AUT Journal of Mathematics and Computing

AUT J. Math. Comput., 3(1) (2022) 113-127
DOI: 10.22060/AJMC.2022.20710.1073

A new approach to solve the reliability problem in any VoIP steganography system

Mohammad-Reza Rafsanjani Sadeghi*[a], Parvane Amirzade Dana[a], Bahram Javadi[a]

[a]*Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran*

ABSTRACT: VoIP is naturally an unreliable communication system. Thus, using the best VoIP steganographic systems, the accuracy of the hidden message is impaired as a result of the VoIP packet loss. There are many steganography and steganalysis researches that try to improve the robustness and accuracy of VoIP steganography methods. In addition to the fact that these works are done depend on a particular method, none of them have solved the problem of packet loss. Applying error correcting codes, prior to embedding, is a well-known technique in telecommunication to improve robustness and to reconstruct Missing data. However, in the case of VoIP communication, a codeword entirely embedded in the packet may be lost due to the packet loss and therefore ECC techniques will not be capable of reconstructing the lost bits. In this paper, we design a novel scheme to increase the reliability of VoIP steganography systems. We emphasize that our proposed method, independent of the embedding and extracting algorithm, can be used in all VoIP steganography systems. After encoding the secret message to the codewords of n bits, we distribute these n bits into n successive RTP packets, in such a way that, losing one packet leads to miss only one bit of each codeword. Then, with the idea of telecommunication solutions in recovering lost data, when up to t of n packets are lost we can recover the secret message using a t-error correcting code $\mathbf{C}(n, k, d)$. Provided that the average of packet loss over the network is less than 1%, using a t-error correcting code $\mathbf{C}(n, k, d)$, the probability of losing hidden data, in each category of n-packets, P_e, is less than $\leq 10^{-2t}$. Hence, applying the t-error correcting codes with larger t, in the proposed scheme, results in more reliable steganographic systems.

Review History:
Received:26 October 2021
Accepted:29 January 2022
Available Online:01 February 2022

Keywords:
Steganography
VoIP
Reliability
Error correcting codes

1. Introduction

Steganography is the science of concealing secret information in apparently innocent media [1]. The media that carries the secret message is called stego-cover. In general, the main purpose of steganography is to establish a hidden connection in the context of normal communication [2], [3]. As communication methods have evolved over the years, steganographic carriers have changed. Recently, the proliferation of the Internet, together with the widespread use of digital media on the network platform have sparked an interest in steganography [4], [5].

The first use of digital media as a cover is suggested by Bender et al. [6]. Most digital steganographic methods use least significant bits (LSB) to hide data [7, 8, 9]. Nowadays, IP telephony or voice over IP (VoIP) is one of the most important services of IP-based networks. VoIP is a set of technologies that delivers voice communication over the Internet protocol [10]. Due to the fact that too much information is transmitted over a VoIP service, an opportunity is created to use this service for steganography [11, 12, 13, 14, 15]. The purpose of steganography is to convey a hidden message without any suspicion or ability to reveal. If existence of the hidden message is revealed, then this goal is defeated. Steganalysis is a new art of detecting such messages [16]. Statistical analysis is one of

*Corresponding author.
E-mail addresses: msadeghi@aut.ac.ir, pamirzade@gmail.com, bahramjavadi207@aut.ac.ir

the methods to identify and to detect a secret message from stego-cover [17], [18]. Since VoIP is a real-time service, steganalysis of VoIP data is hard to accomplish due to the ephemerality of the carrier [19], [20].

Applying the well-established digital media steganography will give rise to methods that target the digital representation of the transmitted voice over IP. In a VoIP environment, a transport protocol, called *user datagram protocol* (UDP), is used to transmit voice data which is intrinsically unreliable. Therefore, using the best embedding algorithms in VoIP steganographic systems, the integrity of the secret message is undermined due to the packets being lost during the transmission.

Applying error correcting codes, prior to the embedding, is a well-known technique in communication to improve robustness and to reconstruct lost bits caused by error or loss. However, in the case of VoIP communication, a codeword entirely embedded in the packet can be lost due to the packet loss and thus ECC technique will not be capable of reconstructing the lost bits. ECC has been commonly used in steganography and watermarking applications for many years [16], [21, 22, 23]. In this paper, we also use ECC as some tools, however, our aim is not to propose a VoIP steganographic method based on ECC, instead, our main contribution is to design a novel algorithm to improve the reliability of any steganographic methods which is summarized as follows. After encoding the secret message to the n-bit codewords, we distribute these n bits into the n successive RTP packets, in such a way that, losing one packet leads to miss only one bit of each codeword. Then with the idea of telecommunication methods in recovering lost data, using any t-error correcting code $\mathbf{C}(n, k, d)$, we can recover the secret message, when up to t of n packets are lost.

The rest of the paper is organized as follows. In section 2 we introduce VoIP steganography and error-correcting codes. Section 3 presents a detailed description of challenges of VoIP steganography and our motivation. Section 4 is devoted to describe our proposed method and section 5 contains our performance results. In Section 6 we summarize our results.

2. PRELIMINARIES

2.1. VoIP

VoIP is a real-time technology that enables an end-to-end voice conversation over IP-based networks. During a VoIP service, four protocols are commonly used, SIP (session initiation protocol), RTP (real-time transport protocol), UDP (user datagram protocol) and IP (Internet protocol).

Similar to the other data networks, the Internet allocates data into small pieces called packets. Each network protocol in order to organize its data packets defines some rules and semantics. Protocols generally divide each packet into two parts: header and payload. For example, an RTP packet is shown in Fig. 1.

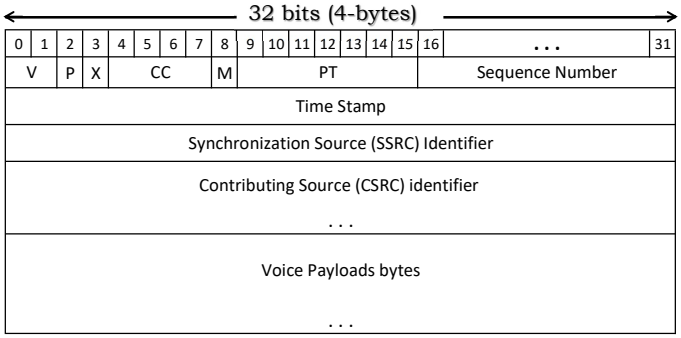

Figure 1: RTP packets format

In a VoIP service, the audio data is transmitted by the RTP payload domain and the rest of the communication features such as the receiver or sender's address, time, etc. are transmitted by the protocol's header.

In order to transmit signals with a large dynamic range over facilities with smaller dynamic range, *compounding* (**com**pressing and ex**panding**) methods are used. compounding, which is used in audio devices such as professional wireless microphones and analog recording, compresses data before it is entered in an analog-to-digital converter and expands it after exiting from a digital-to-analog converter. For example, G.711, G.723, G.729 are samples of speech codecs that allow us to compound a digitalized voice and to transmit it in IP networks. G.711, as a high-bit rate (64 Kbps) speech codec, is the most commonly voice codec for VoIP devices and G.723 is a low-bit rate (40 Kbps) speech codec.

2.2. VoIP Steganography

VoIP steganography involves methods that use VoIP capabilities to embed secret messages. Generally,VoIP steganographic methods are divided into two groups. The first class embeds a secret message in a voice payload which is transmitted by RTP payload domain. The second class targets the VoIP protocol's headers.

2.2.1. payload of RTP packets

The primary VoIP steganography systems have used least significant bits (LSB) of payload in RTP packets [24]. Also, Tian et al. proposed a scheme for embedding a secret message into RTP payloads [25]. They first compute the similarity between the secret message bits and the cover bits, then define a threshold for them. In [26], in order to provide higher steganographic bandwidth of 133.3 *bps*, the bits of secret message are embedded in LSB of LSP (linear spectrum pairs) quantization parameter.

In 2020, Anguraj [27] introduced a steganographic approach based on an optimized audio embedding technique (OAET). Obtained results showed that, compared with the previous LSB steganography methods, this scheme improved security and accuracy. But, this algorithm is not applicable to all voice formats, and therefore it needs further improvement.

2.2.2. Protocol header

These methods try to embed confidential data either in unused or optional fields of protocol headers or modulated inter-packet times. They used specific fields of VoIP protocols such as signaling protocol (SIP), transport protocol (RTP) and control protocol (RTCP) [28, 29, 30, 31]. They described methods for embedding a secret message in protocol headers. They suggested using optional and some possible fields of IP headers to embed a secret message. Some systems of this group try to embed the secret data by changing inter-packet time relation, the sequence order of packets or making intentional losses [32, 33, 34].

2.2.3. Hybrid

In [35] authors, modifying voice payload and time affiliations of RTP packets, proposed a hybrid steganography named lost audio packets steganography (LACK). The sender randomly selects some audio packets and then transmits them with a deliberate delay. A receiver unfamiliar with the hiding algorithm prevents the transmission of packets with excessive delay to the audio decoder. Finally, confidential information transmitted over the contents of the deliberately delayed packets to method-aware recipients. According to QoS necessities of a VoIP call, the packet lost ratio needs to be limited. For example, in G.711 codec a maximum of 3% packet loss is tolerated. whiles, loss tolerance for G.729 is 1%. Therefore, although any intentionally lost packet can contain a hidden message as much as its capacity, the total number of packets that can be deliberately lost is restricted.

There are many different ways for VoIP steganography. One of them changes speech codec that applies codec G.723, which has low-bit rate speech codes to keep similarity [36], [37]. Also, in [38] speech codec G.711 is used with high bandwidth to increase the capacity of steganography system.

2.3. Error Correcting Codes

Many communication channels are exposed to channel noise. Hence, errors may occur during the transmission. There are many different channels. Two important binary channels are as follows, binary symmetric channel (BSC) and binary erasure channel (BEC).

Error correction techniques make it possible to recover original data in many ways. Generally, the error correcting code (ECC) is used to control and correct data errors through unreliable or noisy communication channels. The first ECC was (7,4)-Hamming presented by Hamming in 1950 [39]. ECCs are classified into two fundamental categories: block codes and convolution codes. Here, our focus is on binary block codes. A binary block code is a code whose sequence of bits can be converted to n-bit blocks. These blocks are called codewords and n is the block length.

As mentioned in [40], the main parameters of a block code are *block length, message length, minimum distance, rate and error capability*. A block code is denoted by $\mathbf{C}(n, k, d)$, in which k represents the length of the message block, n indicates the length of the codeword, and d denotes the Hamming distance of the code. For every two codewords $\mathbf{X}$ and $\mathbf{Y}$, Hamming distance $d(\mathbf{X}, \mathbf{Y})$ is the number of elements in which they differ. Smallest Hamming distance between any two different codewords, which is equal to the minimum Hamming weight of the non-zero codewords, is called the Hamming distance or minimum distance of code. The rate of a block code, denoted by R, means the ratio between the message block length and the codeword length, $R = \frac{k}{n}$. A block code $\mathbf{C}$ with minimum distance d is capable to correct up to t errors, where $t = \lfloor \frac{d-1}{2} \rfloor$.

In the VoIP channel, we encounter with two facts, we receive a packet whose payload bits are certainly correct or, we have a packet loss. Therefore, our communication channel can be considered as a binary erasure channel (BEC). However, in communication systems binary symmetric channel (BSC) is mostly used and therefore most of decoding algorithms are proposed for this channel [40, 41, 42, 43, 44].

In order to compensate the noise e, caused by the packet loss, randomly considering 0 or 1 instead of e for each erased bit, we convert the BEC to BSC. Then, using decoding methods proposed for BSCs, we can obtain all missed bits through the packet loss.

3. Challenges of VoIP Steganography and Our Motivation

3.1. Challenges

The followings are some most essential challenges of designing steganographic schemes for VoIP.

3.1.1. Security

The security of a steganographic system is based on the fact that an unauthorized person is not able to detect cover-objects from stego-objects [16], [19]. Tang et al. [45], suggested using the AES encryption method for VoIP steganography. AES-based steganography increases security, because it is impossible to detect the presence of an encrypted message using simple statistical analysis. Moreover, in [37] authors presented a method that achieves a high speech quality while avoiding the detection.

There are some evaluation coefficients in steganography to evaluate the imperceptibility of the steganographic methods such as mean opinion score (MOS), peak signal-to-noise ratio (PSNR), bits per cluster of bits (BPCoB) and Spectrogram. Recently, using new techniques as, pulse distribution model (PDM) [46], matrix embedding (ME) [23] and multi-matrix embedding (MME) [47] has improved evaluation coefficients and thus provided more security for some steganographic algorithms.

3.1.2. Latency

Generally, due to the packet latency on VoIP, a call is very inclined to the media distortion. Therefore, if a steganographic algorithm adds overhead processing into the cover channel, it causes significant degradation in quality of service.

3.1.3. Reliability

Unlike an unreliable service, a reliable service is one that, in case of non-delivery, informs the user. UDP is an unreliable and connectionless protocol which, using low-overhead operation, reduces latency to meet the real time communication. In contrast, TCP is reliable but, time-consuming communication protocol.

since the RTP protocol implements the transmission of voice data via the UDP protocol, there is a possibility of packet loss. A packet loss has a slight effect on the sound quality but, if the lost packet contains a secret data, it will be difficult to extract the embedded data in receiver's side. Therefore, the reliability is the most essentially challenge in VoIP steganography. There are some ways to enhance the reliability in VoIP steganography, which will be discussed next.

Generally, wireless networks are exposed to factors that can enforce packets to be lost during transmission. Also network congestion is a cause of packet loss. VoIP is not tolerant of packet loss. Even 3% packet loss can significantly degrade a VoIP call using G.711. Whiles, in G.723.1 codec a maximum of 2% packet loss is tolerated, it is 1% for G.729.

Designing a steganography system, in such a way that its function is equivalent to the performance of a VoIP system without any incorporated steganographic algorithm, is necessary.

3.2. Related Work

Robustness is an important indicator for evaluating the capability of VoIP-based steganography algorithms. It demonstrates counter-attack capability of the steganography methods. Like many communication channels, there are many unintentional or intentional interferences during transmission over a VoIP channel. Due to the unreliability of VoIP system, packet loss is an unintentional interference that the carrier receives during transmission. In this scenario, a VoIP steganography system is robustness or reliable if it can extract the hidden data with a low error rate to ensure the integrity of the original message. Robustness is evaluated by some coefficients such as test error rate (TER), accurate detection rate(ADR) and non-parametric test (N-PT).

Many previous VoIP steganography methods, including [36, 37], do not address the problem of reliability. In [35], in order to solve this problem, it is assumed that the recipient requests that the missing messages be resent. However, in addition to reducing steganographic bandwidth, the recently posted message may be lost again. In [48] the authors, changing signal codec, controled packet loss. They applied G.711 speech codec and transmitted pieces of desired data. Also, in [49], using the G.711 codec, the rate of packet loss was reduced. Zhang et al. [50] used a model, called one packet loss prediction model, which decided if an RTP packet would be removed for embedding

and used Gilbert packet loss model for extracting. The first empirical implementation of renowned LACK scheme was presented in [51]. This experiment was performed in a LAN network that no RTP packet would be lost or overly delayed but, these assumptions are very different from the reality of the VoIP channel. In order to increase the reliability of this method, ReLACK was proposed in [52]. ReLACK modifies (n, k) secret sharing scheme based on Lagrange interpolation. In the following we summarize some deficiencies with this scheme. The receiver calculates the parameter k as the distance between the first two delayed packets. However, due to the unreliability of the VoIP channel, a false value of k may be used to identify the hidden message.

Recently, researchers have tried to improve robustness by applying new methods to a variety of VoIP steganography systems based on voice payload or protocol [27, 46, 54, 55, 56, 57, 58, 59]. In the following, we have described the details of some these methods and summarized them in the Table 1.

Quantization index modulation (QIM) is a common steganographic method that uses redundancy in the signal encoding procedure. Tian et al. [54], presented a codebook segmentation method based on QIM, neighbor-index-division steganography (NID). They divided neighbor-indexed codewords into distinct partitions combined with a suitable stego coding method.

Adaptive multi-rate (AMR), is a widely used audio compression standard and has become a modern carrier for steganography. In order to provide a reliable steganographic system, Ren et al. [46], proposed a steganographic scheme in the AMR fixed codebook (FCB) domain based on the characteristics of pulse distribution. Since the embedding rule is obtained from the principle of the smallest change in the pulse distribution characteristics of the FCB values in the cover audio, the statistical distribution of the pulse positions in stego audio is close to that of the cover audio. This steganography method enhances the statistical security but, the steganographic capacity is maintained compared with the existing schemes.

Aiming to improve security and imperceptibility of the LSB steganography methods based on the optimized audio embedding technique (OAET), Anguraj et al. [27] used a new elevated bit range least significant bit (LSB) audio steganography technique and adopted optimized audio embedding technique from the technological observation. This cladding of the OAET provides high-level security to the universal cyber data but, it can not be applied to all formats of voice.

Yang [56], finding the fact that the pitch delay of the voiceless section of AMR speech has no short period relative stability and large redundancy, proposed an adaptive steganography algorithm based on the unvoiced pitch delay jitter characteristics. The results showed that this steganographic system is resistant to statistical attacks.

Also, to improve the performance of steganographic system, Liu et al. [57], designed a different steganography plan based on the pitch delay characteristics. The novelty of their idea was that they used the decimal pitch delay parameter instead of the integer pitch delay parameter as steganography cover.

Jiang et al. [58], in 2016, to realize a VoIP steganographic system in the presence of packet loss, proposed a fractal-based VoIP steganographic approach. By simulating a real network situation based on Gilbert model they determined the suitable VoIP packets for data embedding, based on the fractal interpolation. The average variance of speech quality metrics, as the average PESQ scores and the SNR values, indicated the importance of the success rate of the fractal prediction model in the performance of VoIP steganographic systems.

In [59] a hash-based steganography algorithm was proposed. In this scheme, the appropriate bit position for embedding the secret data in each frame is determined by constructing a hash array from the frame data. actually, in this approach, embedding and extracting the hidden massage are done based on the hash array. Although, the proposed method provided a good performance in terms of the computational complexity, undetectability, and voice quality but, the hash array took up extra bandwidth in the process of VoIP communication.

Table 1: VoIP Steganography Method Based on Voice Payload or Protocol.

Work	Technique	Steganography method	Cover
54	Codebook segmentation method based on Neighbor Segmentation(NID)	Fixed codebook (FCB)	Voice payload
46	Pulse distribution model (PDM)	Fixed codebook (FCB)	Voice payload
55	Cepstrum distortion cost function and Syndrome Trellis Codes(CD-STC)	Linear prediction coefficients (LPC)	Voice payload
27	Optimized audio embedding technique(OAET)	Linear prediction coefficients (LPC)	Voice payload
56	Pitch delay adaptive steganography (PDAS)	Adaptive codebook (ACB)	Voice payload
57	Adaptive partial matching steganography based on fractional pitch delay search(FPD-APMS)	Adaptive codebook (ACB)	Voice payload
58	Gilbert model and fractal interpolation model(GM and FIM)	Internet Layer	Protocol
59	Hash	Transport Layer	Protocol

Since, in all these tasks, the secret data is embedded in the payload or protocol headers of voice packets, the hidden data is lost as soon as some packets are lost. Thus, although these methods provide more robustness to some attacks, they are not able to solve the problem of reliability. Furthermore, each of these tasks is designed based on a specific VoIP steganographic system and cannot be generalized to all systems.

In [53] the authors have proposed a scheme which enhances the reliability of any VoIP steganographic method. They distributed k message bits into k consecutive RTP packets and use parity-check bits to rebuild lost bits due to the packet loss. Although this method reduces the probability of error by up to 10 times but, it can compensate for only one lost packet in each k consecutive RTP packets and if in one block of k RTP packets more than one packet are lost, the problem of packet loss recovery remains unresolved.

3.3. Our Motivation

In this paper, we propose a scheme which, independent of the speech codec and the embedding algorithm, enhances the reliability of every VoIP steganography system. An obvious method to recover lost bits in communication channels is to use Error correcting codes. But, due to the packet loss, the codewords embedded in a packet may be entirely lost. Hence, this solution is not applicable to the VoIP communication channels. To overcome this problem, we propose a new algorithm. In this scheme, a secret message is first encoded to the codewords of n bits and then these n bits are distributed into the n successive RTP packets, in such a way that, losing one packet leads to miss only one bit of each codeword. Then, using a t-error correcting code $\mathbf{C}(n, k, d)$, we can recover the secret message when up to t of n packets are lost.

4. PROPOSED SCHEME

Consider an arbitrary VoIP steganography system that targets the digital representation of the transmitted voice over IP with steganographic capacity of m bits per packet. Our main goal is to provide a scheme that can increase the reliability of this proposed steganographic system. In each iteration of the proposed algorithm, m blocks of length n of the secret message are embedded in n RTP packets. In order to extract the secret message, the receiver needs to know which packets are lost in the same iteration. To address this goal, it is necessary to allocate $q = \lceil \log_2 n \rceil$ bits of m bits for packet numbering.

Let $\mathbf{M} = m_1, m_2, \ldots, m_s$ be the secret message. Our proposed algorithm is illustrated as follows:
Embedding Algorithm:

- **step1** : Divide the message $\mathbf{M}$ into blocks of length k. If necessary, add some zero bits to the end of the last block to make it of length k. As a result, we will have z blocks of length k, $\mathbf{M_1}, \mathbf{M_2}, ..., \mathbf{M_z}$ (see Fig.3).
- **step2** : Encode each message block, by using code $\mathbf{C}(n, k, d)$, to codewords $\mathbf{C_1}, \mathbf{C_2}, \ldots, \mathbf{C_z}$ of length n (see Fig.3).
- **step3** : Divide codewords $\mathbf{C_1}, \mathbf{C_2}, \ldots, \mathbf{C_z}$ into categories of length $m - q$.
- **step4** : For the sake of packet numbering, create codewords $\mathbf{N_i}$, $1 \leq i \leq q = \lceil \log_2 n \rceil$, as follows. For every $1 \leq i \leq q$, suppose that $\mathbf{N'_i}$ is a vector of length 2^q consisting of a pattern of 2^{q-i} zeros followed by 2^{q-i} ones. Put $\mathbf{N_i}$ as the first n components of $\mathbf{N'_i}$. (this is illustrated for $q = 3$, $n = 5$ in Fig.2).
- **step5** : Append blocks $\mathbf{N}_i$, $1 \leq i \leq q$, in the first position of each category and make categories of m vectors.

  Note that steps 1 to 5 are performed before the VoIP communication starts. In each embedding iteration a category of m blocks and n RTP packets are buffered as input.

- **step6** : For $i = 1, 2, ..., n$, the i-th bit of all vectors in a category is embedded in the i-th packet of n buffered RTP packets.

Now, assume that the embedding operation has been completely performed and the receiver get the packets including some packet loss.

According to the embedding algorithm, if less than t packets in each category are lost, this will result in a loss of less than t bits per codeword. Since our coding system is able to correct t errors in a codeword of length n, by losing up to t packets in each category this method will be able to recover the secret message.

$$N_1' = (0\,0\,0\,0\,1\,1\,1\,1) \longrightarrow N_1 = (0\,0\,0\,0\,1)$$

$$N_2' = (0\,0\,1\,1\,0\,0\,1\,1) \longrightarrow N_2 = (0\,0\,1\,1\,0)$$

$$N_3' = (0\,1\,0\,1\,0\,1\,0\,1) \longrightarrow N_3 = (0\,1\,0\,1\,0)$$

Figure 2: Create number codewords for $q = 3$, $n = 5$, $i = 1, 2, 3$

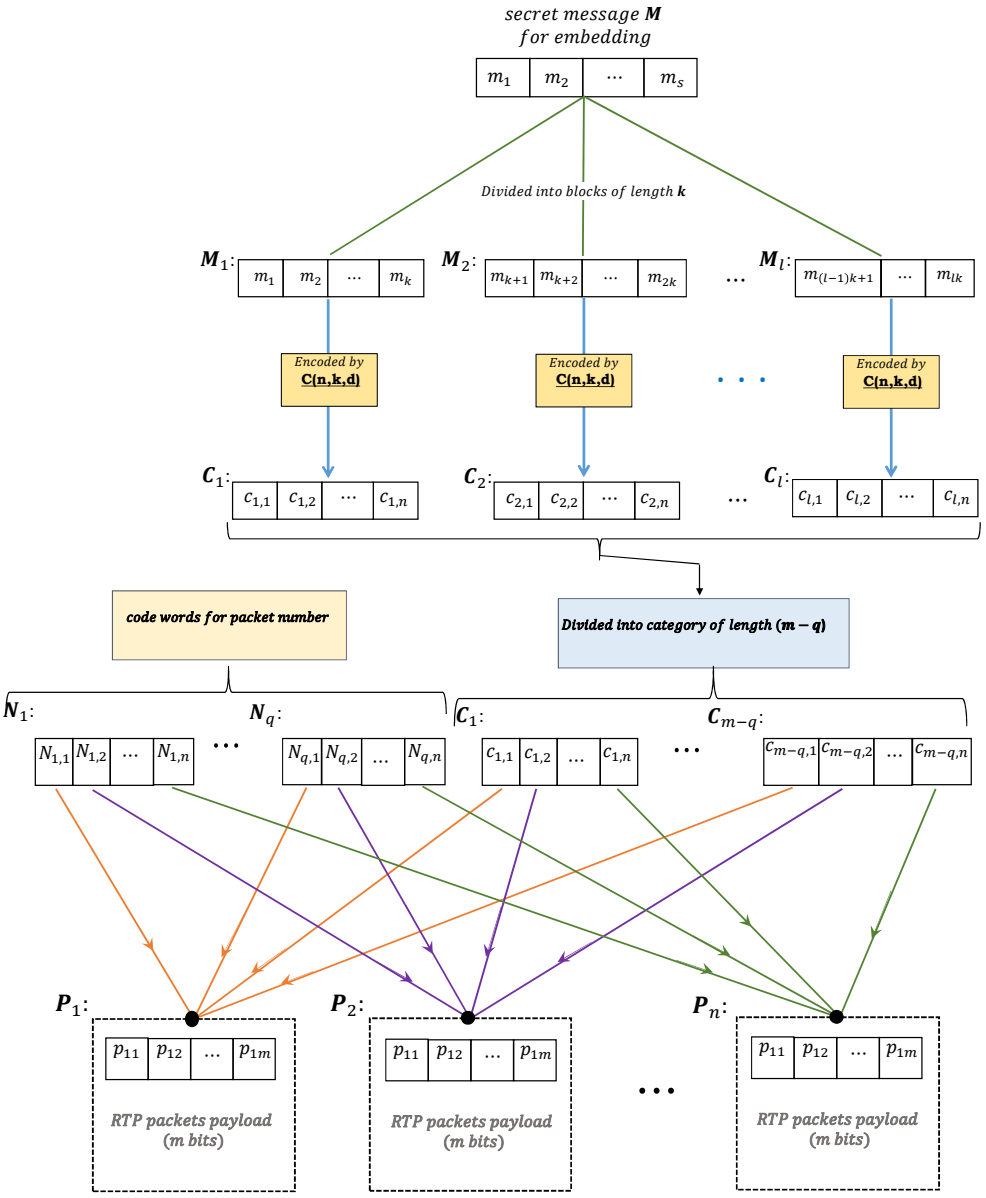

Figure 3: Proposed schema for embedding secret message

Extracting algorithm:

- **step1** : Using numbering vectors, lost packets can be recognized.

- **step2** : Create $(m-q)$ codewords of length n to obtain a category. According to the Fig.4, the i-th bit of the j-th codeword is $p_{j,q+i}$ (the $(q+i)$-th bit of j-th packet). Obviously, if a packet loss occurs (for example the i-th packet of one category is lost) then we miss the i-th bit of every codeword. In order to recover these codewords, we set random bits $0, 1$ in the positions of the missing bits.
- **step3** : Decode the received words $\mathbf{R_i} = \mathbf{C_i} + \mathbf{e_i}$, where e_i is error, to obtain message blocks.

According to the embedding and extracting algorithms, block code $\mathbf{C}(n, k, d)$ must be chosen in such a way that $q = \lceil \log_2 n \rceil \leq m$.

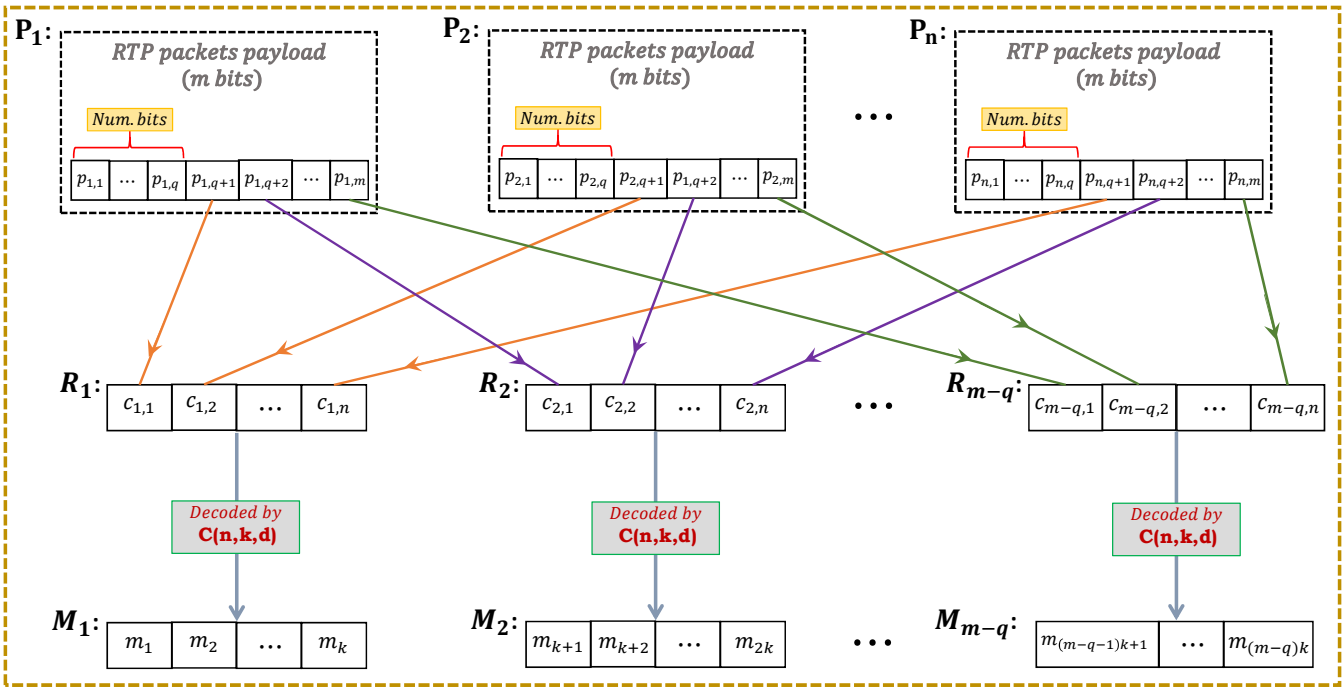

Figure 4: Proposed scheme for extract secret message

5. PERFORMANCE ANALYSIS

In order to evaluate the feasibility and effectiveness of our proposed method, we use the open source Linphone project to establish a VoIP connection [60]. Our scheme increases the reliability of any VoIP steganography system. However, in order to verify the performance of the proposed scheme in increasing the reliability of any VoIP steganographic system, we use a steganographic system based on LSB embedding. Conventional LSB matching is a commonly used algorithm that embeds secret message bits in all LSBs of cover [16]. Although this method has a low security, we choose this steganographic method for simplicity. Embedding Efficiency (EE) of this algorithm is:

$$EE = \frac{\text{number of embedded bits}}{\text{average number of change}} = 2 \tag{1}$$

and the capacity of this method is 8000 bps. Also we consider that our secret message length is 10 KB.

One of the benefits of our method is that encoding and decoding processes are performed off-line and ECCs with higher encoding and decoding complexity can also be used. Therefore, more desirable ECCs with high error correction capability can be applied. In the following, we show that, even by applying classical error correcting codes such as BCH (Bose-Chaudhuri-Hocqenghem) codes and RS (Reed-Solomon) codes, our algorithm results in a reasonable reliability. Since these codes are design distance codes, we can have high error correction capabilities. Therefore, based on modern ECCs, our proposed method greatly enhances the reliability of VoIP steganography.

5.1. BCH Performance

BCH codes are cyclic error correcting codes over finite fields. They were independently introduced in 1959 by French mathematician Hocquenghem [61] and in 1960 by Bose and Chaudhuri [62]. For every positive integer $m \geq 3$, there exists a binary BCH code with the following parameters: $n = 2^m - 1$, $n - k \leq mt$, $d \geq 2t + 1$. In fact, a t-error correcting BCH code of length n is a cyclic code whose generator polynomial is the lowest common multiple of the minimal polynomials of 2t consecutive powers of α, a primitive n-th root of unity in F_{2^m}. A prominent feature of these codes is *design distance property*. This means that, for a fixed code length, there are different amounts of the rates and Hamming distances (Fig. 5). BCH codes have a good flexibility, which means that if the number of lost packets is greater than the code's error correction capability, we can change the code to another code with the same length, but a higher error correction capability (Also see Fig. 5).

n	k	t	n	k	t	n	k	t	n	k	t	n	k	t
15	11	1	63	57	1	127	120	1	127	64	10	255	163	12
	7	2		45	3		113	2		57	11		155	13
	5	3		39	4		106	3		50	13		147	14
31	26	1		36	5		99	4		43	14		139	15
	21	2		30	6		92	5		36	15		131	18
	16	3		24	7		85	6		29	21		123	19
	11	5		18	10		78	7		22	23		115	21
	6	7		16	11		71	9		15	27		107	22

Figure 5: Some BCH codes generated by primitive elements of order less than 2^9

We perform our proposed method for different modes and the related results are listed in Fig. 7.

With regard to Fig. 7, it is clear that the percentage of success for recovering secret data is different for the same codes with different packet loss percentages, and it is reduced by an increase in the percentage of packet loss. To address this problem we use another BCH code with similar length and higher error correction capability. Clearly, this will reduce the code rate and decrease capacity of VoIP steganography. however, we achieve more reliability. Also we can choose another code of different length with higher rate and error correction capability.

5.2. Reed-Solomon Performance

Reed-Solomon codes are the most important subgroup of non binary BCH codes that are described in a paper by Reed and Solomon in 1960 [63], for the first time. An RS code is a $\mathbf{C}(n, k, n-k+1)$ BCH code; in other words, it is a linear block code of length $n = 2^m - 1$ with message length k and minimum Hamming distance $n - k + 1$. This code is optimal in the sense that the minimum distance has the maximum value possible for a linear code of size (n, k). Such a code is also called a *maximum distance separable* (MDS) code.

there are many communication systems, including: storage devices, wireless or mobile communications, satellite communications, etc, which use RS codes as error correcting code. A popular RS code is RS(255,223) with 8-bit symbols. Every 16 symbol errors in the codeword can be corrected by the decoder. So, errors in up to 16 bytes in the codeword are automatically corrected. In order to correct bursts of errors in the base field, it is more effective to use RS codes over extension fields. Due to the fact that, in the most cases packet loss occurs sequentially, using burst codes can be very helpful. We perform our scheme based on some of RS codes and summarize their results in Fig. 8. According to these results, as long as the packet drop is less than 1%, our proposed algorithm, based on RS code, can correctly recover all lost bits in more than 90 percents of examined cases. In addition, in the cases where packet loss are consecutive, RS codes compared to BCH cods have a better performance.

6. CONCLUSION and FUTURE WORK

We designed an algorithm to increase the reliability of any VoIP steganography system. We described a novel approach to use ECCs to rebuild lost bits due to the packet loss. Generally, using t-error correcting code $\mathbf{C}(n, k, d)$, we can recover secret message, when up to t of n packets are lost. In order to analyze the performance of the proposed scheme in terms of execution time, we illustrate it in the following diagram in 5 steps.

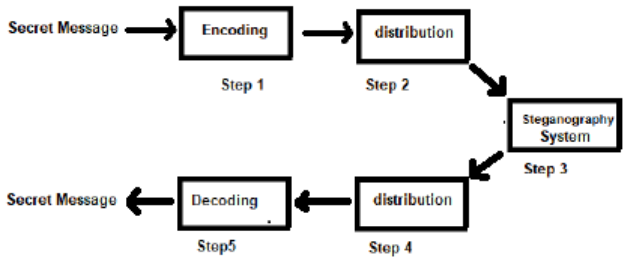

Figure 6: Diagram of proposed scheme

As shown in the diagram, after the message encoding operation, $m-q$ codewords of length n are distributed in n packets; under the method described in Section 4. Also, on the other hand, after the message decoding operation, m extracted blocks of length n are distributed in $m-q$ code blocks of length n. Since these two distributions operate such as a permutation function of order mn, the steps 2 and 4 of the diagram Fig. 6 are performed in a polynomial time. Therefore, using practical coding algorithms and VoIP steganographic systems, our proposed scheme will be performed in a polynomial time.

Two main factors of the applied channel codes that affect the performance of the packet loss recovery method are the error correction capability of the code and the decoding performance of the code. Therefore, channel codes with higher error correction capabilities are promising tools which is the reason for using designing distance codes in this paper. On the other hand, using some modern codes such as turbo and LDPC codes that have a very good decoding performance can potentially improve the performance of our method. But, in general, the time and spatial complexity of modern codes may cause delays in sending and receiving audio packet that result in audio degradation and therefore reduce the robustness and reliability of the steganography system. According to the diagram Fig. 6, encoding and decoding processes, steps 1 and 5 respectively, are performed off-line and thus have no effect on the time complexity of VoIP performance. This feature of the proposed scheme is one of the important contributions to the steganography system to increase robustness.

On the other hand, provided that the average of packet loss over the network is less than 1%, by applying the proposed packet loss recovery method based on a t-error correcting code $\mathbf{C}(n,k,d)$, the probability of losing hidden data, in each category of n-packets, satisfies in the following inequality:

$$P_e \leq 10^{-2t}. \tag{2}$$

Obviously, using t-error correcting codes with larger t, in the proposed scheme, results in more reliable steganographic systems. In order to present some numerical results, in Table 2, we summarize the error probability when using some modern types of LDPC codes in [64]. For these codes, we utilize the same notation as used in [64]. All of them are quasi-cyclic LDPC codes.

Table 2: Error probabilities of some LDPC codes.

Name	n	k	t	P_e
C_3^*	546	275	5	10^{-10}
C_3^*	396	125	10	10^{-20}
C_2^*	399	135	11	10^{-22}
C_{26}	399	135	12	10^{-24}
C_{32}	570	345	25	10^{-50}

Finally, it is obvious that we need to sacrifice steganographic capacity to reach reliance. Assuming that the embedding capacity of a steganographic system is m bits per packet. After using the proposed scheme, this value is changed to

$$\frac{k}{n}(m-q) \quad \textit{bits per packet.} \tag{3}$$

Code Attribiute				Packet loss	Burst	Success
m	n	k	t			
5	31	16	3	1%	1	77%
					3	71%
					7	10%
					12	1%
				3%	1	26%
					3	21%
					7	0%
					12	0%
				5%	1	1%
					3	0%
					7	0%
					12	0%
Code Attribiute				Packet loss	Burst	Success
m	n	k	t			
6	63	30	6	1%	1	74%
					3	80%
					7	69%
					12	0%
				3%	1	24%
					3	44%
					7	5%
					12	0%
				5%	1	3%
					3	4%
					7	0%
					12	0%
Code Attribiute				Packet loss	Burst	Success
m	n	k	t			
7	127	71	9	1%	1	89%
					3	96%
					7	98%
					12	100%
				3%	1	76%
					3	76%
					7	33%
					12	13%
				5%	1	35%
					3	20%
					7	5%
					12	4%

Figure 7: Implementation result for BCH codes

Code Attribiute				Packet loss	Burst	Success
m	n	k	t			
4	15	9	3	1%	1	97%
					5	92%
					10	100%
					15	99%
				3%	1	16%
					5	63%
					10	53%
					15	22%
				5%	1	0%
					5	20%
					10	12%
					15	3%
Code Attribiute				Packet loss	Burst	Success
m	n	k	t			
5	31	19	6	1%	1	100%
					5	100%
					10	100%
					15	100%
				3%	1	43%
					5	100%
					10	97%
					15	90%
				5%	1	1%
					5	81%
					10	81%
					15	
Code Attribiute				Packet loss	Burst	Success
m	n	k	t			
6	63	45	9	1%	1	100%
					5	100%
					10	100%
					15	100%
				3%	1	35%
					5	100%
					10	100%
					15	100%
				5%	1	0%
					5	91%
					10	100%
					15	100%

Figure 8: Implementation result for RS codes

References

[1] H. Wang, X. Zhao, Y. Shi, H. J. Kim, A. Piva, Digital forensics and watermarking: 18th International Workshop, IWDW 2019, vol 12022. Springer Nature (2020).

[2] A. Durafe, R. Desai, A. Kashyap, S. Gupta, P. Bagul, Steganography for public security, vol 8, no 4. IJCRT (2020).

[3] G. Xin, Y. Liu, T. Yang, Y. Cao, An adaptive audio steganography for covert wireless communication, Security and Communication Networks (2018).

[4] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, B. Balusamy, Securing data in Internet of Things (IoT) using cryptography and steganography techniques, IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol 50, no 1 (2019), 73-80.

[5] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, C. Qin, A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network, IEEE Access, vol 8 (2020), 25777-25788.

[6] W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM Systems Journal, vol 35, no 3.4 (1996), 313-336.

[7] B. I. Neelgar, C. D. Kumar, A. S. Vyshnavi, A. O. S. Vigna, U. S. Anush, Audio wavelet compression and audio steganography using LSB technique, International Research Journal of Advanced Engineering and Science, vol 5, no 3 (2020), 111-114.

[8] H. A. Nassrullah, W. N. Flayyih, M. A. Nasrullah, Enhancement of LSB audio steganography based on carrier and message characteristics, J. Inf. Hiding Multim. Signal Process, vol 11, no 3 (2020), 126-137.

[9] J. C. T. Arroyo, A. J. P. Delima, LSB image steganography with data compression technique using Goldbach G0 code algorithm, International Journal, vol 8, no 7 (2020).

[10] D. Qu, B. Wang, B. Li, L. Zhang, Q. Chen, W. Zhang, VoIP speech processing and recognition, National Defense Industry Press, Beijing, China, (2010), 3-6.

[11] W. Mazurczyk, VoIP steganography and its detection—a survey, ACM Computing Surveys (CSUR), vol 46, no 2 (2013), 1-21.

[12] W. Mazurczyk, P. Szaga, K. Szczypiorski, Using transcoding for hidden communication in IP telephony, Multimedia Tools and Applications, vol 70, no 3 (2014), 2139-2165.

[13] H. Tian, H. Jiang, K. Zhou, D. Feng, Transparency-orientated encoding strategies for voice-over-ip steganography, The Computer Journal, vol 55, no 6 (2012), 702-716.

[14] S. Deepikaa, R. Saravanan, VoIP steganography methods, a survey, Cybern. Inf. Technol, vol 19, no 3.4 (2019), 73-87.

[15] J. Li, Z. Liu, H. Peng, Security and privacy in new computing environments, Springer Science and Business Media LLC: Berlin/Heidelberg, Germany (2019).

[16] J. Fridrich, Steganography in digital media: Principles, algorithms and applications. Cambridge University Press (2009).

[17] H. Tian, W. Yanpeng, H. Yongfeng, L. Jin, C. Yonghong, W. Tian, C. Yiqiao, Steganalysis of Low Bit-Rate Speech Based on Statistic Characteristics of Pulse Positions, In Proceedings of the 2015 10th International Conference on Availability Reliability and Security, Toulouse, France (2015).

[18] P. Yadav, S. Dhall, Comparative analysis of steganography technique for information security, I. J. Mathematical Sciences and Computing, vol 4 (2020), 42-69.

[19] X. Liu, H. Tian, J. Liu, J. Lu, Survey for voice-over-IP steganography and steganalysis, J. Chongqing Univ. Posts Telecommun.(Nat. Sci. Ed.), vol 31, no 3 (2019), 407-418.

[20] H. Yang, Z. L. Yang, Y. J. Bao, S. Liu, Y. F. Huang, Fast steganalysis method for Voip streams, IEEE Signal Process. Lett., vol 27 (2020), 286-290.

[21] A. Westfeld, F5, a steganographic algorithm, International Workshop on Information Hiding, Springer (2001), 289-302.

[22] R. Zhang, V. Sachnev, M. B. Botnan, H. J. Kim, J. Heo, An efficient embedder for BCH coding for steganography, IEEE Transactions on Information Theory, vol 58, no 12 (2012), 7272-7279.

[23] S. Li, P. Liu, H. Wang, Steganography integrated into linear predictive coding for low bit-rate speech codec, Multimed. Tools Appl., vol 76 (2017), 2837-2859.

[24] N. Komaki, N. Aoki, T. Yamamoto, A packet loss concealment technique for voip using steganography, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol 86, no 8 (2003), 2069-2072.

[25] H. Tian, K. Zhou, H. Jiang, Y. Huang, J. Liu, D. Feng, An adaptive steganography scheme for voice over IP, IEEE International Symposium on Circuits and Systems (2009), 2922-2925.

[26] T. Xu, Z. Yang, Simple and effective speech steganography in g.723.1 low-rate codes, International Conference on Wireless Communications and Signal Processing, IEEE (2009), 1-4.

[27] S. Anguraj, S. Shantharajah, J. J. Emilyn, A steganographic method based on optimized audio embedding technique for secure data communication in the internet of things, Comput. Intell., vol 36 (2020), 557-573.

[28] W. Han, L. Zhu, F. Yan, Trusted computing and information security, Springer Science and Business Media LLC: Berlin/Heidelberg, Germany (2020).

[29] J. Han, C. Huang, F. Shi, J. Liu, Covert timing channel detection method based on time interval and payload length analysis, Comput. Secur., vol 97 (2020).

[30] M. Mehic, J. lachta, M. Voznak, Hiding data in sip session, International Conference on Telecommunications and Signal Processing (TSP), IEEE (2015), 1-5.

[31] C. Arackaparambil, G. Yan, S. Bratus, A. Caglayan, On tuning the knobs of distribution-based methods for detecting voip covert channels, Hawaii International Conference on System Sciences, IEEE (2012), 2431-2440.

[32] X. Zhang, Y. Tan, C. Liang, Y. Li, J. Li, A covert channel over volte via adjusting silence periods, IEEE Access, vol 6 (2018), 9292-9302.

[33] F. Li, B. Li, Y. Huang, Y. Feng, L. Peng, N. Zhou, Research on covert communication channel based on modulation of common compressed speech codec, Neural Comput. Appl. (2020), 1-14.

[34] Z. Wu, C. Li, Y. Sha, Speech information hiding algorithm based on complete binary tree dynamic codebook grouping, IEEE Access vol 7 (2019), 147513-147522.

[35] W. Mazurczyk, J. Lubacz, Lack—a VoIP steganographic method, Telecommunication Systems, vol 45, no 2-3 (2010), 153-163.

[36] Y. F. Huang, S. Tang, J. Yuan, Steganography in inactive frames of VoIP streams encoded by source codec, IEEE Trans. Inf. Forensics Security, vol 6, no 2 (2011), 296-306.

[37] Y. F. Huang, C. Liu, S. Tang, S. Bai, Steganography integration into a low-bit rate speech codec, IEEE Trans. Inf. Forensics Security, vol 7, no 6 (2012), 1865-1875.

[38] A. Ito, Y. Suzuki, Information hiding for g.711 speech based on substitution of least significant bits and estimation of tolerable distortion, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol 93, no 7 (2010), 1279-1286.

[39] R. W. Hamming, Error detecting and error correcting codes, The Bell System Technical Journal, vol 29, no 2 (1950), 147-160.

[40] S. Lin, W. Ryan, Channel codes: classical and modern, Cambridge university press (2009).

[41] J. Bierbrauer, Introduction to coding theory, Chapman and Hall/CRC (2016).

[42] O. Gazi, Information theory perspective of polar codes and polar encoding. In polar codes, Springer, Singapore (2019), 1-25.

[43] E. E. Gad, Y. Li, J. Kliewer, M. Langberg, A. Jiang, J. Bruck, Asymmetric error correction and flash-memory rewriting using polar codes, U.S. Patent No. 10,379,945. Washington, DC: U.S. Patent and Trademark Office (2019).

[44] S. Liu, J. Li, P. Reviriego, M. Ottavi, L. Xiao, A double error correction code for 32-bit data words with efficent decoding, IEEE Transactions on Device and Materials Reliability, vol 18, no 1 (2018), 125-127.

[45] S. Tang, Y. Jiang, L. Zhang, Z. Zhou, Audio steganography with aes for real-time covert voice over internet protocol communications, Science China Information Sciences, vol 57, no 3 (2014), 1-14.

[46] Y. Ren, H. Yang, H. Wu, L. Wang. A secure steganography method for AMR fixed codebook based on pulse distribution model, Patent CN201910347984.3 (2019).

[47] X. Liu. Speech steganography based on adaptive codebook partition and its detection, Huaqiao University: Quanzhou, China (2020).

[48] H. Neal, H. ElAarag, A reliable covert communication scheme based on VoIP steganography, Transactions on Data Hiding and Multimedia Security, Springer (2015), 55-68.

[49] H. Neal, H. ElAarag, A packet loss tolerant algorithm for information hiding in voice over IP, Proceedings of IEEE Southeastcon, IEEE (2012), 1-6.

[50] Y. Jiang, S. Tang, L. Zhang, M. Xiong, Y. J. Yip, Covert voice over internet protocol communications with packet loss based on fractal interpolation, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol 12, no 4 (2016), 1-20.

[51] W. Mazurczyk, Lost audio packets steganography: the first practical evaluation, Security and Communication Networks,vol 5, no 12 (2012),1394-1403.

[52] M. Hamdaqa, L. Tahvildari, Relack: a reliable voip steganography approach, Secure Software Integration and Reliability Improvement (SSIRI), 2011 Fifth International Conference, IEEE (2011), 189-197.

[53] P. A. Dana, Z. Esmaeilbeig, M. R. Sadeghi, Reliability enhancement and packet loss recovery of any steganographic method in voice over IP, Wireless Networks, Springer (2020), 1-7.

[54] H. Tian, Y. Chen, J. Lu, Y. Chen, Neighbor-index-division steganography based on QIM method for G.723.1 speech streams, J. Ambient. Intell. Humaniz. Comput., No 7 (2016), 139-147.

[55] P. Yue, Research on self-adaption VoIP steganographic method based on LPC cepstrum distortion cost, Wirel. Internet Technol., No 4 (2017), 100-103.

[56] J. Yang, Research on technologies of AMR steganography and steganalysis based on pitch delay. Wuhan University: Wuhan, China (2017).

[57] X. Liu, H. Tian, Y. Huang, J. Lu, A novel steganographic method for algebraic-code-excited-linear-prediction speech streams based on fractional pitch delay search, Multimed. Tools Appl., vol 78 (2019), 8447-8461.

[58] Y. Jiang, S. Tang, L. Zhang, M. Xiong, Y. J. Yip, Covert Voice over Internet Protocol Communications with Packet Loss Based on Fractal Interpolation, ACM Trans. Multimed. Comput. Commun. Appl., vol 12 (2016), 1-20.

[59] S. Deepikaa, R. Saravanan, Coverless VoIP steganography using hash and hash, Cybern. Inf. Technol.,, vol 20 (2020), 102-115.

[60] Linphone open source voip project, http://www.linphone. org/, Accessed: 2019.

[61] A. Hocquenghem, Codes correcteurs d'erreurs, Chiffres, vol 2, no 2 (1959), 147-156.

[62] R. C. Bose, D. K. Ray-Chaudhuri, On a class of error correcting binary group codes, Information and Control, vol 3, no 1 (1960), 68-79.

[63] I. S. Reed, G. Solomon, Polynomial codes over certain finite fields, Journal of the Society for Industrial and Applied Mathematics, vol 8, no 2 (1960), 300-304.

[64] A. Tasdighi, M. R. Sadeghi, On advisability of designing short length QC-LDPC codes using perfect difference families, arXiv preprint, 2017.

Please cite this article using:

Mohammad-Reza Rafsanjani Sadeghi, Parvane Amirzade Dana, Bahram Javadi, A new approach to solve the reliability problem in any VoIP steganography system, AUT J. Math. Comput., 3(1) (2022) 113-127
DOI: 10.22060/AJMC.2022.20710.1073