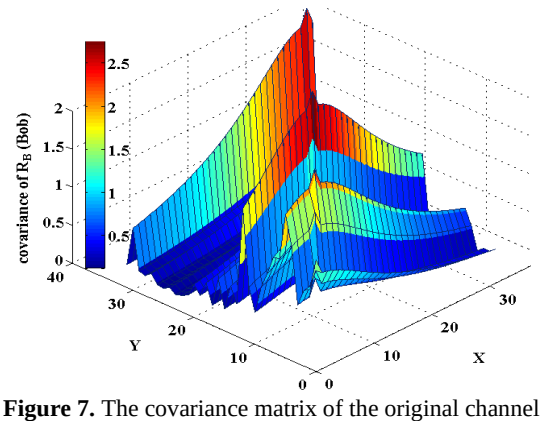

Figure 7. The covariance matrix of the original channel

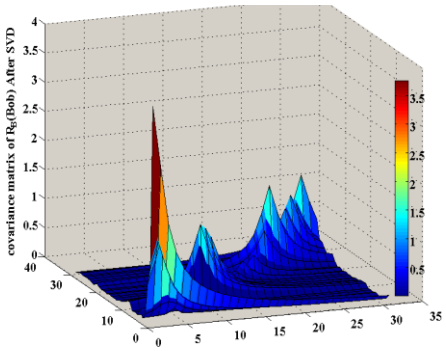

Figure 8. The covariance matrix of $\mathbf{R}_B$ (Bob) after SVD

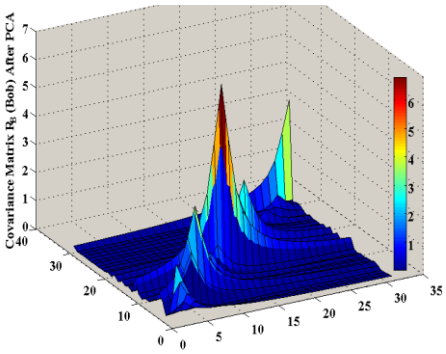

Figure 9. The covariance matrix of of $\mathbf{R}_B$ (Bob) after PCA

Figure 10 shows a comparison among the effect of the SVD, PCA, SVD and Wavelet matrix transforms on the MI. As expected, the proposed SVD-based method performs better than the other conventional methods from the MI aspect. In our simulations, the conventional OFDM-based key generation rate is first numerically plotted by substituting the covariance matrix $\mathbf{R}_A$ in Equation (13). Then, the transformed channel $\mathbf{R}_A$ is applied to Equation (12). As seen, where an OFDM symbol is utilized including *32* correlated sub-channels, 16 bits are otained in terms of the key generation rate at a target SNR of *8 dB*. It can be observed that using each of the above mentioned transform matrices will lead to improvements in terms of MI.

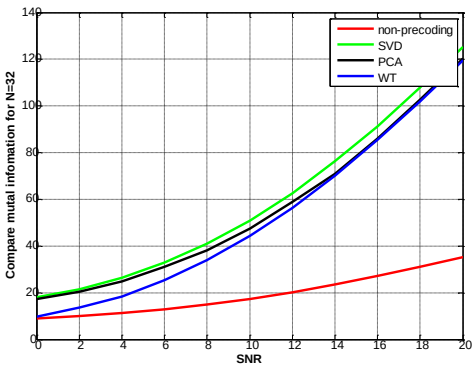

Figure 10. The effect of SVD-based pre-coding on the MI and comparison with DCT, PCA, and WT

4. 3. Example 3: On the Optimality of the SVD-Based Pre-coding In this simulation, we aim to obtain a contact zone between the SVD and PCA methods. As a result of SVD based pre-coding, we can achieve this optimal zone in which the performance of both methods are equal and complex. Ultimately, the proposed SVD-based pre-coding has a promising computational complexity. The comparison of MI performance is further performed in Figures 11 and 12 according to the variable *M* defined in Equation (14), for SNR=20 dB and SNR=10 dB respectively according to the results obtained from *32* correlated sub-channels, the SVD-based method outperforms the PCA-based method for both of the two scenarios.

Figures 12 and 13 show that the proposed SVD-based scheme has a promising superiority in terms of computational complexity due to adopting decomposition property of the SVD and eliminating of the non-related sub-routines of the PCA procedure. Assessment of the results for a case study including 32 correlated sub-channels verifies that the SVD based method achieves the optimal performance while consuming less processing time which is a crucial parameter for high-speed applications in 5G communications and other low-delay demanded secure applications.

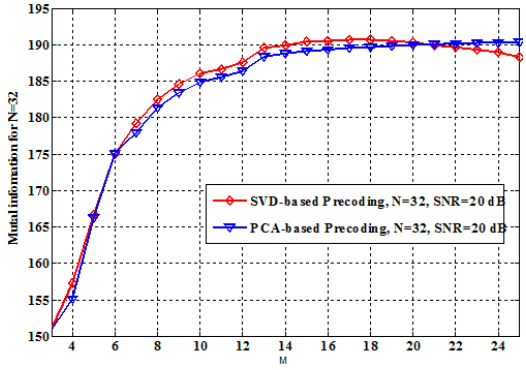

Figure 11. A comparison between the MI performance of the SVD and PCA methods for SNR=20db

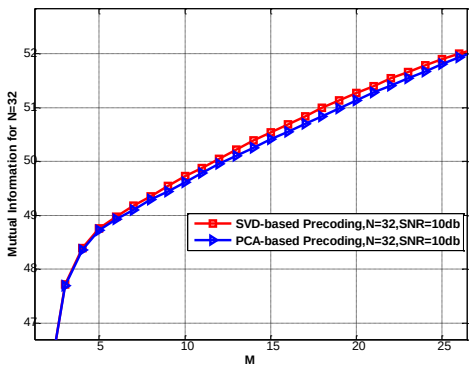

Figure 12. A comparison between the MI performance of the SVD and PCA methods for SNR=10db

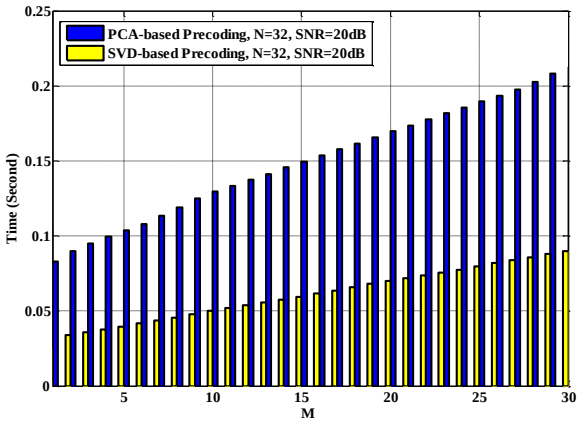

Figure 13. A comparison between the computational complexity of the SVD and PCA-based methods

5. CONCLUSION

In this paper, an SVD-based method was addressed for key extraction in OFDM-based communication systems. It was demonstrated that applying our proposed method has considerable advantages over the PCA, WT and DCT-based methods. Having considered a practical assumption, we investigated the effect of correlation among sub-channels on the secret key rate. Moreover, it was numerically shown that if we deal with temporal correlation alongside frequency correlation, KGR decreases and a more accurate value for secret key rate is obtained. Simulation results demonstrated that the computational complexity of our proposed SVD-based pre-coding has promising superiorities as a better MI is obtained.

6. REFERENCES

1. Melki, R., Noura, H.N., Mansour, M.M. and Chehab, A., "A survey on ofdm physical layer security", ***Physical Communication***, Vol. 32, No., (2019), 1-30. https://doi.org/10.1016/j.phycom.2018.10.008
2. Chen, Y., Wen, H., Wu, J., Song, H., Xu, A., Jiang, Y., Zhang, T. and Wang, Z., "Clustering based physical-layer authentication in edge computing systems with asymmetric resources", ***Sensors***, Vol. 19, No. 8, (2019), 1926. https://doi.org/10.3390/s19081926
3. Jiang, Y., Zou, Y., Guo, H., Zhu, J. and Gu, J., "Power allocation for intelligent interference exploitation aided physical-layer security in ofdm-based heterogeneous cellular networks", ***IEEE Transactions on Vehicular Technology***, Vol. 69, No. 3, (2020), 3021-3033. doi: 10.1109/TVT.2020.2966637
4. Zhan, F. and Yao, N., "Efficient key generation leveraging wireless channel reciprocity and discrete cosine transform", ***KSII Transactions on Internet and Information Systems***, Vol. 11, No. 5, (2017), 2701-2722. https://doi.org/10.3837/tiis.2017.05.022
5. Zhang, J., Duong, T.Q., Marshall, A. and Woods, R., "Key generation from wireless channels: A review", ***IEEE Access***, Vol. 4, (2016), 614-626. doi: 10.1109/ACCESS.2016.2521718
6. Cheng, L., Zhou, L., Seet, B.-C., Li, W., Ma, D. and Wei, J., "Efficient physical-layer secret key generation and authentication schemes based on wireless channel-phase", ***Mobile Information Systems***, Vol. 2017, (2017), 1-13. https://doi.org/10.1155/2017/7393526
7. Genkin, D., Pachmanov, L., Pipman, I., Tromer, E. and Yarom, Y., "Ecdsa key extraction from mobile devices via nonintrusive physical side channels", In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. (2016), 1626-1638. https://doi.org/10.1145/2976749.2978353
8. Liu, H., Yang, J., Wang, Y. and Chen, Y., "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks", In Proceedings IEEE INFOCOM, IEEE, (2012), 927-935. doi: 10.1109/INFCOM.2012.6195843
9. Li, G., Hu, A., Zhang, J., Peng, L., Sun, C. and Cao, D., "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing", ***IEEE Transactions on Communications***, Vol. 66, No. 7, (2018), 3022-3034. doi: 10.1109/TCOMM.2018.2814607
10. Bloch, M., Thangaraj, A., McLaughlin, S.W. and Merolla, J.-M., "Ldpc-based secret key agreement over the gaussian wiretap channel", In IEEE International Symposium on Information Theory, IEEE, (2006), 1179-1183. doi: 10.1109/ISIT.2006.261991
11. Peng, L., Li, G. and Hu, A., "Channel reciprocity improvement of secret key generation with loop-back transmissions", In IEEE 17th International Conference on Communication Technology (ICCT), IEEE, (2017), 193-198. doi: 10.1109/ICCT.2017.8359629
12. Shehadeh, Y.E.H. and Hogrefe, D., "An optimal guard-intervals based mechanism for key generation from multipath wireless channels", In 4th IFIP International Conference on New Technologies, Mobility and Security, IEEE, (2011), 1-5. doi: 10.1109/NTMS.2011.5720584
13. Liu, H., Wang, Y., Yang, J. and Chen, Y., "Fast and practical secret key extraction by exploiting channel response", In Proceedings IEEE INFOCOM, IEEE, (2013), 3048-3056. doi: 10.1109/INFCOM.2013.6567117
14. Zhang, J., Marshall, A., Woods, R. and Duong, T.Q., "Efficient key generation by exploiting randomness from channel responses of individual ofdm subcarriers", ***IEEE Transactions on Communications***, Vol. 64, No. 6, (2016), 2578-2588. doi: 10.1109/TCOMM.2016.2552165
15. Chen, C. and Jensen, M.A., "Secret key establishment using temporally and spatially correlated wireless channel coefficients", ***IEEE Transactions on Mobile Computing***, Vol. 10, No. 2, (2010), 205-215. doi: 10.1109/TMC.2010.114
16. Margelis, G., Fafoutis, X., Oikonomou, G., Piechocki, R., Tryfonas, T. and Thomas, P., "Physical layer secret-key generation with discreet cosine transform for the internet of things", In IEEE International Conference on Communications (ICC), IEEE, (2017), 1-6. doi: 10.1109/ICC.2017.7997419
17. Margelis, G., Fafoutis, X., Oikonomou, G., Piechocki, R., Tryfonas, T. and Thomas, P., "Efficient dct-based secret key generation for the internet of things", ***Ad Hoc Networks***, Vol. 92, (2019), 101744. https://doi.org/10.1016/j.adhoc.2018.08.014
18. Wu, Y., Sun, Y., Zhan, L. and Ji, Y., "Low mismatch key agreement based on wavelet-transform trend and fuzzy vault in body area network", ***International Journal of Distributed Sensor Networks***, Vol. 9, No. 6, (2013), 1-16. https://doi.org/10.1155/2013/912873
19. Zhan, F. and Yao, N., "On the using of discrete wavelet transform for physical layer key generation", ***Ad Hoc Networks***, Vol. 64, (2017), 22-31. https://doi.org/10.1016/j.adhoc.2017.06.003
20. Cheng, L., Li, W., Zhou, L., Zhu, C., Wei, J. and Guo, Y., "Increasing secret key capacity of ofdm systems: A geometric program approach", ***Concurrency and Computation: Practice***

and Experience, Vol. 29, No. 16, (2017), e3966. https://doi.org/10.1002/cpe.3966

21. Poor, H.V. and Schaefer, R.F., "Wireless physical layer security", ***Proceedings of the National Academy of Sciences***, Vol. 114, No. 1, (2017), 19-26, https://doi.org/10.1073/pnas.1618130114
22. Lai, L., Liang, Y., Poor, H.V. and Du, W., Key generation from wireless channels. In Physical Layer Security in Wireless Communications (pp. 47-92). CRC Press, (2013).
23. Arcidiacono, C. and Simoncini, V., "Approximate nonnegative matrix factorization algorithm for the analysis of angular differential imaging data", In Adaptive Optics Systems VI, International Society for Optics and Photonics. Vol. 10703, United States, (2018). https://doi.org/10.1117/12.2311681
24. Marques, O. and Vasconcelos, P.B., "Computing the bidiagonal svd through an associated tridiagonal eigenproblem", In International Conference on Vector and Parallel Processing, Springer, (2016), 64-74. https://doi.org/10.1007/978-3-319-61982-8_8
25. Gillis, N., Mehrmann, V. and Sharma, P., "Computing the nearest stable matrix pairs", ***Numerical Linear Algebra with Applications***, Vol. 25, No. 5, (2018), 1-19. https://doi.org/10.1002/nla.2153

Persian Abstract

چکیده

در امنیت مبتنی برلایه فیزیکی، استخراج کلید امن مسئله‌ای مهم است که در نسل‌های مخابراتی 5G و نسل‌های مخابراتی آتی، روشی با پیچیدگی کم و در عین حال مقاوم می‌باشد. برخلاف تحقیقات گذشته که زیرکانال‌ها در سیستم‌های OFDM مستقل فرض می‌گردید، در این مقاله به تأثیر همبستگی زیرکانال‌ها پرداخته شده است و یک مدل واقعی برای همبستگی زیرکانال‌ها استفاده شده است. نتایج شبیه‌سازی نشان می‌دهد که که همبستگی زیرکانال‌ها باعث کاهش اطلاعات متقابل تا ۷۲ درصد می‌شود. رویکرد جدیدی برای دست یافتن به اطلاعات متقابل بهینه و استخراج کلید بکار گرفته شده است. بدین منظور از پیش پردازش SVD برای کاهش میزان همبستگی مابین مقادیر اندازه‌گیری شده کانال و همچنین کاهش نویز استفاده گردید. پیچیدگی محاسباتی کم در رویکرد پیشنهادی، روش امیدوار کننده‌ای برای توسعه‌ی شبکه‌های امن و پرسرعت می‌باشد. نتایج شبیه‌سازی نشان می‌دهد که اعمال پیش‌پردازش بر روی مقادیر اندازه‌گیری شده‌ی وابسته، منجر به بهره حداقل ۹ دسی‌بل شده است. همچنین برتری عملکرد SVD نسبت به روش‌های دیگر نظیر PCA, DCT, WT با شکل، نمایش داده شده است.