Synergy: Cross-Disciplinary Journal of Digital Investigation
(ISSN 2995-4827) VOLUME 02 ISSUE 6, 2024

A COMPREHENSIVE REVIEW OF VOICE ENCRYPTION TECHNIQUES

Ravinder
Student, ECE, Sat Kabir Institute of Technology and Management, Bahadurgarh, Haryana

Sumit Dalal, Sumiran
Assistant Professor, ECE, Sat Kabir Institute of Technology and Management, Bahadurgarh

Rohini Sharma
Assistant Professor, GPGCW, Rohtak

Abstract:

This paper presents a comprehensive review of voice encryption techniques, focusing on the various methods and algorithms developed to secure voice communication. Voice encryption is critical in ensuring the privacy and security of conversations, particularly in sensitive applications such as military communications, confidential business discussions, and personal privacy. The review covers traditional and contemporary encryption methods, analyzing their strengths, weaknesses, and applicability in different scenarios. Key aspects such as computational efficiency, resistance to attacks, and quality of the encrypted voice signal are examined. Furthermore, emerging trends and future directions in voice encryption are discussed, providing insights into the potential advancements and challenges in this evolving field. This review aims to serve as a valuable resource for researchers and practitioners seeking to understand the current state and future prospects of voice encryption technologies.

Keywords: Fading Channel, Wireless Communication, Rayleigh Fading; Rician Fading.

Introduction: Voice encryption is a critical component of modern communication systems, providing essential security for voice data transmitted over various networks. As the proliferation of digital communication increases, so does the necessity for robust encryption methods to protect sensitive information from unauthorized access and eavesdropping. Voice encryption ensures the confidentiality, integrity, and authenticity of spoken communications, making it indispensable in sectors such as military, governmental, corporate, and personal communications[1].

Historically, voice encryption methods have evolved from simple analog scrambling techniques to sophisticated digital algorithms. Early techniques, such as frequency inversion and time-domain

scrambling, offered limited security and were relatively easy to break. With the advent of digital signal processing and cryptographic algorithms, more secure and efficient methods have been developed. Modern voice encryption leverages advanced techniques such as symmetric and asymmetric cryptography, often employing protocols like Secure Real-Time Transport Protocol (SRTP) to ensure secure voice transmission over the Internet Protocol (IP) networks[2]. Symmetric encryption algorithms, including Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) [3], are commonly used for their high speed and efficiency in encrypting real-time voice data. Asymmetric encryption, although computationally intensive, is also utilized for key exchange mechanisms, ensuring that the encryption keys themselves are securely transmitted. Techniques such as RSA (Rivest-Shamir-Adleman) [4]and Elliptic Curve Cryptography (ECC) are prominent examples in this domain[5]. Voice encryption faces unique challenges compared to other forms of data encryption. The need for real-time processing, low latency, and minimal computational overhead are crucial for maintaining the quality and usability of voice communication. Additionally, encrypted voice signals must be resilient against various attacks, including replay attacks, man-in-the-middle attacks, and signal interference[6].

Attacks like eavesdropping, man-in-the-middle (MitM), and spying malware are very common in voice communication. An eavesdropping attack occurs when someone listens in on a discussion without the individuals involved knowing or agreeing to the intercept. When an attacker listens in on a discussion between two people, they can record or alter it. This is known as a MitM attack. An attack using spying malware (spyware) occurs when malicious software is put straight into communication devices and gathers data from them, including voice data, without the user's knowledge or agreement [7]. Considering the communication network's high level of security, a spyware assault makes the device untrustworthy. Despite the implementation of security protocols by well-established networks like GSM and VoIP, security weaknesses persist. For example, the GSM network's A5 algorithm is vulnerable to hacking [8], and security flaws have been noted in commercial VoIP communications [9]. Moreover, an end-to-end voice security system is not offered by the current one [10]. It follows that the user must have faith in third-party services and cell operators.

In this review, we explore the diverse landscape of voice encryption techniques, providing a detailed analysis of their mechanisms, advantages, and limitations. By examining both historical and contemporary methods, we aim to offer a comprehensive understanding of how voice encryption has developed and where it is headed in the future. Emerging trends and future directions in voice encryption are also discussed, highlighting the ongoing advancements and potential challenges in this field.

Related Research work

A few studies assessing the state of confidential audio, secure communication, and secure voice communication today can be found in the available research. A review article on security solutions for voice communication, particularly in relation to GSM mobile networks and Voice over IP technology, was released in [10]. The study looks into both commercial and research-level options. This article claims to be the first to classify and thoroughly assess speech encryption strategies for mobile networks. Certain publications that have been evaluated provide solutions for end-to-end data communication security rather than end-to-end voice communication security. In these situations, voice is not directly represented by the bit-stream. The bit-stream is sent over the voice channel after being encrypted and modulated into a signal that resembles speech.

Authors in [11] reviewed earlier audio steganography-based techniques. The analysis revealed that most studies used the Least Significant Bit (LSB) method to secure sensitive data, combining it with additional encryption schemes to fortify the LSB family. Two categories of audio steganography were established: audio file concealment within a cover audio file and any kind of secret data

concealment within a cover audio file. The topic of this work is restricted to secure voice communication, and the evaluation parameters used are infrequently used in all reviewed papers.

A study of audio cryptography methods was done by the authors in [12], with a particular emphasis on different methods of encryption and decoding that use chaotic maps. The evaluation examines current advancements in audio encryption and rates the methods according to three criteria: quality, computational difficulty, and security. It observes that chaotic maps a common method for protecting digital and analog voices is encryption. This paper's evaluation is restricted to the degree of randomness and security. Furthermore, voice communications encryption methods are not really covered in this work. The latest review paper, written in 2022 and published by [13], covers covert communication strategies, covering the newest developments, difficulties, and potential paths. The conversation on voice communication security is not thorough and targeted because of the survey's wide purview. Moreover, the communication security approaches covered in this study are limited to steganography methods; cryptography is not included in this list.

Three categories comprise the prior research work: Steganography, Modem-based Cryptography, and Chaotic Cryptography. The methods used by these three groups to increase safety of voice communication differ. Papers that suggest hiding the secret voice within the cover speech to secure voice communication fall under the Steganography group. Papers in the Modem-based Cryptography category suggest using modem techniques like Codebook Optimization, Optimized Modulation, Parameter Mapping, and Hardware Codec to modulate encryption results so they sound like speech in order to secure voice conversations. Papers that suggest using mathematical chaos theory in cryptography to secure voice communications are included in the category of Chaotic Cryptography.

CLASSIFICATION OF VOICE ENCRYPRTION METHODS

STEGANOGRAPHY

The cryptography methodology has many drawbacks, including the assurance of the existence of secret information and the challenges of retrieving secret information in the event of a signal processing attack or distortion caused by technologies like noise addition, compression, cropping, and resampling[14]. The hidden information can be restored with the least amount of mistake since the steganography methodology hides the existence of the confidential data and shows strong robustness to the signal processing distortion. Two methods are available for preparing the secret speech for the embedding process in secure voice communication based on steganography: segmentation and compression. In order to decrease hiding capacity, the hidden speech is compressed using the compression method. The cover audio is segmented using the same segmentation type as the secret speech in the segmentation procedure. Then, the segmented or compressed secret speech is embedded into the appropriately processed cover audio.

Voice steganography (Figure 1) is a method used to conceal secret information within a voice signal in such a way that it is imperceptible to human listeners and difficult for malicious actors to detect. Unlike encryption, which scrambles the content of a message to make it unreadable without a decryption key, steganography hides the existence of the message itself. This dual approach enhances security by not only protecting the content but also concealing the fact that a secret communication is taking place. Different types of voice encryption methods are demonstrated in Figure 2.

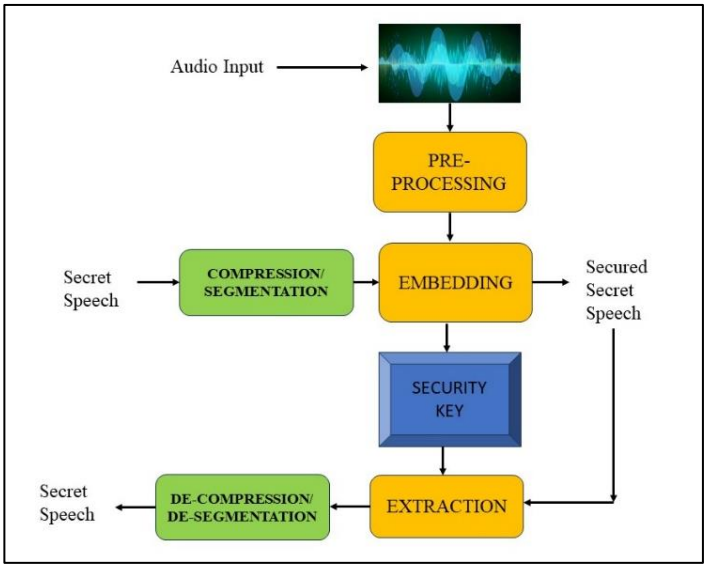

Figure 1: Steganography Process

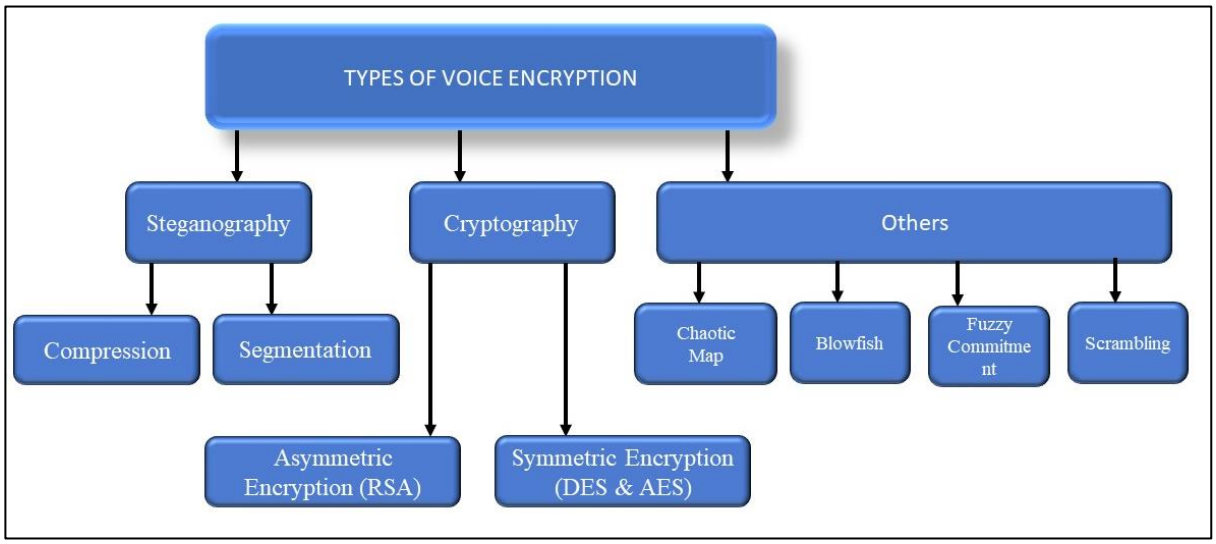

Figure 2: Different types of Voice Encryption Methods

Techniques in Voice Steganography

Several techniques are employed in voice steganography to embed information within audio signals:

1. **Least Significant Bit (LSB) Encoding**:

- This is one of the simplest and most widely used techniques. LSB encoding involves modifying the least significant bits of the audio samples to embed the secret information. Since changes in the least significant bits have minimal impact on the overall audio quality, this method is highly effective for maintaining the perceptual transparency of the steganographic message [15].

2. **Phase Coding**:

- Phase coding works by altering the phase of an audio signal. The secret message is encoded in the phase spectrum of the audio signal, which is less sensitive to modifications than the amplitude spectrum. This method is robust against common audio processing attacks such as compression [16].

3. **Echo Hiding**:

- Echo hiding introduces echoes into the original audio signal to encode the secret information. The parameters of the echo, such as the delay and amplitude, are varied according to the secret data. This method leverages the fact that small echoes are perceptually masked by the original signal, making them difficult to detect[17].

4. **Spread Spectrum**:

- Spread spectrum steganography embeds the secret message by spreading it across the frequency spectrum of the audio signal. This technique distributes the information over a wide range of frequencies, making it resilient to various forms of signal degradation and attack[18].

Table 1: A comparative review of Steganography research work

Paper	Method of Speech Security	Key Contributions	Application
[19]	➢ compression using dynamic time warping (DTW) recognition. ➢ Encoded and embedded in the host speech through Discrete Fourier Transform (DFT) ➢ Information Hiding	Development of real-time secure communication system, Speech recognition for authentication and encryption, Experimental validation	Real-time secure voice communication, Military and confidential business communications
[20]	Compressed Sensing Information Hiding,	Integration of information hiding and compressed sensing, Efficient compression and encryption, Maintenance of voice quality	Secure voice communication with limited bandwidth, Mobile networks
[21]	Sound Masking, Speech Corpus	Introduction of sound masking techniques, Utilization of speech corpus, Evaluation in different scenarios	Speech privacy protection in public or crowded spaces
[22]	Modified Blind Source Separation (BSS)	Enhancement of traditional BSS methods, Focus on voice quality and security, Experimental validation	Securing mobile voice calls, Relevant for mobile network operators and users
[1]	Steganography, Modem-based Cryptography, Chaotic Cryptography	Comprehensive review of various techniques, Comparison of methods, Integration into real-world applications	Resource for researchers and developers, Enhanced security methods

CRYPTOGRAPHY BASED VOICE ENCRYPTION

RSA-based Voice Encryption

It is an Asymmetric Encryption. It uses public key for encryption, Private key for decryption. Security relies on the difficulty of factoring large integers. It provides Secure voice communication in sensitive environments secure key exchange for symmetric encryption systems[23].

Encryption Phase:

- Convert voice data into a numeric format (e.g., PCM).
- Split the numeric data into blocks such that each block is smaller than nnn.

- Encrypt each block using the public key

$$c = m^e mod\ n \quad (1)$$

Decryption Phase

- Receive the encrypted blocks.
- Decrypt each block using the private key

$$m = c^d mod\ n \quad (2)$$

- Convert the decrypted numeric data back into the original voice format.

Implementing RSA in real-time voice communication requires efficient algorithms and possibly dedicated hardware to handle the computational load. Hybrid approaches can use RSA to securely exchange symmetric keys, which then encrypt the actual voice data for better performance.

AES-based Voice Encryption

AES (Advanced Encryption Standard) is a symmetric encryption algorithm widely used for securing data, including voice communications. It provides robust security and efficient performance, making it suitable for real-time applications. A single key used for both encryption and decryption. AES operates on fixed-size blocks (128 bits) and supports key lengths of 128, 192, or 256 bits. Generate a symmetric key. The key length can be 128, 192, or 256 bits, with AES-128 being the most commonly used for real-time applications due to its balance of security and performance[24].

Encryption Phase:

- Convert the voice data into a digital format, such as Pulse Code Modulation (PCM).
- Split the digital voice data into 128-bit blocks.
- Encrypt each block using the AES algorithm

$$C_i = AES_{encryption}(K, P_i) \quad (3)$$

Where $C_i$is the ciphertext block, K is the symmetric key, and P_i is the plaintext block.

- Transmit the encrypted blocks over the communication channel.

Decryption Phase

- Receive the encrypted blocks.
- Decrypt each block using the AES algorithm

$$P_i = AES_{Decryption}(K, C_i) \quad (4)$$

Where P_i is the plaintext block. Convert the decrypted digital data back into the original voice format. AES security is based on multiple rounds of substitutions, permutations, and mixing of the input data, making it resistant to various cryptographic attacks. The security level increases with the key length.

DES-based Voice Encryption Overview

DES (Data Encryption Standard) is a symmetric key encryption algorithm that has been widely used for securing data, including voice communications. A single key used for both encryption and decryption. DES operates on fixed-size blocks of 64 bits and uses a 56-bit key for encryption and decryption. Generate a 56-bit symmetric key. DES keys are typically derived from a longer key that includes 8 parity bits, resulting in a total of 64 bits, but only 56 bits are used for encryption[25].

Encryption Phase

- Convert the voice data into a digital format, such as Pulse Code Modulation (PCM).
- Split the digital voice data into 64-bit blocks.
- Encrypt each block using the DES algorithm

$$C_i = DES_{encryption}(K, P_i) \quad (5)$$

- Transmit the encrypted blocks over the communication channel.

Decryption Phase

- Receive the encrypted blocks.
- Decrypt each block using the DES algorithm

$$P_i = DES_{Decryption}(K, C_i) \quad (6)$$

- Convert the decrypted digital data back into the original voice format.

Table 2: comparison of RSA, DES, and AES based voice encryption methods

Encryption Method	Algorithm	Key Features	Advantages	Disadvantages	References
RSA (Rivest-Shamir-Adleman)	Asymmetric encryption	Uses a pair of public and private keys for encryption and decryption, Strong security based on factoring large integers	High security, Public key distribution is easier	Computationally intensive, Slower than symmetric algorithms, Larger key sizes required	[23]
DES (Data Encryption Standard)	Symmetric encryption	56-bit key, Block cipher that encrypts data in 64-bit blocks, Uses a series of permutations and substitutions	Simplicity and ease of implementation, Faster encryption and decryption compared to RSA	Short key length makes it vulnerable to brute-force attacks, Not recommended for high-security applications	[26]
AES (Advanced Encryption Standard)	Symmetric encryption	Variable key lengths (128, 192, 256 bits), Block cipher that encrypts data in 128-bit blocks, Uses multiple rounds of substitution, permutation, and mixing	High security, Efficient performance, Resistant to various attack types, Flexible key lengths	More complex implementation than DES, Requires careful key management	[25]

CHAOTIC CRYPTOGRAPHY

Chaotic cryptography leverages the properties of chaotic systems to secure data, including voice communications. Chaotic systems are highly sensitive to initial conditions, making them suitable for encryption due to their inherent randomness and complexity. It has mathematical functions that exhibit chaotic behavior, such as the logistic map, Lorenz system, and Chen system. Initial Conditions and Parameters serve as keys in chaotic cryptography. Small changes in these values result in significant differences in the output, ensuring high sensitivity and security[27].

Encryption Phase

- Convert the voice data into a digital format, such as Pulse Code Modulation (PCM).

- Generate a chaotic sequence using the defined chaotic map and initial conditions.
- Combine the chaotic sequence with the voice data using operations such as XOR:

$$C_i = P_i \otimes S_i \quad (7)$$

The chaotic sequence is S_i.

Decryption Phase

- Using the same initial conditions and parameters, regenerate the chaotic sequence.
- Combine the received encrypted data with the chaotic sequence to retrieve the original voice data using equation (7).
- Convert the decrypted digital data back into the original voice format.

Chaotic systems provide security through their sensitivity to initial conditions and parameters, making it difficult for an attacker to reproduce the chaotic sequence without knowing the exact values. The unpredictability and complexity of chaotic maps add an extra layer of security.

Table 3: comparison of CHAOTIC CRYPTOGRAPHY based voice encryption methods

References	[28]	[29]	[30]	[31]	[32]
Encryption Basis	Digital Signal Processor (DSP)	Chaotic System	Real-time Encryption Algorithm for Mobile Terminals	Chaotic Encryption Using FPGA	Circular Chaotic Permutation
Key Features	➢ Utilizes DSP for secure voice communication ➢ Focus on efficient processing and real-time performance	Utilizes chaos theory for encryption Emphasizes	robustness against attacks	➢ Uses FPGA for implementing chaotic encryption ➢ 128-bit key length	➢ Multiple circular chaotic permutations ➢ Emphasis on end-to-end encryption
Strengths	➢ Efficient processing ➢ Suitable for real-time communication	➢ High security due to chaotic properties ➢ Robust against traditional cryptographic attacks	Real-time performance Focus on mobile applications	➢ High security from chaotic properties ➢ Hardware implementation for efficiency	High security with multiple permutations Ensures end-to-end encryption
Weaknesses	Potentially limited by DSP hardware capabilities	Complexity in implementing and managing chaotic systems	➢ Specific to mobile terminals ➢ May not be generalized for other platforms	➢ Requires specialized hardware (FPGA) ➢ Potential complexity in hardware implementation	➢ Complexity in managing chaotic permutations ➢ Performance overhead
Applications	Secure voice communication in systems with DSP	Secure voice communication leveraging chaotic systems	Real-time voice encryption for mobile devices	Secure voice communication with hardware acceleration	Secure end-to-end voice communication
Implementation Complexity	Moderate	High	Moderate	High	High

Table 4: Comparative Table of Various Security Techniques

Aspect	**Steganography**	**DES**	**RSA**	**Scrambling Techniques** [33]	**Blowfish Data Encryption** [34]	**Fuzzy Commitment Based Voice Encryption**[35]	**Chaotic Maps**
Purpose	Conceal the existence of data	Encrypt data for confidentiality	Encrypt data for confidentiality and authenticity	Obfuscate data for security	Encrypt data for confidentiality	Encrypt voice data with fuzzy commitment	Secure data using chaos theory principles
Security Mechanism	Hides data within another file	Symmetric key encryption	Asymmetric key encryption	Rearranges data elements to obscure meaning	Symmetric key encryption	Combines biometric data with cryptographic commitment	Uses deterministic chaotic systems
Key Type	Typically, none, or very simple keys	Symmetric (same key for encryption and decryption)	Asymmetric (public and private keys)	Typically none, relies on obfuscation pattern	Symmetric (variable key length)	Biometric features as key along with cryptographic key	Key based on initial conditions of chaotic system
Algorithm Complexity	Varies (simple to complex methods)	Moderate (56-bit key)	High (key lengths typically 2048 bits or more)	Generally simple to moderate	Moderate to high (variable key length)	Moderate to high (depends on biometric processing)	Can be complex depending on the chaotic system
Computational Efficiency	High efficiency especially with LSB	Efficient, but considered insecure by	Computationally intensive	High efficiency	Efficient	Efficient	Varies, generally efficient

		modern standards					
Resistance to Attacks	Depends on the method; LSB is weak, phase coding is stronger	Vulnerable to brute-force attacks, considered obsolete	Strong resistance to brute-force and cryptanalysis	Low to moderate, depending on scrambling method	Strong resistance, especially with longer keys	High resistance due to biometric data and cryptographic combination	High resistance due to sensitive dependence on initial conditions
Perceptual Transparency	High (if properly implemented)	*NA	NA	NA	NA	NA	NA
Data Embedding Capacity	Limited by the host file's characteristics	NA	NA	High, as it does not add data but rearranges it	NA	NA	NA
Latency	Low, suitable for real-time applications	Low	High due to complex calculations	Low, suitable for real-time applications	Low to moderate depending on implementation	Low to moderate	Low, suitable for real-time applications
Key Management	Simple (if any key is used)	Requires secure key distribution	Complex, requires secure key exchange and management	Simple to none	Requires secure key distribution	Complex due to involvement of biometric data	Depends on the implementation
Applications	Covert communication, watermarking	General data encryption	Secure data transmission, digital signatures	Secure communication, media content protection	General data encryption	Secure voice communication, biometric authentication	Secure communication, cryptography
Example Techniques	LSB, Phase Coding, Echo Hiding	Feistel network, 16 rounds	Modular exponentiation, prime factorization	Frequency hopping, time-domain scrambling	Feistel network, 16 rounds	Cryptographic commitment with error correction	Logistic map, Lorenz attractor

*NA: Not applicable

CONCLUSION

The selection of encoding technique relies upon the specific requirements of the application. For general-purpose voice encryption, Blowfish offers a good balance of security and efficiency. Chaotic maps provide high security for specialized applications but are complex to implement. Fuzzy commitment is best suited for error-tolerant applications like biometric data encryption. DES, while simple and fast, is generally not recommended owing to its vulnerability to brute-force attacks. In modern applications, using DES is often replaced with more secure algorithms like AES. RSA is best suited for secure key exchange due to its strong security properties and is typically used to protect the symmetric key in a hybrid encryption scheme. DES is more efficient for encrypting large datasets such as voice signals but is less secure by modern standards. It is often used in conjunction with RSA to leverage the strengths of both algorithms. In practical voice encryption systems, a hybrid approach is often employed where RSA encrypts the DES key, and DES encrypts the actual voice data, combining the benefits of both symmetric and asymmetric encoding.

REFERENCES

1. A. A. Pekerti, A. Sasongko, and A. Indrayanto, “Secure End-to-End Voice Communication: A Comprehensive Review of Steganography, Modem-based Cryptography, and Chaotic Cryptography Techniques,” *IEEE Access*, 2024.
2. A. Sayeed and A. Perrig, “Secure wireless communications: Secret keys through multipath,” in *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2008, pp. 3013–3016.
3. W. Diffie and M. E. Hellman, “New directions in cryptography,” in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, 2022, pp. 365–390.
4. R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
5. N. Koblitz, “Elliptic curve cryptosystems,” *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
6. D. Boneh and H. Shacham, “Group signatures with verifier-local revocation,” in *Proceedings of the 11th ACM conference on Computer and communications security*, 2004, pp. 168–177.
7. J. Scott-Railton, B. Marczak, B. Abdul Razzak, M. Crete-Nishihata, and R. Deibert, “Reckless

exploit: Mexican journalists, lawyers, and a child targeted with NSO spyware," 2017.

8. P. K. Gundaram, A. N. Tentu, and S. N. Allu, "State Transition Analysis of GSM Encryption Algorithm A5/1," *J. Commun. Softw. Syst.*, vol. 18, no. 1, pp. 36–41, 2022.
9. M. Srivastava, "WhatsApp voice calls used to inject Israeli spyware on phones," *Financ. Times*, vol. 13, 2019.
10. C. Ntantogian, E. Veroni, G. Karopoulos, and C. Xenakis, "A survey of voice and communication protection solutions against wiretapping," *Comput. Electr. Eng.*, vol. 77, pp. 163–178, 2019.
11. S. B. Sadkhan, A. A. Mahdi, and R. S. Mohammed, "Recent Audio Steganography Trails and its Quality Measures," in *2019 First International Conference of Computer and Applied Sciences (CAS)*, 2019, pp. 238–243.
12. E. A. Albahrani, T. K. Alshekly, and S. H. Lafta, "A review on audio encryption algorithms using chaos maps-based techniques," *J. Cyber Secur. Mobil.*, vol. 11, no. 1, pp. 53–82, 2022.
13. I. Makhdoom, M. Abolhasan, and J. Lipman, "A comprehensive survey of covert communication techniques, limitations and future challenges," *Comput. Secur.*, vol. 120, p. 102784, 2022.
14. S. S. Bharti, M. Gupta, and S. Agarwal, "A novel approach for audio steganography by processing of amplitudes and signs of secret audio separately," *Multimed. Tools Appl.*, vol. 78, no. 16, pp. 23179–23201, 2019.
15. M. Hussain and M. Hussain, "A survey of image steganography techniques," *Int. J. Adv. Sci. Technol.*, vol. 54, pp. 113–124, 2013.
16. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, no. 3.4, pp. 313–336, 1996.
17. D. Kirovski and H. S. Malvar, "Spread-spectrum watermarking of audio signals," *IEEE Trans. signal Process.*, vol. 51, no. 4, pp. 1020–1033, 2003.
18. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. image Process.*, vol. 6, no. 12, pp. 1673–1687, 1997.
19. Z. Deng, Z. Yang, and L. Deng, "A real-time secure voice communication system based on speech recognition," in *2006 International Conference on Systems and Networks Communications (ICSNC'06)*, 2006, p. 22.
20. T. Xu, Z. Yang, and X. Shao, "Novel speech secure communication system based on information hiding and compressed sensing," in *2009 Fourth international conference on systems and networks communications*, 2009, pp. 201–206.
21. D. Qi and N. Longmei, "A speech privacy protection method based on sound masking and speech corpus," *Procedia Comput. Sci.*, vol. 131, pp. 1269–1274, 2018.
22. O. A. L. A. Ridha, G. N. Jawad, and S. F. Kadhim, "Modified blind source separation for securing end-to-end mobile voice calls," *IEEE Commun. Lett.*, vol. 22, no. 10, pp. 2072–2075, 2018.
23. M. M. Rahman, T. K. Saha, and M. A.-A. Bhuiyan, "Implementation of RSA algorithm for speech data encryption and decryption," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 12, no. 3, pp. 74–82, 2012.
24. S. Mondal and R. K. Sharma, "Application of Advanced Encryption Standard on Real Time

Secured Voice Communication using FPGA," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2019, pp. 1–6.

25. Z. Chang and M. Woźniak, "Encryption technology of voice transmission in mobile network based on 3DES-ECC algorithm," *Mob. Networks Appl.*, vol. 25, pp. 2398–2408, 2020.
26. K. S. Mohamed and K. S. Mohamed, "Cryptography concepts: Confidentiality," *New Front. Cryptogr. Quantum, Blockchain, Light. Chaotic DNA*, pp. 13–39, 2020.
27. W. Dai, X. Xu, X. Song, and G. Li, "Audio encryption algorithm based on chen memristor chaotic system," *Symmetry (Basel).*, vol. 14, no. 1, p. 17, 2021.
28. H. Lei, Y. Zhao, Y. Dai, and Z. Wang, "A secure voice communication system based on DSP," in *ICARCV 2004 8th Control, Automation, Robotics and Vision Conference, 2004.*, 2004, vol. 1, pp. 132–137.
29. K. W. Tang and W. K. S. Tang, "A chaos-based secure voice communication system," in *2005 IEEE International Conference on Industrial Technology*, 2005, pp. 571–576.
30. J. Liu and Y. Cheng, "The Design and Simulation of Real-Time Encryption Algorithm for Mobile Terminal Voice Source," in *2017 International Conference on Computer Systems, Electronics and Control (ICCSEC)*, 2017, pp. 1016–1021.
31. M. A. Riyadi, N. Pandapotan, M. R. A. Khafid, and T. Prakoso, "FPGA-based 128-bit Chaotic encryption method for voice communication," in *2018 International Symposium on Electronics and Smart Devices (ISESD)*, 2018, pp. 1–5.
32. N. Hayati, Y. Suryanto, K. Ramli, and M. Suryanegara, "End-to-end voice encryption based on multiple circular chaotic permutation," in *2019 2nd International Conference on Communication Engineering and Technology (ICCET)*, 2019, pp. 101–106.
33. K. Madono, M. Tanaka, M. Onishi, and T. Ogawa, "Sia-gan: Scrambling inversion attack using generative adversarial network," *IEEE Access*, vol. 9, pp. 129385–129393, 2021.
34. M. abd ulkareem Nasser and I. Q. Abduljaleel, "Speech encryption using chaotic map and blowfish algorithms," *J. Basrah Res.*, vol. 39, no. 2A, 2013.
35. A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM conference on Computer and communications security*, 1999, pp. 28–36.