Encryption technology of voice transmission in mobile network based on 3DES-ECC algorithm

Zhixian Chang¹ · Marcin Woźniak²

Published online: 17 August 2020

© The Author(s) 2020

Abstract

The traditional design of voice collector has poor anti attack ability, which makes the encryption effect of voice transmission poor. Therefore, taking the mobile network voice collector as the research object, 3des-ecc algorithm is applied to the information transmission encryption of the mobile network voice collector. An improved speech signal collector is designed, which combines 3DES and ECC algorithm to realize the encryption of speech transmission information. An improved voice signal collector is designed, which combines 3DES and ECC algorithm to realize the encryption of voice transmission information. In the process of encryption, 168-bit random key is generated first, and it is grouped according to 56 bits as 3DES key, and then the plaintext is encrypted by the key to generate ciphertext; the random key is encrypted by ECC public key of the receiver. The experimental results show that the encryption time of this method is less than 1 s, the data integrity is 93%, and the data loss rate is only 0.33%. It has better anti attack ability, fast encryption speed and good encryption effect.

Keywords 3DES-ECC · Voice collector · Transmission encryption · Mobile network · Hardware and software design · Security

1 Introduction

In recent years, with the popularity of mobile communication services, mobile phones and other mobile terminal devices have gradually penetrated into all aspects of people's lives. In addition to personal use, mobile voice services have also brought a lot of convenience to administrative, military, business and other fields [1, 2]. While the public enjoy the convenience brought by mobile voice service, they also face the problem of communication security that can not be ignored. The eavesdropping of voice content is one of the most common security issues. Nowadays, with the improvement of public security awareness, the call security of mobile terminals has become a research hotspot in the field of information security [3]. The voice of mobile communication network users will pass through mobile terminal equipment, air wireless transmission, base station, trunk line and other facilities and links, among which there are many potential security

threats [4]. Although corresponding security mechanisms are provided in the design of mobile communication network to protect the security of data, there are loopholes in these security mechanisms that may lead to message leakage. The threat of voice content theft in mobile communication network mainly comes from the eavesdropping of attackers in wireless link or core service network [5]. With the popularity of intelligent mobile terminals, the security problems inside mobile terminals are increasingly prominent, which can not be ignored. A group of data from the national computer network emergency technology processing and coordination center shows that there are more than 6600 theft incidents caused only by malicious eavesdropping software every day [6, 7]. This kind of eavesdropping software is just a mixture of mobile Trojan and recording software. After installation, there is no main interface, and it is difficult to find the trace of installation. The whole transformation, redesign of mobile communication network and the transformation of mobile terminals are common in all kinds of mobile communication security schemes. Because network data encryption is of great significance to information security and other aspects, relevant personnel in this field have invested in the research and obtained many excellent results. Most of the research results ignore the risk of information leakage in the process of voice acquisition, and the relevant research results have some limitations.

✉ Marcin Woźniak
marcin.wozniak@polsl.pl

¹ Department of Information Engineering, Xi'an University of Posts & Telecommunications, Xi'an 710000, China

² Faculty of Applied Mathematics, Silesian University of Technology, 44-100 Gliwice, Poland

In reference [8], a 128-bit chaotic encryption method for speech communication based on FPGA is proposed. The algorithm uses the ID, creation time and number of concerns of the login user as the initial value and parameters of the encryption function, and obtains the key sequence through the interactive operation of two chaotic systems: Logistic map and Tent map. Due to the particularity of input parameters of voice collector, ciphertext is unpredictable [8]. In reference [9], a method of fully homomorphic encryption public key compression based on genetic algorithm is studied. An improved trapdoor generation algorithm is used to improve Stehle's selective plaintext attack (CPA) security scheme [9]. Then, combined with the fast compression function, a hybrid encryption public key compression scheme with indistinguishable (IND-CCA2) security and adaptive selective ciphertext attack in an untrusted environment is proposed. This method can be adaptively selected Encryption public key compression scheme, but the encryption time is limited by the encryption algorithm, and a larger size public key must be generated. The complexity and encryption efficiency of the encryption public key compression scheme is low. In reference [10], an extended AES with DH key exchange is proposed to enhance VoIP encryption in mobile networks. With the development of VoIP, the application of VoIP based on SIP protocol is increasing. However, because SIP protocol is highly dependent on open IP network, its security has gradually become the focus of attention and discussion. This paper mainly analyzes some security threats faced by SIP protocol network, including typical external attack technology and loopholes in the protocol itself. This paper discusses the encryption, authentication and other security policies proposed in response to sip security threats, analyzes the advantages and disadvantages of these security policies, and puts forward the direction for further improvement of SIP security policies, aiming to continuously improve the security performance based on SIP protocol [10].

The above methods solve a lot of security problems in network communication, but the anti-attack ability of voice acquisition process is poor, and the encryption effect is poor. Therefore, a new type of voice collector is designed by combining 3DES and ECC. 168-bit key is randomly generated and grouped according to 56 bits. This key is used as 3DES key to encrypt plaintext and generate ciphertext. ECC public key of the receiver is encrypted to realize voice transmission encryption in mobile network. The validity of the encryption method for voice transmission in mobile network is verified by experiments.

2 Voice transmission encryption based on 3DES-ECC algorithm in mobile network

Through the improvement of the voice collector, the hardware structure and the main program flow are designed. On this basis, the encryption algorithm of the voice collector is

designed to realize the transmission encryption of the whole mobile network voice.

2.1 Improved design and application of voice collector

2.1.1 Improvement on the design of voice signal collector

The voice acquisition system is composed of voice acquisition terminal, communication network and acquisition's main control terminal [11]. The voice acquisition terminal is composed of voice collector and voice input and output equipment. The communication network is PSTN. The main control terminal is composed of upper computer, local adapter and voice input and output equipment. Voice acquisition terminal and acquisition's main control terminal are connected with PSTN through telephone line. The local adapter is connected with the host computer through the network cable. Figure 1 shows the structure of voice acquisition system.

A plurality of voice collectors are connected with the public telephone network through the communication link, and then connect with the local adapter through the communication link, and then send the language to the host to complete the whole communication process. In this process, the risk of voice information leakage is very high, so we need to focus on it. Speech collector is an important part of speech acquisition system, and it is also the focus of the whole encryption process. Next, the design idea of the voice collector in this paper is introduced, including hardware design, speech compression coding scheme selection, software design and other aspects [12].

Figure 2 shows the principle block diagram of voice processing of voice collector.

Fig. 1 Structure of voice collector

Fig. 2 Schematic diagram of voice processing of voice collector

It can be seen from the analysis of Fig. 2 that when the language is input, the voice signal is first changed through low-pass filtering method, and then the voice is synthesized through D/A conversion, and the voice frame is split to encrypt the voice frame. Output speech is the inverse process of encryption. First, decrypt the speech frames, encapsulate the decrypted speech frames, synthesize the complete speech content, and then amplify the output speech through D/A conversion to obtain a higher quality speech signal and output the decrypted speech. The voice collector uses modem as the communication component, uses telephone line to connect the public telephone exchange network to transmit data, and also considers the monitoring of the line status. In this paper, a new voice signal generation model based on frequency domain is proposed, that is, multi-spectrum excitation model. The multi-spectrum excitation MBE model is a frequency domain model, which divides the frequency spectrum of a frame speech into several harmonic bands according to each harmonic frequency of the pitch, and then divides the frequency spectrum into several harmonic bands as a group to judge the voiced/unvoiced (V/U) of each band respectively [13]. The total excitation signal is composed of the sum of the excitation signals of each band. For the voiced band, the pulse sequence spectrum with the pitch period as the period is used as the excitation signal spectrum; for the unvoiced band, the white noise spectrum is used as the excitation signal spectrum. The function of the time-varying digital filter is to determine the relative amplitude and phase of each harmonic band, and to map

the mixed excitation signal spectrum to the spectrum [14]. This model makes the synthetic voice spectrum and the original voice spectrum fit well in the detailed structure, more in line with the characteristics of the actual voice, and the voice quality of the synthetic end is higher. The basic method is [15]: firstly, 160 digital voice sampling points of each frame are divided into overlapping segments, and the model parameters of the frame are obtained after the model. The encoder quantizes these model parameters, adds the error correction code, and then transmits them in a data stream of 2.4–9.6 kb/s. The decoder receives the bitstream, reconstructs the parameters of the model, and uses these parameters to generate the synthetic speech information. Figure 3 shows the signal generation model of MBE coding scheme.

The voice coding analysis model of MBE algorithm is shown in Fig. 4. In this algorithm, two effective methods, synthetic analysis and sensory weighting, are used to improve the accuracy of parameter analysis and extract pitch period T_p and spectral envelope parameters. Using smoothing technology to track the pitch of the first estimated pitch, the accuracy of the pitch is improved. According to the fitting error between the synthetic spectrum and the original spectrum, the unvoiced/voiced judgment information of a certain harmonic zone is determined. After uv/v is determined, the amplitude line X_m of each harmonic spectrum can be determined. For voiced sound spectrum, the spectral amplitude is equal to the

Fig. 3 Signal generation model of MBE coding scheme

Fig. 4 Voice coding model of MBE algorithm

optimal envelope modulus; for unvoiced sound spectrum, the spectral amplitude is the average spectral amplitude of the harmonic spectrum in the original voice spectrum.

Figure 5 shows the improved software structure of voice collector.

The underlying hardware control program is responsible for controlling the initialization configuration of peripheral chips and data reading and writing operations. The task processing program mainly completes the line status monitoring, communication link establishment, data transmission and other functions, while the main program completes the call of these task functions. From the perspective of CPU use, the software can be divided into interrupt processing program and query program [16]. In order to be able to process the transmission of voice signal coding and compression coding data in real time, the data transmission among CPU, vocoder, modem chip and FPGA is completed by interrupt mode. The call of task function adopts the way of CPU polling. Each task is divided into several sub functions or sub phases, each sub function or sub phase corresponds to a state [17, 18]. The CPU circularly polls the task in the main program, and determines the processing operation according to the current state.

When the voice collector starts to collect the input voice signal, it is necessary to establish a communication link to transmit the voice coding data to the local adapter. The establishment of the communication link is completed by

Fig. 5 Software structure of voice collector

establishing a connection between the MODEM chip of the voice collector and the MODEM chip of the local adapter. The process of establishing the link connection (Fig. 6) is divided into the following steps:

Local adapter MODEM dials to contact voice collector MODEM;

Configure the working mode and setting register of the voice collector MODEM;

According to the communication protocol parameters set in the register, the voice collector modem and the local adapter modem conduct training and other operations according to the procedures set in the corresponding communication protocol;

The training is successful and the link connection establishment process is completed.

Figure 7 is the schematic diagram of V.32 protocol communication procedure.

2.1.2 Hardware design

The hardware composition of the voice collector is shown in Fig. 8. The microcontroller C8051F120, as the control core of voice collector, is responsible for line switching, program scheduling, data interaction between voice acquisition module and voice transmission module [19]. Voice acquisition module is mainly composed of voice codec chip AMBE-1000, A/D-D/A conversion chip CSP1027, audio amplification filter chip TLC2272 and voice signal amplification output chip LMX358.

The hardware composition of the local adapter is shown in Fig. 9. The hardware composition of the local adapter is similar to the voice collector, including CPU, voice acquisition module, voice transmission module, power module, line interface module, etc. In addition, the local adapter also adds memory module, PHY, RJ45 interface. The memory includes SRAM and FLASH, which are used to store voice data and program code respectively. PHY is a network card chip,

Fig. 6 Link connection establishment process

which is responsible for receiving and sending data when the local adapter communicates with the upper computer.

2.1.3 Software design

In the main cycle, there are three functions: line detection, system link building, voice signal acquisition and transmission. The line detection is responsible for detecting whether there is ringing signal on the line, controlling the internal relay state of voice collector, ending communication, and corresponding processing after the link is disconnected. System link building is responsible for the establishment of communication link between voice collector and local adapter [20]. Data transmission is responsible for all data communication between the voice collector and the local adapter. Each stage is divided into several states, and each stage has a global variable to hold the current state value. When executing the performance function, the corresponding subroutine is firstly called to execute the code according to the state. After executing the corresponding code, the state variable is reassigned according to the current state of the voice collector, and the execution of the program is exited in this stage to enter the

Fig. 7 Schematic diagram of V.32 protocol communication procedure

next stage. Figure 10 shows the main program flow of voice collector.

Analysis of Fig. 10 shows that the CPU needs to be initialized first to detect the hardware. If the self-test is successful, data initialization will be started, otherwise an error message will be thrown. After opening the interrupt, judge whether the response times are 3 times. If the result is yes, it will be automatically disconnected. Otherwise, it will return to the interrupt state and continue to cycle the response times. Set the link status. When the link connection is established successfully, set the transmission status for language transmission, judge whether the line is disconnected, and then connect automatically, reset the modem, and complete the acquisition process. Otherwise, go back to the previous step and continue with voice transmission.

Fig. 8 Hardware composition of voice collector

2.2 Encryption algorithm design of voice collector

On the basis of the above voice signal acquisition, the communication encryption of the voice collector is realized by combining 3DES and ECC.

2.2.1 3DES algorithm

3DES encryption mechanism is mainly for different data modules to achieve DES iterative encryption, with a total of 3 times. It is encrypted according to the 192 bits security key by four operations of replacement, XOR, substitution and

Fig. 9 Hardware composition principle of local adapter

Fig. 10 Main program flow of voice collector

shift, of which 168 bits are valid. The encryption process mainly includes:

$$C = ED3(DK2(EK1(P))) \quad (1)$$

The decryption process is:

$$P = DK1(DK2(DK2(C))) \quad (2)$$

Compared with the traditional DES encryption technology, it has more advantages, because in the traditional encryption process, 64 bit key is used, 56 bits of which are effective, and the resistance ability is less than 3DES, and 3DES has more advantages in encryption speed; especially in algorithm, it is simpler [21, 22]. However, in terms of defects, when using 3DES encryption and decryption, the key is the same, so the risk of key disclosure is relatively high. Therefore, in the

specific application, it needs to add key management, which is relatively complex.

2.2.2 ECC algorithm

Key obtaining: in ECC algorithm, the key is obtained by mathematical model, the most important one is elliptic curve equation, which has 160 bits in total [23]. The result can produce RSA1024 bit key, which has a very high security intensity, but it is relatively small in calculation, and it is fast and occupies less resources, which is suitable for higher-level encryption system. In the expression, generally, there is an elliptic equation $E: y^2 = x^3 + ax + b$ (P, Q are on the ellipse, the former is obtained from the latter). Therefore, the solution of the discrete logarithm k needs to be completed by the equation, whose equation is $Q = [k]P$. According to the definition, we can know that E is an elliptic curve on FP, the number of which satisfies $\#E(FP) = p + 1 + t$, and the error term $|t| < 2\sqrt{p}$. $g = \#E(FP) = p + 1 + t = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p} \right)$. Thus, when k is given, the public key $K = k * \#E(FP)$, where k is the private key. Its security can be judged by P value. When P increases, the security will also increase. Its defect is that the encryption speed will be affected. Generally, P can be selected near 200-bit according to comprehensive judgment.

Encryption operation method: in ECC algorithm design, elliptic encryption is completed by point multiplication, multiple point, point addition, modular multiplication and other series of operations [24, 25]. But it can be explained by three layers: interface layer, application layer, middle layer (such as complex mixed operation), and bottom layer (modular multiplication and other unitary operations). For example, modulo addition is directly performed by bitwise XOR operation and XOR gate, and square operation is directly rotated left by bitwise.

2.2.3 Voice encryption process based on 3DES-ECC algorithm

In many information systems, DES long plaintext encryption is commonly used, and its speed is better than 3DES. However, DES ciphertext will be conquered with the increase of CPU operation speed. Therefore, on the basis of reducing the development cost, the hybrid information encryption method based on 3DES-ECC algorithm can protect the security of network information, and its applicability is strong. For example, to transmit plaintext p to B through A, the encryption process is as follows:

There are four steps for A-sender: one is to generate 168 bit random key Kd; the second is to group it according to 56 bits as 3DES key K1, K2, K3; the third is to encrypt plaintext P through the key to generate ciphertext C; at this time, the random key is encrypted through B-receiver ECC public key.

B-receiver needs to complete three steps: one is to use private decryption to decrypt the envelope to get random key; the second is to group the key 56 bits to get 3DES key K1, K2, K3; the third is to use the key to decrypt ciphertext C to get clear text information P.

3 Experiment and discussion

3.1 Acquisition function test

In the process of testing the performance of encryption technology of voice transmission based on 3DES-ECC algorithm, the performance of voice signal acquisition and encryption are carried out respectively.

In order to test the work of the voice collector, a test system is built to simulate the working environment of the voice acquisition system and test the operation of the voice collector. The structure of the test system is shown in Fig. 11.

The test system consists of voice collector, small switch, local adapter and upper computer. Among them, small switch is used to simulate PSTN network, voice collector and local adapter are connected with small switch through telephone line. The upper computer is connected with the local adapter through the network cable, and the voice collector and the local adapter are connected with microphone and horn as the input and output components of voice.

The test results are shown in Table 1.

Fig. 11 Test system of acquisition function

Table 1 Test items and results of acquisition function

Test items	Result
Voice capture and playback function of voice collector	Normal
Data transfer function between voice collector and local adapter	Normal
Ringer signal detection and automatic pick-up	Normal
Data transmission between local adapter and host computer	Normal
Voice quality played by the voice collector and local adapter	Good
Communication duration of voice picker and local adapter	>24 h

In the process of voice signal acquisition, all functions operate normally, and the communication between the voice collector and the local adapter lasts for more than 24 h, showing good performance.

3.2 Encryption verification

3.2.1 Encryption effect

Taking a segment of voice as the test object, the voice transmission encryption in mobile network based on 3DES-ECC algorithm is realized by using Visual C++ 6. Figure 12 shows the principle of encryption test experiment. Figure 13 shows the original voice, encrypted voice and decrypted voice.

Through the analysis of the above process, we can see that after the encryption of the method in this paper, the voice changes significantly, which improves the security of voice transmission, and after the decryption, the decrypted voice and the original voice are in the same frequency, ensuring the accuracy of voice transmission.

The time of encryption process is tested, and the results are shown in Table 2.

In many experiments, the encryption time is less than 1 s, and the encryption speed is fast. This is because the encryption technology of voice transmission in mobile network based on

Fig. 12 Principle of setting up encryption test experiment **(a) Original voice** **(b) Voice after encryption** **(c) Voice after decryption****Fig. 13** Encryption effect

3DES-ECC algorithm has good overall performance. On the basis of reducing the development cost, the above research adopts the 3DES-ECC hybrid information encryption method, which integrates the advantages of the two encryption algorithms. It can protect the security of network information, has strong applicability, and can also do well with the increase of CPU operation speed.

On the basis of the above, the encryption time of different methods is detected, and the experimental results are shown as follows:

According to Fig. 14, the encryption time of different methods is different. When the number of iterations is 5, the encryption time of document [8] method is 13 s, the

Table 2 Results of encryption time test

Number of experiments	Time
1	0.070
2	0.160
3	0.240
4	0.320
5	0.401
6	0.480
7	0.551
8	0.641
9	0.435
10	0.569
11	0.632
12	0.324
13	0.548
14	0.426
15	0.541

encryption time of document [9] method is 7S, the encryption time of document [10] method is 9 s, but the encryption time of this method is only 0.4 s, and the encryption time of this method is shorter. When the number of iterations is 12, the encryption time of document [8] method is 15 s, the encryption time of document [9] method is 20s, the encryption time of document [10] method is 25 s, and the encryption time of this method is 0.32 s, which shows that the encryption speed of this method is the fastest. This is because the design of the encryptor is innovated, which improves the connection efficiency of the receiver's voice signal.

3.2.2 Comparison of data integrity

In order to further obtain the performance of encryption technology of voice transmission in network, the data integrity of different methods is tested, and the experimental results are shown as follows:

Fig. 14 encryption time of different methods. **Fig. 15** Data integrity of different methods

It can be seen from the analysis of Fig. 15 that the data integrity is different after encryption by different methods. When the amount of data is 5GB, the data integrity of the method in reference [8] is 69%, the data integrity the method in reference [9] is 78%, the data integrity the method in reference [10] is 87%, and the data integrity of the proposed method is 96%, so that the data integrity of the proposed method is the largest. With the increase of data encryption, the data integrity of the method in reference [8] is 68%, the data integrity of the method in reference [9] is 72%, the data integrity of the method in reference [10] is 73%, and the data integrity of the proposed method is 93%, which shows that the proposed method has the best data integrity. This is because the method in this paper generates a random key in the encryption process, and groups it according to 56 bits as a 3DES key, and then encrypts the plaintext through the key to generate a ciphertext, so that the integrity of the data is high and the interference is small.

Fig. 16 Data loss rate of different methods

3.2.3 Comparison of data loss rate

The results of data loss rate under different attack intensity coefficients are as shown in the figure.

Analysis of Fig. 16 shows that the data loss rate will increase with the increase of network attack intensity. When the strength coefficient of network attack is 0.2 (at this time, it is under strong attack), the data loss rate of the method in reference [8] is 0.9%, the data loss rate of the method in reference [9] is 1.6%, the data loss rate of the method in reference [10] is 1.8%, and the data loss rate of the proposed method is 0.05%. With the increase of strength coefficient to 1.5, the data loss rate of the method in reference [8] is 9.8%, the data loss rate of the method in reference [9] is 12%, the data loss rate of the method in reference [10] is 9.5%, and the data loss rate of the proposed method is less than 1%, only 0.33%, which shows that the proposed method has better anti-attack ability. This is because the method in this paper will generate random key. After grouping according to 56 bits, a new 3DES key is obtained, which makes the encryption process more complex. When receiving, ECC public key is used to encrypt the random key twice, so that the encrypted data has better anti attack ability.

4 Conclusions

In view of the practical needs, this paper proposes a encryption technology of voice transmission based on 3DES-ECC algorithm. The speech data encryption is realized by the combination of speech signal acquisition, 3DES algorithm and ECC algorithm. The following conclusions are drawn through experiments:

- (1) This method can effectively encrypt the voice transmission process. For many experiments, the encryption time is less than 1 s, the encryption speed is fast, and the encryption effect is good.
- (2) After encryption, the data integrity is high. When the data encryption amount reaches 50GB, the data integrity reaches 93%, and the encryption performance is good.
- (3) After encryption, the data loss rate is low. When the attack strength coefficient is 1.5, the data loss rate is only 0.33%, which has strong anti-attack ability.

In this paper, the design of the encryptor is innovated. By using the characteristics of 3DES and ECC algorithm that can generate random key to encrypt plaintext, the voice signal collector is improved to realize the encryption of voice transmission information.

In the future practice, we should learn computer and network technology as much as possible, make a reasonable network system structure and strengthen system management.

Relevant departments also need to increase the awareness of network information security, improve the analysis ability of network crime, increase technical training and learning, so as to provide a safer online environment for network users.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Hafsa A, Alimi N, Sghaier A, et al. (2017). A hardware-software co-designed AES-ECC cryptosystem[C]//2017 international conference on advanced systems and electric technologies (IC_ASET). IEEE, 50–54
2. Liu S, Wang S, Liu X, et al (2020) Fuzzy detection aided real-time and robust visual tracking under complex environments. IEEE Trans Fuzzy Syst. <https://doi.org/10.1109/TFUZZ.2020.3006520>
3. Sultan A, Yang X, Hajomer A A E, et al. (2018). Chaotic constellation mapping for physical-layer data encryption in OFDM-PON. IEEE photonics technology letters, PP:1–1
4. Hazzaa F, Yousef S, Sanchez E, et al. (2018). Lightweight and Low-Energy Encryption Scheme for Voice over Wireless Devices[C]//IECON 2018–44th Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2992–2997
5. Vaidyanathan S, Sambas A, Mamat M, WS MS (2017) Analysis, synchronisation and circuit implementation of a novel jerk chaotic system and its application for voice encryption. Int J Model Identif Control 28(2):153–166
6. Liu S, Wang Y, Zhang Q et al (2017) A VoLTE encryption experiment for android smartphones[C]//international conference on geo-spatial knowledge and intelligence. Springer, Singapore, pp 115–125
7. Liu S, Bai W, Liu G, et al. (2018) Parallel Fractal Compression Method for Big Video Data, Complexity, 2016976
8. Riyadi M A, Pandapota N, Khafid M R A, et al. (2018). FPGA-based 128-bit chaotic encryption method for voice communication[C]//2018 international symposium on electronics and smart devices (ISESD). IEEE, 1–5
9. Gavinho Filho J, Silva G P and Miceli C. (2016). A public key compression method for fully Homomorphic encryption using genetic algorithms[C]//2016 19th international conference on information FUSION (FUSION). IEEE, 1991–1998
10. Zaghal R, Salah S, Jabali N (2018) Extending AES with DH key-exchange to enhance VoIP encryption in Mobile networks[C]// world conference on information systems and technologies. Springer, Cham, pp 511–521
11. Bi M, Fu X, Zhou X et al (2017) Chaotic nonlinear encryption scheme for CPAs resistance and PAPR reduction in OFDM-PON. IEEE Photon Technol Lett 29:1–1
12. Gao S, Li Z, Xiao B, et al. (2018). Security threats in the data plane of software-defined networks. IEEE Network, PP: 1–6

13. Hayati N, Suryanto Y, Ramli K, et al. (2019). End-to-end voice encryption based on multiple circular chaotic permutation[C]//2019 2nd international conference on communication engineering and technology (ICCET). IEEE, 101-106
14. Ridha OALA, Jawad GN, Kadhim SF (2018) Modified blind source separation for securing end-to-end Mobile voice calls. *IEEE Commun Lett* 22(10):2072–2075
15. El Bakry HM, Taki El Deen AE, El Tengy AH (2016) Implementation of an encryption scheme for voice calls. *International Journal of Computer Applications* 144(2):24–27
16. Wang Y and Tan Z. (2018). Modified RSA encryption algorithm based on chaos and its application in voice encryption system[C]//2018 14th international conference on computational intelligence and security (CIS). IEEE, 439-444
17. Mondal S and Sharma R K. (2019). Application of advanced encryption standard on real time secured voice communication using FPGA[C]//2019 10th international conference on computing, communication and networking technologies (ICCCNT). IEEE, 1-6
18. Shuai L, Chunli G, Fadi A. T, et al (2020). Reliability of response region: a novel mechanism in visual tracking by edge computing for IIoT environments, *Mech Syst Signal Process*, 138: 106537
19. Liu J and Cheng Y. (2017). The design and simulation of real-time encryption algorithm for Mobile terminal voice source[C]//2017 international conference on computer systems, electronics and control (ICCSEC). IEEE, 1016-1021
20. Yarman B S, Ulger C and Aslan A B. (2017). SYMPES technique encoded IP-based secure voice communication system[C]//2017 international symposium on signals, circuits and systems (ISSCS). IEEE, 1-3
21. Misra C and Hota M K. (2018). Hybrid technique for voice recognition, encryption and analysis using MATLAB[C]//2018 international conference on communication and signal processing (ICCSP). IEEE, 200-203
22. Zheng P, Shuai L, Arun S et al (2018) Visual attention feature (VAF) : A novel strategy for visual tracking based on cloud platform in intelligent surveillance systems. *Journal of Parallel and Distributed Computing* 120:182–194
23. Hu X, Zhang L, Huang T, et al. (2018). A security evaluation method for voice-over-IP streaming media information hiding[C]//2018 14th international conference on computational intelligence and security (CIS). IEEE, 228-232
24. Mota A V, Azam S, Shanmugam B, et al. (2017). Comparative analysis of different techniques of encryption for secured data transmission[C]//2017 IEEE international conference on power, control, signals and instrumentation engineering (ICPCSI). IEEE, 231-237
25. Liu S, Liu G, Zhou H (2019) A robust parallel object tracking method for illumination variations. *Mobile Networks and Applications* 24(1):5–17

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.