IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

Voice-Over-IP

Likitha K. M.[1], Nidhi N. Shetty[2], Prajakta Shetty[3], Mr. Pradeep Nayak[4], Vaishali[5]
Assistant Professor, Department of Information Science and Engineering[4]
Students, Department of Information Science and Engineering[1,2,3,5]
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India

Abstract: *A type of IP network-based digital transmission technology is voice-over-IP (VoIP) technology. Using VoIP voice service as a steganographic carrier is one of the key strategies for ensuring secure transmission. A new method of information concealment called steganography in dormant Voice-over-IP frames allows for high steganographic capacity while still maintaining excellent imperceptibility. The entropy-based and poker test-based steganalysis methods have been presented to prevent the improper application of this technology.However, when there are few inactive frames or low embedding rates, the detection performance of these two approaches is not as good.So, based on fundamental frequency statistics, we provide a novel steganalysis technique This leads to the proposal of a steganographic method that combines the F5 and simplified wet paper code (SWPC) algorithms.The fundamental concept is to utilise the F5 technique to secretly encode each row of the carrier matrix, after which the SWPC algorithm is used to encode the columns in accordance with the wet and dry properties of the wet paper code without impacting the previous row embedding results. We test the suggested strategy using VoIP streams encoded with the ITU-T G.729a codec as a carrier. The experimental findings show that the suggested system outperforms F5-WPC and SWPC approaches and can produce considerably superior IP voice data steganographic transparency.*

Keywords: Wet paper code, streaming video, voice over IP, and the F5 algorithm

I. INTRODUCTION

Steganography is a covert communication technique that involves obfuscating information in digital media (such as images, videos, audio, and text) without observable deformation. Due to its simplicity, cheap cost, and excellent speech quality, Voice over Internet Protocol (VoIP), which permits phone calls based on IP networks, has become widely used in people's daily lives.In order to meet the goals of secrecy and security, information hiding is a new type of secure communication technology that may conceal secret information in an apparent ordinary carrier. It hides the existence of covert communication and, frequently, offers more security than conventional communication channels. As a result, it has been growing quickly recently [1] [3]. Currently, streaming media has replaced the original picture as the cover carrier in information concealment. It is important to note that many academics have given IP voice technology a great deal of attention [4] .The key reason is that voice over IP (VoIP) voice stream may give superior steganography performance and embedding capacity and the secret information embedded in VoIP is dynamic and not simple to be detected by unauthorised attackers. Research on VoIP streaming media information hiding may be separated into two categories: voice carrier-based information hiding and network protocol-based information hiding.The first is an information-hiding technique based on the IP voice transmission process network protocol, while the second is an information-hiding technique based on the voice carrier. In general, there are two types of VoIP-based steganography. One uses network protocols as carriers, whilst the other conceals information by altering voice stream payloads. The second group has been the norm for VoIP-based steganography because of its strong steganographic capacity. VoIP frequently uses code excited linear prediction (CELP) codecs, such as ITU T G. 723.1, ITU-T G.729a, Speex, Internet Low Bitrate Codec (iLBC), and adaptive multi-rate (AMR) codec, to encrypt speech signals into digital frame streams to achieve the necessary low data rates. In their studies of the information concealing technique based on the parity of matrix coding and the iLBC codebook index, respectively, Xu and Yang [1] and Miao and Huang [2] found that while the hiding effect was good, the hiding capacity was not. In order to reduce the size of the speech payload and provide space for concealing information, Mazurczyk et al. [3] proposed transcoding the speech payload; the LSB approach is

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

the most popular and has the benefits of having a high embedded capacity and low computing complexity. The LSB technique, however, heavily relies on the need that the sender and receiver employ the consensus overlay bit [4]. As a result, security issues still exist. In general, for a given embedding rate (ER), the less the steganographic method modifies the carrier, the less likely it is that concealed information would be discovered, increasing security [5],coding theory was applied to the information embedding process in order to further increase the efficiency and security of steganography, and a number of steganography codes, including matrix coding and Wet Paper Code, were devised (WPC). Among these, Crandall was the first to suggest matrix encoding as a steganographic approach to increase coding efficacy.With the use of additional carrier data, this method can increase embedding efficiency while reducing carrier data modification. The F5 method, which can contain secret information when the carrier change is up to 1 bit, was the first algorithm to use matrix encoding. In order to improve the security of steganography, Fridrich et al. [2] proposed the WPC in 2005. The WPC determines which positions in the image can be modified through a selection rule known only to the sender, allowing the sender to embed information without changing the sensitive area of the carrier.

II. RELATED WORK

2.1 Hidden Communications via VoIP

Based on the concept of VoIP streaming media, information hiding is implemented by embedding secret data in the IP voice streaming carrier or LSB included in the network protocol when transmitting IP voice [2]. on figs. 1 shows a VoIP streaming media masking communication procedure. Hiding VoIP Streaming Media is shown in Figure 1. 1 Forms of a generalized model of the communication process. Communication consistency required by both parties to achieve the communication mode is shown, including the use of VoIP voice and data streaming media transfer, secret coding algorithms and specific voice coding methods, etc. First, by common agreement, callers included sensitive information in their IP voice carriers. The receiver then receives the IP voice data containing the secret information and extracts the secret information using a reserved method. To meet the VoIP service's requirements for confidential communication, information hiding security, and low latency, third-party rogue attackers can intercept IP voice data, but cannot verify whether the operator data is actually a hidden secret message.

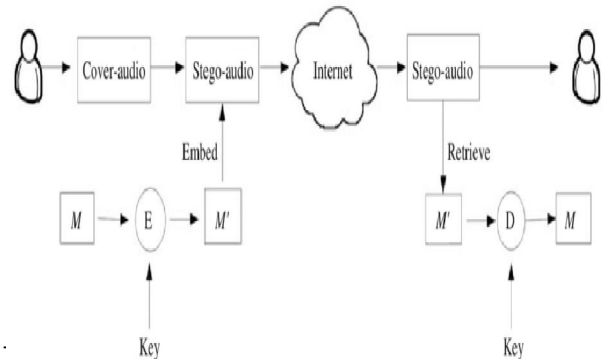

Figure 1: Covert communication over VoIP.

1.2 F5 Algorithm

A steganographic method to increase coding efficiency is matrix coding. The basic premise is to minimize carrier data modification to improve embedding efficiency using more carrier data. The F5 algorithm is the first to use matrix encoding, which can contain x bits of secret information by changing up to 1 bit per n(n D 2x 1) bit carrier. This algorithm greatly improves the efficiency of steganographic embedding and qualitatively improves non-aggressiveness by reducing carrier distortion [3]. Suppose l0 is the embedded carrier object obtained by embedding the secret m into l. l0 has n elements fig, {li}, l = {l1, l2, ... The original carrier object composed of . . . , ln}, carrier with n modifiable elements after replacement. The following is just an introduction to the F5 algorithm, which is the reverse process of the embedding method. Here's his approach.

1) Define a function f that can contain x bits of secret information m on carrier l defined as:

$$f(l) = n \oplus i=1\ li \bullet i$$

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

2) Using the XOR operation of function f and secret message m to find the point in l that needs to be updated, we get:
v = f(l) ⊕m
3) Change l's guide to view:

$$l = (l\ v = 0(l1, l2,..., li, . . . , ln)\ v = i$$

4) Continue repeating steps 1-3 until all hidden messages are inserted. Therefore, the extraction function of the F5 algorithm is expressed as:

$$f(l) = f(m, l) = n \oplus i=1\ li \bullet i \oplus m$$

As a result, the extraction function of the F5 algorithm can be described as follows.

$$f(x0) = f(0, x0) = f(m, x) \oplus f(0, x) = m$$

1.3 Properties of Hamming Code

The following list includes four important properties of Hamming codes described in [24] and [25]. Theorem 1. Let C be the Hamming code of length 2x − 1. i, j ∈ {1, . . . , 2x - 1}. Then the unique coordinates g1(i, j) ∈ {1, . . . , 2 x − 1} Let the vectors supporting {i, j, g1(i, j)} belong to C. Lemma 2. Let C be the Hamming code of length 2x − 1. i, j ∈ {1, . . . , 2x - 1}. For any coordinate 1 ≤ i ≤ 2 x-1 - 1 you can always take a check matrix with two coordinates: (2x-1 - 1 i)-i and (2x - 1)-i. Support g1(i, j) ∈ {1, . . . , 2 x −1} belongs to code C, where g2(i) = 2 t −1 −1 i. Theorem 3. Let C be a Hamming code of length 2x − 1 with check matrix H. i, j, r ∈ {1, . . . , 2 x−1 −1} and i < j < r, so the vector u with supports i, j, r belongs to code C. Then the vector v with supports {j, g2(i), g2(r)} belongs to code C and g2(i), g2(r) ∈ {2 x − 1, . . . , 2x - 2}. Theorem 4. Let C be the Hamming code of length 2x − 1. k = (k1, k2, ... , kn) ∈ GF(2n) and supp(k) = {i1, i2, i3}. According to the embedding function F5, we have a vector k0 with a fourth component i4 supporting supp(k0) = {i1, i2, i3, i4}. where i4 = i1 ⊕ i2 ⊕ i3.

1.4 Improved WPC using Simplified Hamming Parity Check (SWPC) Matrix

The original carriers are divided into two groups according to the classic WPC design philosophy [26]. The caller separates the cover part into a wet part and a dry part. Users may include all information secrets in the dry area only if the secret message must be included in the original media. This is like standing on a blank piece of writing paper, but only in a dry location. Information cannot be written in a humid environment. The receiver obtains the hidden information contained in the source medium when the source medium selects several locations according to predetermined wet and dry criteria, implements the embedded hidden information, sends the information to the recipient, and then includes the secret. The original media no longer differentiates between dry and wet locations and directly contains confidential information. received by the receiver. Therefore, it is guaranteed that the wet and dry sharing bases selected by the sender will not be leaked in the process of information transmission, thereby improving the security of information hiding.

Assume that the cover object L has n elements, denoted by L = {l1, l2, . . . ,ln}. The sender could discretionarily choose k elements lj in L to hide information, denoted by L 0 = {l1 0 , l2 0 , . . . , lt 0 }, j ∈ J ∈ {1, 2, . . . , n}, |J|=k. The receiver has the following options for extracting embedded data:

$$DL0 = m$$

where D is the p × n random binary matrix. Subtracting DL from both sides, we can get the following:

$$D(L\ 0 - L) = m - DL$$

Similar to Equation , based on the discrepancy between the encoded information m and DL, the sender may ascertain the bits in L that need to be updated. Denoting v = (L 0 −L), we have the following:

$$Hv = m - DL$$

where H is a submatrix made up of D's k column vectors. It is obvious that the element in v that is non-zero corresponds to the element for which the sender must adjust L throughout the embedding process.

In contrast to the conventional WPC building technique, the expandable matrix is formed in accordance with the parameters, and the WPC of the check matrix is constructed from the opposite direction. While guaranteeing that the encoding scheme always has a solution, each steganographic SWPC method to the carrier for no more than 2 bits of alteration can accomplish quick coding.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

III. AN ENHANCED STEGANOGRAPHIC CODE CONSTRUCTION METHOD FOR VoIP

In this work, we offer a technique for creating IP voice streams that combines SWPC and F5 codecs. The IP voice streams are first organised into a matrix, and the secret information is initially embedded on the matrix block using the F5 coding technique. The second embedding, however, is done on the column using the more effective SWPC algorithm. The suggested method preserves the IP voice streams' steganographic transparency and increases the secret information's embedding efficiency when compared to the F5-WPC algorithm and SWPC algorithm methods.

The concept is that the ITU-T G.729a encoder divides the IP speech streams L into independent matrix blocks of length N (2x-1), where N is the grouping length of the WPC chosen by the sender in the SWPC algorithm, and the secret information m embedded in x bits is grouped according to R for each length.

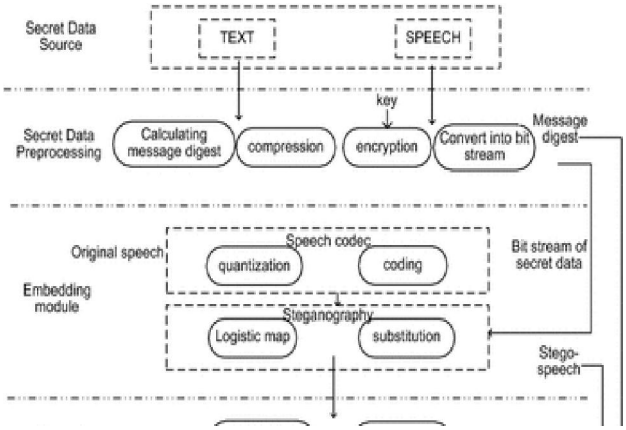

Figure 1.2: The embedding end of VoIP steganography system

In order to embed concealed information, the rows of the matrix must first be scanned. Due to the nature of the F5 technique, the row embedding result may be preserved without the need for significant alteration. Most of the time, only one piece has to be changed. The percentage of "dry" items in the WPC and the location that has to be changed in the event of a row dispute must be taken into account while column embedding. If row j is not changed when the first column is embedded, the j position in the first column is recorded as "wet," and the percentage of "dry" position is (2x 1)/2 x. As a result, there can be Nx(2x 1)/2 x (2x 1) bits of secret information encoded in the first column, resulting in an average change of (2x N/2)N(2x 1)/(2x 1). Based on this, it is believed that each column of the matrix is scanned and that the subscript of the updated carrier data in the row is ri ($1 \le i \le N$). In accordance with Lemma 1 and 2, scan only the first through second embedded columns of the matrix element split by the last column in the matrix. Assume that ri is in conflict with the subscript of the column index ci ($1 \le j \le 2x-1-1$) that needs to be updated in the matrix column. The column index is modified using the following process:

If either ri or cj needs to be modified or neither needs to be modified, in order not to affect the embedding result of row i, according to Lemma 2, change the subscripts of $2x-1-1+j$

1) and $2x-1$. Further reduce the number of modifications, according to Lemma 4, modify ri$\oplus$ 2 $x-1-1+j \oplus (2x-1)$ to replace $2x-1-1+j$ and $2x-1$.

2) Coordinate ri corresponding to cj , judge the magnitude of ri and cj . If ri<cj , according to Lemma 2, change $2x-1-1+i$ and $2x-1$. If ri>cj , the subscript of g1 = (ri, cj) >cj . According to Lemma 3, change the subscript of g2 = (ri) and g2 = (cj).

IV. EMBEDDED ALGORITHM FOR SECRET MESSAGES

The specific embedding algorithm is presented in this section based on the main concept that was previously introduced. Fig. 2 depicts the embedding algorithm's flow. The F5 encoding technique is used in row embedding to consecutively encode rows 1 through N. The following is a description of the detailed embedding algorithm:

1) Using (4) embed the secret messages m after reading the secret messages m bit.

2) Continue until every row has been embedded. Since the F5 method is what it is, the outcome of row embedding can only be changed by a maximum of one bit. After calculating the percentage of "dry" positions in column embedding, use the SWPC method to embed from column 1 to column $2x-1-1$ and calculate the number of elements that may be changed, k. These are the steps:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

1) Create the A matrix for the R–N hamming check.
2) To obtain the reduced matrix H, remove the 2x 1 k columns from matrix A.
3) Create the R (2x 1) zero matrix D, replace the subscripts of D with the subscripts of lj (j = 1, 2,..., k) for each column in H, then produce random binary sequences for replacement in the unreplaced columns of D.
4) To incorporate secret messages m, solve vector v using formula (8) and alter carrier data L's position to correspond to the positions of non-zero elements.

V. THE EXTRACTION ALGORITHM OF SECRET MESSAGES

The typical streaming media application, with its strong real-time and dynamic qualities, is voice-over IP. VoIP-based real-time secret communication requires a network infrastructure that can support both robust stability and little network latency. Since the real-time voice call uses IP packet encapsulation, the receiving end acquires the G.729a encoded IP voice carrier bit stream by deconstructing the data packet and performing pre-processing operations after receiving the encrypted IP voice data packet. The suggested extraction algorithm is extracted, and Fig. 3 depicts the extraction algorithm's operation. Determine N and R. The ITU-T G.729a encoder divides the IP voice streams L into many independent matrix blocks, each of which has a length of N (2x-1). To retrieve the hidden messages, the carrier matrix's first and second layers are combined. Following are the steps:
1) Extract the hidden messages from each row of the matrix using the formula (5).
2) Create the zero matrix R (2x-1).
3) To obtain the reduced matrix H, construct the R-N hamming check matrix A and remove its 2x-1-k columns.
4) For each column in H, swap the subscripts of D with the subscripts of lj ((j = 1, 2,..., k)), and use the other zero columns in D to build replacement binary sequences at random.
5) Locate L 0 and use step 6 to retrieve hidden messages m.
The aforementioned procedure demonstrates that the extraction process for secret information is easier than the embedded process, and the primary job is to find a solution so that the secret information can be extracted with ease.

VI. SYNCHRONIZATION MECHANISM

It is important to keep in mind that the effectiveness of the extraction and recovery of secret information depends on the synchronised processing of secret IP communication. The method put forth in this paper involves using the connectionless UDP protocol for real-time transmission over the IP network in order to embed and extract confidential information from the bitstream of IP speech carrier encoded by each voice packet according to parameters agreed upon by both parties. Through PCM encoding, 8kHz sampling, and 16-bit quantization, the gathered analogue impulses are transformed into the matching digital signals. In order to make sure that network performance and other variables do not impact the embedding and extraction of secret information throughout the communication process, We look a VoIP secret synchronisation technique from the following two perspectives to fulfil the real-time need [27, 28]. One the one hand, the compressed IP speech data bitstream is grouped in accordance with the SWPC coding characteristics, the secret messages are grouped in accordance with the carrier length, and the secret information is embedded by an embedding algorithm, so the loss of any secret speech packet [29] will not affect other packets. In order to reduce latency and packet loss during real-time transmission over IP network channels and packet reception by the receiver, the extraction algorithm must be used in time to carry secret hidden information extracted from VoIP packets. This is done by grouping and embedding secret messages almost simultaneously. On the other hand, this study develops a method to test whether each IP speech packet can be embedded and extracted separately, which is a better solution to the issue of VoIP communication synchronization's ability to extract and restore secret information. A technique for figuring out a voice packet is called Determine Current Operation (DCOP). It can synchronise how the transmitter and the receiver embed and extract information. No voice packet containing secret information will be missed by the receiver, and no voice packet containing secret information will be extracted by the receiver. The DCOP computation is fairly simple and straightforward to use. The DCOP method's flowchart is depicted in Fig. 4. In conclusion, the entire communication process involves preprocessing the speech carrier from the standpoint of coding, introducing steganography coding strategy, and demonstrating through experiments that the algorithm suggested in this paper can guarantee the real-time broadcast of IP speech while also receiving secret messages.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

VII. PERFORMANCE EVALUATION AND ANALYSIS

7.1 Steganographic Performance

We use the embedding rate (ER) to assess steganographic capacity, the bit change rate after encoding secret messages (BCR) to assess steganographic transparency, and the embedding efficiency (EE) to assess overall steganographic performance in order to assess the effectiveness of the enhanced steganographic codes construction method proposed in this paper. We assume that a N (2x 1) encoding matrix is used for the sake of simplicity. ER, which is defined as the ratio of the number of secret messages to the total number of cover bits, is as follows:

$$ER = 2\ x{-}P1{-}1\ t{=}1\ Nx(2x - t)/2\ x\ (2x - 1) + Nx\ N \times (2x - 1)$$

where x is the number of secret message bits inserted and N is the packet length encoded by SWPC.

The average number of cover bits modified is as follows:

$$d = 2\ xX{-}1{-}1\ t{=}1\ N(2x - 5)(2x - t)\ 2\ x + N \times 2\ x - 1\ 2\ x$$

BCR stands for bit-cover-ratio, which is the ratio of the average number of cover bits to the total number of cover bits, which can be defined as follows:

$$BCR = d\ N \times (2x - 1)$$

Additionally, EE refers to the ratio of the average change number to the number of bits embedded in secret messages, which may be represented as follows:

$$EE = 2\ x{-}P1{-}1\ t{=}1\ Nx(2x - t)/2\ x\ (2x - 1) + Nx\ d$$

7.2 Speech Quality Testing and Analysis

We chose the speech data from different audio libraries included in ITU-T P.501 standard Appendix B of the International Telecommunication Union Standard as the speech samples in order to test the algorithm proposed in this paper. We also chose the representative ITU-T G.729a encoder [30] as the IP voice encoder. Chinese male, Chinese female, English male, and English female are among the languages represented in the original voice samples. During the test, an external player is utilised to play the audio speech as the carrier voice input in order to simulate genuine VoIP communication.

All of the speech samples were first converted into PCM format with an 8 kHz sampling rate and 16-bit quantized mono speech. Then, the ITU-T G.729a encoder incorporates the hidden messages into the IP voice data. Finally, the G. 729a decoder extracts the secret information from the IP voice data that has been encrypted. Before being embedded in a test, the original speech waveform is shown in Fig. 5, and the resulting speech waveform is shown in Fig. 6. The carrier's waveform barely altered before and after concealment, as seen in the comparison figure, demonstrating the viability of the steganography process. We also used the Perceptual Evaluation of Speech Quality (PESQ) technique from ITU-T P.862 [31, 32] in order to further test the algorithm's concealing impact. By calculating a PESQ score and comparing the original speech signal with the degraded speech signal, the PESQ is used to predict perceived quality.

The quality of the voice signal increases with increasing PESQ score. In the experiment, the PESQ's original speech was represented by the PCM speech data in the audio library, and the PESQ's degraded speech was represented by the steganographic of the PCM speech data. The average voice steganography PESQ score, as determined by the data analysis in Table 1, is around 3.601, which satisfies the VoIP call quality criteria. The PESQ rating in [3] is poor because the prolonged communication procedure degrades speech quality. Although the technique utilised in this paper's PESQ calculation somewhat outperforms that in [4], the embedding capacity is constrained. The steganographic technique suggested in this research has excellent embedding performance and satisfies VoIP call quality standards, making it highly valuable.

7.3 Steganographic Performance Comparison Analysis

We also created a simulation test environment in accordance with the steganographic method suggested in this research and contrasted it with the F5-WPC and SWPC steganographic algorithms. The embedding rate is shown in Fig. 7. When the embedding rate is more than 0.1, we can see in Fig. 7 that the suggested approach has a higher embedding rate than the F5-WPC technique. However, the embedding performance falls short of SWPC and F5-WPC steganalysis algorithms when the embedding rate is less than 0.1. This is such that the chance that one modification is required to embed x bit secret messages in the data of the 2x 1 bit carrier progressively grows and the embedding rate in rows of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

hamming code [2 x 1, x, 1] gradually reduces as the parameter x increases. When x rises to a certain point, the likelihood of a column modification tends to be zero, which lowers embedding performance. The BCR values of algorithms, SWPC, F5-WPC, and the technique suggested in this article are displayed in Table 2 based on the results of the simulation. The experimental findings of BCR in Fig. 8 are drawn in accordance with the experimental data in Table 2 in order to more clearly reveal the hidden transparency of the three methods. The concealed transparency is often better the smaller the BCR. As shown in Fig. 8, this algorithm's carrier data are more visible when compared to those of the F5-WPC and SWPC steganographic algorithms. Combining Figs. 7 and 9 reveals that while embedding efficiency reduces with a drop in x, the embedding rate decreases with a bigger value of x.

The chance of the carrier's average change digit is correlated with embedding efficiency. The average change digit of the carrier increases with embedding rate but decreases with embedding efficiency. As a result, you may compromise to select the appropriate x and change the amount of digits to suit actual requirements.

VIII. CONCLUSION

A cutting-edge method of covert communication based on VoIP, steganography in idle voice frames can achieve high steganographic capacity while preserving great embedding transparency. Its unauthorised use by terrorists and criminals would, however, make cybercrimes easier to commit and represent a severe threat to cybersecurity. Therefore, the purpose of this paper is to create an effective steganalysis technique to identify this kind of steganography. Wethoroughly assess the steganographic performance from the perspectives of embedding rate, carrier bit change rate, and embedding efficiency in order to assess the performance of the steganographic approach described in this study. On the IP voice streams encoded using the ITU-T G.729a encoder, experiments are performed. The outcomes of the experiments demonstrate the viability of the steganography algorithm and its ability to ensure the call quality of VoIP services. In comparison to previous methods, the suggested solution not only achieves steganography transparency and embedding effectiveness but sufficiently meets VoIP's real-time requirement. The tradeoff between the suggested method's embedding rate and embedding efficiency is what we shall examine next, though.

REFERENCES

[1]. J. Liu, H. Tian, C.-C. Chang, T. Wang, Y. Chen, and Y. Cai, ‘‘Steganalysis of inactive voice-Over-IP frames based on poker test,’’ Symmetry, vol. 10,p. 336, Aug. 2018.

[2]. X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, ‘‘Reversible image steganography scheme based on a U-Net structure,’’ IEEE Access, vol. 7,pp. 9314–9323, Jan. 2019.

[3]. G. Kaur, J. Kaur, S. Aggarwal, C. Singla, N. Mahajan, S. Kaushal, andA. K. Sangaiah, ‘‘An optimized hardware calibration technique for transmission of real-time applications in VoIP network,’’ Multimedia Tools Appl., vol. 78, no. 5, pp. 5537–5570, 2019.

[4]. A. Bakri, A. Amrouche, M. Abbas, and L. Bouchakour, ‘‘Automatic speech recognition for VoIP with packet loss concealment,’’ Procedia Comput.Sci., vol. 128, pp. 72–78, Jan. 2018.