Provably secure and efficient audio compression based on compressive sensing

Enas Wahab Abood[1], Zaid Alaa Hussien[2], Haifaa Assy Kawi[1], Zaid Ameen Abduljabbar[3,4,5], Vincent Omollo Nyangaresi[6], Junchao Ma[7], Mustafa A. Al Sibahee[7,8], Saad Ahmad Ali Kalafy[9]

[1]Department of Mathematics, College of Science, University of Basrah, Basrah, Iraq
[2]Information Technical Department, Management Technical College, Southern Technical University, Basrah, Iraq
[3]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
[4]Technical Computer Engineering Department, Al-Kunooze University College, Basrah, Iraq
[5]Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen, China
[6]Faculty of Biological and Physical Sciences, Tom Mboya University, Homaba, Kenya
[7]College of Big Data and Internet, Shenzhen Technology University, Shenzhen, China
[8]Computer Technology Engineering Department, Iraq University College, Basrah, Iraq
[9]Basra Oil Training Institute, Ministry of Oil, Basrah, Iraq

Article Info

Article history:

Received Feb 17, 2022
Revised Jul 16, 2022
Accepted Aug 11, 2022

Keywords:

Audio compression
Audio securing
Compressive sensing
Moore-Penrose pseudoinverse
Signal compressing

ABSTRACT

The advancement of systems with the capacity to compress audio signals and simultaneously secure is a highly attractive research subject. This is because of the need to enhance storage usage and speed up the transmission of data, as well as securing the transmission of sensitive signals over limited and insecure communication channels. Thus, many researchers have studied and produced different systems, either to compress or encrypt audio data using different algorithms and methods, all of which suffer from certain issues including high time consumption or complex calculations. This paper proposes a compressing sensing-based system that compresses audio signals and simultaneously provides an encryption system. The audio signal is segmented into small matrices of samples and then multiplied by a non-square sensing matrix generated by a Gaussian random generator. The reconstruction process is carried out by solving a linear system using the pseudoinverse of Moore-Penrose. The statistical analysis results obtaining from implementing different types and sizes of audio signals prove that the proposed system succeeds in compressing the audio signals with a ratio reaching 28% of real size and reconstructing the signal with a correlation metric between 0.98 and 0.99. It also scores very good results in the normalized mean square error (MSE), peak signal-to-noise ratio metrics (PSNR), and the structural similarity index (SSIM), as well as giving the signal a high level of security.

Corresponding Author:

Junchao Ma
College of Big Data and Internet, Shenzhen Technology University
Shenzhen, 518118, China
Email: majunchao@sztu.edu.cn

1. INTRODUCTION

Audio is one of the main forms of information interchange, it performs an essential part of the communication process, irrespective of the kind of communication device used, whether mobiles, personal digital assistants (PDA) smart devices (SD) or computers [1]. Therefore, it is a matter of concern to improve and extensively study coding schemes to enhance the ability to encrypt and compress audio signals. The signal sampling of audio signals is based on the Shannon-Nyquist theorem standard method. This theorem states that the signal should be sampled with double or more than its maximum frequency, and most real signals take more than that rate [2]. Since such a signal demands a high bit rate channel to be transmitted, a signal compression process is required [2]. Compressed sensing is a supplementary process in the area of data recovery and security; it has been invested in many applications and signals such as radio, image, speech, and wireless sensor networks (WSNs), as well as being used in medical fields like medical resonance imaging (MRI) and radar imaging [3]. This technique relies on the sparsity advantage of the signal in a given domain to reduce the number of samples required to reconstruct the original signal; this requires several fewer samples than Nyquist sampling [4]. Many methods have been presented to implement signal compression, one of which is based on a discrete cosine transform (DCT) where the compressed signal is computed by transforming the input signal frames into a sparse one. Then these frames are multiplied by a sensing matrix, which can reduce a large amount of data by having fewer columns than rows. For retrieving original signal, the sensing matrix is used in its inverse form, this operation is known as reconstruction [5].

The process of reconstructing an original signal from compressed frames requires knowledge of the sensing matrix; since the process involves finding the best and most appropriate numerical solutions for a linear system of equations that are undetermined in the form ($y=\phi x$), in which the sensing matrix ϕ and the signal y are given; notably, there is no need to know anything about x except that it is sparse [6]. Sparsity is a mathematical term, where the sparse data set contains a large set of zeros while the remainders are a few non-zero numbers that represent meaningful and significant data [7]. Many applications have used compressive sensing as data compression in biomedical signal and imaging systems [8], agriculture machinery, digital signal processing [9], enhancing signal quality [10], electrocardiogram processing [11], analyzing power quality, communications, noise reduction [12], and signal security (either encryption or hiding) [6]. Furthermore, compressive sensing (CS) can be utilized as an encryption system in which the sensing matrix is a private key [2], [13]. The encryption system based on CS has many advantages, the decryption process needs fewer computations that are low in complexity, compared with other encryption systems due to using only standard matrix multiplication and is also considered a block-encryption system. However, the sensing matrices in both the encryption and decryption stages should be the same, while the whole system should be ensured because the encryption and decryption operations are both linear [1], [14].

Recently, it has become necessary to compress and encrypt data over transmission lines for securing information and reducing transmission bandwidth and storage space. To do so, CS has been widely used in signal compression and encryption applications, which provide less simultaneous sampling, compression and encryption of files [15]. Most data compression systems either have computational restrictions or incur large costs when compressing and decompressing, as well as being expensive in terms of computation time and storage space. There are also issues with accuracy in reconstruction and data loss, especially when working online. Moreover, the loss of time and additional storage requirements may be caused by waiting while decompressing finishes. Therefore, several factors must be taken into account and balanced when designing data compression systems, including the degree of compression, the amount of distortion that can be tolerated and the number of computational resources required to decompress the data. This paper will therefore present an algorithm based on an inexpensive mathematical principle to compress audio files using the pseudoinverse and compressive sensing technique, which is characterized by speed and a high percentage of compression with the ability to retrieve compressed files with high accuracy.

The main contribution of this paper is that the proposed system allows audio files to be compressed with high compression rates of up to 25%, while it is also efficient in terms of time consumption, calculations, and storage requirements, which significantly reduces data size when transferring files over the network. This also reduces storage and processing, making it suitable for adoption in tablets and smart devices. Furthermore, it provides a good level of security by changing the file samples and converting them to an incomprehensible format that varies in number from the original file. Only the person authorized to decompress can restore the original file.

This paper is organized: Section 2 presents the compressed sensing standard formula. Section 3 provides a detailed evaluation of Moore-Penrose Pseudoinverse. Section 4 contains this paper's proposed system. Section 5 shows the experiments and statistical analysis of the system evaluation. Finally, the conclusion has taken place within Section 6.

2. RELATED WORKS

Moore-Penrose inverse of full rank $r\times m$ matrices is used to get a fast and accurate digital image reconstruction [16]. This uses the fast and reliable (*ginv*) function method to calculate the Moore-Penrose pseudoinverse, which requires a lower computational effort, particularly for larger matrices, compared to those provided by the singular value decomposition (SVD) method. Chountasis *et al.* [16] produced a study of the mathematical aspects of CS and proposed a model for noise reduction based on CS for speech signals; they formulated a CS system using a random partial fourier as an optimization problem and used the gradient descend line search (GDLS) to solve it. Bala and Arif [7] proposed applying a compressed sensing technique to provide reliable reconstruction algorithms based on discrete fourier transform (DFT) and discrete cosine transform (DCT) for a speech signal using a small number of samples, they compared the performance of both algorithms and found that DCT runs relatively faster than DFT with less time. A video snapshot compressive imaging (SCI) system was proposed by building a digital micro-mirror device; developing a convolutional neural network of an end-to-end kind (E2E-CNN) with a plug-and-play (PnP) framework and adding deep denoising priors to solve the inverse problem [8]. Multiple-input multiple-output (MIMO) systems were studied [17], with an adaptive scheme based on CS, which used an efficient generalized multiple measurement vector approximate message passing (GMMV-AMP) algorithm to detect active users and estimate their channels in a regular manner, had been proposed. Moreno-Alvarado *et al.* [13] proposed a system to compress and encrypt audio signals based on CS, which segmented the audio signal into frames of 1024 samples and transformed it using DCT to get sparse frames, then they were multiplied by a sensing matrix. The sensing matrix was generated by the chaotic mixing system to satisfy the extended Wyner secrecy (EWS) criterion.

Chai *et al.* [9] used CS for security by proposing an efficient visually meaningful image compression and encryption (VMICE) scheme which consisted of CS and least significant bit (LSB) embedding. A compression and steganography system had been proposed [1]. First, the discrete wavelet transform (DWT) was applied to transform the plain image into sparse, then adding confusion operation on pixel positions based on a logistic-tent map. To get the cipher image, the sensed images were multiplied with the sensing matrix generated by a low-dimension complex tent-sine. A steganography step was added to the resulting image by applying singular decomposition for both secret and cover images, then the singular values of the secret image are embedded into the singular values of the cover image. Haneche *et al.* [10] proposed an approach for speech enhancement based on compressed sensing. Firstly, it removed noise, which was estimated during pauses then, the voice activity detection (VAD) was used for classifying frames as speech or silence while orthogonal matching pursuit was implemented as sparse recovery for speech enhancement.

Although the works detailed above have proven ability and trustworthiness in file compression and security, several drawbacks must be discussed and improved to build trusted compression and encryption systems based on CS. Some of these proposed systems have issues with higher computational costs, time consumption or recovery accuracy. To solve these problems, this paper proposes a system that uses basic linear operations to reduce implementation time, together with a pseudo-inverse with a Gaussian measurement matrix to improve the accuracy of reconstruction operations and a good compression ratio to save memory usage.

2.1. Compressed sensing standard formula

Compressive sensing (CS) is a technique for digital signal data acquisition and reconstruction that has several benefits for signal processing applications [18]. According to Nyquist sampling, the signal must be acquired at a rate more than twice its original frequency, which presents a lot of redundant data for the acquired signal. Traditional compression algorithms are used to eliminate any redundancy and produce a smaller number of bits for the signal representation [19]. On the other hand, the CS technique exploits the information rate within the signal, eliminating the signal redundancy in the sampling process that leads to a decreased efficient sampling rate [20]. The standard formula for compressive sensing can be represented with a linear system of equations, mathematically as (1),

$$Y_{m\times 1} = A_{m\times n} X_{n\times 1} \tag{1}$$

where the signal vector x is an n-length $\in R^n$, which is compressively sensed to be y with m-length $\in R^m$ through $m \times n$ samples of the signal vector A [21]. Figure 1 presents a diagram of the CS system. Remark: this is called “compressive sensing” because m is much smaller than n (i.e., m<n) and A is the compressive sensing matrix (or measuring matrix) which can be defined as (2),

$$A = \Psi\Phi \tag{2}$$

where Ψ is used to transform the original signal to a sparse basis, while Φ represents the compressed sensing measurement. Both Ψ and Φ are combined in one matrix called sensing matrix A [22]. The linear system in (1) can be written as a set of linear equations.

$$A_{11}X_1 + A_{12}X_{21} + \cdots + A_{1n}X_n = Y1,$$
$$A_{21}X_1 + A_{22}X_2 + \cdots + A_{2n}X_n = Y2,$$
$$A_{m1}X_1 + A_{m2}X_2 + \cdots + A_{mn}X_n = YM \quad (3)$$

To find the values of n variables, it is necessary to have n or more equations. Here the number of equations is much smaller than variables, so there are an infinite number of possible solutions. The true solution of vector x could be found by sensing (in a deterministic recovery way) whether A reflects some properties, then the recovery is possible [23], using non-deterministic CS. It may also be resolved by using optimization methods like the metaheuristic evolutionary method [24] or linear programming (LP) based on pseudo-inverse methods. Other solutions could use deterministic CS that demands a certain recovery process to sense the signal vector, which looks like an encoding-decoding technique [25]. The system proposed in this paper is based on CS technology to compress data and reduce signal size by multiplying it with an appropriate sensing matrix. This technology guarantees the retrieval of the signal with the least possible data loss, which is almost less than 0.01. It is also computationally inexpensive and uncomplicated, making the system more efficient.

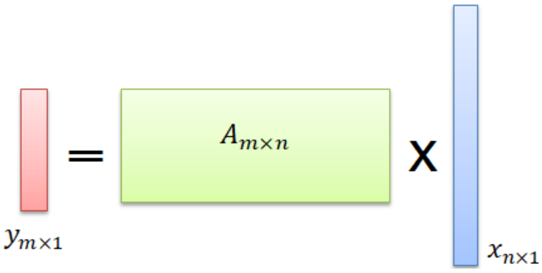


Figure 1. General diagram of compressive sensing

2.2. Moore-Penrose pseudoinverse

In linear algebra and particularly in linear inverse problems in (1), the Moore-Penrose inverse A+ of a matrix A is the most well-known inverse matrix in cases of *m≠n* [26]. It was first proposed by Moore in 1920 [27] and subsequently by many others. The Moore-Penrose pseudoinverse has been widely used to compute the best solution (least squares) for a system of linear equations that have infinite solutions and can be used for proofing results in linear algebra. The pseudo-inverse can be defined uniquely for all matrices of real or complex numbers and can be computed with the singular value decomposition [28].

Having A∈R^(m×n), where m≠n, a pseudoinverse of matrix A is a matrix A+ which satisfies four criteria (the Moore-Penrose conditions):

$$A^+A = A$$
$$A^+AA^+A = A^+$$
$$(AA^+)^T = AA^+$$
$$(A^+A)^T = A^+A \quad (4)$$

where A^+ is an inverse, AA^+ and A^+A meet the Hermitian condition. The last two conditions provide uniqueness property of the A^+ [28], [29]. In general, each matrix has its inverse but when A has unequal dimensions there are two possible situations:

a) If A has linearly independent columns, the solution would exist and be unique, A^+ can be calculated as:

$$A^+ = (A^TA)^{-1}A^T \quad (5)$$

where $A^+A = I$.

b) If A has linearly independent rows, the solution would exist and be infinite with an indeterminate system, A^+ can be calculated as:

$$A^+ = A^T(A^TA)^{-1} \quad (6)$$

where $AA^+ = I$

Sparse pseudo-inverse is applicable in the underdetermined system, as well as in compressed sensing. Therefore, if the solution of an underdetermined linear inverse problem y=Ax in case of x is low dimensional, the Moore-Penrose is desirable due to its ability to reduce the complexity of calculations [30]. To solve the linear system Y=AX, A+ is calculated with (5) or (6), then X can be found with the relation (7).

$$X = A^{+}Y \tag{7}$$

It can be said that (7) is the reconstruction equation. Remark: the Moore-Penrose pseudoinverse is used to compute the solution in this paper's proposed system because of its simplicity in implementation and the need for fewer requirements. It provides the solution (the best fit) for systems that have multiple solutions [28].

3. PROPOSED SYSTEM

In this work, a simplified and efficient system is exploited for compressing an audio signal. The system is based on compressive sensing principle to reduce the number of samples of the audio signal. It uses Moore-Penrose pseudo-inverse for reconstruction operation. The general scheme of the system is shown in Figure 2. In Figure 2(a), the steps of CS scheme are illustrated while Figure 2(b) shows the reconstruction scheme for the retrieved signal.

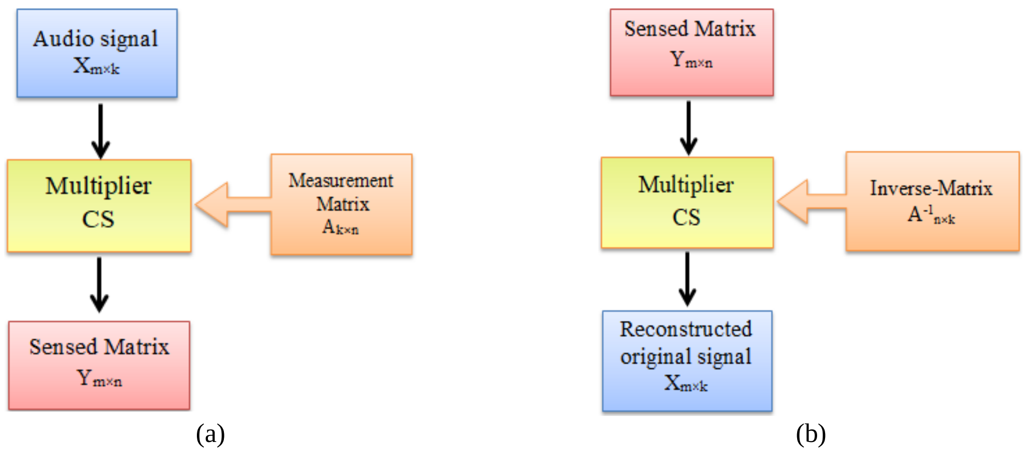


Figure 2. General diagram of the proposed system (a) CS Scheme and (b) reconstruction scheme

The system comprises three steps:

a) Measurement matrix generation: the choice of measurement matrix A is an essential step in an audio compression system based on CS. Its values affect the quality of recovered data, while it could act as secret key encryption [31]. To obtain more accurate signal reconstruction, the measurement matrix values would be selected as Gaussian random variables [32].
b) Audio compression: in this part, an audio signal is sensitively compressed by using a measurement matrix in Algorithm 1.

Algorithm 1. The signal compression
- Begin
- Dividing the signal into frames of sub-matrix, each frame contains $m \times k$ samples from the original signal.
- These frames are multiplied by the measurement matrix of size $k \times n$ values as in (1), Figure 2(a). To accomplish the data reduction aim, this paper chose $k>m$ and $k>n$.
- Gathering the resulting sub-matrix of the new size $m \times n$ in one new compressed file to be sent or exchanged.
- End.

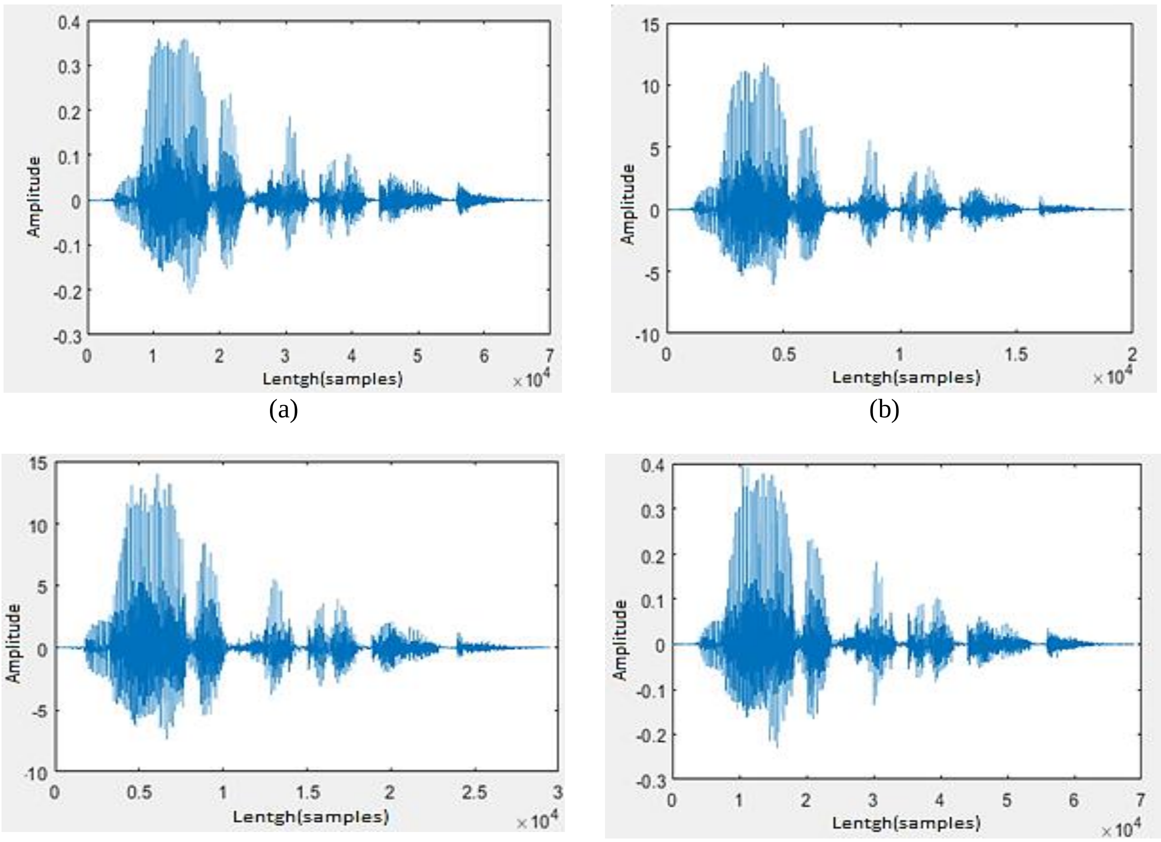
c) Signal reconstruction: when the compressed data has been sent to the recipient or transferred through transmission lines, a reconstruction operation must take place to retrieve the original signal. This operation is carried out using Algorithm 2.

Algorithm 2. The signal reconstruction
- Begin
- Dividing the sensed matrix resulting from Algorithm 1 into frames of size $m \times n$.
- Calculating the inverse of the measurement matrix using the Moore-Penrose pseudoinverse.
- Since the measurement matrix is not a square matrix (i.e., $k \neq n$), the inverse matrix is estimated by (6).
- Multiplying sensed frames with the inverse of the measurement matrix as in (7), Figure 2(b).
- Joining all resulting frames and reshaping them to get a one-dimensional vector of the original signal.
- End.

4. EXPERIMENTS AND ANALYSIS

To prove the ability of the proposed system, it was evaluated and tested with different audio signals, such as music, songs, and speech, in different sampling frequencies ranging from 11-48 kHz. The system was simulated with MATLAB R2018a on Intel® Core i7-3520M CPU 2.90 GHz 8.00 GB RAM of memory. The compression was implemented with two rates (30% and 50%) with two measurement matrices, and then two CS systems were built: i) $Y_{3\times4}=A_{3\times8}\ X_{8\times4}$ for 30% compression rate; ii) $Y_{4\times4}=A_{4\times8}\ X_{8\times4}$ for 50% compression rate.

The result is shown in Figure 3(a) which shows an original speech signal with FS 48 kHz and length 6.8e+4 samples. Figure 3(b) sensed signal with compression rate 30% with length 1.96e+4 samples. in Figure 3(c) a sensed signal with compression rate 50% with length 2.95e+4 samples, while in Figure 3(d), the reconstructed signal. Note how the sensed file shrinks in size while keeping the critical influencing values.



(a) (b) (c) (d)

Figure 3. Speech signal with FS 48 kHz (a) original signal with length 6.8e+4 samples, (b) sensed signal with compression rate 30% with length 1.96e+4 samples, (c) sensed signal with compression rate 50% with length 2.95e+4 samples, and (d) reconstructed signal

Figure 4 shows audio signals before and after being reconstructed with a 30% rate, in Figure 4(a) the original was 48,000 fs while in Figure 4(b) was 11,025 fs, in Figure 4(c) the signal was with frequency

44,100 fs. The reconstructed signals were the same as their original signals either in length or in peaks. This indicates the accuracy of retrieval due to the reliance on the Gaussian matrix as a sensing matrix, which has the characteristics of retaining the effective values of the compressed matrix, supporting the retrieved values. Furthermore, several statistical analysis tests were performed to evaluate the reconstruction quality of the system in both compression rates.

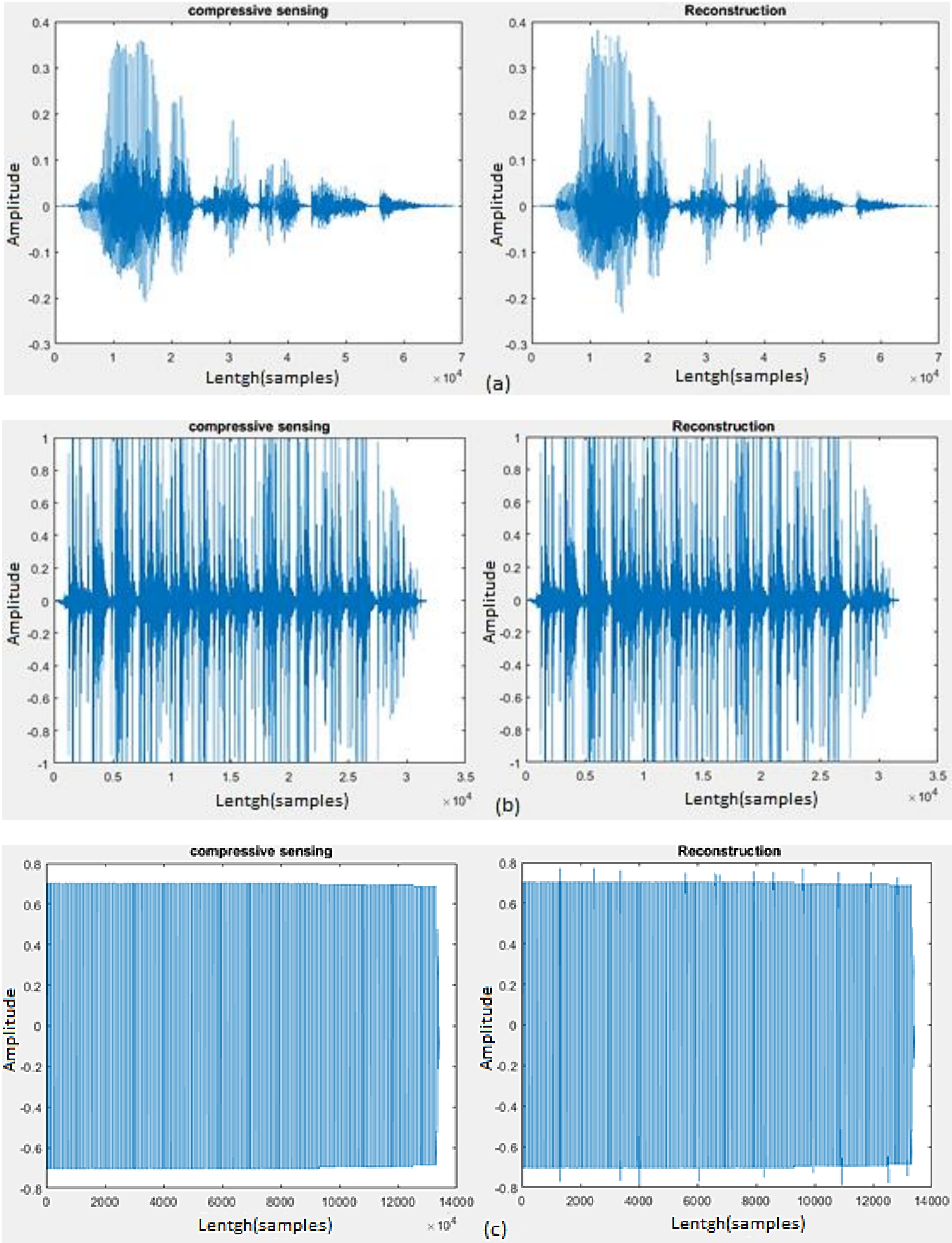


Figure 4. The original signal vs reconstructed signal with Fs (a) 48000 fs, (b) 11025 fs, and (c) fs44100

4.1. Elapsed time and compression rate

The pseudo-inverse technique used allowed the system to score excellent results in time consumption for implementation for both compression and reconstruction. Many different-sized files were compressed with the 30% and 50% compression rates. The size of the compression file had steadily shrunk in the number of samples, while the storage size in bytes had shrunk in different sizes based on the original file size, as illustrated in Tables 1 and 2. Tables 1 and 2 show that the time was relatively low and suitable for online systems and smart devices, as well the compression rate was very convenient. Remark: if the file size is large, its compression rate would also be high.

Table 1. The size of the tested file before and after compression and time consumed by the system with 50% rate

File size				Time(s)		file size rate%
before		after				
Size(byte)	sample	size	sample	compress	extract	
31 kB	31744	18 K	15800	0.004	0.0039	58
50 kB	51740	28 K	26124	0.011	0.011	56
147 kB	150680	81K	76245	0.048	0.049	55.1
505 kB	129488	254 K	66235	0.045	0.0402	50.2
1.02 MB	268236	501 K	136214	0.109	0.11	48.9
2.04 MB	536472	846 K	271234	0.39	0.41	40.2
4.98 MB	1306624	2.01 M	657241	1.8	1.9	40.3
9.9 MB	2601616	4.1 M	1401234	3.1	3.21	41.4

Table 2. The size of the tested file before and after compression and time consumed by the system with 30% rate

File size				Time(s)		file size rate%
before		after				
Size(byte)	sample	size	sample	compress	extract	
31 kB	31744	20	9069	0.005	0.005	64.5
50 kB	51740	37 K	14783	0.012	0.016	74
147 kB	150680	83	43051	0.051	0.05	56.46
505 kB	129488	118 K	36997	0.031	0.032	23.36
1.02 MB	268236	276 K	76639	0.125	0.123	26.28
2.04 MB	536472	548 K	15328	0.409	0.4105	24.35
4.98 MB	1306624	1.28 M	373320	2.00566	2.001	25.70
9.9 MB	2601616	2.52 M	743320	4.5969	4.601	25.45

4.2. Pearson correlation analysis

This is a significant metric for evaluating the similarity between the original and the reconstructed audio signals, which is computed:

$$r = \frac{\sum (x_i - \underline{x})(y_i - \underline{y})}{\sqrt{\sum (x_i - \underline{x})^2 \sum (y_i - \underline{y})^2}}$$

where x_i is the sample value of the original signal, $\underline{x}$ is its mean, y is the reconstructed signal. The matric scores from 1-0 according to the similarity ratio between signals, 1 is identical and 0 different ones.

4.3. PSNR and MSE analysis

To evaluate the recovery capability of the proposed system, the normalized mean square error (MSE) and peak signal-to-noise ratio metrics (PSNR) parameters were used [33]. These parameters were computed between the original and reconstructed signals, given by:

$$MSE = \frac{\sum_{i=0}^{m-1} (X_i - Y_i)^2}{m}$$

where X is the original signal and Y is the reconstructed signal.

$$PSNR = 10 * log_{10}\left(\frac{Max_X^2}{MSE}\right)$$

4.4. The structural similarity index (SSIM)

The SSIM is a perceptual metric that quantifies the matrix quality distortion caused by processing operations such as data compression or encryption. It is used here to evaluate the system's ability to reconstruct the signal accurately. It is given by:

$$SSIM = \frac{(2\underline{x}\underline{y}+c_1)(2\sigma xy+c2)}{(\sigma x2+\sigma y2+c2)(\underline{x}\ 2+\underline{y}2+c1)}$$

where c_1=$(Z_1L)^2$, and c_2=$(Z_2L)^2$ are both constant to avoid null dominator; L is the high range of the signal sample values; Z_1 and Z_2 have default values of 0.01 and 0.03, respectively. The identical score between the two measured signals is 1, decreasing to -1 as the signal changes [34]. See Table 3.

Table 3 shows that the two compression ratios were implemented on audio files of different sizes from 31 kB to 9.9 MB (i.e., the compressed file was sized 0.3 and 0.5 of the original size). In testing the proposed system implementation, the PSNR, MSE, SSIM and correlation metrics all scored relatively good results. For the 30% compression ratio, the PSNR scored 16-20 dB, MSE reached 3.0E-4, while the SSIM was in range (0.5-0.99), demonstrating good recovery; the correlation factor was almost 0.99 compared to the scores for the 50% compression ratio, the last compression ratio (50%) scored better results overall for all metrics.

Remark: despite the slight discrepancy between the results of the two compression ratios, it is clear that 50% compression gives a better ability to retrieve with a small difference from 30% especially with bigger files. This was proved by the correlation factor (R) for both the 30% and 50% compression ratios. So, both remain acceptable compared to the system's outputs in terms of reducing the size and time consumed in implementation.

Table 3. Statistical analysis values (PSNR, MSE, SSIM, correlation) of the proposed system calculated for different-sized files and compression rates (30% and 50%)

SIZE (BYTE)	COMPRESS BY 30%				COMPRESS BY 50%			
	PSNR	MSE	SSIM	R	PSNR	MSE	SSIM	R
31 kB	16.0976	0.0245	0.56669	0.991	16.573	0.0220	0.6072	0.989
50 kB	17.5795	0.0174	0.71358	0.991	17.692	0.01700	0.724	0.98
147 kB	20.949	0.008	0.7057	0.994	21.562	0.00697	0.7435	0.98
505 kB	20.55	8.79925E-05	0.9579	0.9916	40.647	8.61505E-05	0.9592	0.98
1.02 MB	33.287	4.6912E-04	0.8431	0.99	33.85	4.12098E-04	0.8634	0.9907
2.04 MB	34.3557	3.66796E-04	0.8778	0.9902	35.31	3.06184E-04	0.8968	0.9989
4.98 MB	32.87235	5.16139E-04	0.9049	0.999	33.7241	4.242108E-04	0.921	0.9914
9.9 MB	34.358	3.665831E-04	0.92	0.9907	35.237	2.99971E-04	0.935	0.9956

4.5. Comparison with previous systems

4.5.1. Comparative computational complexity analysis

CS aims to reduce and standardize sampling and compression operations and reduce computational complexity during encoding and decoding. CS greatly reduces coding complexity and storage requirements. The presented algorithm does not require scattering operations and pre-construction operations. The compression is carried out using the sensing matrix, which is a key in the form of an array. Encryption is done by multiplication. This algorithm provides inconsistency and provides security as well as reducing the size and thus reducing storage. The reconstruction operation requires only simple operations of multiplication and division. Consequently, our system significantly reduces the computational complexity because the complexity time of the proposed algorithm is *O(n)* which is better than in [35], [36] that are $O\left(10^{(2m)^2}\right)$ and $O(10^{mn})$ respectively.

4.5.2. Comparative performance analysis

Table 4 shows a comparison between the proposed system performance and that of the previous system in [13] for the Pearson correlation and MSE when implementing files with the same attributes, musical audio files and speech signals were recorded with the same characteristics as the files used in [13] in terms of length and size. The results indicate that the proposed system has good scores in both metrics, proving its efficiency in compression and reconstruction. The proposed system can also be used for securing files as an encryption technique.

Table 4 shows that the proposed system has good results compared with the earlier proposed system. The model of this paper has better correlation coefficients and MSE values than [13], which means that this system has a better signal recovery ability. The compression ratio in the proposed system also reached 30% of the original file, which is less than the compression ratio of [36] and close to the MSE values.

Table 4. Comparison of the proposed system, Moreno-Alvarado *et al.* [13], and Abduljaleel and Khaleel [36] by MSE and correlation values

File size (sample/frame)	Moreno-Alvarado *et al.* [13]		Abduljaleel and Khaleel [36]		Proposed	
	MSE	R	MSE	R	MSE	R
128	0.28	0.8952	7.2978E-05	0.99	0.007	0.9906
256	0.11	0.9787	6.5874E-05	0.999	8.3065e-05	0.998
512	0.026	0.9978	6.2188E-05	0.999	8.154e-05	0.99
700	0.006	0.9987	6.8680E-05	0.99	7.051e-05	0.99
1024	4e-6	1.00	8.7965E-05	0.9999	4.001e-04	0.993

5. CONCLUSION

This paper presents a CS-based compression system for compressing and securing audio signals. The audio signals are segmented as frames of 8×4 small matrices. The frames are then multiplied by a sensing matrix of 3×8 or 4×8, which are generated using Gaussian random numbers. The whole system is a linear system Y=AX and could be solved to reconstruct X using the Moore-Penrose pseudoinverse to calculate A^{-1}, which makes the system low-cost and easy to implement with less time consumption, while it provides good compression ratios with a reasonable rate of security.

The implementation results and statistical analysis metrics prove that the proposed system provides a reliable compression system and a reconstruction of the good quality signal. This is demonstrated by the correlation coefficients and SSIM, which are very close to 1, the MSE values are small, such as 5.0E-4, while PSNR is within an acceptable range. The analytical results also show that the proposed system provides results that are close to, and better than, an alternative system. Finally, it should be noted that when the file size is bigger, the system performance is better.

ACKNOWLEDGMENT

This work is supported by Natural Science Foundation of Top Talent of SZTU (grant No. 20211061010016).

REFERENCES

[1] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, "Image encryption and hiding algorithm based on compressive sensing and random numbers insertion," *Signal Processing*, vol. 172, Jul. 2020, doi: 10.1016/j.sigpro.2020.107563.
[2] I. Orovic, S. Stankovic, B. Jokanovic, and A. Draganic, "On compressive sensing in audio signals," 2012.
[3] K. Zhen, H. D. Nguyen, F.-J. Chang, A. Mouchtaris, and A. Rastrow, "Sparsification via compressed sensing for automatic speech recognition," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Jun. 2021, pp. 6009–6013, doi: 10.1109/ICASSP39728.2021.9413844.
[4] D. F. Resende, M. Khosravy, H. L. M. Monteiro, N. Gupta, N. Patel, and C. A. Duque, "Neural signal compressive sensing," in *Compressive Sensing in Healthcare*, Elsevier, 2020, pp. 201–221.
[5] D. L. Currie III and C. E. Irvine, "Surmounting the effects of lossy compression on steganography," 1996.
[6] H. Rabah, A. Amira, B. K. Mohanty, S. Almaadeed, and P. K. Meher, "FPGA implementation of orthogonal matching pursuit for compressive sensing reconstruction," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 10, pp. 2209–2220, Oct. 2015, doi: 10.1109/TVLSI.2014.2358716.
[7] S. Bala and M. Arif, "Performance comparison of discrete transforms on speech compressed sensing," in *2015 IEEE International Conference on Computational Intelligence and Communication Technology*, Feb. 2015, pp. 632–637, doi: 10.1109/CICT.2015.136.
[8] M. Qiao, Z. Meng, J. Ma, and X. Yuan, "Deep learning for video compressive sensing," *APL Photonics*, vol. 5, no. 3, Mar. 2020, doi: 10.1063/1.5140721.
[9] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding," *Optics and Lasers in Engineering*, vol. 124, Jan. 2020, doi: 10.1016/j.optlaseng.2019.105837.
[10] H. Haneche, B. Boudraa, and A. Ouahabi, "A new way to enhance speech signal based on compressed sensing," *Measurement*, vol. 151, Feb. 2020, doi: 10.1016/j.measurement.2019.107117.
[11] B. Mohanty, M. Sahoo, and S. Mohapatra, "R-D optimization of EED-based compressed image using linear regression," in *Computational Vision and Robotics*, Springer India, 2015, pp. 125–133.
[12] D. Wu, W.-P. Zhu, and M. N. S. Swamy, "A compressive sensing method for noise reduction of speech and audio signals," in *2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug. 2011, pp. 1–4, doi: 10.1109/MWSCAS.2011.6026662.
[13] R. Moreno-Alvarado, E. Rivera-Jaramillo, M. Nakano, and H. Perez-Meana, "Simultaneous audio encryption and compression using compressive sensing techniques," *Electronics*, vol. 9, no. 5, May 2020, doi: 10.3390/electronics9050863.
[14] J. Lin *et al.*, "An image compression-encryption algorithm based on cellular neural network and compressive sensing," in *2018 IEEE 3rd International Conference on Image, Vision and Computing (ICIVC)*, Jun. 2018, pp. 673–677, doi: 10.1109/ICIVC.2018.8492882.
[15] Y. Tang, M. Zhao, and L. Li, "Secure and efficient image compression-encryption scheme using new chaotic structure and compressive sensing," *Security and Communication Networks*, pp. 1–15, Dec. 2020, doi: 10.1155/2020/6665702.

[16] S. Chountasis, V. N. Katsikis, and D. Pappas, "Applications of the moore-penrose inverse in digital image restoration," *Mathematical Problems in Engineering*, pp. 1–12, 2009, doi: 10.1155/2009/170724.
[17] M. Ke, Z. Gao, Y. Wu, X. Gao, and R. Schober, "Compressive sensing based adaptive active user detection and channel estimation: massive access meets massive MIMO," *IEEE transactions on signal processing*, vol. 68, pp. 764–779, 2020.
[18] P. Gerstoft, C. F. Mecklenbräuker, W. Seong, and M. Bianco, "Introduction to compressive sensing in acoustics," *The Journal of the Acoustical Society of America*, vol. 143, no. 6, pp. 3731–3736, Jun. 2018, doi: 10.1121/1.5043089.
[19] D. Craven, B. McGinley, L. Kilmartin, M. Glavin, and E. Jones, "Compressed sensing for bioelectric signals: a review," *IEEE Journal of Biomedical and Health Informatics*, vol. 19, no. 2, pp. 529–540, Mar. 2015, doi: 10.1109/JBHI.2014.2327194.
[20] C. Song, A. Wang, F. Lin, J. Xiao, X. Yao, and W. Xu, "Selective CS: an energy-efficient sensing architecture for wireless implantable neural decoding," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 8, no. 2, pp. 201–210, Jun. 2018, doi: 10.1109/JETCAS.2018.2809906.
[21] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, "An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing," *Information Sciences*, vol. 556, pp. 305–340, May 2021, doi: 10.1016/j.ins.2020.10.007.
[22] S. Yu, R. Wang, W. Wan, L. Du, and X. Yu, "Compressed sensing in audio signals and it's reconstruction algorithm," in *2012 International Conference on Audio, Language and Image Processing*, Jul. 2012, pp. 947–952, doi: 10.1109/ICALIP.2012.6376750.
[23] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005, doi: 10.1109/TIT.2005.858979.
[24] M. Khosravy, N. Gupta, N. Patel, and T. Senjyu, Eds., *Frontier applications of nature inspired computation*. Singapore: Springer Singapore, 2020.
[25] N. Gupta, M. Khosravy, N. Patel, S. Gupta, and G. Varshney, "Artificial neural network trained by plant genetic-inspired optimizer," in *Springer Tracts in Nature-Inspired Computing*, Springer Singapore, 2020, pp. 266–280.
[26] S. L. Campbell and C. D. Meyer, *Generalized inverses of linear transformations*. SIAM, 2009.
[27] E. H. Moore, "On the reciprocal of the general algebraic matrix," *Bulletin of the American Mathematical Society*, vol. 26, pp. 394–395, 1920.
[28] I. Dokmanic, M. Kolundzija, and M. Vetterli, "Beyond moore-penrose: sparse pseudoinverse," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, May 2013, pp. 6526–6530, doi: 10.1109/ICASSP.2013.6638923.
[29] J. Stoer and R. Bulirsch, *Introduction to Numerical Analysis*, 3rd ed. New York, NY: Springer New York, 2002.
[30] M. Bayati, M. Lelarge, and A. Montanari, "Universality in polytope phase transitions and message passing algorithms," *The Annals of Applied Probability*, vol. 25, no. 2, Apr. 2015, doi: 10.1214/14-AAP1010.
[31] Y. C. Eldar and G. Kutyniok, *Compressive sensing: theory and applications*. Cambridge university press, 2012.
[32] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Processing*, vol. 134, pp. 35–51, May 2017, doi: 10.1016/j.sigpro.2016.11.016.
[33] "Securing text messages using graph theory and steganography," *Baghdad Science Journal*, vol. 19, no. 1, Feb. 2022, doi: 10.21123/bsj.2022.19.1.0189.
[34] E. W. Abood, Z. A. Abduljabbar, M. A. Al Sibahee, M. A. Hussain, and Z. A. Hussien, "Securing audio transmission based on encoding and steganography," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 22, no. 3, pp. 1777–1786, Jun. 2021, doi: 10.11591/ijeecs.v22.i3.pp1777-1786.
[35] L. Zeng, X. Zhang, L. Chen, Z. Fan, and Y. Wang, "Scrambling-based speech encryption via compressed sensing," *EURASIP Journal on Advances in Signal Processing*, no. 1, Dec. 2012, doi: 10.1186/1687-6180-2012-257.
[36] I. Q. Abduljaleel and A. H. Khaleel, "Speech signal compression and encryption based on sudoku, fuzzy C-means and threefish cipher," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 6, pp. 5049–5059, Dec. 2021, doi: 10.11591/ijece.v11i6.pp5049-5059.

BIOGRAPHIES OF AUTHORS

Enas Wahab Abood received the bachelor's and master's degrees in computer science from Basrah University, Iraq, in 2005 and 2011, respectively. Her research interests include image processing, sound processing, encryption systems, similarity measures, NLP, and graph theory. She has many articles in different aspects of computer science. She can be contacted at email: enas.abood@uobasrah.edu.iq.

Zaid Alaa Hussien received the B.Sc. degree in Computer Engineering from University of Basrah, Iraq in 2004, the M.Tech degree in Computer Science and Engineering from Guru Gobind Singh Indraprastha University, India in 2009 and the Ph.D. degree from School of Computer Science and Technology, Huazhong University of Science and Technology, China in 2017. His current research interests include focus on security and integrity issues in cloud computing, big data, and Internet of Things. He can be contacted at zaid.alaa@stu.edu.iq.

Haifaa Assy Kawi received the bachelor's and master's degrees in Mathematics science from University of Basrah, Iraq in 2005. Her research interests include optimization. She can be contacted at haifaa.kawi@uobasrah.edu.iq.

Zaid Ameen Abduljabbar received the bachelor's and master's degrees in computer science from University of Basrah, Iraq, in 2002 and 2006, respectively, and the Ph.D. degree in computer engineering from the Department of Computer Science and Technology, Huazhong University of Science and Technology, China, in 2017. His research interests include cloud security, searchable encryption systems, similarity measures, internet of things, secure computation, biometric, and soft computing. He has published regular articles for more than 40 IEEE International Conferences and High-quality articles in SCI journals, and he holds 3 international patents and 2 international computer software copyright. He has always served as a reviewer for several prestigious journals and has served as the PC chair/PC member for more than 25 international conferences. He can be contacted at zaid.ameen@uobasrah.edu.iq.

Vincent Omollo Nyangaresi received his bachelor's degree in telecommunication and information engineering in 2010 and a master's degree in information technology security and audit in 2018. His first doctorate degree is in information technology security and audit. He is currently pursuing his second doctorate degree in computer science. His research interests include machine learning, computer networks and security protocols, telecommunication engineering and systems modeling. He has published over 40 research articles in peer reviewed journals, conferences, and symposiums. He can be contacted at vnyangaresi@tmuc.ac.ke.

Junchao Ma is an associate professor in Shenzhen Technology University. He received B.Eng. in Automation from Zhejiang University, China in 2006. He received M.Eng. in Department of Electronic and Information Engineering from The Hong Kong Polytechnic University, Hong Kong in 2007. He received Ph.D. degree in Department of Computing from The Hong Kong Polytechnic University, Hong Kong in 2013. He worked in Huawei as a senior engineer from 2013 to 2020. His research interests are broadly in the fields of big data, internet of things, and wireless ad hoc and sensor networks. He can be contacted at majunchao@sztu.edu.cn.

Mustafa A. Al Sibahee current position at college of big data and internet, Shenzhen Technology University, Shenzhen-China. Computer Technology Engineering Department, Iraq University College, Basrah, Iraq. Received his, Ph.D. 2018, from Huazhong University of Science and Technology, Wuhan-China. From April-2019 to March-2021, was a postdoctoral at Shenzhen Huazhong University of Science and Technology, Research Institute, Shenzhen-China. His research interests include computer networks and information security, internet of things and wireless sensor networks (WSNS). He can be contacted at mustafa@sztu.edu.cn.

Saad Ahmad Ali Kalafy has a degree in Computer Science from Basra University, Iraq, in 2001, and a master's degree in Computer Engineering from the Department of Electrical and Computers, Kashan University, Iran, in 2018, and currently a PhD student at Tabriz University. His research interests include cloud security, searchable encryption systems, Internet of things, secure computing, networking, and control algorithms. He can be contacted at Saad.Kalafy@gmail.com.