Wireless Networks (2021) 27:4747–4758
https://doi.org/10.1007/s11276-021-02609-y

Improving data protection in BSS based secure communication: mixing matrix design

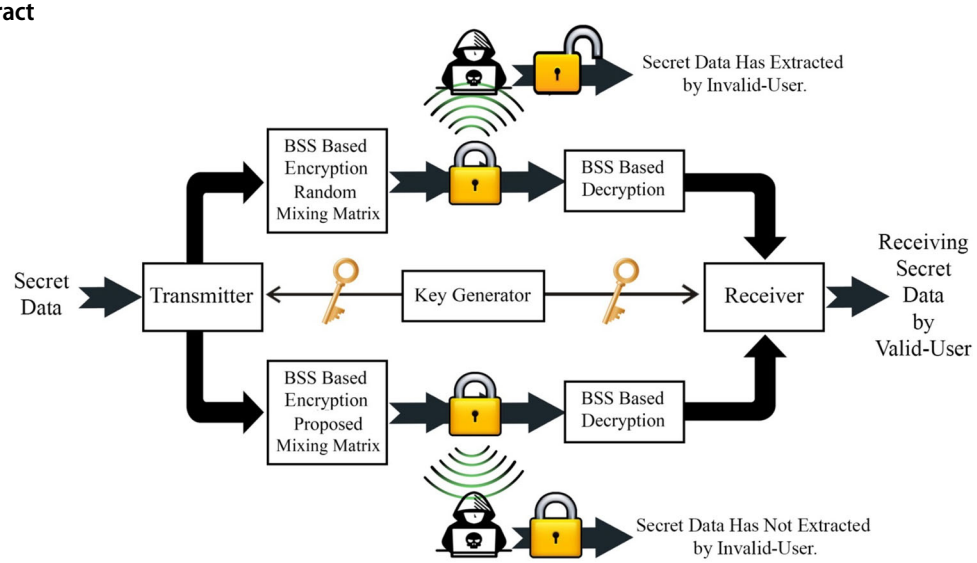
Mohammad Reza Aslani[1] · Mohammad Bagher Shamsollahi[2] · Arefeh Nouri[3]

Published online: 30 August 2021

Abstract

In this paper, a secure and efficient Blind Source Separation (BSS) based cryptosystem is presented. The use of BSS in audio and image cryptography in wireless networks has attracted more attention. A BSS based cryptosystem consists of three main parts: secret data, secret keys, and mixing matrix. In this paper, we propose a new design to create a proper mixing matrix in BSS based cryptosystem. We offer a mathematical criterion to select mixing matrix elements before encryption. The proposed criterion gives a simple way to attach the secret sources to keys, which makes source separation very hard for the adversary. Versus, we show that using the random mixing matrix can lead to data security loss. The attacks used for security tests in this paper are "Differential Attack" and "Denoising Attack," which are among the most effective in this field. These attacks will apply to cryptosystems based on the random and the proposed mixing matrix. The visual results of the attacks in the experiments will show that the "proposed mixing matrix based cryptosystem" will be more secure than the "random mixing matrix based cryptosystem." We also used the correlation coefficient criterion to compare the two cryptosystems more accurately. According to the experiments of this paper, the "proposed mixing matrix based cryptosystem" vs. the "random mixing matrix based cryptosystem" was able to reduce the adversary's source extraction quality rate from about 76% to 16%, on average.

Graphical Abstract



✉ Mohammad Reza Aslani
mr.aslani@shdu.ac.ir

[1] Electrical Engineering Department, Shahab Danesh University, Qom, Iran

[2] Electrical Engineering Department, Sharif University of Technology, Tehran, Iran

[3] Department of Biomedical Engineering, Amirkabir University of Technology, Tehran, Iran

Keywords Blind source separation · Security · Speech encryption · Image encryption · Cryptosystem · Underdetermined BSS

1 Introduction

With the development of wireless communications networks, the importance of data security and user's privacy is also increasing. Different encryption algorithms such as DES [1], RSA [2], and AES [3] have been developed to improve the security of the data exchange on these networks. Cryptographic algorithms require high-speed encryption and decryption to transmit extensively real-time data such as audio, image, and video. In [4, 5], it is shown that to use the mentioned encryption algorithms for some data such as audio, image and video, it is needed to add them several processes. These additional processes make the cryptosystem more complex, more slow, and costly. Therefore, designing a proper encryption method to encrypt extensively real-time data is important.

One of the most popular methods for audio and image encryption is Blind Source Separation (BSS) based encryption [6]. BSS is a problem that seeks to separate unknown and independent sources from observations [7]. The aim of BSS based cryptography is to generate observations with the least possible correlation to secret sources. The observations are made by combining secret parts that are called "Keys" with the secret data (sources). Valid users can use determined separation algorithms such as FastICA by having the keys and can recover the secret sources from observations. Besides, invalid users are in the "Underdetermined mode" without having the keys and cannot recover the secret sources. Various methods have been developed over the years to improve the security of BSS based encryption [8–10]. For example, recently in [11], Ridha et al. have proposed an encrypted end-to-end mobile voice call based on BSS encryption wherein the transmitter uses a Low Pass Filter (LPF) in the output of the key-generator block. In [11], it is shown that crossing keys from an LPF block can lead to an increase in the security of the cryptosystem.

Some algorithms are designed to extract secret sources without any key. These algorithms in BSS based encryption are known as "Attack algorithms. "The most famous attack is "Differential attack," which can extract an approximation of the secret sources by difference two observations existed on the public communication channel. Differential attack is used in many security test in articles [12]. In more recent research, in [13], as one way to test the security of their cryptosystem, Differential attack is used. In [14], Farhati et al. introduce a new algorithm to attack the BSS based cryptosystem, which it has been able to have a useful performance in extracting secret sources. This attack involves a denoising block (noise–reduction block), which is why this attack is called "Denoising attack." Other algorithms for source extraction in underdetermined BSS are also represented, but unlike the two attacks above, they require a set of preconditions for proper performance. For example, source extraction by Sparse Component Analysis (SCA) is one of the fields that have recently received much attention.

According to [15–19], an estimate of the mixing matrix can be obtained if a sparse representation of the sources is available. For example, in [15], to estimate the mixing matrix, "Discrete Wavelet Transforms (DWT)" is used to create a sparse representation of observations. However, in [16, 17], the "creating sparse representation" is done by "Time-Frequency (TF)" analysis and measurement of the "probability density function (PDF)," respectively. Also, in [18], it is tried to estimate a complex mixing matrix by having a sparse representation of sources, and in [19], "a method to increase the accuracy of estimation of mixing matrix" is introduced. Note that all of the researches in [16–19] are based on Single Source Point (SSP). According to SSP, for a good estimation from mixing matrix and sources, in each sample of observation signals (or in each pixel of observation images), just one of the sources must be active.

Many of the SCA based estimation methods are very sensitive to the sparse representation. So, in [20, 21], they are tried to reduce the estimation sensitivity to the sparse representation. In the newest research in this field, in [22], the Ant-colony and K-means algorithms are used mixing matrix estimation. In [22], using these algorithms is led to the "decreasing sensitivity to the sparse representation" and the "increasing accuracy of mixing matrix estimation." The algorithm proposed in [22] can recover six sparse acoustic sounds from three observations. However, in reality, natural sources are not necessarily sparse, so we do not use any added preconditions such as sparse representation for source selection, and in our paper, the sources can be any arbitrary (and independent) signals or images. Also, in our paper, the algorithms that use no precondition (for encryption, decryption or attack) are called "no-precondition" algorithms. For reminder, we provide a robust solution for the proper design of the mixing matrix. By our proposed method, the effect of no-precondition attacks such as Differential attack and Denoising attack on BSS based cryptosystem will be down.

A cryptosystem based on BSS uses linear algebra to encrypt and decrypt secret sources [21, 22]. Also, in this paper, we used known and effective attacks that in some

articles were provided to attack the BSS based cryptosystem, previously [12–14]. According to the above, most methods of increasing BSS-based cryptosystem security try to have a securely key-generator [5–9]. However, in [30], the construction of a proper mixing matrix to have a secure BSS based cryptosystem is discussed and introduces several conditions for making a securely mixing matrix. However, in this paper, we show that even with complying with the conditions introduced in [30], and even with having the most secure keys, BSS based cryptosystem is still at risk of data loss. This paper introducing a concept called MCR vector can be effective in improving the security of wireless networks, especially for the secure transmission of online-data such as audio and video, where the network requires a very high speed and low-cost cryptosystem. Also, this paper consists of six sections. After passing Sect. 1 (introduction), the remainder of the paper is organized as follows: In Sect. 2, the BSS based cryptosystem will be reviewed. In Sect. 3, the no-precondition attacks used for security tests will be discussed. In Sect. 4, the MCR criterion and the proposed method will be discussed. Section 5 deals with simulations and experiments; in this section, the random, and proposed mixing matrix based cryptosystems will be compared together. In this section, for security tests, Differential attack, and Denoising attack are used, and also for evaluating the results, the correlation coefficient is used. Section 6 as the final section will deal with a general conclusion.

2 BSS based cryptosystem

BSS based encryption can be considered low-cost and suitable for real-time security data exchange. Moreover, in [11], this cryptosystem is proposed for mobile networks. This indicates that BSS based cryptosystem can be used in local or wide wireless networks and developed to improve the security of wireless networks. In BSS based cryptosystem, one of the main problem for the transmitters is creating an effective combination by the 'N' number of secret sources and 'P' number of Keys [30]. This combination leads to make 'M' number of observations. The main problem for the receivers (valid or invalid users) is to separate the 'N' number of secret sources from 'M' number of observations [6]. If the receiver is a valid-user then it will have 'P' number of Keys and the BSS problem enter into "Determined mode." Many algorithms have been proposed to solve this case, including FastICA [23–25], Comon [26], Infomax [27]. If the receiver is an invalid-user then it will have not any Keys and the BSS problem enter into "Underdetermined mode." In Underdetermined mode, there is no fundamental solution for the separation of the sources completely; this causes BSS based cryptosystem to seem secure [28]. In Eq. (1), observations production is represented [6, 9]:

$$X_{M\times 1} = A_{M\times(N+P)} \begin{bmatrix} S_{N\times 1} \\ K_{P\times 1} \end{bmatrix}_{(N+P)\times 1} \tag{1}$$

In Eq. (1), $S = [S_1, S_2, \ldots, S_N]^T_{1\times N}$ is the secret sources vector, $K = [K_1, K_2, \ldots, K_P]^T_{1\times P}$ is the keys vector, $X = [X_1, X_2, \ldots, X_M]^T_{1\times M}$ is the observations vector, and 'A' is a mixing matrix with size $M \times (N + P)$. According to [6], the mixing matrix 'A' can be defined by Eq. (2):

$$A = \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_M \end{bmatrix} = \begin{bmatrix} A_{11} & A_{12} \cdots & A_{1N} & A_{1(N+1)} & A_{1(N+2)} \cdots & A_{1(N+P)} \\ A_{21} & A_{22} \cdots & A_{2N} & A_{2(N+1)} & A_{2(N+2)} \cdots & A_{2(N+P)} \\ \vdots & \vdots \ddots & \vdots & \vdots & \vdots \ddots & \vdots \\ A_{M1} & A_{M2} \cdots & A_{MN} & A_{M(N+1)} & A_{M(N+2)} \cdots & A_{M(N+P)} \end{bmatrix}_{M\times(N+P)} \tag{2}$$

According to Equation (1), it is necessary to define several proprietary keys for valid-users. This action leads to dedicated access to secret sources for valid-users in the network. The keys are confidential components that hold the cryptosystem in the determined mode for valid-users and keep it in the underdetermined mode for invalid–users. Also, according to [29], the keys must update continuously. In other words, the keys must be generated by a key-generator, and new keys must replace with old keys. Also, it must be noted that in practice, a key is made by data in a small volume and format that make bandwidth busy, a little. For example, in [5, 6], chaotic and pseudo-random transforms have been used in the creation of key-generators, respectively. These key–generators use the initial-values shared between all to make keys. To provide a secure cryptosystem, while initial-values are going to share, we can encrypt them by robust encryption methods like Advanced Encryption Standard (AES), etc [3]. However, in this paper, we do not discuss how the keys are generated and assume that the keys are arbitrary and ready-made components. We also assume that the keys are shared in an ideally–secured way between valid-users. In Fig. 1, BSS based cryptosystem is shown [6]:

In Fig. 1, the vector $\hat{S}$ is an estimation from the secret sources obtained by the determined algorithms. Also, according to Eq. (3), sources recovery is done in BSS based cryptosystem [6, 9]:

$$\begin{bmatrix} \hat{S}_{N\times 1} \\ K_{P\times 1} \end{bmatrix}_{(N+P)\times 1} = W_{(N+P)\times(M+P)} \begin{bmatrix} X_{M\times 1} \\ K_{P\times 1} \end{bmatrix}_{(M+P)\times 1} \tag{3}$$

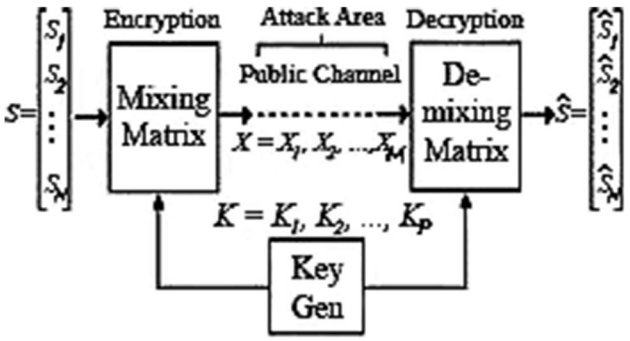


Fig. 1 BSS based cryptosystem [6]

In Eq. (3), 'W' is "Demixing Matrix" with size $(N+P)\times(M+P)$. This matrix is created by the determined algorithms, and whereby this, the independent secret sources will be separated from each other. Necessary to mention that in practical BSS based cryptosystems, the number of secret sources and observations is always equal together ($N=M$). Because, if $N<M$, the valid-users will enter into the "Overdetermined mode" by having the $M+P$ components. In this case, the complete source recovery can be done by the Determined algorithms, but using more than needed observations in the communication channel makes more cost for the cryptosystem. In another case, if $N<M$, the valid-users will enter into the Underdetermined mode, and cannot have a good recovery from the secret sources.

Some attacks do not need to consider any conditions on the features of the sources such as having a sparse time or frequency domain. We called these attacks as "No-precondition attacks." The next section deals with the no-precondition attacks used to test of the security in this paper.

3 No-precondition attacks

This section deals with Differential attack and Denoising attack. We intend to use these attacks to test the security of BSS based cryptosystem. For recall, the adversary model for BSS based cryptosystem is described simply in the mentioned attacks [28, 29]. Both attacks have access to observations on the public channel like valid–users. But the adversary (invalid–user) doesn't have any access privileges. In other words, unlike the valid-users, the adversary doesn't have any information about the secret sources and the keys, like statistical information, how key-generating, etc [28–30]. The adversary only must try to find a way to get an effective source extraction from two observations. In the following, Differential attack and Denoising attack are explained how come to extract of the secret sources. Note that to increase the performance of the attacks, we have added little changes to them which it is discussed below.

3.1 Differential attack

Differential attack is an algorithm based on the difference between two observations. Differential attack is defined as follows [12]:

$$\Delta X = A\Delta S = X_1 - X_2 \tag{4}$$

In Eq. (4), X_1 and X_2 are two different observations available on the public communication channel. Also, in Eq. (5), it is provided a more general form of the difference between two observations:

$$\forall n,m = 1,2,...,M \& n \neq m : \Delta X = X_n - \mu X_m \tag{5}$$

In Eq. (5), 'μ' is a constant and adjustable coefficient that makes ΔX changeable. In general, the observations generated by Eq. (1) can be overwritten as Eq. (6):

$$\begin{aligned} X_n = {} & A_{n1}S_1 + A_{n2}S_2 + \ldots + A_{nN}S_N + A_{n(N+1)}K_1 \\ & + A_{n(N+2)}K_2 + \ldots + A_{n(N+P)}K_P \end{aligned} \tag{6}$$

In Eq. (6), X_n refers to n–th observation, and the coefficients A_{n1} to $A_{n(N+P)}$ refer to the elements of the mixing matrix 'A.' On the other hand, by using Eq. (6), can be rewritten Eq. (5) as follows:

$$\begin{aligned} \Delta X &= X_n - \mu X_m \\ &= A_{n1}S_1 + A_{n2}S_2 + \ldots + A_{nN}S_N + A_{n(N+1)}K_1 + A_{n(N+2)}K_2 \\ &\quad + \ldots + A_{n(N+P)}K_P \\ &\quad -\mu(A_{m1}S_1 + A_{m2}S_2 + \ldots + A_{mN}S_N + A_{m(N+1)}K_1 \\ &\quad + A_{m(N+2)}K_2 + \ldots \\ &\quad + A_{m(N+P)}K_P) = (A_{n1} - \mu A_{m1})S_1 + (A_{n2} - \mu A_{m2})S_2 + \ldots \\ &\quad + (A_{nN} - \mu A_{mN})S_N \\ &\quad + \left(A_{n(N+1)} - \mu A_{m(N+1)}\right)K_1 + \left(A_{n(N+2)} - \mu A_{m(N+2)}\right)K_2 \\ &\quad + \ldots \\ &\quad + \left(A_{n(N+P)} - \mu A_{m(N+P)}\right)K_P \\ &= C_1S_1 + C_2S_2 + \ldots + C_NS_N + C_{N+1}K_1 + C_{N+2}K_2 + \ldots \\ &\quad + C_{N+P}K_P \end{aligned} \tag{7}$$

According to Eq. (7), by different amounts of 'μ' the "power of the independent components existed in observations" can change. In other words, for particular values of 'μ,' each coefficient from C_1 to C_{N+P} can be equated to zero (and follow it every component can be deleted). For two different observations X_i and X_j, these particular values are shown by '$\overline{\mu}$' and defined by Eq. (8):

$$\forall k = 1, 2, \ldots, N + P : C_k = 0 \rightarrow A_{ik} - \overline{\mu} A_{jk} = 0 \rightarrow \overline{\mu}_k = A_{ik}/A_{jk} \tag{8}$$

Clearly, for these particular values, the best extraction of the attacks is expected.

3.2 Denoising attack

Denoising attack attempts to reduce the effect of the keys by crossing the observations through a denoising block. To improve the extraction of secret sources, outputs of the denoising block with observations are entered into a FastICA block. Figure 2 shows the block diagram of Denoising attack represented in [14]. In [14], the denoising block has consisted of a Wiener filter. However, in this paper, the denoising block has consisted of an adaptive filter instead of a Wiener filter. This change is because an adaptive filter, unlike a Wiener filter, is tended to the optimal point without any knowledge of statistical information of the inputs (it is reminded that in BSS, there is no statistical information about the independent components). Also, an adaptive filter, unlike a Wiener filter, is consisted of a time-variant system. By replacing the adaptive filter instead Wiener filter, we can also be sure that the denoising block will be a time-variant system. This ability of the adaptive filter makes Denoising attack suitable to extract non-stationary components (like speech signals).

In BSS based cryptosystem, system security can be improved by "proper keys" and a "proper mixing matrix." Mostly in the articles, designing a key-generator is discussed to provide the proper keys [5–10]. In the next section, we attend to the design of a proper mixing matrix for improving the security cryptosystem.

4 Proposed method

Requirements to hold the security of BSS based cryptosystem are as follows:

1. The keys must be made by many bits; in other words, the number of quantization levels of the keys must be huge [30].
2. The keys should not be sparse in the Time–Frequency domain [30].

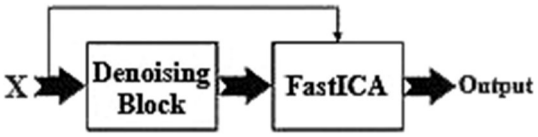


Fig. 2 Denoising attack presented in [14]

3. The mixing coefficients should be chosen such that the "variances of the keys" been greater than the "variances of the secret sources [30]."

The three conditions above could be considered as BSS based cryptosystem defaults. Does not comply with these three conditions can cause to reduce the security of the cryptosystem. However, we will show that even with fulfilling these three conditions, still the security of the cryptosystem is vulnerable. So the aim of this section is to represent a proper design for the mixing matrix to improve the security of the cryptosystem.

Consider two observation signals X_i and X_j. Equation (2) can be rewritten as follows:

$$\begin{bmatrix} A_i \\ A_j \end{bmatrix} = \begin{bmatrix} A_{i1} & A_{i2} \cdots & A_{iN} & A_{i(N+1)} & A_{i(N+2)} \cdots & A_{i(N+P)} \\ A_{j1} & A_{j2} \cdots & A_{jN} & A_{j(N+1)} & A_{j(N+2)} \cdots & A_{j(N+P)} \end{bmatrix} \tag{9}$$

$$= \begin{bmatrix} \rho_1 A_{j1} & \rho_2 A_{j2} \cdots & \rho_N A_{jN} & \rho_{N+1} A_{j(N+1)} & \rho_{N+2} A_{j(N+2)} \cdots & \rho_{N+P} A_{j(N+P)} \\ & A_{j1} \quad A_{j2} \cdots & A_{jN} & A_{j(N+1)} & A_{j(N+2)} \cdots & A_{j(N+P)} \end{bmatrix}$$

Because 'ρ' is a concept of the mixing coefficients division so, we call 'ρ,' the "Mixing Coefficients Ratio (MCR)," and for two different observations X_i and X_j, MCR vector can be defined by Eq. (10):

$$\forall k = 1, 2, \ldots, N + P : \rho_k = A_{ik}/A_{jk} \tag{10}$$

$$\mathrm{MCR_{ij}} = \begin{bmatrix} \rho_1 & \rho_2 \cdots & \rho_N & \rho_{N+1} & \rho_{N+2} \cdots & \rho_{N+P} \end{bmatrix}_{1 \times (N+P)}$$

If all of the independent components in the BSS problem are normalized, then MCR associated with each independent component can be introduced as the "power ratio of the component." Given the explanation above, if the following two proposed conditions have complied, then BSS based cryptosystem can be more secure:

(i) "Attaching one or more secret source to only one key" occurs when MCR of one or more secret sources are close to MCR of a key. This condition makes the power of one or more secret sources always smaller than the power of the key. Besides, according to Eq. (8), this condition causes whenever $C_{key} = 0$, then $C_{secretsources} = 0$. In other words, if the key is removed by the attacks, then the attached secret sources will be deleted at the same time, so the secret sources will not be extracted. This condition is done by $N > = P$. But, in a specific case, if $P = N$, then the mixing matrix can be changed to a particular matrix according to Eq. (11):

$$A = \begin{bmatrix} \varepsilon \times I & I \end{bmatrix}_{N \times (N+P)} = \begin{bmatrix} \varepsilon \times I & I \end{bmatrix}_{N \times (2N)} \tag{11}$$

In Eq. (11), 'ε' is a factor that its absolute is smaller than one, and 'I' refer to the identity matrix

(eye matrix). Also, because the particular mixing matrix uses eye matrix, we call it "Eye Mixing Matrix." Besides, in this specific case, the MCR vector is included only three values $+\infty$, $-\infty$, and zero. Based on this specific case, each of the observations will contain a unique key and a unique secret source; therefore, the attacks will not be able to extract secret sources.

(ii) Non–attaching the keys together

"Non-attaching the keys together" occurs when MCR of a key is not close to MCR of another key. This condition makes the power of a key always non-equal to the power of another key. Besides, according to Eq. (8), this condition causes whenever $C_{key} = 0$, then $C_{anotherkey} \neq 0$. In other words, if one of the keys is removed by the attacks, then another key will not be deleted, at the same time.

In the next section, the validity of the proposed method will be evaluated by experiments.

5 Simulation results

This section is going to evaluate the proposed mixing matrix and compare it with the random mixing matrix. This evaluation will do by the Differential attack and Denoising attack. For two signals 'x' and 'y,' correlation coefficient criterion is used to measure the performance of the methods [10]:

$$Corr_{xy} = \frac{N\sum_{i=1}^{N}(x_i \times y_i) - \sum_{i=1}^{N} x_i \times \sum_{i=1}^{N} y_i}{\sqrt{N\sum_{i=1}^{N} x_i^2 - \left(\sum_{i=1}^{N} x_i\right)^2} \times \sqrt{N\sum_{i=1}^{N} y_i^2 - \left(\sum_{i=1}^{N} y_i\right)^2}} \quad (12)$$

In Eq. (12), x_i and y_i are ith element of 'x' and 'y,' respectively. Also, 'N' refers to length of 'x' and 'y.' In the following, to show the robustness of the proposed method, different experiments is considered. In each experiment, first, the security of the cryptosystem based on a random mixing matrix is evaluated. Then, with a slight change in the elements of the random mixing matrix associated with secret sources (and without making any change in the other elements), we will try to improve the security of the cryptosystem according to the MCR criterion.

Note that all of the mixing matrices used in these experiments always comply the three conditions mentioned in [30]. In other words, all signals or images used in the experiments are high quantized, no sparse, and also in terms of variance, always the keys are more extensive than the secret sources. As a reminder, the BSS based cryptosystem can exchange any data securely, and we have no limitation on choosing data such as audio, image, and video. However, we provide the experiments in two modes, audio transmission, and image transmission. We also note that the keys must be generated by a key–generator, such as key–generators based on chaotic or pseudo–random or both transformations [5–9]. However, since this article does not focus on key-generating, we have selected the keys as arbitrary and assumptive signals or images in the experiments.

5.1 Experiment one

Experiment one consists of three independent components. Two speech signals are entered into the cryptosystem as two secret sources and one white noise signal as a secret key. The secret sources waveforms and the secret key waveform are shown in Fig. 3.

$$A = \begin{bmatrix} 0.1224 & 0.2195 & 0.8724 \\ 0.1493 & 0.0881 & 0.6710 \end{bmatrix}_{2\times 3}$$

The three components will combine by the mixing matrix above and will produce two observations (encrypted signals). The observations are shown in Fig. 4. Also, the outputs of the attacks are shown in Fig. 4.

The correlation coefficients between the observations and independent sources and also, the correlation coefficients between the outputs of the attacks and independent sources are given in Table 1.

According to the table above, the attacks were able to reduce the effect of the key and were able to extract a combination from secret speeches. It is also clear that the quality of the second secret speech is better than the first; in other words, the second secret speech is better extracted by the attacks. The reason is that the measure of proposed conditions compliance for the second secret speech is less than the first. Notice the MCR vector of the random mixing matrix below:

$$MCR_{12} = [0.8202 \quad 2.4915 \quad 1.3002]_{1\times 3}$$

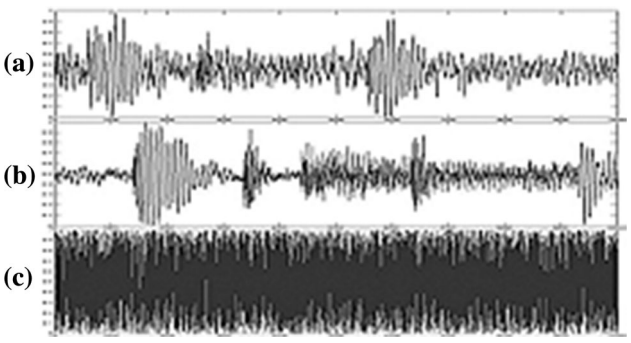


Fig. 3 Waveforms of the three independent components used in experiment one; **a** First secret speech, **b** Second secret speech, and **c** Secret white noise key

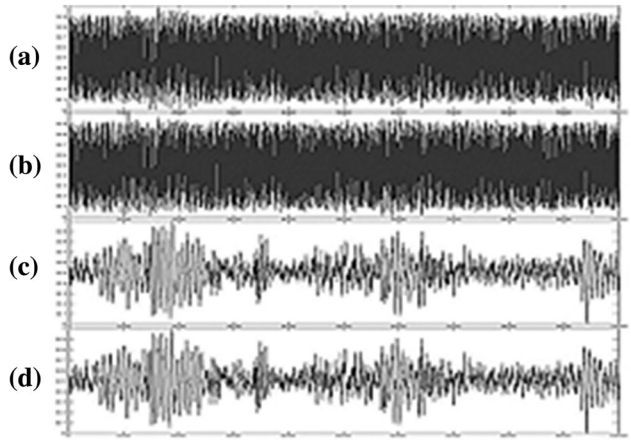


Fig. 4 Waveforms of the "observations made by the random mixing matrix" and the "output of the attacks" in experiment one; **a** First observation, **b** Second observation, **c** Output of Differential attack, and **d** Output of Denoising attack

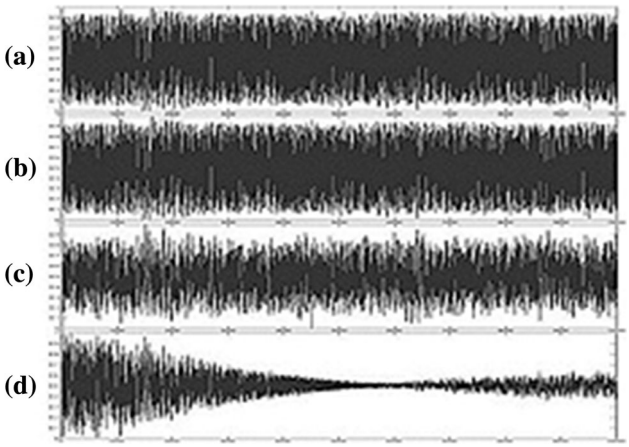


Fig. 5 Waveforms of the "observations made by the proposed mixing matrix" and the "output of the attacks" in experiment one; **a** First observation, **b** Second observation, **c** Output of Differential attack, and **d** Output of Denoising attack

According to the MCR vector of the random mixing matrix, the difference between the "element associated with the second secret speech" and the "element related to the key" is more significant than the difference between the "element associated with the first secret speech" and the "element related to the key." In other words, the first proposed condition has less complied with the "second secret speech" than the "first secret speech."

Now the mixing matrix according to the proposed conditions can be modified as follows:

$$A = \begin{bmatrix} 0.1219 & 0.1792 & 0.8724 \\ 0.0936 & 0.1381 & 0.6710 \end{bmatrix}_{2\times 3}$$

The MCR vector of the mixing matrix above has come as follows:

$$\mathrm{MCR}_{12} = \begin{bmatrix} 1.3026 & 1.2980 & 1.3002 \end{bmatrix}_{1\times 3}$$

In the MCR vector of the proposed mixing matrix, the "elements related to the secret speeches " are very close to the "element associated with the secret key" which means the first proposed condition is fulfilled. Therefore, the "resistance of the observations vs the attacks" is expected to increase by using the proposed mixing matrix. Figure 5 shows the "observations made by the proposed mixing matrix" and the "output of each attacks."

Table 2 represents the correlation coefficients between the "observations made by the proposed mixing matrix" and independent sources and also, the correlation coefficients between the output of the attacks and independent sources.

According to Table 2, the attacks had not a proper extraction from secret speeches. Also, by comparing Table 1 and Table 2, it is easy to conclude that the performance of the attacks in the "cryptosystem based on proposed mixing matrix" was been weaker than their performance in the "cryptosystem based on random mixing matrix."

5.2 Experiment two

Experiment two consists of four independent components. Two images as two secret sources, also an assumptive and arbitrary image as one of the secret keys, and a white noise image as another secret key are entered into the cryptosystem. In Fig. 6, the images of the components are shown:

Table 1 Correlation coefficients (%) between the "observations made by the random mixing matrix" and independent sources and also, correlation coefficients between the output of the attacks and independent sources in experiment one

	Secret speech 1	Secret speech 2	White noise key
Observation 1	7.0400	10.4806	99.3421
Observation 2	10.4310	5.8458	99.4306
Differential attack	−60.7701	76.8705	−14.8468
Denoising attack	−59.7270	78.9952	−4.9883

Table 2 Correlation coefficients (%) between the "observations made by the proposed mixing matrix" and independent sources and also, correlation coefficients between the output of the attacks and independent sources in experiment one

	Secret speech 1	Secret speech 2	White noise key
Observation 1	7.0087	8.7031	99.5031
Observation 2	6.9979	8.7161	99.5027
Differential attack	−10.4306	−14.7520	−93.7440
Denoising attack	−8.9452	−11.4085	−46.3635

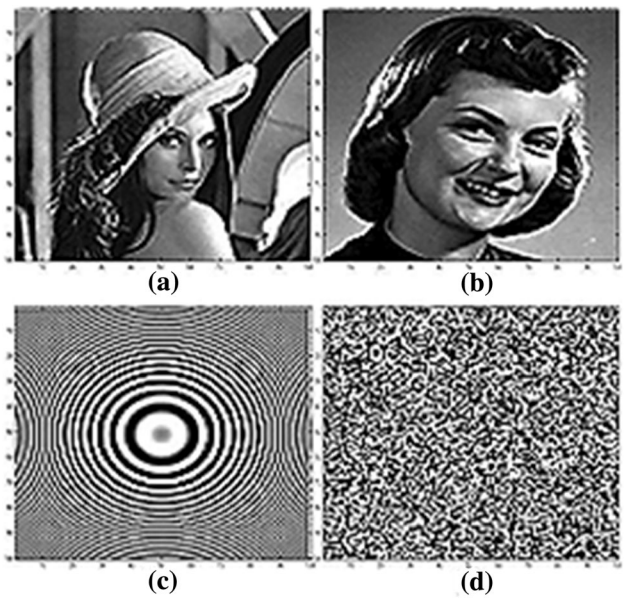


Fig. 6 Images of the four independent components used in experiment two; **a** First secret image (Lena image), **b** Second secret image (Girl image), **c** Secret image key and **d** Secret white noise key

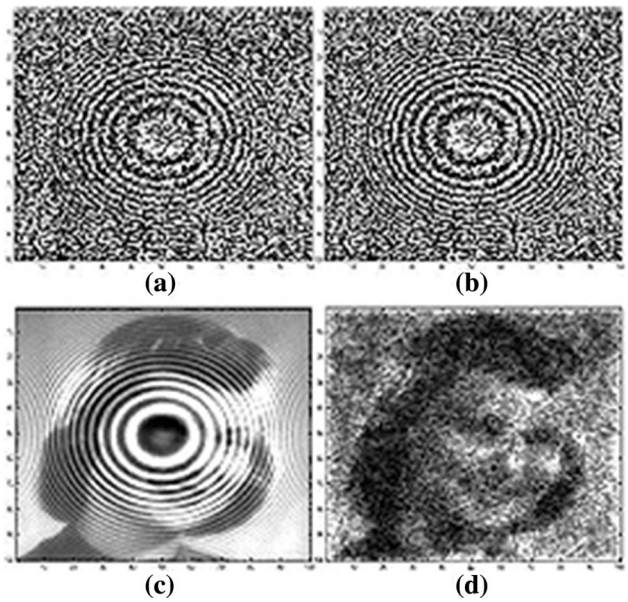


Fig. 7 Images of the "observations made by the random mixing matrix" and the "output of the attacks" in experiment two; **a** First observation, **b** Second observation, **c** Output of Differential attack, and **d** Output of Denoising attack

In this experiment, the components are combined together by the following random mixing matrix and will produce two observations in accordance with Fig. 7. Also, the outputs of Differential attack and Denoising attack are inserted in Fig. 7.

$$A = \begin{bmatrix} 0.1987 & 0.2231 & 0.5185 & 0.7354 \\ 0.1800 & 0.1300 & 0.5803 & 0.6387 \end{bmatrix}_{2\times 4}$$

Table 3 represents the correlation coefficients between the "observations made by the random mixing matrix" and independent sources and also, the correlation coefficients between the output of the attacks and independent sources.

According to Table 3, the attacks were able to extract one of the secret images (second secret image). The second secret image is extracted because the measure of proposed conditions compliance for the second secret image is less than the first. Notice the MCR vector of the random mixing matrix below:

$$\mathrm{MCR}_{12} = \begin{bmatrix} 1.1039 & 1.7168 & 0.8935 & 1.1514 \end{bmatrix}_{1\times 4}$$

According to the above MCR vector, the difference between the "element associated with the second secret image" and the "elements related to the keys" is more significant than the difference between the "element associated with the first secret image" and the "elements related to the keys." In other words, the first proposed condition has less complied with the "second secret image" than the "first secret image."

The mixing matrix according to the proposed conditions can be modified as follows:

$$A = \begin{bmatrix} 0.1987 & 0.2131 & 0.5185 & 0.7354 \\ 0.2225 & 0.1850 & 0.5803 & 0.6387 \end{bmatrix}_{2\times 4}$$

And also, the MCR vector of the above mixing matrix is in follows:

$$\mathrm{MCR}_{12} = \begin{bmatrix} 0.8930 & 1.1522 & 0.8935 & 1.1514 \end{bmatrix}_{1\times 4}$$

Clearly, in the MCR vector above, the "secret images related elements" are very close to the "secret keys

Table 3 Correlation coefficients (%) between the "observations made by the random mixing matrix" and independent sources and also, correlation coefficients between the output of the attacks and independent sources in experiment two

	Secret image 1	Secret image 2	Arbitrary key	White noise key
Observation 1	17.2224	19.3971	50.2290	82.7098
Observation 2	16.9171	12.3277	60.1130	77.5150
Differential attack	−7.1749	77.1748	−46.0669	−0.8637
Denoising attack	20.0120	73.9546	3.1061	30.9839

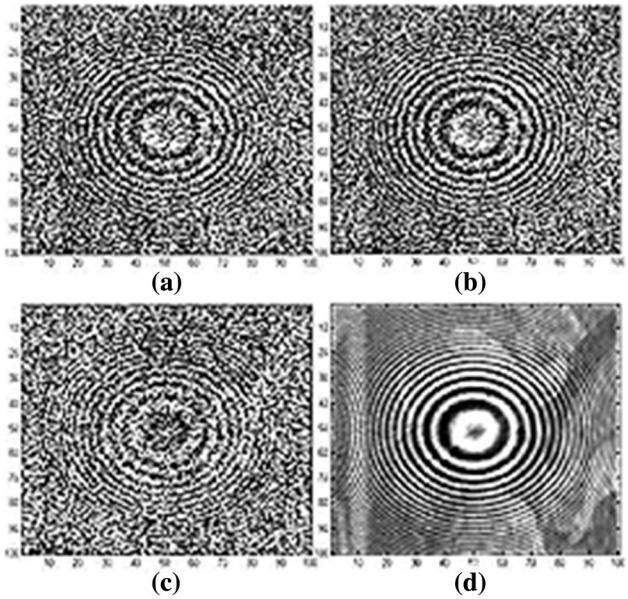


Fig. 8 Images of the "observations made by the proposed mixing matrix" and the "output of the attacks" in experiment two; **a** First observation, **b** Second observation, **c** Output of Differential attack, and **d** Output of Denoising attack

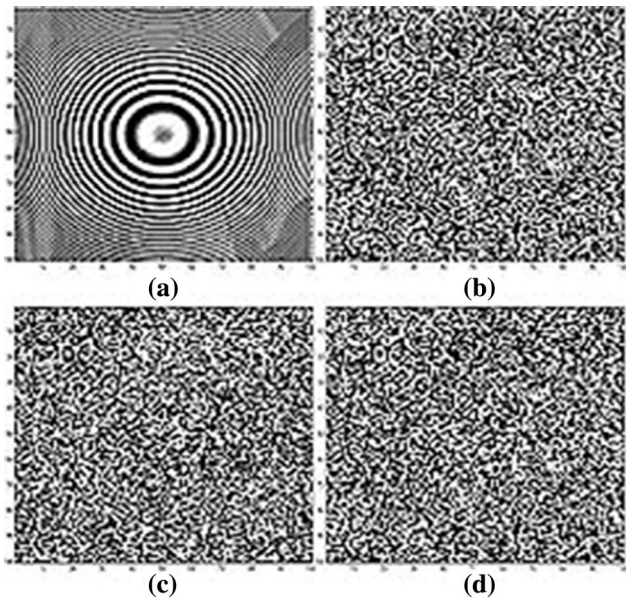


Fig. 9 Images of the "observations made by the eye mixing matrix" and the "output of the attacks" in experiment two; **a** First observation, **b** Second observation, **c** Output of Differential attack, and **d** Output of Denoising attack

associated elements" which means the first proposed condition is fulfilled. On the other side, the "secret keys associated elements" are not close to each other which means the second proposed condition is fulfilled. Therefore, the "resistance of the observations vs the attacks" is expected to increase by using the proposed mixing matrix.

Figure 8 shows the "observations made by the proposed mixing matrix" and the "output of each attacks."

Also, in Table 4, the correlation coefficients between the "observations made by the proposed mixing matrix" and "independent sources," and also the correlation coefficients between the "output of the attacks" and "independent sources," are reperesented.

By comparing the results of Table 3 and Table 4, it is clear that the effect of the attacks in the "cryptosystem based on proposed mixing matrix" was weaker than the

Table 4 Correlation coefficients (%) between the "observations made by the proposed mixing matrix" and independent sources and also, correlation coefficients between the output of the attacks and independent sources in experiment two

	Secret image 1	Secret image 2	Arbitrary key	White noise key
Observation 1	17.2446	18.5430	50.2957	82.8646
Observation 2	20.5592	17.3357	59.3726	76.2420
Differential attack	−17.2146	16.9693	−45.8163	84.9594
Denoising attack	−47.8867	3.1461	−79.5178	2.6715

Table 5 Correlation coefficients (%) between the "observations made by the eye mixing matrix" and independent sources and also, correlation coefficients between the output of the attacks and independent sources in experiment two

	Secret image 1	Secret image 2	Arbitrary key	White noise key
Observation 1	19.0302	2.1054	98.4171	0.4399
Observation 2	−0.5716	13.7998	0.8807	98.7828
Differential attack	5.0208	−12.9456	22.2291	−96.1003
Denoising attack	−0.4580	13.8109	1.2766	98.7800

"cryptosystem based on random mixing matrix." Note, in this experiment (that the number of secret sources is equal to the number of keys), we can use the eye mixing matrix as follows:

$$A = \begin{bmatrix} 0.2000 & 0.0000 & 1.0000 & 0.0000 \\ 0.0000 & 0.2000 & 0.0000 & 1.0000 \end{bmatrix}_{2\times 4}$$

The MCR vector of the eye mixing matrix is in the following:

$$\mathrm{MCR}_{12} = [\infty \quad 0 \ \infty \quad 0]_{1\times 4}$$

Figure 9 shows the "observations made by the eye mixing matrix" and the "output of each attack."

Besides, in Table 5 the correlation coefficients between the "observations made by the eye mixing matrix" and "independent sources," and also the correlation coefficients between the "output of the attacks" and "independent sources" are reperesented.

According to Table 3 and Table 5, it is clear that the attacks have disabled in the cryptosystem based on the eye mixing matrix, and the security of the cryptosystem has come at a high level.

6 Conclusions

In Eqs. (7) and (8), we showed that the effect of components can be reduced or even eliminated by linear algebra. In other words, for the particular coefficients introduced with '$\overline{\mu}$,' the effect of some keys can be attenuated or removed from the observations. In fact, the attacks like Differential attack and Denoising attack are also looking for such coefficients to provide a better perception of secret sources for the next processes and analyses of the adversary. Achieving such coefficients was seen to be critical for attack algorithms. Therefore, prevention of the occurring these coefficients could play a vital role in increasing the security of the BSS based cryptosystem. According to Eqs. (7) and (8), in Eq. (9) and (10), we introduced some coefficients with 'ρ' that were elements of the MCR vector. By observing the two proposed conditions, and attention to the MCR vector, the mixing matrix was provided to more secure communication and we prevented the occurrence of secret sources revelation for the adversary. In continuing the random and the proposed mixing matrix based cryptosystem were simulated. We used the correlation coefficient criterion for a more accurate comparison of both cryptosystems. Summarized, in the experiment of the BSS based encryption for audio transmission, the "proposed mixing matrix based cryptosystem" vs. the "random mixing matrix based cryptosystem" was able to reduce the adversary's source extraction quality rate from 76.8705% to 14.7520% for Differential attack, also was able to reduce from 78.9952% to 11.4085% for Denoising attack. Moreover, in the experiment of the BSS based encryption for image transmission, the "proposed mixing matrix based cryptosystem" vs. the "random mixing matrix based cryptosystem" was able to reduce the adversary's source extraction quality rate from 77.1748% to 16.9693% for Differential attack, also was able to reduce from 73.9546% to 3.1461% for Denoising attack. So, random and proposed mixing matrices comparison tests confirm improving the security in the proposed scheme. The proposed system appeared high immunity against Differential attack and Denoising attack in different tests. Because of the simple structure of the proposed encryption scheme, the proposed system can be nominated to be used in many multimedia applications like local or wide wireless communication, audio–video broadcasting, video chat, and mobile communication.

References

1. Menezes, A. J., Oorschot, P. C. V., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. . FL: CRC Press.
2. Smid, M. E., & Branstad, D. K. (1988). The data encryption standard: Past and future. *Proceeding of the IEEE, 76*, 550–559.
3. Daemen, J., & Rijmen, V. (2002). *The design of rijndael: AES-the advanced encryption standard*. . Berlin: Springer-Verlag.
4. Kamali, S. H., Shakerian, R., Hedayati, M., & Rahmani, M. (2010). A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption. In International Conference on Electronics and Information Engineering, ser. ICEIE2010, Kyoto, Japan, 1:141–145

5. Liu, S., Sun, J., & Xu, Z. (2009). An improved image encryption algorithm based on chaotic system. *Journal of Computers, 4*(11), 1091–1100.
6. Lin, Q. H., Tin, F. L., Mei, T. M., & Liang, H. L. (2004). A Speech Encryption Algorithm Based on Blind Source Separation. In International Conference on Communications, Circuits and Systems, ser. ICCCAS2004, Chengdu, China, 2:1:1013–1017
7. Kohmura, S., Togawa, T., & Otani, T. (2017). Source Separation Based on Transfer Function between Microphones and its Dispersion. In: Computing and Communication Workshop and Conference ser. CCWC 1-6
8. Abbas, N. A. (2015). Image encryption based on independent component analysis and arnold's cat map. *Egyptian Informatics Journal, 17*(1), 139–146.
9. Zhao, H., He, S., Chen, Z., & Zhang, X. (2014). Dual key speech encryption algorithm based underdetermined BSS. *Hindawi The Scientific World Jornal, 2014*, 751–758.
10. Sadr, A., & Okhovat, R. S. (2015). An implementing consideration for the key in a BSS-based cryptosystem. *Springer Wireless Personal Communication, 80*(1), 17–28.
11. Ridha, O. A. L. A., Jawad, G. N., & Kadhim, S. F. (2018). Modified blind source separation for securing end-to-end mobile voice calls. *IEEE Communications Letters, 22*(10), 2072–2075.
12. Li, S., Li, C., Lo, K. T., & Chen, G. (2008). Cryptanalyzing an encryption scheme based on blind source separation. *IEEE Transactions on circuit and systems, 55*(4), 1055–1063.
13. ElSafty, A. H., Tolba, M. F., Said, L. A., Madian, A. H., & Radwan, A. G. (2020). Hardware realization of a secure and enhanced s-box based speech encryption engine. *Springer Analog Integrated Circuits and Signal Processing*. https://doi.org/10.1007/s10470-020-01614-z.
14. Farhati, A., Aicha, A. B. & Bouallegue, R. (2018). Decryption of BSS Based Encrypted Speech Without A Priori Knowledge of the Key Signal. In: The 4th International Conference on Advanced Technologies for Signal and Image Processing, ser. ATSIP'2018, Sousse, Tunisia, 1–4
15. Tazehkand, B., & Tinati, M. (2010). Underdetermined blind mixing matrix estimation using STWP analysis for speech source signals. *Wireless Sensor Network, 2*(11), 854–860.
16. Reju, V. G., Koh, S. N., & Soon, I. Y. (2009). An algorithm for mixing matrix estimation in instantaneous blind source separation. *Elsevier Signal Processing, 89*(9), 1762–1773.
17. Li, Y., Nie, W., Ye, F., & Lin, Y. (2016). A mixing matrix estimation algorithm for underdetermined blind source separation. *Springer Circuits, Systems, and Signal Processing, 35*(9), 3367–3379.
18. Li, Y., Nie, W., & Ye, F. (2015). A complex mixing matrix estimation algorithm based on single source point. *Springer Circuits, Systems, and Signal Processing, 34*(11), 3709–3723.
19. Guo, Q., Ruan, G., & Na, P. (2017). Underdetermined mixing matrix estimation algorithm based on single source point. *Springer Circuits, Systems, and Signal Processing, 36*(11), 4453–4467.
20. Chen, P., Peng, P., Zhen, L., Luo, Y., & Xiang, Y. (2017). Underdetermined blind separation by combining sparsity and independence of sources. *IEEE Access, 5*, 21731–21742.
21. Eqlimi, E., Makkiabadi, B., Samadzadehaghdam, N., Khajehpour, H., Mohagheghian, F., & Sanei, S. (2018). A novel underdetermined source recovery algorithm based on k-sparse component analysis. *Springer Circuits, Systems, and Signal Processing, 38*(3), 1264–1286.
22. Wei, S., Wang, F. & Jiang, D. (2019). Sparse Component Analysis Based on an Improved Ant K-means Clustering Algorithm for Underdetermined Blind Source Separation. In: IEEE 16th International Conference on Networking, Sensing and Control, ser. ICNSC, 200-205
23. Hyvärinen, A., & Oja, E. (2000). Independent component analysis: Algorithms and applications. *Elsevier Neural Networks, 13*, 411–430.
24. Hyvärinen, A. (1999). Fast and robust fixed-point algorithms for independent component analysis. *IEEE Transactions on Neural Networks, 10*(3), 626–634.
25. Pal, M., Roy, R., Basu, J., & Bepari, M. S. (2013). Blind Source Separation: A Review and Analysis. *International Conference Oriental COCOSDA held jointly with Conference on Asian Spoken Language Research and Evaluation, ser.* (pp. 1–5). O-COCOSDA/CASLRE.
26. Comon, P. (1994). Independent component analysis, a new concept. Elsevier. *Signal Processing, 36*(3), 287–314.
27. Bell, A. J., & Sejnowski, T. J. (1995). An information maximization approach to blind separation and blind deconvolution. *Neural Computation, 7*(6), 1129–1159.
28. Lin, Q.H., Yin, F.L., & Liang, H. (2005). Blind Source Separation-Based Encryption of Images and Speeches. Proceedings of the Second international conference on Advances in neural networks, ser. ISNN'05 2:544–549.
29. Lin, Q. H., Yin, F. L., Mei, T. M., & Liang, H. (2008). A blind source separation based method for multiple images encryption. *Elsevier Image and Vision Computing, 26*, 788–798.
30. Sadr, S., & Okhovat, R. S. (2015). Security in the speech cryptosystem based on blind sources separation. *Springer Multimedia Tools and Applications, 74*(21), 9715–9728.

Mohammad Reza Aslani received his B.Sc. degree in electrical engineering, electronics, and his M.Sc degree in system communication from Shahab Danesh University, Qom, Iran, in 2016 and 2019, respectively. He is co-founder of Zraster that is a digital audio processing hardware production company. He is currently a researcher in the R&D unit of Zraster. His research interests include real-time communication networks, speech processing and blind source separation.

Mohammad Bagher Shamsollahi (M'02) received the B.Sc. degree in electrical engineering from Tehran University, Tehran, Iran, in 1988, the M.Sc. degree in electrical engineering, telecommunications, from the Sharif University of Technology, Tehran, in 1991, and the Ph.D. degree in electrical engineering, biomedical signal processing, from the University of Rennes 1, Rennes, France, in 1997.He is currently a Professor with the Department of Electrical Engineering, Sharif University of Technology. His research

interests include biomedical signal processing, brain–computer interface, and time-scale and time–frequency signal processing.

Arefeh Nouri received his B.Sc. degree in biomedical engineering from Amirkabir University of Technology, Tehran, Iran, in 2021. She is interested in brain mapping, machine learning and signal processing.