Design and Implementation of Audio Steganography in Healthcare using IoT

K. Revathi[1]*S. Kaja Mohideen[2]*
[1,2]Department of Electronics and Communication Engineering,
[1,2]B.S.Abdur Rahman Crescent Institute of Science and Technology,
[1,2]Vandalur, Chennai, TamilNadu, India.
[1]revathivigneswaranphd@gmail.com,
[2]kajamohideen@crescent.education.

ABSTRACT

Audio steganography is a technique to hide information within an audio file of type WAV,MIDI, AVI, MPEG, and MP3 files. Audio Files have acted as a cover for secretly communicating multimedia files (text, images, audio, and video). Least Significant Algorithm (LSB) is the standard and traditional algorithm in audio steganography. The patient's medical record is in the text file concealed in an audio file of type WAV using the LSB algorithm. The resulting stego audio file is exchanged within or outside the organization to facilitate the remote diagnosis with security and imperceptibility. Merging audio steganography with IoT enhances secured communication in medical records with confidentiality and integrity. The similarity between the cover and stego audios is measured using normalized cross-correlation. Mean Squared Error (MSE), Peak signal-to-noise ratio (PSNR),and Bit Error Rate (BER) performance metrics measure the distortion between the cover audio and stego audio files.The Audio Steganography utilizing IoT with Telemedicine model surpasses stego audio clearness with an average PSNR of 34.5dB and a lower BER of 0.00035.

Keywords~~Au~~dioSteganography; Least Significant Bit (LSB);Mean Squared Error (MSE);Peak Signal-to-Noise Ratio (PSNR);Bit error rate (BER);Patient-doctor dialogue (PDD).

I. INTRODUCTION

Remote diagnosis plays a vital role during periods of communicable diseases like COVID-19, raising the necessity of protecting patient medical data. The three methods used for security systems in data are cryptography, steganography, and watermarking. Medical professional's primary concerns are data privacy and security in medical data. Cryptography and Steganography play vital roles in solving the issues of medical professionals by securely communicating medical records with robustness and integrity.Figure 1 furnishes the types of information security techniques[1][2].

Cryptography in Greek means secret writing. The hidden information is termed plaintext and converted to unreadable text called cipher text. The process is known as encryption, achieved using encryption algorithms and keys. In the reception end, cipher text converts to plain text using a decryption algorithm and decryption key. Cryptography focuses on changing the message's meaning [3],[4]. For example, a patient's medical records in the text file are communicated in an unreadable form called cipher text and securely transmitted to the authorized receiver for accessing the information.

Steganography in Greek means hidden writing. Steganography aims to hide the existence of a message through another medium called a cover[5]. Multimedia files, namely audio, image, text, and video, act as the cover files. Steganography's basic principle is statistical undetectability[6], [7]and is different from cryptography in that it concentrates on secure and secret interaction as opposed to cryptography's focus on secure communication. Steganography and cryptography are, therefore, excellent tools for shielding data from unauthorized users [8].

Watermarking is one of the disciplines in information hiding and focuses on protecting digital content. The goal of watermarking is for watermarked information to be irremovable. Typically, watermarking is a one-to-many relationship where communication is one-way, but in steganography, it is a one-to-one relationship with two-way communication [8].

Development in the field of information and communication technology keeps the patient's medical records electronically. Along with e-medical information and the revolution in the World Wide Web, Remote diagnosis was successful. As digital data sharing has risen, network security has become an issue. Therefore, an information-hiding technique called steganography communicates the e-records of patients with integrity and confidence. Hence, steganography in the medical field is discussed [9].

The rest of the chapter is organized as follows: Section II Literature of Steganography and IoT Steganography.

Steganography overview in section III. Section IV describes the model for audio steganography in the medical field. Section V describes the simulated experiments and then evaluates the outcomes. Section VI concludes the paper with future scope.

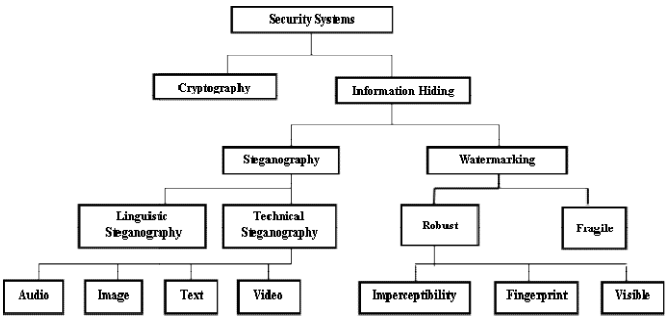

Figure 1 Different types of security systems

II. RELATED WORKS

Data hiding strategies use a cover to conceal confidential data. Audio, text, images, and video are multimedia files that serve as data carriers. An image is a commonly used steganography carrier. Image steganography is popular due to the redundant data in the cover image and the inability of the human visual system (HVS) to find the distortion in an image[10].

Image steganography for concealing the patient data in grayscale and color images using integer wavelet transform (IWT-LSB). The above technique invokes the need for distant diagnosis[11].Similarly, e-health services require patient medical data to be confidential and protected during transformation. The integer wavelet filter decomposes medical images as a cover for hiding patient's medical data. The data are compressed using arithmetic coding (AC) and encrypted using a data encryption standard before concealing the images[12]. Recently, communicable diseases have created a situation for remote diagnosis. For this, image steganography securely communicates COVID-19 patient records in their X-ray scans. Steganography, in conjunction with cryptography, improves robustness in remote diagnostics. The patient data was encrypted twice using the encrypted DNA technique in combination with the generation of the Baconian cipher for the data. The data set (COVID chest x-ray) utilized in the algorithm is available on GitHub[2]. A new framework in image steganography is quantum steganography, a secure communication using a hash function and quantum entangled states in Fog Cloud IoT was successful[13]. Similarly, data steganography securely communicates medical records of patient's names, ages, and genders, referred by a doctor, referred to a doctor, dates, and medicines in an image called image steganography[9].

Another medium for data hiding using steganography is audio. Here, audio files act as a cover for concealing hidden data. Various Steganography techniques are successful in hiding data. The Least Significant Bit Algorithm (LSB) is the conventional and established steganographic technique.LSB algorithm is simple in computations. Audio steganography is discussed in-depth in later sections.

III. STEGANOGRAPHY OVERVIEW

Steganography is a covert communication technique in which only the sender and receiver know about the secret communication.

The secret message hidden among seemingly innocuous communications is known as cover Works. The combined cover works and concealed messages are stego work. The cover in the stego file is multimedia files. Figure 2 shows different types of steganography covers [6][14].

Audio Steganography is the habit of undetectably modifying an audio file to incorporate a message of type audio, text, image, and video. Audio steganography with hidden patient medical records in the text file format is detailed in the later sections. Figure 3 depicts the block diagram of the Audio steganography system [15].

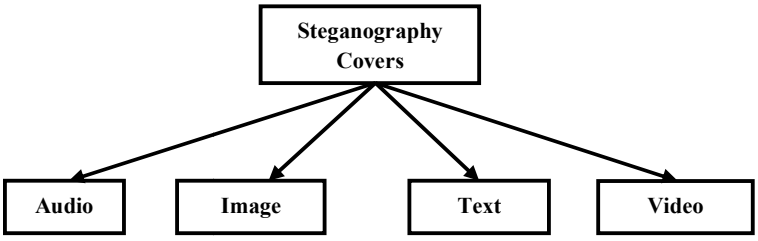

Figure 2 Types of steganography covers

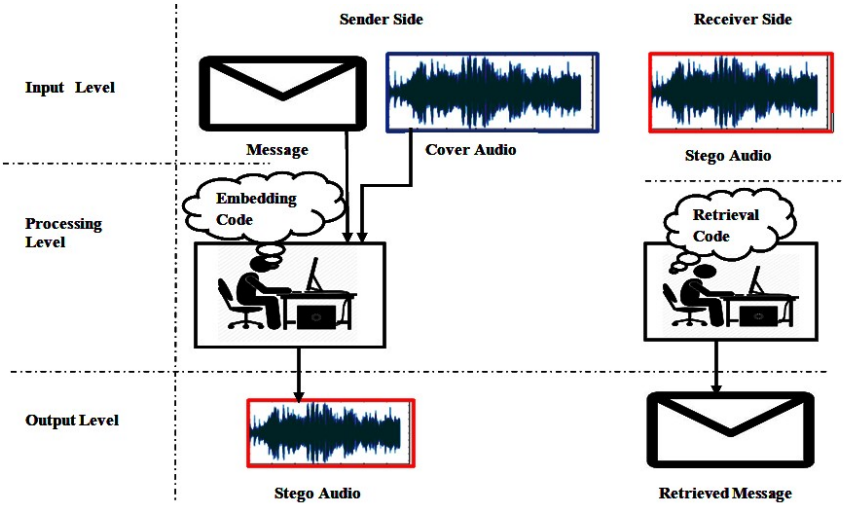

Figure 3Block Diagram of Audio Steganography

A. Principle of Audio Steganography

A secret message (M) of a type text file (.txt) is hidden in a randomly chosen cover object (C) of a type audio file WAV by using a key (K) called stego key. The cover (C) changes to the stego file (S), communicated to the receiver. A perfect audio steganography is sameness between cover and stego audios. With a mutually agreed embedding and retrieval code between sender and receiver and with the stego key (K), the receiver will retrieve the secret message (M) from the stego file(S) [6].

B. Protocols in Audio Steganography

A system of rules followed in audio steganography is classified as pure steganography, secret key steganography, and public key steganography[6].

1. Pure Steganography

A steganographic system without prior exchange of stego key is pure steganography. Mapping in Embedding (E) and Retrieval (D) functions is given by (1) and (2). Both sender and receiver should have access to the embedding and retrieval algorithm, which is not public.

$$E : C \times M \rightarrow C \quad (1)$$

$$D : C \rightarrow M \quad (2)$$

The necessary conditions on pure steganography are $|C| \geq |M|$ and $D(E(c,m)) = m$ for all $m \in M$ and $c \in C$.
The correlation between two cover and stego audios is measured by the similarity function (sim) given in (3).

$$Sim: C^2 \rightarrow (-\infty, 1] \text{ for } x,y \in C \quad (3)$$

The practical steganographic system should satisfy the similarity condition given in (4).

$$sim(c, E(c, m)) \approx 1 \text{ for all } m \in M \text{ and } c \in C \quad (4)$$

For successful steganographic communication, thecover in the embedding phase ischosen by the property given in (5).

$$c = max_{x \in C}\, sim(x, E(x, m)) \quad (5)$$

2. Secret Key Steganography

A steganographic system with a stego key is secret key steganography. Equations (6) and (7) provide the mapping between the cover and secret message in the embedding and retrieval function with the property $|C| \geq |M|$ and $D_K(E_K(c, m, k), k) = m$ for all $m \in M$, $c \in C$ and $k \in K$.

$$E_K : C \times M \times K \rightarrow C \quad (6)$$

$$D_K : C \times K \rightarrow M \quad (7)$$

3. Public Key Steganography

Using a steganographic system with private and public keys is public-key steganography. The public key gets accessed from the public key database used in the embedding phase, while the private key gets used in the retrieval phase for extracting the secret message.

C. Properties of steganography

The three major parameters of the audio steganography technique are capacity, robustness, and imperceptibility. Capacity is the maximum amount of confidential data embedded in a multimedia file like the cover audio file. Capacity, measured in percentage (%) or bit per second audio file[16], [17].

Imperceptibility indicates both cover and stego audios should be indistinguishable for perfectly secure steganography. Robustness withstands various steganalysis attacks and retrieves the embedded secret message with minimal error[16], [18]. The trade-off between the above parameters is difficult, as shown in Figure 4[19].Hence, steganography aims to enhance the steganographic capacity with strengthened imperceptibility and robustness.

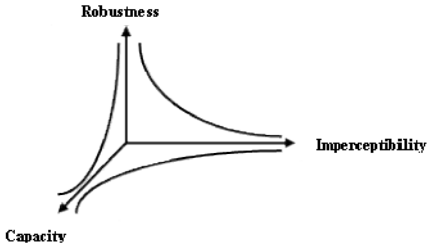

Figure 4 TheTrade-off between the properties of the steganography system.

D. Steganographic methods

Six categories of steganographic methods based on cover modifications applied in the embedding process are listed in Figure 5[6].In Substitution systems, secret messages are embedded in redundant parts of the cover file. In this section, the secret message of type text (.txt) is embedded in the redundant bits of the audio file to act as a cover. The standard and traditional algorithm in substitution systems is the least significant bit algorithm (LSB).

1. Least significant Algorithm

The LSB algorithm works by embedding each bit of the secret message in the least bit of the cover file. So, to embed a one-byte text file, eight one-byte samples of audio files are required.LSB algorithm is simple in practice and computations. In the retrieval phase, the LSB of selected cover elements is retrieved and lined up to reconstruct the secret message. The algorithm for the embedding and retrieval phase in LSB is briefed below[6].

Algorithm 1: Embedding phase in the least significant bit substitution

For i = 1 to L(C) do #Sequence of cover element (c_i) in cover C with length L(C)
$s_i \leftarrow c_i$ #Sequence of stego object (s_i) of length l(C)
End for
For i = 1 to L(M) do #Sequence of message bits(m_i) in message M of length l(M)
Compute index j_i where to store i^{th} message bit
$s_{ji} \leftarrow c_{ji} \leftrightarrows m_i$ #j is the index of cover element c_i
End for

Algorithm 2: Retrieval phasein the least significant bit substitution

For i = 1 to L(M) do
Compute index j_i where the i^{th} message bit is stored
$m_i \leftarrow LSB(C_{ij})$
End for

E. Applications of Steganographic System

Covert steganographic communication has shown its excellence in various fields, like medical, military, multimedia, and industry. The healthcare industry uses the DICOM (Digital Imaging and Communications in Medicine) standard protocol for internal and external healthcare communications of medical images and their related data. DNA sequence acts as a carrier for communicating intellectual property in medicine, and genetics as an advancement in steganographic communication in healthcare[6].

Information hiding techniques used in a military organization are prone to multiple attacks on its multilevel secure system. The Commonly used steganographic systems are spread spectrum modulations. Cryptography with steganography enhances the security level in military organizations[1].

Steganographic communication in various multimedia applications includes Automatic monitoring of copyrighted material on the Web, Automatic audit of radio transmissions, Data augmentation, and Tamper proofing[6].

Steganography is popular due to its presence in both ethical and unethical strategies. Xiao steganography is an online steganography tool available for hidden message communication. In forthcoming sections, secured communications of patient medical data concealed in a cover audio file are detailed. Figure 6 shows the applications of steganography in different fields[1], [20].

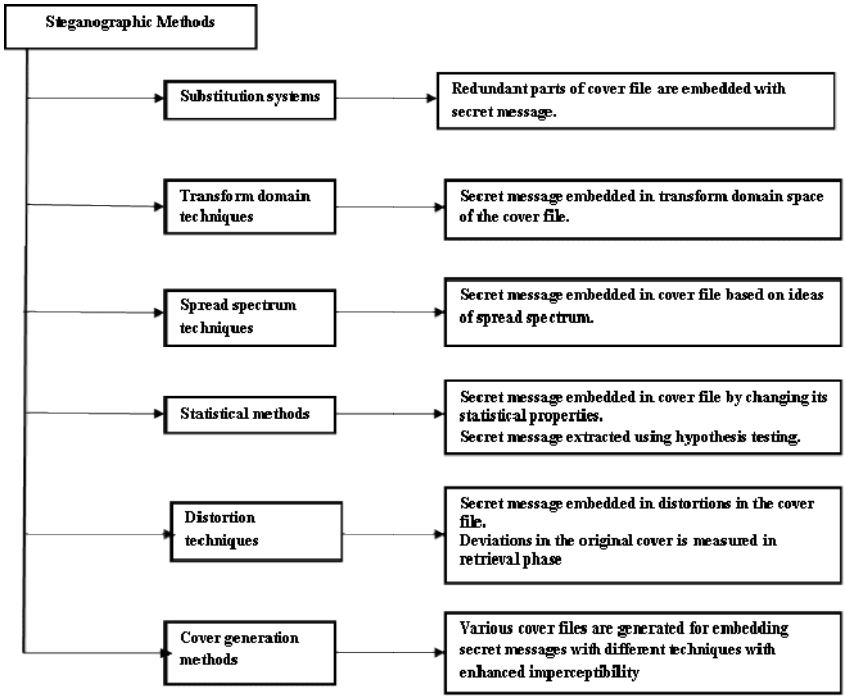

Figure 5Classifications of Steganographic Techniques and its Functions.

IV. AUDIO STEGANOGRAPHY IN THE MEDICAL FIELD

Interactive audiovisual and data communications are known as telemedicine in the healthcare system. The data includes medical care services, diagnosis, consultation, treatment, health education, and the transfer of medical data. IoT-based telemedicine sends and receives medical information with confidentiality and security, which is significant [21], [22]. In the Internet of Things, steganography is crucial for data security. Here is a brief note of an audio steganographic communication of medical records in a text file (.txt). Figure 7 depicts the audio steganography in healthcare using IoT.

A 16-bit uncompressed digital audio file of type WAV acts like a cover file. The cover audio file is transformed into a train of binary bits for concealing the secret message. Health care is served by professionals at different levels depending on the emergency.Primary care is professional consultation, secondary care is skilled professional consultation, tertiary care is advanced medical investigation, and quaternary care is treatment and surgical procedures. Health professionals are in charge of various types of information, including patient medical histories, clinical and other data, and other private and personal information, at all of the above-mentioned levels.

The digitization of clinical evaluations and medical records in the healthcare system has become a habit and widely accepted practice with the development of computer systems. The computerized medical data of patients is termed electronic health records(EHR), chosen by the National Academies of Sciences, engineering, and Medicine (Institute of Medicine). The EHRs and IoT help the healthcare industry with extensive remote healthcare (Telemedicine)[22][21]. The medical records communicated covertly taken from EHRs and converted into binary streams. The least significant bit of audio file concealed with medical records using the LSB embedding algorithm. The LSB algorithm repeated for the entire medical records disguised in the audio file. The generated audio file with hidden medical records is a stego file transmitted through IoT routers for internal and distant diagnoses of a healthcare organization. The telemedicine network enables Internet of Things (IoT) applications to connect to the network's backbone, making it easier for patients and medical professionals to send and receive medical information. LSB retrieval algorithm extracts the stego audio file in the retrieval phase. The extracted bits queued up to reconstruct the binary streams of medical records and transformed to their equivalent ASCII values. Hence, the traditional LSB algorithm securely communicates the patient's medical records over the internet for distant diagnosis.

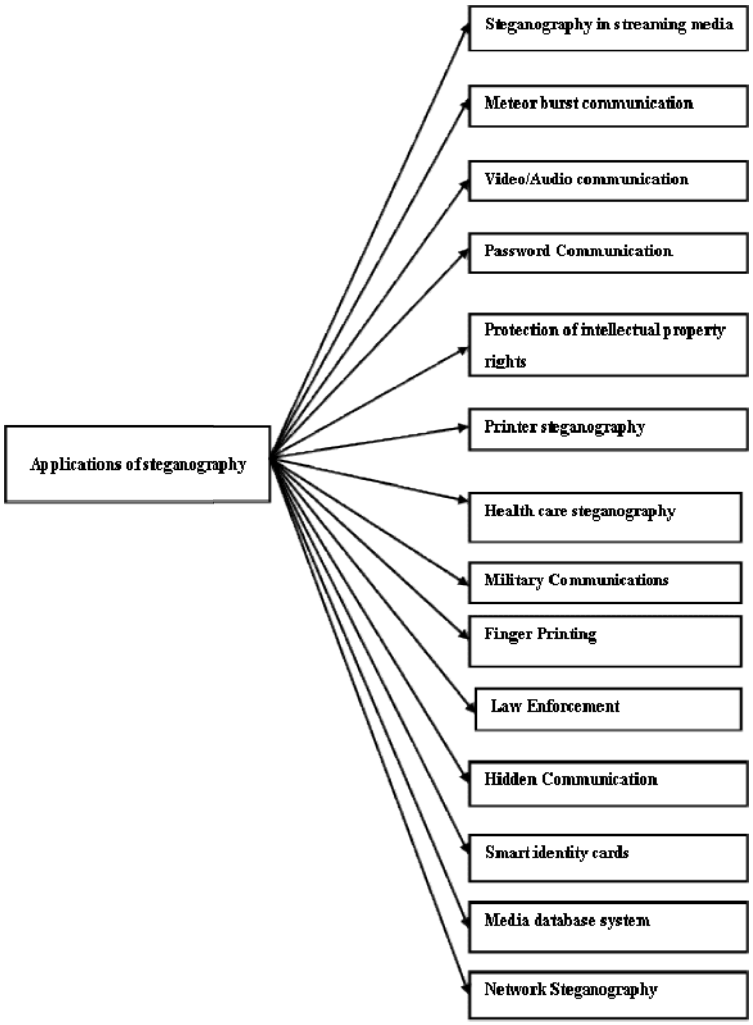

Figure 6 depicts the applications of steganography in various fields.

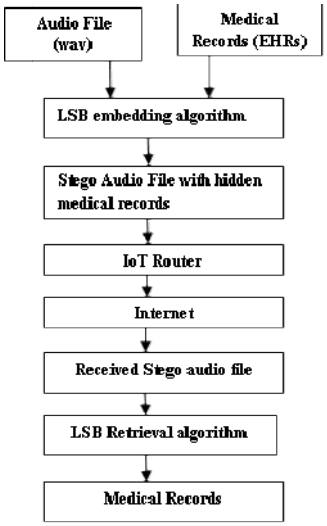

Figure 7 shows the audio steganography using IoT in Telemedicine.

V.Results and Discussion

MATLAB software tested the standard traditional algorithm, the least significant algorithm (LSB). Table 1 lists the specifications of cover audio files of type WAV from the GTZAN dataset used in the algorithm. Similarly, patient's medical records in text files(.txt) are from the Kaggle dataset. The medical data are the Covid Dialogue Dataset between patient and doctor (PDD)about COVID-19 and other types of pneumonia from websites icliniq.com, healthcaremagic.com, and healthtap.com. Performance metrics to evaluate the LSB algorithm are Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), and Bit Error Rate (BER).

Table 1. Description of Audio Files

Specifications	
Bit per sample	16
Number of Samples	661794
Channel	Mono
Audio Type	Music
Duration in seconds	1-30

Mean squared error (MSE) and Peak signal-to-noise ratio (PSNR) in Decibels (dB) calculate the error between cover and stego audios. Similarly, the Bit error rate finds the incorrect bits in the cover and stego audios. Equations (8), (9), and (10) calculate the above-listed performance metrics. Finally, the sameness between the cover and stego audios is measured by normalized cross-correlation (NCC) given by (11). Table 2 depicts the experimental results to examine the performance of the LSB algorithm tested over three audios(Blues, Metal, and Reggae) with medical data of varying capacity from 10 B to 90B[16], [18].

$MSE = \frac{1}{L}\sum_{j=1}^{L}(I_j - O_j)^2$(8)

I_j and O_j are the input and output audio files j^{th} samples, and L is the number of audio file samples.

$$PSNR = 10\,log_{10}\frac{(2^p-1)^2}{MSE}$$(9)

Where p is the maximum number of bits used to show every signal sample.

$BER = \frac{P_{error}}{p_{bits}}$(10)

Where P_{error} is the incorrect bits, and P_{bits} is the total number of bits embedded in the audio file.

$$NCC(C,S) = \frac{\sum_{h=1}^{L} C(h)S(h)}{\sqrt{\sum_{h=1}^{L} C(h)^2}\sqrt{\sum_{h=1}^{L} S(h)^2}}$$(11)

Where C andS are cover and stego audio files.L is the number of samples in each one of them.

Table 2 Experimental results of the LSB algorithm over performance metrics like MSE, PSNR, BER, and NCC.

Cover Audio File(wav)	Text File (Character)	MSE	PSNR(dB)	BER	NCC
Blues	**561-1599**	**0.0415**	**34.5**	**0.00034**	**1**
Reggee	**561-1599**	**0.0207**	**34.6**	**0.00036**	**1**
Metal	**561-1599**	**0.0260**	**34.5**	**0.00036**	**1**

Figure 8 depicts the experimental values of MSE, approximately zero. Hence, the distortion between the cover and stego audios is less, and the performance of the LSB algorithm is efficient.

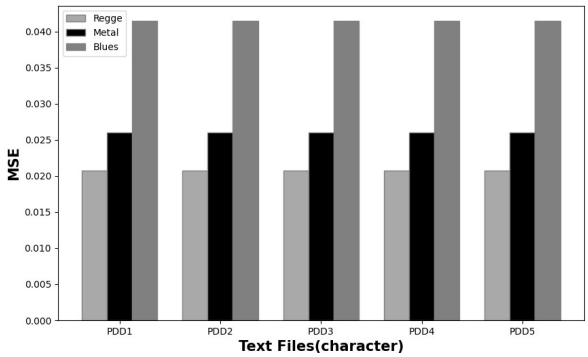

Figure 8 results of the MSE versus Patient-doctor dialogue set (PDD).

The average PSNR of the LSB algorithm is 34.5 dB, shown graphically in Figure 9. The higher the PSNR value, the higher the embedding quality of medical data in the cover audio file of type WAV.

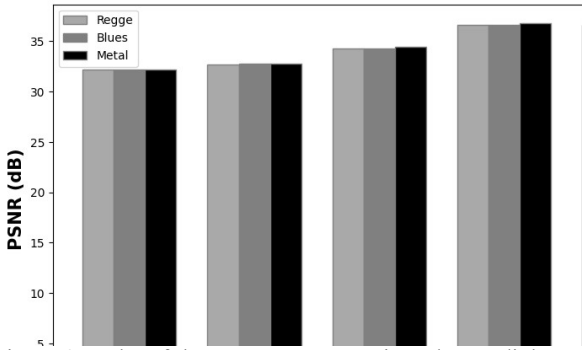

Figure 9results of the PSNR versus Patient-doctor dialogue set (PDD).

The average BER of the LSB algorithm is 0.00035, which ensures a low ratio of incorrect bits. Figure 10 shows the BER experimental values and proves that the LSB algorithm is better in imperceptibility.

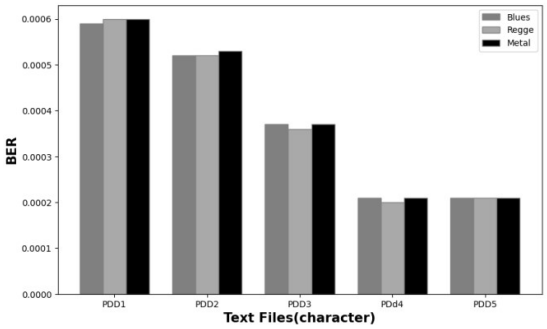

Figure 10results of the BER versus Patient-doctor dialogue set (PDD).

NCC values of all tested audios are 1. Hence, the LSB algorithm efficiently conceals the medical data with sameness between cover and stego audios.

VI. CONCLUSION

Audio steganography covertly and confidently embeds patient-doctor dialogues (PDD) in an audio file of type WAV. The algorithm used in audio steganography is LSB.MSE and PSNR measure the quality of stego audio. BER calculates the distortion between cover and stego audios. NCC measures the degree of closeness between cover and stego audios. The experimental results examined the LSB algorithm for concealed communication of medical data (PDD) of type text (.txt) in an audio file of type WAV with better results in MSE, PSNR, BER, and NCC. In the future, the embedding rates of LSB will increase to 25%, 50%, or 100%, increasing the embedding capacity. Redesign the LSB algorithm by randomly selecting audio samples for concealing the secret data with robustness.

REFERENCES

[1] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, “Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research,” Neurocomputing, vol. 335, pp. 299–326, 2019, doi: 10.1016/j.neucom.2018.06.075.

[2] S. Sahoo, Sony Snigdha Sahoo, “A new COVID-19 medical image steganography based on dual encrypted data insertion into minimum mean intensity window of LSB of X-ray scans”,IEEE (INDICON) ,978-1-7281-6916-3,20,2020 ,doi: 10.1109/INDICON49873.2020.9342067..

[3] Milind Kaushal, “Cryptography : A Brief Review,”International Journal for Research in Applied Science & Engineering Technology (IJRASET)Volume 10,Issue II, February, 2022,https://doi.org/10.22214/ijraset.2022.40401.

[4] A. M. Qadir, Nurhayat Varol “A Review Paper on Cryptography,” 2019 7th Int. Symp. Digit. Forensics Secur., no. October, pp. 1–6, 2019, doi: 10.1109/ISDFS.2019.8757514.

[5] E Ardhianto, H L H S Warnars, B Soewito, F L Gaol and Abdurachman, “Improvement of Steganography Technique : A Survey,” vol. 410, no. Imcete 2019, pp. 289–292, 2020.

[6] S. Katzenbeisser and F. Petitolas, "Information Hiding Techniques for Steganography and Digital Watermaking", vol. 28, no. 6. London: Artech House computing library, 2000.

[7] J. C. Ingemar, M. L. Miller, A. B. Jeffrey, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography", Second. Burlington: Denise E. M. Penrose, 2008.

[8] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Overview of Digital Steganography Methods and Its Applications," International Journal of Advanced Science and Technology, vol. 60, pp. 45–58, 2013, http://dx.doi.org/10.14257/ijast.2013.60.05..

[9] P. D. Bhave, S. S. Desai, R. N. Mahale, and R. L. Mhatre, "Hospital Database System Using Image Steganography," Alexandria Engineering Journal,vol. 9, no. 5, pp. 97–101, 2021, https://doi.org/10.1016/j.aej.2022.03.056.

[10] D. Nashat and L. Mamdouh, "An efficient steganographic technique for hiding data," Journal of the Egyptian Mathematical Society , vol. 6, 2019, https://doi.org/10.1186/s42787-019-0061-6.

[11] H. N. Aleisa, "Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things," Hindawi,Journal of Healthcare Engineering, vol. 2022, https://doi.org/10.1155/2022/7528583.

[12] M. A. Ahmad, Mourad Elloumi, Ahmed H. Samak , Ali M. Al-Sharafi ,Ali Alqazzaz , Monir Abdullah Kaid , Costas Iliopoulos, "Hiding patients ' medical reports using an enhanced wavelet steganography algorithm in DICOM images," Alexandria Eng. J., vol. 61, no. 12, pp. 10577–10592, 2022, doi: 10.1016/j.aej.2022.03.056.

[13] A. A. A. B. D. El-latif, B. Abd-el-atty, M. S. Hossain, Samir Elmougy, and Ahmed Ghoneim, "Secure Quantum Steganography Protocol for Fog Cloud Internet of Things," IEEE Access, vol. 6, pp. 10332–10340, 2018, doi: 10.1109/ACCESS.2018.2799879.

[14] A. S. Mohammad, H. T. Haider, and F. Baji, "Text Hiding Using Artificial Neural Networks," Engineering and Technology Journal, Vol.30, No.20. October 2018, 2012, doi: 10.30684/etj.30.20.6.

[15] A. A. Alsabhany, A. H. Ali, F. Ridzuan, A. H. Azni, and M. R. Mokhtar, "Digital audio steganography: Systematic review, classification, and analysis of the current state of the art," Comput. Sci. Rev., vol. 38, p. 100316, 2020, doi: 10.1016/j.cosrev.2020.100316.

[16] M. M. Mahmoud and H. T. Elshoush, "Enhancing LSB Using Binary Message Size Encoding for High Capacity, Transparent and Secure Audio Steganography-An Innovative Approach," IEEE Access, vol. 10, pp. 29954–29971, 2022, doi: 10.1109/ACCESS.2022.3155146.

[17] R. Tanwar and M. Bisla, "Audio Steganography," International Conference on Reliability, Optimization and Information Technology -ICROIT-IEEE,pp. 322–325, 2014.

[18] H. T. Elshoush and M. M. Mahmoud, "Ameliorating LSB Using Piecewise Linear Chaotic Map and One-Time Pad for Superlative Capacity, imperceptibility and Secure Audio Steganography," IEEE Access, vol. 11, no. April, pp. 33354–33380, 2023, doi: 10.1109/ACCESS.2023.3259902.

[19] M. Begum and M. S. Uddin, "Digital Image Watermarking Techniques : A Review," MDPI-Information,pp. 1–42, 2020, doi: 10.3390/info11020110.

[20] A. K. Sahu, and M. Sahu, "Digital image steganography and steganalysis : A journey of the past three decades,"Open Comput. Sci, pp. 296–342, 2020.

[21] A.S. Albahri, Jwan K. Alwan, Zahraa K. Taha, Sura F. Ismail, Rula A. Hamid, A.A. Zaidan, O. S. Albahri, B. B. Zaidan, A. H. Alamoodi, and M. A. Alsalem et al., "IoT-based telemedicine for disease prevention and health promotion: State-of-the-Art", J. Netw. Comput. Appl., p. 102873, 2020, doi: 10.1016/j.jnca.2020.102873.

[22] S. Dash, S. K. Shakyawar, M. Sharma, and S. Kaushik, "Big data in healthcare : management , analysis and future prospects," J. Big Data, 2019, doi: 10.1186/s40537-019-0217-0.