Research Article

An Adaptive Audio Steganography for Covert Wireless Communication

Guojiang Xin ¹, **Yuling Liu** ², **Ting Yang**² and **Yu Cao**³

¹*School of Informatics, Hunan University of Chinese Medicine, 410208, China*

²*College of Computer Science and Electronic Engineering, Hunan University, 410082, China*

³*Department of Computer Science, University of Massachusetts Lowell, 01854, USA*

Correspondence should be addressed to Yuling Liu; yuling_liu@126.com

Received 27 May 2018; Accepted 1 August 2018; Published 16 August 2018

Academic Editor: Zhaoqing Pan

Copyright © 2018 Guojiang Xin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In recent years, the wide applications of the wireless sensor networks have achieved great success. However, the security is a critical issue in many scenarios ranging from covert military operations to the organization of the social unrest. Because the traditional encrypting methods are easy to arouse suspicion, an adaptive audio steganography method is proposed. The method is based on interval and variable low bit coding, which can be applied to covert wireless communication. The interval for embedding secret messages into the audio file and the threshold in variable low bit coding are used for selecting the embedding location and embedding bits adaptively; thus the embedding capacity and the embedding rate are variable. Experimental results demonstrate that the proposed method has better performance in embedding rate and invisibility than other audio steganography methods.

1. Introduction

Nowadays, wireless sensor networks (WSNs) and multimedia are getting increasing attention from both academic and industry communities, which hold the promise of facilitating large-scale and real-time data processing including video and audio in complex real-time multimedia environments, retrieving multimedia content, and object detection [1–3]. The security for real-time communication is a critical issue that must be resolved. In this paper, real-time audio communication is focused. Most often, cryptography techniques are utilized for the security of WSNs, which are based on rendering the content of a message garbled to unauthorized people [4]. However, it is well known that cryptography methods make people become aware of the existence of secret information. Hence, steganography, which is a process of embedding secret messages into a cover signal to avoid illegal detection [5], was introduced to ensure the transmission safety of the secret information and authenticate the multimedia data in WSNs [6, 7]. A verifiable diversity ranking search scheme over encrypted outsourced data is proposed while preserving privacy in cloud computing, which also supports search results verification [8].

In recent years, many methods have been proposed for steganography and steganalysis, such as coverless information hiding [9], steganography, and steganalysis based on deep learning [10, 11]. However, it is still a challenging problem to use audio signal as the cover signal, because Human Auditory System (HAS) is very sensitive. The existing typical audio steganography methods can be divided into time domain methods, transform domain methods, compressed domain methods, and phase methods. Most time domain methods refer to the methods based on least significant bits (LSB) of the audio data [12]. The algorithm performs scrambling pretreatment using logistic chaotic on the secret watermarking information to make watermarking bits garbled. The public audio signal is transformed by DWT, so that the secret information is embedded into the selected wavelet coefficients with multi-resolution. The original carrier is not required in watermarking recovery. Another time domain method is echo hiding method [13]. Because the weak signal becomes unable to hear after the strong signal disappears, the echo is introduced to achieve information hiding. This method is robust but has high computational complexity, low capacity, and low extraction accuracy. The transform

domain methods firstly need to do discrete Fourier transform (DFT), discrete cosine transform (DCT), or discrete wavelet transform (DWT), or a combination of the three transforms, and then select certain frequency coefficients to embed the secret message. These methods have good robustness but low capacity and relatively complex calculation [14, 15]. The compressed domain methods are suitable for the compressed audio files. These methods are not only difficult to implement but also have limited hiding capacity [16]. Because HAS is sensitive to relative phase, but not sensitive to absolute phase, the methods based on phase coding are proposed. The secret message is embedded by replacing the absolute phase of the original audio with the relative phase. These methods are robust, but the capacity is limited and the calculation is more complicated [17, 18]. According to the different application scenarios, a method with a rational selection among hiding capacity, invisibility, and robustness is expected.

There are some data embedding algorithms based on LSB. The lowest bit coding is the method that embeds secret data only in LSB. This method can minimize the transition and obtain the embedding capacity up to 12.5% of the wav file [19]. The parity coding method breaks a signal down into separate regions of samples instead of individual sample. If the secret bit to be encoded does not match with the sample region's parity bit, then it flips the LSB of one sample in the region [20]. Exclusive OR (XOR) operation is firstly performed on the LSB, and then the LSB of the sample is modified or kept unchanged according to the result of XOR operation and the message bit to be embedded [21]. About bit selection, the different bits are selected to hide the secret data in each sample. For instance, the first two most significant bits (MSB) of a sample are used for bit selection and only the first three LSB are used for data embedding [22]. A parameter R , which is an interval, is set for embedding the bit stream of a secret message into each byte of audio packets. If $R = 1$, the secret message is embedded into every 2 bytes of audio streams, while if $R = 2$, the secret message is embedded into every 3 bytes of audio streams [23]. While through selecting some samples, only a few samples are used for data hiding instead of using all the samples. For instance, the first three MSB are used to select the next sample for embedding the secret bits [22]. Fibonacci sequence is used to select the samples for data hiding [24]. In average amplitude method, the average amplitude data of surrounding audio data is used as a threshold. If the amplitude level is bigger than the average value, then 2 LSB are used for embedding; otherwise the secret data will not be embedded [19]. The variable low bit coding is the improved version of the lowest bit coding which can increase the embedding capacity. Because the sound is a silence at the middle range of audio data, the data cannot be embedded in the middle range. Two thresholds are defined based on the standard level, which is calculated by the middle range. The thresholds are used for selecting the embedding bits.

Many improved LSB methods are based on the combination of several algorithms. In [25], a dual random LSB method is proposed by combining Huffman coding with RSA encryption. The method embeds the data in variable LSB

depending on the MSB of cover audio samples. Also, there is an increase in capacity due to the use of Huffman coding. In [26], for each sample, the third and fourth LSB are replaced with the secret message and the second and fifth LSB are altered by using an intelligent algorithm so that the stego sample gets minimized. In [27], the audio samples are 16 bits. The secret message is embedded into the coefficients of a cover audio. Each secret bit is embedded into the selected position of a cover coefficient. The positions are selected from the 0th to 7th LSB based on the MSB. In [28], a wav-audio steganography algorithm based on modifying amplitude is proposed. Sampling points are grouped by each three successive ones and the amplitude values are calculated. Secret message is embedded by modifying the amplitude value of the second sampling point by comparing the amplitude value of the second sampling point with the average value of the first and the third sampling points. In [29], a novel reversible natural language watermarking method combines arithmetic coding and synonym substitution operations. The original context can be perfectly recovered by decompressing the extracted compressed data and substituting the replaced synonyms with their original synonyms.

In this paper, an improved audio steganography method for covert wireless communication is proposed by incorporating the variable low bit coding with the embedding intervals. Different from the steganography methods based on Voice over Internet Protocol (VoIP) [30], the proposed method will be applied to nonreal-time audio data in covert wireless communication, in which the hiding capacity, instantaneity, and security are concerned. The method has good performance in terms of the embedding rate, hiding capacity, and invisibility.

The rest of the paper is organized as follows. The variable low bit coding and the interval setting are described in Section 2. In Section 3, the proposed method is presented in details. The experiments and results analysis are shown in Section 4. The conclusion is in Section 5.

2. Related Work

2.1. Variable Low Bit Coding. Variable low bit coding is an improved LSB method, which can increase the capacity. The middle range of data represents the silence. Supposing that the audio file is sampled every 16 bits, the range of audio data is -32768~32767. When the audio data is zero, the sound is silent. Suppose that the audio file is sampled every 8 bits; the range of audio data is from 0 to 255. The middle range of data is 128 and the sound is silent in that range. Because embedding data into the silent sound will reveal the secret data, the data cannot be embedded in the middle range. By calculating the standard level, two thresholds t_1 and t_2 are set. If the amplitude value is smaller than t_1 , the secret data will not be embedded; if it is between t_1 and t_2 , then one bit is used for data embedding; if it is bigger than t_2 , then two bits are used for data embedding.

2.2. The Interval Setting. Parameter R is set as the interval for embedding secret message into the audio file, which means

FIGURE 1: Embedding the secret message with different values of R . (a) $R = 0$; (b) $R = 1$; (c) $R = 2$.

FIGURE 2: The framework of the proposed method.

that $R+1$ bits of secret message are embedded into the sample while the interval is R .

Figure 1 shows embedding of the secret message with different values of R . Suppose that the audio file is sampled every 8 bits. Figure 1(a) shows that when $R = 0$, the traditional LSB method is used. The bits of the secret message are embedded into the LSB of each sample. It is obvious that 1 byte message can be embedded into 8 bytes of audio signal. Figure 1(b) illustrates that when $R = 1$, 2 bits of secret message can be embedded into the current sample while the interval is one sample. In this case, 1 byte of secret message is embedded into 7 bytes of the audio file. Figure 1(c) illustrates that the method can embed 3 bits of the secret message into the current sample while the intervals are two samples, when $R = 2$. Thus 3 bytes of the secret message can be embedded into 22 bytes of the audio data.

3. The Proposed Method

In this section, a new audio steganography method is described in details. The proposed method can adaptively select the embedding location and embedding bits through setting the interval and variable low bit coding. In this method, wav files are used as the audio files, because the wav file format is a subset of Microsoft's RIFF specification for the storage of multimedia files, which are widely used in Windows Operating System. A wav file includes two parts, the header of the audio file and the audio data. The first 44 bytes of the audio file are the header and the rest are the data. Because the header is constant, the secret data should be embedded into the audio data, not into the header. The framework of the proposed method is shown in Figure 2.

FIGURE 3: Flowchart of the embedding procedure.

3.1. Improved Variable Low Bit Coding. The LSB method is to embed secret data only in the LSB. The variable low bit coding method improves the lowest bit coding and can increase embedding capacity. In this paper, the variable low bit coding is improved by combining the embedding interval, which means that not every audio sample data is used for embedding the secret information. The 8 bits mono wav files are selected as the carriers, whose sampling frequency is 11.025 kHz. Two thresholds T_1 and T_2 are set. If the absolute value of the difference between 128 and the audio data is less than T_1 , then one bit of LSB is used for data embedding; if it is between T_1 and T_2 , then two bits are used for data embedding; if it is more than T_2 , then three bits are used for data embedding.

3.2. The Embedding Procedure. Parameter R is set as the interval for embedding the secret message into the audio file, which is shown in Figure 1. According to the improved variable low bit coding method, T_1 and T_2 are the thresholds, which can select the embedding bits of a sample. Therefore, combining the interval R with the thresholds, the proposed method can adaptively select the embedding location and the embedding bits. The embedding procedure is shown in Figure 3.

The detail steps are presented as follows:

Input: It is a cover audio file C and a secret message S .

Output: It is a stego cover audio file C' .

Step 1: Read a cover audio file C in binary form.

Step 2: The converted binary audio file is sampled every 8 bits. Put it into an array A .

Step 3: Input the secret message S to be embedded.

Step 4: Encrypt S with AES algorithm to B , and then put B into an array D in the form of binary sequence.

Step 5: Calculate the length of B as L .

Step 6: Set the thresholds T_1 and T_2 according to the middle range of the audio data.

Step 7: Put the absolute value of the difference between the audio data and 128 into an array Z .

For $i = 45: L + 45 - 1$

$Z(i-44) = \text{abs}(A(i)-128);$

//Compare the relationship between $Z(i-44)$ and the thresholds T_1, T_2 .

If $Z(i-44) < T_1$, **then** set $R = 0$ and the LSB of $A(i)$ are replaced by the being embedded messages. Put i into a key array K_1 ;

Else if $Z(i-44) \geq T_1 \ \&\& \ Z(i-44) \leq T_2$, **then** set $R = 1$ and the 2 LSB of $A(i)$ are replaced by the being embedded messages. Put i into a key array K_2 , $i = i + 1$;

Else set $R = 2$ and the 3 LSB of $A(i)$ are replaced by the being embedded messages. Put i into a key array K_3 , $i = i + 2$.

End.

Step 8: The modified audio samples are formed into the stego audio signal C' , and then send C' , K_1 , K_2 , and K_3 as the hiding key to the receiver.

FIGURE 4: Flowchart of the extracting procedure.

3.3. The Extracting Procedure. The extracting procedure is an inverse process of the embedding procedure and is shown in Figure 4.

The detail steps are described as follows:

Input: It is the stego cover audio file C' .

Output: It is the secret message.

Step 1: Read the stego audio file C' in binary form.

Step 2: The converted binary audio file is sampled every 8 bits and is put into an array A' .

Step 3: Extract the secret message according to the hiding key arrays K_1 , K_2 , and K_3 , and the secret message is put into an array D' .

Calculate the length of K_1 , K_2 , and K_3 as L_1 , L_2 , and L_3 ,

For $i = 1 : L_1$

$D'[K_1(i)-44] = \text{bitget}(A'(K_1(i)), 1);$

End

For $i = 1 : L_2$

$D'[K_2(i)-44] = \text{bitget}(A'(K_2(i)), 2);$

$D'[K_2(i)-43] = \text{bitget}(A'(K_2(i)), 1);$

End

For $i = 1 : L_3$

$D'[K_3(i)-44] = \text{bitget}(A'(K_3(i)), 3);$

$D'[K_3(i)-43] = \text{bitget}(A'(K_3(i)), 2);$

$D'[K_3(i)-42] = \text{bitget}(A'(K_3(i)), 1);$

End

Step 4: Decrypt the L bits of D' to obtain the corresponding secret information S' .

4. Experiments and Results Analysis

For implementing the program, the programming techniques based on socket and multithread are used, Microsoft Visual C++ 2013 is used to compile and assemble, and Windows 7 is the operating platform.

The program is composed of two parts, the ordinary wireless communication and the application of steganography. The sending node and the receiving node can transmit the audio data to embed and extract the secret information. For simplicity, both the sending node and the receiving node are implemented in one program. The communicating parties just need to install the program to their PC and enter the host's IP, and then they can communicate with each other by hiding information. Because the wav format is widely used, we use the wav-audio files as the steganography carriers. We collected 50 wav files with mono from the WSNs. The sampling rate is 11.025 KHz with 8 bits per sample. The size of the audio files varies from 39KB to 652KB.

4.1. An Example. The following is an example to illustrate the embedding and extracting procedures. Suppose that the encrypted message to be embedded is "10011011"; the cover audio file is put into the array A after sampling and quantization. The cover audio data is shown in Table 1.

Setting $T_1 = 30$, $T_2 = 40$, according to the embedding method, if $|A(45)-128| < T_1$, $R = 0$, then LSB of $A(45)$ are replaced by "1"; putting "45" into the array K_1 ; if $|A(46)-128| > T_2$, $R = 2$, then 3 LSB of $A(46)$ are replaced by "001"; putting "46" to the array K_3 ; if $T_1 < |A(49)-128| < T_2$, $R = 1$, then 2 LSB of $A(49)$ are replaced by "10"; putting "49" into the array K_2 ; if $T_1 < |A(51)-128| < T_2$, $R = 1$, then 2 LSB

TABLE 1: The cover audio data.

i	$A(i)$
.....	
45	123
46	235
47	228
48	155
49	89
50	120
51	165
.....	

TABLE 2: The stego audio data.

i	$A'(i)$
.....	
45	123
46	233
47	228
48	155
49	90
50	120
51	167
.....	

of $A(51)$ are replaced by “11”; putting “51” into the array K_2 . The stego audio data A' is shown in Table 2.

When the receiver obtains the stego audio file and the hiding key, he can extract the secret message. The extracted secret bits are put into the array D' .

According to the array K_1 , the receiver can obtain $D'(45-44) = D'(1) = \text{bitget}(123, 1) = 1$.

According to the array K_2 , the receiver can obtain the following:

$$\begin{aligned}
 D'(49-44) &= D'(5) = \text{bitget}(90, 2) = 1, \\
 D'(49-43) &= D'(6) = \text{bitget}(90, 1) = 0, \\
 D'(51-44) &= D'(7) = \text{bitget}(167, 2) = 1, \\
 D'(51-43) &= D'(8) = \text{bitget}(167, 1) = 1.
 \end{aligned} \tag{1}$$

According to the array K_3 , the receiver can obtain the following:

$$\begin{aligned}
 D'(46-44) &= D'(2) = \text{bitget}(233, 3) = 0, \\
 D'(46-43) &= D'(3) = \text{bitget}(233, 2) = 0, \\
 D'(46-42) &= D'(4) = \text{bitget}(233, 1) = 1.
 \end{aligned} \tag{2}$$

Finally, the receiver can obtain the message “10011011” and then decrypt it to obtain the secret message.

4.2. Selecting the Thresholds. According to the embedding procedure, two thresholds T_1 and T_2 are set based on the

FIGURE 5: $T_1 = 10, 20, 30$, the value of SNR under different T_2 .

middle range 128 to select the embedding bits. If the absolute value of the difference between the audio data and 128 is lower than T_1 , one bit is embedded; if it is between T_1 and T_2 , two bits are embedded; if it is more than T_2 , three bits are used for embedding. Therefore, the thresholds T_1 and T_2 will influence the embedding capacity and the quality of stego audio. T_1 should not be too big. If T_1 is very big, the method may become the traditional LSB method. In the experiments, the embedding rate is set to 0.1bps. When $T_1 = 10, 20$, and 30 , compare the value of signal-to-noise ratio (SNR) under different T_2 , which is shown in Figure 5. As we can see in Figure 5, when $T_1 = 10$, the value of SNR grows slowly after $T_2 = 40$; when $T_1 = 20$, the growth of the value of SNR is slower after $T_2 = 40$, and when $T_1 = 30$, the value of SNR grows very slowly. Therefore, in the simulation experiment, we set $T_1 = 30$ and $T_2 = 40$.

4.3. The Embedding Rate. The embedding rate means that the number of the secret information can be embedded in a byte of cover audio data. For instance, in the LSB method, 1 byte of secret message should be embedded in 8 bytes of carrier data; thus the embedding rate is 12.5%. In the proposed method, the embedding location and embedding bits are selected adaptively, and thus the embedding rate is variable. When $R = 0$, it is 12.5%; when $R = 1$, it is 14.3%; when $R = 2$, it is 13.6%. Therefore, the average embedding rate is 13.5%. In Table 3, the embedding rate of the proposed method has been compared with the other LSB methods.

4.4. The Embedding Capacity. The proposed method is an adaptive embedding algorithm and the embedding capacity is related to the thresholds T_1 and T_2 , the size of wav-audio file, the sampling rate, and the quantization value. Because audio data is one of the most important covers in wireless communication, there is a large amount of audio data. Thereby the embedding capacity is considerable.

TABLE 3: Comparison of the embedding rate.

Method	Embedding Rate
Lowest Bit Coding [19]	12.5%
Variable Low Bit Coding [20]	12.7%
XOR of LSB [21]	12.5%
Sample Selection [22]	2.78%
Bit Selection [22]	12.5%
Based on the Interval R [23]	$R = 1$
	$R = 2$
	$R = 3$
Fibonacci [24]	4.17%
the Proposed Method	13.5%

TABLE 4: The average value of SNR, MSE, and BER at different embedding rates.

Evaluating Indicator	Embedding Rate (bps)							
	0.005	0.01	0.05	0.1	0.2	0.3	0.4	0.5
SNR	67.873	64.698	57.318	54.203	51.338	49.609	48.427	47.483
MSE	0.0025	0.0051	0.0253	0.0492	0.0984	0.1481	0.1967	0.2459
BER	0.0024	0.0049	0.0248	0.0487	0.0979	0.1473	0.1955	0.2447

In variable low bit coding methods, the thresholds determine the embedding capacity. If most of the audio data are around 128, the embedding capacity will be very low, while in the proposed method, even though most of the audio data are around 128, the embedding capacity is higher than the LSB methods.

4.5. Imperceptibility Analysis. SNR, mean square error (MSE), bit error rate (BER), and the waveform are widely used to evaluate the imperceptibility of the audio steganography methods. Suppose x is the original audio, y is the stego audio, and N is the sampling point number of x and y .

SNR is calculated by (3). Higher SNR means better invisibility of the algorithm.

$$SNR = 10 \log_{10} \frac{\sum_{i=1}^N x(i)^2}{\sum_{i=1}^N [x(i) - y(i)]^2} \quad (3)$$

MSE is defined as the mean square error between the cover audio and the stego audio. MSE can measure the distortion in the audio and it is calculated by (4). Lower MSE means better performance of the algorithm.

$$MSE = \frac{1}{N} \sum_{i=1}^N [x(i) - y(i)]^2 \quad (4)$$

BER describes the ratio of the modified bit number of the stego audio and the bit number of the original audio. Lower BER means better imperceptibility of the algorithm. BER is calculated by

$$BER = \frac{1}{N} \sum_{i=1}^N \begin{cases} 1, & y(i) \neq x(i) \\ 0, & y(i) = x(i) \end{cases} \quad (5)$$

Table 4 shows the average value of SNR, MSE, and BER at different embedding rates. The results indicate that, at different embedding rates, SNR is kept at a high value but MSE and BER are kept at a low value. And in Figure 6, the proposed method has been compared with the LSB method [19], Variable Low Bit Coding method [20], and bit selection method [22] in SNR, MSE, and BER. In Figure 6(a), the SNR value of the proposed method is lower than [19] and higher than [20, 22]. This means that the invisibility of the proposed method is lower than [19] and better than [20, 22]. In Figure 6(b), the MSE value of the proposed method is the same as [19] and lower than [20, 22]. This means that the proposed method has better performance than [20, 22] and the same performance with [19]. In Figure 6(c), the BER value of the four methods is the same and this means that they have the same imperceptibility. In a word, the results demonstrate that the proposed method has good imperceptibility.

Figure 7 shows the waveforms of the original audio and the stego audio when the embedding rate is 0.1 bps. Obviously, the difference between the original audio and the stego audio is very tiny, which also means that the imperceptibility of the proposed method is satisfying.

5. Conclusion

An adaptive audio steganography method for wireless communication has been presented based on interval and the variable low bit coding in this paper. The interval R for embedding secret message into audio file and the thresholds T_1 and T_2 in variable low bit coding are used for selecting the embedding location and the embedding bits adaptively. The embedding capacity and the embedding rate are variable. The proposed method is simple and fast, which can

FIGURE 6: The comparison of SNR, MSE, and BER under different embedding rates between the proposed method and the other methods.

meet the instantaneity of wireless communication. In the future, we should investigate another low bit-rate speech codec applicable to wireless communication and design new steganographic algorithms.

Data Availability

The [software code and data] data used to support the findings of this study are available from the corresponding author upon request. Correspondence should be addressed to Yuling Liu: yuling_liu@126.com.

Conflicts of Interest

The four authors, Guojiang Xin, Yuling Liu, Ting Yang, and Yu Cao, all declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant no. 61103215 and Hunan Provincial Natural Science Foundation of China under Grant no. 2018JJ2062.

FIGURE 7: The waveforms of the original audio and the stego audio when the embedding rate is 0.1 bps.

References

- [1] Z. Pan, J. Lei, Y. Zhang, and F. L. Wang, "Adaptive fractional-Pixel motion estimation skipped algorithm for efficient HEVC motion estimation," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 14, no. 1, pp. 1–19, 2018.
- [2] J. Han, D. Zhang, G. Cheng, N. Liu, and D. Xu, "Advanced Deep-Learning Techniques for Salient and Category-Specific Object Detection: A Survey," *IEEE Signal Processing Magazine*, vol. 35, no. 1, pp. 84–100, 2018.
- [3] J. Han, R. Quan, D. Zhang, and F. Nie, "Robust object co-segmentation using background prior," *IEEE Transactions on Image Processing*, vol. 27, no. 4, pp. 1639–1651, 2018.
- [4] F. Peng, X.-Q. Gong, M. Long, and X.-M. Sun, "A selective encryption scheme for protecting H.264/AVC video in multimedia social network," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 1–19, 2016.
- [5] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 32–44, 2003.
- [6] X. R. Xiao, X. M. Sun, L. C. Yang et al., "Secure data transmission of wireless sensor network based on information hiding," in *Proceedings of Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, pp. 1–6, 2007.
- [7] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 26–31, 2015.
- [8] Y. L. Liu, H. Peng, and J. Wang, "Verifiable diversity ranking search over encrypted outsourced data," *CMC: Computers, Materials & Continua*, vol. 55, no. 1, pp. 37–57, 2018.
- [9] Y. Cao, Z. Zhou, X. Sun, and C. Gao, "Coverless information hiding based on the molecular structure images of material," *Computers, Materials and Continua*, vol. 54, no. 2, pp. 197–207, 2018.
- [10] J. Ye, J. Ni, and Y. Yi, "Deep Learning Hierarchical Representations for Image Steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2545–2557, 2017.
- [11] R. H. Meng, S. G. Rice, J. Wang et al., "A fusion steganographic algorithm based on faster R-CNN," *CMC: Computers, Materials & Continua*, vol. 55, no. 1, pp. 1–16, 2018.
- [12] J. J. Wang, M. O. Qian, D. X. Mei et al., "A robust audio watermarking algorithm based on LSB," *Journal of Guangxi University*, 2013.
- [13] F. Djebbar, B. Ayad, H. Hamam, and K. Abed-Meraim, "A view on latest audio steganography techniques," in *Proceedings of the 7th International Conference on Innovations in Information Technology (IIT)*, pp. 409–414, Abu Dhabi, United Arab Emirates, April 2011.
- [14] V. Bhat K, I. Sengupta, and A. Das, "An adaptive audio watermarking based on the singular value decomposition in the wavelet domain," *Digital Signal Processing*, vol. 20, no. 6, pp. 1547–1558, 2010.
- [15] H. Morsy, J. Gluckman, A. Hussein, and F. Amer, "Block based steganography," in *Proceedings of the 9th European Conference on Information Warfare and Security 2010, ECIW 2010*, pp. 218–228, Greece, July 2010.
- [16] Y. Diqun, W. Rangding, and Z. Liguang, "Quantization step parity-based steganography for MP3 audio," *Fundamenta Informaticae*, vol. 97, no. 1-2, pp. 1–14, 2009.
- [17] P. Dutta, D. Bhattacharyya, and T. Kim, "Data hiding in audio signal: a review," *International Journal of Database Theory and Application*, vol. 2, no. 3, pp. 1–8, 2009.
- [18] K. Geetha and P. V. Muthu, "Implementation of ETAS (embedding text in audio signal) model to ensure secrecy," *International Journal on Computer Science and Engineering*, vol. 2, no. 4, pp. 1308–1313, 2010.
- [19] M. Wakiyama, Y. Hidaka, and K. Nozaki, "An audio steganography by a low-bit coding method with wave files," in *Proceedings of the 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2010*, pp. 530–533, Germany, October 2010.
- [20] P. P. Balgurgi and S. K. Jagtap, "Audio Steganography Used for Secure Data Transmission," in *Proceedings of International Conference on Advances in Computing*, vol. 174 of *Advances in Intelligent Systems and Computing*, pp. 699–706, Springer India, New Delhi, 2012.
- [21] P. P. Balgurgi and S. K. Jagtap, "Intelligent processing: an approach of audio steganography," in *Proceedings of the International Conference on Communication, Information & Computing Technology*, pp. 1–6, 2012.
- [22] M. Asad, J. Gilani, and A. Khalid, "An enhanced least significant bit modification technique for audio steganography," in *Proceedings of the 1st International Conference on Computer Networks and Information Technology (ICCNIT '11)*, pp. 143–147, IEEE, Pakistan, July 2011.
- [23] S. Tang, Y. Jiang, L. Zhang, and Z. Zhou, "Audio steganography with AES for real-time covert voice over internet protocol communications," *Science China Information Sciences*, vol. 57, no. 3, pp. 1–14, 2014.
- [24] H. Kumar and Anuradha, "Enhanced LSB technique for audio steganography," in *Proceedings of the 2012 3rd International Conference on Computing, Communication and Networking Technologies, ICCCNT 2012*, pp. 1–4, India, July 2012.
- [25] J. Vimal and A. M. Alex, "Audio steganography using dual randomness LSB method," in *Proceedings of the 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies, ICCICCT 2014*, pp. 941–944, India, July 2014.

- [26] R. Tanwar, B. Sharma, and S. Malhotra, "A robust substitution technique to implement audio steganography," in *Proceedings of the 2014 International Conference on Reliability, Optimization and Information Technology, ICROIT 2014*, pp. 290–293, India, February 2014.
- [27] P. Pathak, A. K. Chattopadhyay, and A. Nag, "A new audio steganography scheme based on location selection with enhanced security," in *Proceedings of the 2014 1st International Conference on Automation, Control, Energy and Systems, ACES 2014*, India, February 2014.
- [28] M. Zou and Z. Li, "A wav-audio steganography algorithm based on amplitude modifying," in *Proceedings of the 10th International Conference on Computational Intelligence and Security, CIS 2014*, pp. 489–493, China, November 2014.
- [29] L. Y. Xiang, Y. Li, W. Hao et al., "Reversible natural language watermarking using synonym substitution and arithmetic coding," *CMC: Computers, Materials & Continua*, vol. 55, no. 3, pp. 541–559, 2018.
- [30] S. Tang, Q. Chen, W. Zhang, and Y. Huang, "Universal steganography model for low bit-rate speech codec," *Security and Communication Networks*, vol. 9, no. 8, pp. 747–754, 2016.