



Security of Voice Using an Enhanced Data Encryption Standard Algorithm

¹I. M. Danjuma, ²K. B. Labbo, ³S. Lawan, ⁴O. A. Sadiq, ⁵A. Danladi
Department of Electrical and Electronic Engineering,
Nigerian Defence Academy, Kaduna

ABSTRACT

Secure communication of voice data is a contemporary issue in this information age. Voice data signals are vulnerable to cybercrime, affecting economic and business ventures of government and non-governmental organizations. This paper aims to secure voice data using the Enhanced Data Encryption Standard (EDES) Algorithm. The method included acquiring voice samples and designing a robust encryption and decryption algorithm leveraging Matlab. It incorporated Structural Similarity Index Metrics (SSIM) to evaluate the performance of the EDES algorithm. The system's performance was comprehensively evaluated, focusing on quality of service (QoS) and quality of experience (QoE). The performance of the EDES algorithm was tested, showing average results for Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Structural Similarity Index Metric (SSIM) and Average Difference (AD), reaching 31.0337dB, 31.7079dB, 87.7653, 0.99385, and 0.9148 respectively, using Matlab simulations. The results of the presented enhanced algorithm were validated with ITU voice transmission standards (P.800, P.862, and P.863) and reference [5]. In terms of SNR, PSNR performance, its SNR is 11.4% and PSNR is 14.4% better than the one in reference [5]. This indicated that it is secure, reliable, and efficient for secure voice data communications, with intelligibility of the recovered voice data signal. The developed EDES algorithm plays a pivotal role in safeguarding data privacy and fortifying defenses against cyber threats, thereby elevating communication security standards.

ARTICLE INFO

Article History

Received: January, 2026

Received in revised form: March, 2026

Accepted: May, 2026

Published online: June, 2026

KEYWORDS

EDES, DES, 3DES, GUI, QoS, QoE, Voice data, Encryption, Decryption, Communication Security

INTRODUCTION

In everyday life we engage in both visual and verbal communication. Today, electronic multimedia communication system using mobile Handset is the most common way of communication. These communications are vulnerable to cybercrimes. In the last few decades, various data protection techniques have been developed to address cybercrimes, provide data security, and protect confidential information or privacy interest of voice data. Data security is one of the most significant features in the field of data transmission. A high level of security is needed in case of data privacy and storage. It is

necessary to implement data protection with a high-security rate and confidentiality. Cryptographic techniques are often widely applied to secure transmission of multimedia communication. Cryptography is the process of transforming plain text or original information into an unintelligible form known as Ciphertext so that it may be sent over unsafe channels of communications [1] [2].

Cryptography is utilized to provide security to the data by preventing it from unauthorized users. In cryptography, the content of voice data is protected using an encryption/decryption algorithm. Authorized users

Corresponding author: I. M. Danjuma



Department of Electrical and Electronic Engineering, Nigerian Defence Academy, Kaduna.

© 2026. Faculty of Technology Education. ATBU Bauchi. All rights reserved

can have access to the original content by using the decryption algorithm with the correct encryption key. The main goals of using cryptography are authentication, integrity, confidentiality, non-repudiation, and availability [1].

Data encryption is the process of converting data from a readable format to a scrambled piece of information. This is done to prevent unauthorized people or hackers from accessing confidential information in transit. Encryption can be applied to documents, files, audio, videos, text messages, or any other form of communication [3]. The main mechanism in cryptography is encryption and decryption that guide the flow of data. Depending on the sensitivity level, multimedia data can either be totally, partially, or perceptually encrypted. Audio encryption techniques have gained ground in multimedia security for audio communication over networks [4]. Voice data is different from other data like digital images and text messages due to the high redundancy, strong correlation and bulk capacity between voice samples.

Encryption of voice information is performed by filling specific parts of the message which represent the silent parts of the voice signal with noise signal before transmission, extraction this noise will yield the original voice signal at the receiver. Voice communication is almost utilized in every activity of daily life like military applications, education, e-learning, commerce, phone banking, politics, news broadcasting and so forth. Therefore, protecting voice data while transmitting

over any insecure communication channel by using cryptography techniques became an important issue [5].

Furthermore, encryption is considered the basic building block of data security, widely used by many organizations and individuals for protecting useful and confidential data by encoding it in such a way that it can only be decrypted or accessed by an individual who holds the correct encryption key or password. The decryption key must be kept secret at all times. The plain text and the ciphertext are the key elements in cryptography. The plain text is the original data and ciphertext is the incomprehensible data formed from the plain text using encryption. The original data must be protected during the process of transmission or storage. Consequently, encryption is utilized for data security [2].

Ensuring adequate security measures for this system is crucial, therefore, the need for proper use of Network Security Model can never be over emphasized. The Network Security Model provides the new professionals with the knowledge to discover what has been implemented and what has not been implemented from a security stand point. The implementation of security has two parts: the code and the setup/configuration. The code is the program which security depends. The setup is whole data that controls the operations of these programs: folder structure, access control lists, group memberships, encryption keys [6]. The Fig. 1.1 depicted Network Security Model.

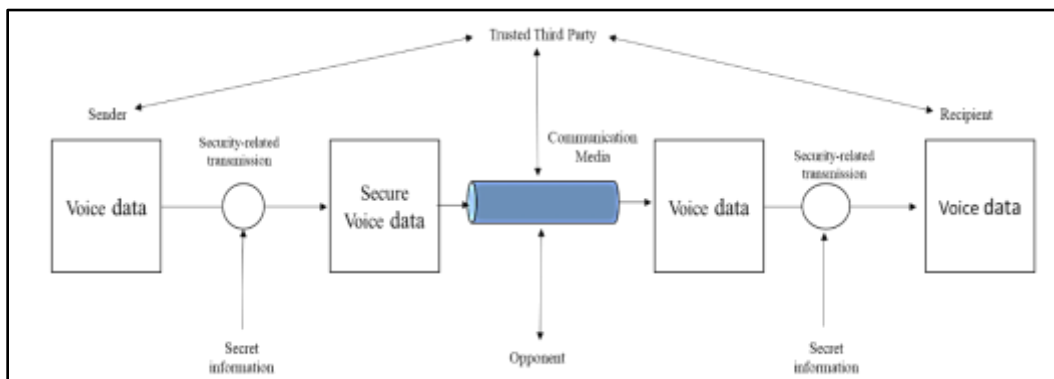


Fig. 1.1: Model for Network Security.

Corresponding author: I. M. Danjuma

Department of Electrical and Electronic Engineering, Nigerian Defence Academy, Kaduna.
© 2026. Faculty of Technology Education. ATBU Bauchi. All rights reserved

METHODOLOGY

The methodologies adopted in this paper are as follows:

1. The first stage involves assigning prime numbers and then recording voice for a period of 5 seconds.
2. Designing an EDES encryption/decryption algorithm using the MATLAB programming environment.
3. After that, a key is generated for the voice encryption, the decryption process involves inputting the private key and then uploading the encrypted voice data into the system. Use the same key for decryption, the original voice data is recovered.
4. Finally, objective and subjective evaluations were performed to verify the effectiveness of the system.

RESULTS AND DISCUSSIONS

The test results were presented and discussed in this chapter to enable evaluation of the performance of the work. The plotted diagrams analyse, SNR, PSNR, MSE, SSIM and AD, in graphical form of the simulation process. Original voice, spectrogram, encrypted and decrypted voice signals presented. Also, Graphical User Interface results were presented.

Graphical Interpretation of Original, Encrypted and Decrypted Voice Signals

Figure 1.2 shows the original speech signal that was loaded into the EDES algorithms and it is clear that no encryption has been added yet. Figures 4.2 shows the spectrogram of the original speech signal after being subjected to audio listening using Matlab codes.

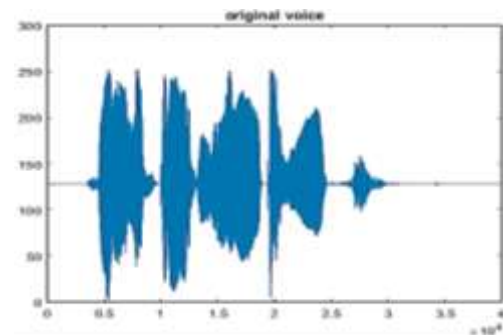


Figure 1.2: Waveform of the Original Voice1 Signal.

The spectrogram was obtained by using the *MATLAB*® function 'spectrogram (x, window, noverlap, nfft, fs)'. 'x' is the speech signal (data vector), 'window' is the window function (Hanning), 'noverlap' is the number of samples (50%) in this case, 'nfft' is the fft length (integer), and 'fs' is the sampling frequency of the data vector x.

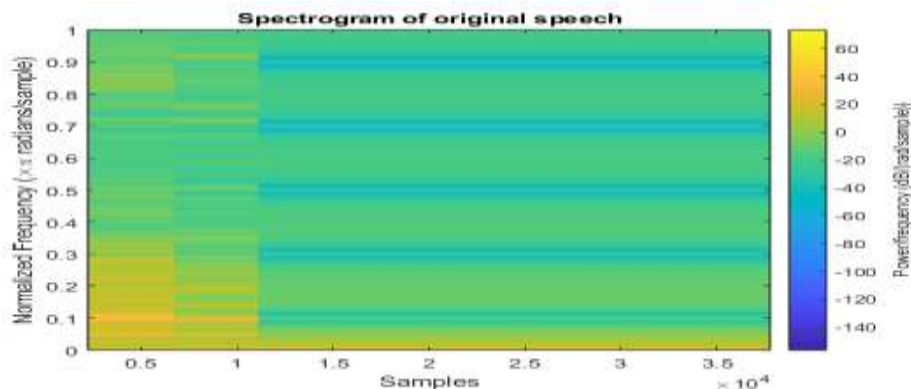


Figure 1.3: Spectrogram of the Original Voice 1 Signal.

The result demonstrated that the simulation waveform of the encrypted voice 1

signal is shown in Fig. 4.3 after applying EDES encryption algorithm and filling the silent parts of

the original signal (from 0.5s to 3.5s) with noise before transmission. From this figure, it is clear that the encrypted speech signal is contaminated by unwanted background noise components which degrades the original voice 1 signal. The amplitude of the voice signal waveform (from 0 to 300) represented the loudness or intensity of the voice signal. It varies continuously over time, corresponding to the variations in air pressure caused by the vocal cords or loudness of the speech signal.

During voiced speech, the waveform exhibits a regular, repeating patterns due to the periodic vibration of the vocal cords as shown. During unvoiced speech (silence periods), the waveform is more irregular and noisier. It contains some pauses or intervals of silence or low amplitude between words or phrases. The waveform envelope outlines the general shape or contour of the signal's amplitude over time, while the time structure represents the rapid oscillations within the envelope. The signal is plotted on a graph with time on the x-axis, and amplitude on the y-axis.

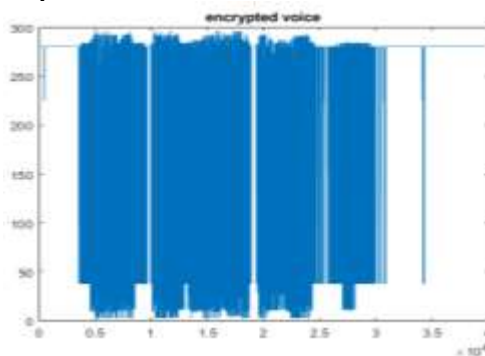


Figure 1.4: Waveform of the Encrypted Voice 1 Signal.

Fig. 1.4 shows the decrypted voice 1 signal after being subjected to decryption algorithm in Matlab and noise extraction to recover the original voice. The extraction was stated from 0 to 3.5 second, at an amplitude from 0 to 250, after which the original voice was recovered. As can be seen, the decrypted voice signal is exactly a replica of the original voice 1 signal. This indicates the effectiveness of the EDES algorithm.

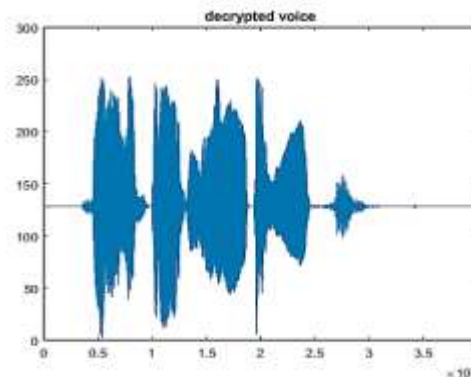


Figure 1.5: Waveform of the Decrypted Voice 1 Signal.

While Fig. 1.5 below shows its spectrogram. The spectrogram returns the Short-time Fourier transform of the input voice signal, x . Each column of s contains an estimate of the short-term, time-localized frequency content of x . The spectrogram indicates the formants corresponding to frequencies of greater energy. It can be seen from the spectrogram obtained the grey scale level at each point; the grey scale is typically used to indicate the energy at each point. The intensity of a point is proportional to the spectrum magnitude at that frequency and time. The difference in performance of the various speech signals can be seen on spectrogram of the decrypted speech.

CONCLUSION

In conclusion, this paper successfully achieved its primary objectives of developing of an EDES algorithm for secured voice communication. Through careful design, and testing, the algorithm demonstrated robust performance in securing the voice data. The EDES algorithm was implemented using MATLAB® R2021a on Windows 10. The development successfully encrypted and decrypted voice data with accuracy, demonstrating the algorithm's effectiveness in securing sensitive information. Performance metric tests on the QoE indicated that the algorithm operated efficiently within acceptable limits. SSIM, AD, PSNR, SNR and MSE quality metric tests were all conducted on five voice data samples and the results were found to be within the acceptable limits.

Corresponding author: I. M. Danjuma



Department of Electrical and Electronic Engineering, Nigerian Defence Academy, Kaduna.
© 2026. Faculty of Technology Education. ATBU Bauchi. All rights reserved



The developed EDES algorithm is better in terms of speed of encryption, and quality of decrypted voice. This work can be used on fourth generation (4G) of Mobile Telecommunications Technology (Long-term Evolution). Therefore, it can be concluded that the developed system will be a suitable choice for encrypting data in modern applications and sets a foundation for ongoing advancement in cryptographic technologies.

REFERENCES

- [1] S. Ravi, S. A. Yadav, A. Singh, & S. Sharma, "Design and Implementation of Improved Data Encryption Standard," Unpublished.
- [2] S. J. Sabeena and S. Antelinvijila, "Identification Of Better Encryption Algorithm in Securing Data," vol. 10, pp. 889–896, 2023. *Network, Ad Hoc Networks*, vol. 129, p. 102807, 2022.
- [3] O. G. Abood, S. K. Guirguis, "A Survey on Cryptography Algorithms," *International Journal of Scientific and Research Publications*, vol. 8, no. 7, pp. 495-516, 2018.
- [4] A Sambas, et al., "A new hyperchaotic hyperjerk system with three nonlinear terms, Its synchronization and circuit simulation," *International Journal of Engineering & Technology*, vol. 7, no. 3, pp. 1585-1592, 2018.
- [5] S.Yousif, F. Sura, Secure voice cryptography based on Diffie-Hellman algorithm. IOP Conference Series: Materials Science and Engineering, 1076(1), 012057, 2021. <https://doi.org/10.1088/1757-899x/1076/1/012057/>
- [6] M. Khan, "Computer security in the human life," *International Journal of Computer Science and engineering*, ISSN(P): 2278-9960; Vol. 6, Issue 1, Dec – Jan 2017; pp. 35-42, 2017.
- [7] P. Rakheja,, R. Vig, P. Singh, An asymmetric hybrid cryptosystem using the hyperchaotic system and random decomposition in hybrid multi resolution waveletdomain, *Multimedia Tools and Applications* 78(15), Pp. 20809–20834, 2019. doi :10.1007/s11042-019-7406-x.
- [8] A. Ghasemzadeh, E. Esmaeili, "A novel method in audio message encryption based on a Mixture of chaos function," *International Journal of Speech Technology* 20(4), pp. 829 –37, 2017.
- [9] Z. Shahid, M. Chaumont, & Puech, W. "Selective encryption of C2DVLC of AVS video Coding standard for I & P frames," 2010 IEEE International Conference on Multimedia and Expo (pp. 1655-1660). Suntec City, Singapore: IEEE Access, 2010.
- [10] A. J. Raphael, & V. Sundaram, "Cryptography and Steganography – A Survey," *International Journal of Computer and Technology Applications*, 2(3), pp. 626-630, 2010.
- [11] Vaidyanathan, et al., "A new chaotic jerk system with three nonlinearities and Synchronization via adaptive backstepping control," *International Journal of Engineering & Technology*, vol. 7, no. 3, pp. 1936-1943, 2018.
- [12] A. Aishwarya, R. Pratibha, and K. Sandhya, "Secured Audio Encryption using AES Algorithm," *International Journal of Computer Applications* (0975-8887) Vol. 178, 2019.
- [13] C. Zhixian, and W. Marcin, "Encryption Technology of Voice Transmission in Mobile network based on 3DES-ECC Algorithm," *Mobile Networks and Applications*, 2020 <https://doi.org/10.1007/s11036-020-01617-0>
- [14] S. N. Sayyad, P. S.Sutar, R. S. Pise, V. H Raut. And C.V. Nalawade, "Dual-layer Video Encryption & Decryption using RSA Algorithm," *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 5, Issue 4, April,7 Pp. 661-7668, 2017.
- [15] A. Yahia, A. Mohamad, S. Mohamed, and M. M. Atiewi, "Speech Encryption by Multiple Chaotic Maps with Fast Fourier Transform," *International Journal of Electrical and Computer Engineering (IJECE)* Vol. 10, No. 6, December 2020, pp. 5658~5664, ISSN: 2088-8708, 2020. DOI: 10.11591/ijece.v10i6.pp5658-5664.
- [16] A. Salamudeen, M. I. Mohammed, and I. D. Mohammed, "Securing audio data using K-shuffle technique," *Multimedia Tools and Applications*, 2019. <https://doi.org/10.1007/s11042-019-08151-6>.
- [17] A. Savita, A.K. Yadav, S. Phool, and S. Hukum. "Audio and Image Encryption Scheme Based on QR decomposition and Random Modulus decomposition in the Fresnel domain," *Optica Applicata*, Vol. LII, No. 3, 2022. DOI: 10.37190/oa220303,
- [18] S. Astha, and E. A. Nitin, "Secure Communication between Two Computers using MATLAB with DES Algorithm and Arduino board," *International Journal of Advanced*

Corresponding author: I. M. Danjuma



Department of Electrical and Electronic Engineering, Nigerian Defence Academy, Kaduna.
© 2026. Faculty of Technology Education. ATBU Bauchi. All rights reserved



- Research in Electrical, Electronics and Instrumentation Engineering. Vol. 6, Issue 5, 2017.
- [19] T. Irma, P. Edward, B. Panganiban, B. B. Bryan, "A Security Approach for File Management System using Data Encryption Standard (DES) algorithm," *International Journal of Advanced Trends in Computer Science and Engineering*. Volume 8, No.5, ISSN 2278-3091, 2019.
- [20] A. Salamudeen, M. I. Mohammed, and I. D. Mohammed, "Securing audio data Using K-shuffle technique," *Multimedia Tools and Applications*, 2019. <https://doi.org/10.1007/s11042-019-08151-6>.
- [21] Tan, Arada, Abad, and Magsino, "A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher", In *Journal of Physics: Conference Series*, vol. 1997, no. 1, p. 012021, 2021.
- [22] Shukla, Dwivedi, and Trivedi, "Encryption algorithm in cloud computing", *Materials Today: Proceedings*, vol. 37, pp. 1869-1875, 2021.
- [23] Hafsa, Sghaier, Malek, and Machhout, "Image encryption method based on improved ECC and modified AES algorithm", *Multimedia Tools and Applications*, vol. 80, no. 13, pp. 19769-19801, 2021.
- [24] Munir, Khan, Hazzazi, Aijaedi, Alharbi, and Hussain, "Cryptanalysis of internet of health things encryption scheme based on chaotic maps", *IEEE Access*, vol. 9, pp. 105678-105685, 2021.
- [25] Seth, Dalal, Le, Jaglan, Dahiya, Agrawal, and Verma, "Secure Cloud Data Storage System Using Hybrid Paillier-Blowfish Algorithm", *CMC-COMPUTERS MATERIALS & CONTINUA*, vol. 67, no.1, pp.779-798, 2021.
- [26] S. Verma, R. Choubey and R. Soni, "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security", *International Journal of Emerging Technology and Advanced Engineering*, ISSN 2250-2459, Volume 2, Issue 7, July 2012.
- [27] S. F. Yousif, "Encryption and Decryption of Audio Signal Based on RSA Algorithm," *International Journal of Engineering Technologies and Management Research*, 5(7), 57 – 64. 2020
<https://doi.org/10.29121/ijetmr.v5.i7.2018.259>
- [28] "Audio Sample Rate." A Complete Guide Voice Talks, 2024. [Online]. Available: <https://www.voice123.com/voicetalk>. [Accessed: May 4, 2024].
- [29] M. A. Al-shabi, "A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security," no. March, 2019. Inc. doi: 10.29322/IJSRP.X.X.2018.pXXXX.
- [30] M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A. Pindar, and N. S. Ahmad, "A Survey on the Cryptographic Encryption Algorithms," no. November, 2017. Inc. doi: 10.14569/IJACSA.2017.081141.
- [31] Z. Hercigonja, D. Gimnazija, and C. Varazdin, "Comparative analysis of cryptographic algorithms and advanced cryptographic algorithms," *International Journal of Digital Technology & Economy*, vol. 1(2), pp. 1–8, 2016.
- [32] N. Xiong, S. Member, and J. Ren, "Data Security and Privacy Protection for Cloud Storage : A Survey," 2020. doi: 10.1109/ACCESS.2020.3009876.
- [33] C. Bhalodia, "Public Key Cryptography and its Application," YouTube, Video, Apr 15, 2024. [Online] Available: <https://youtu.be/HhhYX8wkaKY?si=9vLB3Pq6NizKJl0gp>
- [34] F. J. Farsana, and K. Gopakumar, "A Novel Approach for Speech Encryption: Zaslavsky Map as Pseudo Random Number Generator," 6th International Conference on Advances in Computing & Communications, ICACC 2016, (India: Elsevier), 2016, pp. 816 – 823.
- [35] P. Sathiyamurthi, and S. Ramakrishnan, "Speech encryption algorithm using FFT and 3D-Lorenz-logistic chaotic map," *Multimedia Tools and Applications*, (Springer), 2020.
- [36] P. Sathiyamurth and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication," *EURASIP Journal on Audio, Speech, and Music Processing*, (Springer), 2017, pp. 1-11.
- [37] B. Ratnadewi, P.A. Roy, H. Yonatan, A. Saleh, M.I. Setiawan, "Implementation Cryptography data encryption standard (DES) and triple data encryption standard (3DES) Method in communication system based near field communication (NFC)," *J. Phys: Conf.Ser.* 954, 1–9 2018.

Corresponding author: I. M. Danjuma



Department of Electrical and Electronic Engineering, Nigerian Defence Academy, Kaduna.
© 2026. Faculty of Technology Education. ATBU Bauchi. All rights reserved