INTERNATIONAL JOURNAL OF
RECENT TRENDS IN MULTIDISCIPLINARY RESEARCH
March-April 2026, Vol 6(02), 474-480. ISSN No: 2583-0368

A Comprehensive Survey of Audio Security: Encryption and Watermarking Methods

Ashish Mishra[1], Dheeraj Chillar[2]
[1]*P.G. Student, Department of CSE, Sat Kabir Institute of Technology and Management, Ladrawan, Haryana, India.*
[2]*Director, Sat Kabir Institute of Technology and Management, Ladrawan, Haryana, India.*

OPEN ACCESS
Article Citation:
Ashish Mishra[1], Dheeraj Chillar[2], "A Comprehensive Survey of Audio Security: Encryption and Watermarking Methods", International Journal of Recent Trends in Multidisciplinary Research, March-April 2026, Vol 6(02), 474-480.

Abstract: With the rapid advancement of digital communication technologies, ensuring the security and integrity of audio data has become increasingly important. Audio signals are widely used in applications such as voice communication, multimedia transmission, and confidential information exchange, making them vulnerable to unauthorized access, tampering, and piracy. This survey provides a comprehensive review of audio security techniques, focusing on two major approaches: encryption and watermarking. Encryption methods are examined for their ability to ensure confidentiality and protect audio data during transmission. In parallel, watermarking techniques, including transform-based methods such as Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), are analyzed for their role in embedding hidden information to ensure data integrity, authentication, and ownership verification. The survey highlights the strengths, limitations, and application domains of each technique and discusses the trade-offs between security, robustness, and computational efficiency. Furthermore, recent advancements and challenges in the field are explored, providing insights into future research directions for developing more secure and efficient audio processing systems.

Key Words: Audio Security, Audio Watermarking, Secure Communication.

1. Introduction

With the rapid growth of digital communication and multimedia technologies, the need for secure transmission of audio signals has become increasingly important. Audio data is widely used in applications such as voice communication, broadcasting, teleconferencing, and secure information exchange, making it highly susceptible to unauthorized access, tampering, and piracy. As a result, ensuring the confidentiality, integrity, and authenticity of audio signals has become a critical research area.

Various techniques have been proposed to address audio security, with encryption and watermarking emerging as the two primary approaches. Encryption techniques aim to protect the confidentiality of audio data by transforming it into an unintelligible form. Early methods focused on scrambling techniques, such as Hadamard-based speech scrambling [6] and Fibonacci transformation-based audio scrambling [4]. More advanced approaches include compressed sensing-based encryption methods [1-2] and random matrix-based scrambling techniques [8], which enhance security and efficiency. Additionally, nature-inspired cryptographic methods have been explored to provide adaptive and robust encryption solutions [3], while quasigroup-based encryption techniques have demonstrated effectiveness in securing speech data [7]. Chaos-based encryption systems have also gained significant attention due to their sensitivity to initial conditions and strong security properties [9], [10].

In parallel, audio watermarking techniques have been developed to ensure data integrity, authentication, and copyright protection by embedding hidden information within the signal. The theoretical foundation of information hiding has been extensively studied, highlighting the trade-offs between robustness, capacity, and imperceptibility [5]. Transform-domain techniques, such as the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), have been widely adopted due to their ability to provide robust, imperceptible watermark embedding. Despite significant advancements, there remains a need for a comprehensive understanding of the strengths and limitations of different audio security techniques. Therefore, this survey aims to provide a detailed review of encryption and watermarking methods, analyzing their performance, applications, and challenges. By examining existing approaches, this work highlights key trends and identifies potential directions for developing more secure and efficient audio processing systems.

2. Research Background

The increasing reliance on digital communication systems has led to significant advancements in audio and speech security techniques, particularly in the areas of encryption and secure transmission. Early research in this domain focused on conventional cryptographic algorithms and signal scrambling methods to protect speech data. However, of cyber threats become increasingly complex, more sophisticated approaches have been developed to enhance security and robustness.

One prominent direction in recent research is the use of chaos-based encryption techniques, which leverage the sensitivity of chaotic systems to initial conditions. Farouk et al. [11] presented a comparative analysis of speech cryptosystems based on two-dimensional chaotic maps, demonstrating improved security performance over traditional methods. Similarly, Nasser and Abduljaleel [12] proposed a hybrid speech encryption scheme combining chaotic maps with the Blowfish algorithm, achieving enhanced confidentiality and resistance to attacks. Chaos-based techniques have also been applied beyond audio signals; for instance, Vishwakarma and Qureshi [13] used logistic chaos for secure video transmission, while Oğraş and Türk [14] developed a chaos-based image cryptosystem with improved key-generation mechanisms. Furthermore, chaotic functions have been employed in the design of secure cryptographic components, such as substitution boxes (S-boxes), as demonstrated by Belazi and Abd El-Latif [15].

In addition to chaos-based methods, traditional cryptographic algorithms remain widely used for speech and audio security. The Blowfish algorithm, known for its efficiency and simplicity, has been explored for secure audio applications [16]. Abd El-Sadek et al. [17] introduced a modified Blowfish algorithm specifically tailored for speech encryption, improving both security and performance. Similarly, RSA-based encryption has been applied to audio signals to provide strong asymmetric security [18]. A comprehensive review by Aparna and Chithra [19] highlights the strengths and limitations of various cryptographic algorithms for protecting speech signals, emphasizing the need for hybrid and adaptive approaches.

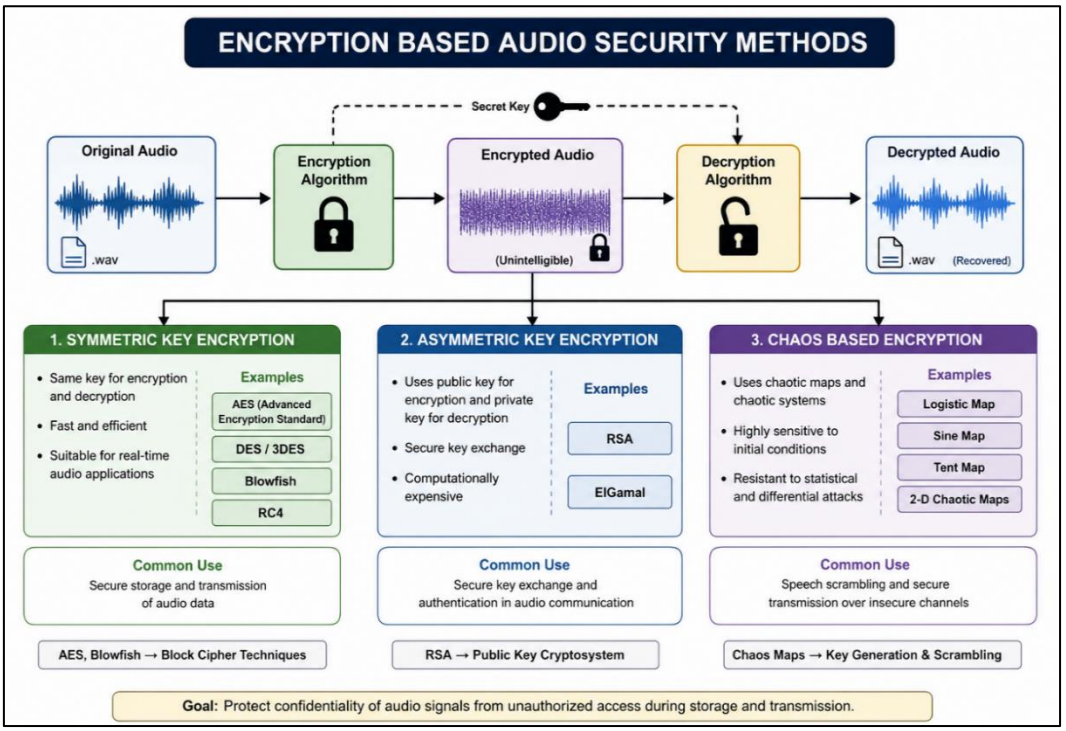
Beyond encryption, advanced security frameworks such as fuzzy commitment schemes have been proposed to enhance authentication and data integrity [20]. These methods combinecryptographic principles with error tolerance, making them suitable for real-world multimedia applications. Additionally, foundational studies in linguistics and speech processing [21] provide essential insights into the structure and characteristics of speech signals, which are critical for the design of effective encryption and watermarking techniques.

3. Encryption-Based Audio Security Techniques

Audio security techniques primarily rely on encryption methods to protect speech and audio data from unauthorized access during storage and transmission. Encryption transforms the original audio signal into an unintelligible format using a secret key, ensuring confidentiality. Traditional cryptographic algorithms such as AES, RSA, and Blowfish [23] are widely used due to their strong security properties. AES, as a symmetric-key algorithm [22], offers high speed and robustness, making it suitable for real-time audio applications. RSA, an asymmetric encryption method, provides secure key exchange but is computationally more intensive. Blowfish, known for its efficiency, has also been adapted for speech encryption with modifications to enhance performance.

In addition to conventional methods, chaos-based encryption [24] techniques have gained significant attention in recent years. These methods utilize the unpredictable and sensitive nature of chaotic systems to generate secure keys and perform signal scrambling. Techniques based on logistic, sine, and multi-dimensional chaotic systems provide high security and strong resistance to attacks. Hybrid approaches that combine traditional encryption with chaotic systems have also been proposed to improve both security and efficiency. Despite these advancements, challenges remain in achieving an optimal balance between security strength, computational complexity, and signal quality, especially for real-time audio applications. Therefore, modern research focuses on developing lightweight, efficient, and robust encryption techniques tailored specifically for audio signals.
Figure 1 presents an overview of encryption-based audio security methods, illustrating how audio data is protected during transmission and storage. The process begins with the original audio signal, which is encrypted using a secret key. This converts the audio into an encrypted (unintelligible) signal, ensuring that unauthorized users cannot interpret the data. At the receiver side, a decryption algorithm uses the appropriate key to recover the original audio signal.

The diagram further classifies encryption techniques into three major categories. The first is symmetric key encryption, where the same key is used for both encryption and decryption. Examples include AES, DES, and Blowfish. This method is fast and efficient, making it suitable for real-time audio applications. The second category is asymmetric key encryption, which uses a pair of keys—a public key for encryption and a private key for decryption. Algorithms such as RSA and ElGamal fall into this category and are mainly used for secure key exchange, although they are computationally more complex. The third category is chaos-based encryption, which utilizes chaotic systems such as logistic maps and sine maps to generate highly unpredictable keys. These methods are known for their sensitivity to initial conditions and strong resistance to attacks, making them suitable for secure audio transmission.



Feature	AES (Symmetric)	Blowfish (Symmetric)	RSA (Asymmetric)	Chaos-Based Encryption
Key Type	Single secret key	Single secret key	Public & Private keys	Secret key + chaotic parameters
Speed	Very High	High (slightly slower than AES)	Low (computationally heavy)	Moderate to High
Security Level	Very High (standardized)	High (strong but older)	Very High	High (depends on design)
Block Size	128 bits	64 bits	Variable	Not fixed
Key Length	128/192/256 bits	32–448 bits	1024–4096 bits	Depends on system
Complexity	Moderate	Low to Moderate	High	Moderate
Suitability for Audio	Excellent (real-time use)	Good (efficient for streaming)	Limited (mainly key exchange)	Good (scrambling applications)
Implementation	Easy and widely supported	Simple and flexible	Complex (key management required)	Moderate (mathematical modeling needed)
Robustness	Very strong	Strong but less modern than AES	Very strong	Strong if properly designed
Typical Use	Secure audio encryption	Lightweight audio encryption	Secure key exchange	Audio scrambling & secure transmission
Advantages	Fast, secure, widely accepted	Flexible key size, efficient	Secure key distribution	High randomness, lightweight
Limitations	Key sharing required	Smaller block size (less secure than AES)	Slow for large data	Less standardized

Table 1: Comparison of Encryption Methods for Audio Security

4. Watermarking-Based Audio Security Techniques

Audio watermarking is an essential technique for ensuring data integrity, authentication, and copyright protection in digital audio systems. Unlike encryption, which secures the content during transmission, watermarking embeds hidden information directly into the audio signal, allowing verification even after decryption. The fundamental challenge in watermarking is to achieve a balance between imperceptibility, robustness, and capacity, as highlighted in the information-theoretic framework proposed by Moulin and O'Sullivan [25].

Watermarking techniques are broadly classified into time-domain and transform-domain methods. Time-domain techniques directly modify audio samples and are simple to implement but are generally less robust against attacks such as noise addition and compression. In contrast, transform-domain techniques, such as Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), provide improved robustness and imperceptibility. DWT-based watermarking decomposes the signal into frequency components and embeds watermark data into selected coefficients, making it highly suitable for audio signals due to its ability to preserve both time and frequency characteristics. SVD-based watermarking, on the other hand, embeds information into the singular values of the signal matrix, which are stable and resistant to small perturbations. Several studies have demonstrated the effectiveness of transform-based watermarking methods. For instance, information hiding techniques have been extensively analyzed from a theoretical perspective in [25], while practical implementations of watermarking in multimedia systems have demonstrated that transform-domain methods offer better resistance to signal-processing attacks. Despite these advantages, challenges remain in maintaining high audio quality while ensuring strong robustness, especially under real-world conditions such as compression, filtering, and transmission noise.

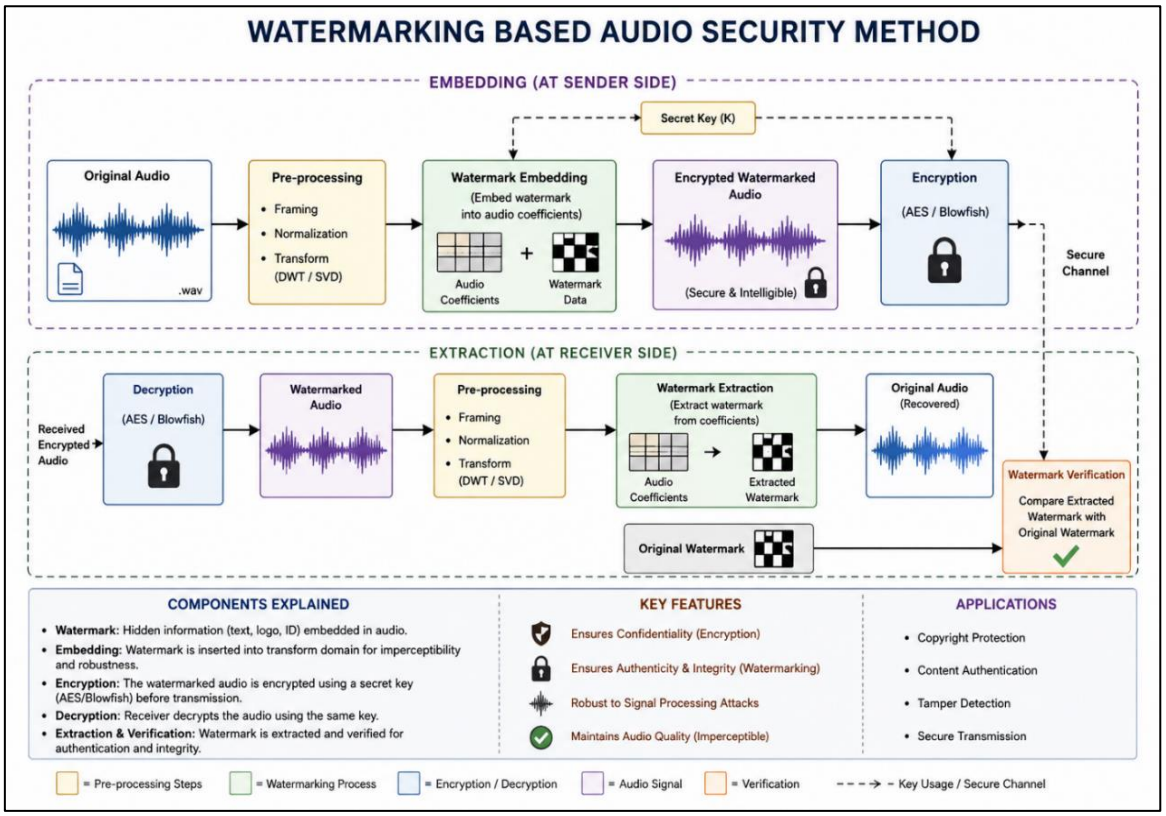


Figure 2: Watermarking-Based Audio Encryption

Figure 2 illustrates a watermarking-based audio security system combined with encryption, showing both the sender (embedding) and receiver (extraction) processes. At the sender side, the process begins with the original audio signal, which is preprocessed using steps such as framing, normalization, and transformations (e.g., DWT or SVD). A watermark (hidden information such as text, an ID, or a logo) is then embedded in the audio signal by modifying its transform coefficients. This produces a watermarked audio signal, which still maintains perceptual quality. To ensure confidentiality, the watermarked audio is further secured using an encryption algorithm (such as AES or Blowfish) with a secret key. The resulting encrypted watermarked audio is then transmitted over a secure channel. At the receiver side, the encrypted audio is first decrypted using the same key to recover the watermarked signal. The signal is then preprocessed again, and the embedded watermark is extracted from the transform coefficients. Finally, the extracted watermark is compared with the original watermark in the verification stage, ensuring authenticity and integrity of the audio signal. At the same time, the original audio signal is reconstructed for playback.

Feature	DWT-Based Watermarking	SVD-Based Watermarking	Time-Domain Watermarking
Working Domain	Frequency (time-frequency) domain	Matrix (linear algebra) domain	Time (sample) domain
Embedding Method	Modify wavelet coefficients	Modify singular values	Directly modify audio samples
Imperceptibility	High (minimal distortion)	Moderate to High	Low to Moderate
Robustness	High (resistant to noise & compression)	Moderate	Low
Audio Quality (SNR)	High	Moderate	Low
Computational Complexity	Moderate to High	Moderate	Low
Suitability for Audio	Excellent	Moderate	Limited
Resistance to Attacks	Strong	Moderate	Weak
Implementation Difficulty	Moderate	Moderate	Easy
Typical Use	Secure audio watermarking	Multimedia watermarking	Basic watermarking
Advantages	Good balance of quality & robustness	Stable embedding	Simple and fast
Limitations	Higher computation time	Signal reshaping may distort audio	Easily removed or degraded

Table 2: Comparison Of Watermarking-Based Audio Security Methods

5. Hybrid Techniques: Combination Of Encryption And Watermarking

With the increasing demand for secure and reliable multimedia communication, hybrid techniques that combine encryption and watermarking have gained significant attention. While encryption ensures confidentiality by transforming audio signals into an unreadable format, it does not provide mechanisms for verifying ownership or detecting tampering after decryption. On the other hand, watermarking embeds hidden information into the signal to ensure authentication, integrity, and copyright protection, but it cannot prevent unauthorized access. Therefore, integrating both approaches provides a dual-layer security framework that enhances overall system robustness.

In a typical hybrid system, the audio signal is first processed using a watermarking technique such as DWT or SVD, where a watermark is embedded into selected coefficients of the signal. The watermarked audio is then encrypted using a strong cryptographic algorithm such as AES or Blowfish before transmission. At the receiver side, the encrypted signal is first decrypted to recover the watermarked audio, followed by watermark extraction and verification. This ensures that the data remains secure during transmission and can be authenticated upon receipt. Hybrid techniques offer several advantages, including improved resistance to attacks, enhanced data integrity, and protection against unauthorized redistribution. Even if the encrypted data is intercepted, it remains unreadable, and even after decryption, the embedded watermark can verify ownership and detect tampering. However, these methods also introduce challenges such as increased computational complexity and the need to balance security, robustness, and audio quality.

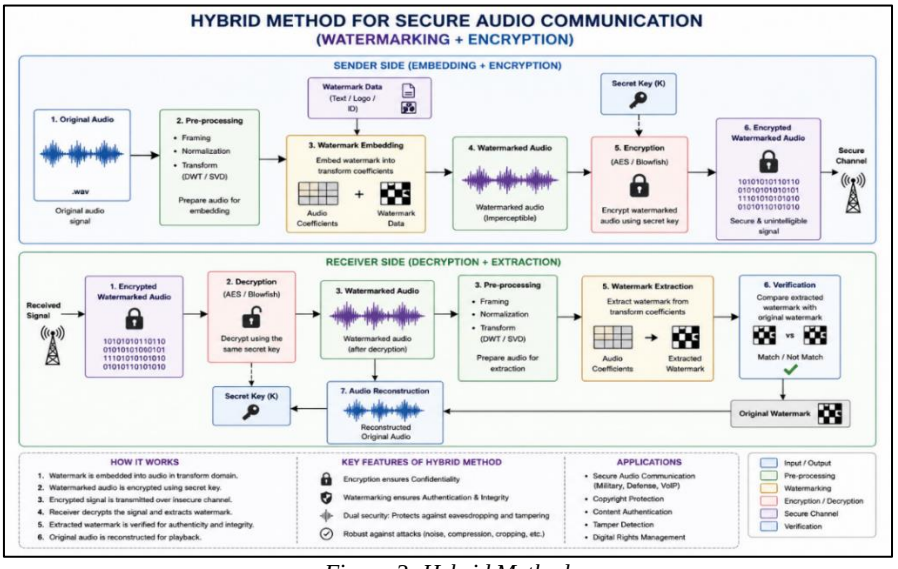


Figure 3: Hybrid Method

Figure 3 illustrates a hybrid audio security system that combines watermarking and encryption to provide dual protection for audio data. It is divided into two main parts: the sender side (embedding + encryption) and the receiver side (decryption + extraction). At the sender side, the process begins with the original audio signal, which is first preprocessed using steps such as framing, normalization, and transformations using techniques such as DWT or SVD. A watermark (such as text, a logo, or an ID) is then embedded in the audio by modifying its transform coefficients, producing a watermarked audio signal that maintains perceptual quality. This watermarked signal is then passed through an encryption stage (e.g., AES or Blowfish) using a secret key, resulting in an encrypted, unintelligible signal. The encrypted audio is then transmitted over a secure communication channel. At the receiver side, the process is reversed. The received encrypted audio is first decrypted using the same secret key, recovering the watermarked audio. The signal is again pre-processed, and the embedded watermark is extracted from the transform coefficients. A verification step compares the extracted watermark with the original watermark to confirm authenticity and integrity. Finally, the original audio signal is reconstructed for playback.

6. Conclusion

This survey provides a comprehensive overview of audio security techniques, focusing on encryption and watermarking methods for protecting digital audio data. With the increasing use of audio in communication systems, ensuring confidentiality, integrity, and authenticity has become a critical requirement. Encryption techniques such as AES, Blowfish, RSA, and chaos-based methods provide strong protection against unauthorized access by transforming audio signals into secure formats. In parallel, watermarking techniques, particularly transform-based approaches like DWT and SVD, enable the embedding of hidden information to support authentication, copyright protection, and tamper detection.

The study highlights that no single technique can fully address all security requirements. Encryption ensures confidentiality but lacks post-decryption verification, while watermarking provides authentication but does not prevent interception. Therefore, hybrid approaches that combine encryption and watermarking offer a more robust solution by integrating the strengths of both methods. Comparative analysis indicates that DWT-based watermarking is more suitable for audio signals due to its ability to preserve signal quality, while SVD shows limitations in maintaining audio fidelity. Similarly, symmetric encryption methods such as AES are preferred for real-time applications due to their efficiency and strong security. Despite significant advancements, challenges remain in achieving an optimal balance between security, computational efficiency, and audio quality, especially for real-time and large-scale applications. Future research should focus on developing lightweight, adaptive, and robust techniques, potentially incorporating machine learning and hybrid models to enhance performance. Overall, this survey provides valuable insights into existing methods and highlights the importance of integrated approaches for building secure and efficient audio communication systems.

Reference

1. L. Zeng, X. Zhang, L. Chen, Z. Fan, and Y. Wang, “Scrambling-based speech encryption via compressed sensing,” EURASIP J. Adv. Signal Process., vol. 2012, pp. 1–12, 2012.
2. Y. Chen, J. Hao, J. Chen, and Z. Zhang, “End-to-end speech encryption algorithm based on speech scrambling in frequency domain,” in *Third International Conference on Cyberspace Technology (CCT 2015)*, 2015, pp. 1–5.
3. J. A. Clark, “Nature-inspired cryptography: past, present and future,” in The 2003 Congress on Evolutionary Computation, 2003. CEC’03., 2003, vol. 3, pp. 1647–1654.
4. L. Nan, S. Yanhong, and Z. Jiancheng, “An audio scrambling method based on Fibonacci transformation,” J. North China Univ. Technol, vol. 16, no. 3, pp. 8–11, 2004.
5. P. Moulin and J. A. O’Sullivan, “Information-theoretic analysis of information hiding,” *IEEE Trans. Inf. theory*, vol. 49, no. 3, pp. 563–593, 2003.
6. V. Senk, V. D. Delic, and V. S. Milosevic, “A new speech scrambling concept based on Hadamard matrices,” IEEE Signal Process. Lett., vol. 4, no. 6, pp. 161–163, 1997.
7. M. Satti and S. Kak, “Multilevel indexed quasigroup encryption for data and speech,” *IEEE Trans. Broadcast.*, vol. 55, no. 2, pp. 270–281, 2009.
8. H. Li, Z. Qin, X. P. Zhang, and L. P. Shao, “An n-dimensional space audio scrambling algorithm based on random matrix,” J. Xi’an Jiaotong Univ, vol. 44, no. 4, pp. 13–17, 2010.
9. L. Huang and Q. Yin, “A chaos synchronization secure communication system based on output control,” 电子与信息学报, vol. 31, no. 10, pp. 2402–2405, 2009.
10. J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” *Int. J. Bifurc. chaos*, vol. 8, no. 06, pp. 1259–1284, 1998.
11. M. Farouk, O. Faragallah, O. Elshakankiry, and A. Elmhalaway, “Comparison of audio speech cryptosystem using 2-D chaotic map algorithms,” *Math. Comput. Sci.*, vol. 1, no. 4, pp. 66–81, 2016.
12. M. abd ulkareem Nasser and I. Q. Abduljaleel, “Speech encryption using chaotic map and blowfish algorithms,” *J. Basrah Res.*, vol. 39, no. 2A, 2013.
13. S. Vishwakarma and S. Qureshi, “Secure Transmission of Video using (2, 2) Visual Cryptography Scheme and Share Encryption using Logistic Chaos Method,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 3, no. 1, pp. 1502–1514, 2018.
14. H. Oğraş and M. Türk, “A secure chaos-based image cryptosystem with an improved sine key generator,” Am. J. Signal Process., vol. 6, no. 3, pp. 67–76, 2016.
15. A. Belazi and A. A. Abd El-Latif, “A simple yet efficient S-box method based on chaotic sine map,” Optik (Stuttg)., vol. 130, pp. 1438–1444, 2017.
16. K. Nagaraj, “Understanding Blowfish Encryption Algorithm.” https://cyberw1ng.medium.com/understanding-blowfish-encryption-algorithm-2023-24eb8f69f85b.
17. A. A. Abd El-Sadek, A. Talaat, and M. M. Fouad, “Speech encryption applying a modified Blowfish algorithm,” in *2014 International Conference on Engineering and Technology (ICET)*, 2014, pp. 1–6.

18. S. F. Yousif, "Encryption and decryption of audio signal based on Rsa algorithn," Int. J. Eng. Technol. Manag. Res., vol. 5, no. 7, pp. 57–64, 2018.
19. R. Aparna and P. I. Chithra, "A review on cryptographic algorithms for speech signal security," Int. J. Emerg. Trends Technol. Comput. Sci., vol. 5, no. 5, pp. 84–88, 2016.
20. 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.
21. A. Akmajian, A. K. Farmer, L. Bickmore, R. A. Demers, and R. M. Harnish, *Linguistics: An introduction to language and communication*. MIT press, 2017.
22. Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J. and Roback, E., 2001. Report on the development of the Advanced Encryption Standard (AES). *Journal of research of the National Institute of Standards and Technology*, *106*(3), p.511.
23. A. A. Abd El-Sadek, A. Talaat, and M. M. Fouad, "Speech encryption applying a modified Blowfish algorithm," in 2014 International Conference on Engineering and Technology (ICET), 2014, pp. 1–6.
24. L. Huang and Q. Yin, "A chaos synchronization secure communication system based on output control," Journal of Electronics & Information Technology, vol. 31, no. 10, pp. 2402–2405, 2009.
25. Moulin, P. and O'Sullivan, J.A., 2003. Information-theoretic analysis of information hiding. *IEEE Transactions on information theory*, *49*(3), pp.563-593.