



A Dual Stage XOR Audio Steganography: Enhancing Secure Data Hiding in Audio Files

Submitted By:
Nasimul Kader
(151-44-107)

A thesis submitted in partial fulfillment of the requirement for the
degree of Masters of Science in Software Engineering

Supervised By:

Md. Maruf Hassan
Associate Professor
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

Department of Software Engineering
Daffodil International University

Spring– 2023

APPROVAL

This thesis titled on “A Dual Stage XOR Audio Steganography: Enhancing Secure Data Hiding in Audio Files”, submitted by Nasimul kader (Student ID: 151-44-107) to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Master of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS



Chairman

Dr. Imran Mahmud

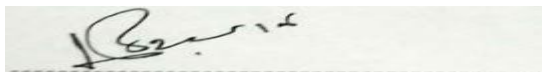
Associate Professor and Head
Department of Software Engineering
Daffodil International University



Internal Examiner 1

Dr. Md. Fazla Elahe

Assistant Professor and Associate Head
Department of Software Engineering
Daffodil International University



Internal Examiner 2

Afsana Begum

Assistant Professor
Department of Software Engineering
Daffodil International University

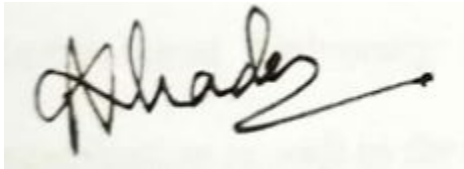


External Examiner

Dr. Md. Sazzadur Rahman,
Associate Professor
Institute of Information Technology
Jahangirnagar University

DECLARATION

I hereby declare that this thesis has been solely composed by myself under the supervision of Md. Maruf Hassan, Associate Professor, Department of Software Engineering, Daffodil International University and the work presented in this thesis, by part or whole, has not been submitted elsewhere for award of any degree.



Md. Nasimul kader

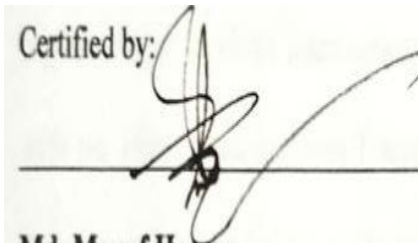
151-44-107

Batch: 22

Department of Software Engineering

Faculty of Science & Information Technology

Daffodil International University



Md. Maruf Hassan

Associate Professor

Department of Software Engineering

Faculty of Science & Information Technology

Daffodil International University

ACKNOWLEDGEMENT

First of all, I want to express my sincere gratitude to my Almighty Allah for granting me the chance to complete the last year. In the past four years of my academic life, I have learned manners, ethics, and other things. I'm appreciative that my teachers gave me the opportunity to achieve this.

My supervisor, Md. Maruf Hassan, an Associate professor in the department of software engineering at Daffodil International University, has my sincere gratitude for providing me with the chance and direction I needed to finish this thesis on "A Dual Stage XOR Audio Steganography." Under his guidance, I was introduced to numerous cutting-edge scientific techniques, for which I will always be thankful.

I acknowledge the authority of my supervisor and the Cyber Security Center at Daffodil International University (CSC, DIU) for allowing me to conduct my research and examination as well as for their cooperation and support in doing so.

Table of Contents

Abstract.....	vi
1. Introduction.....	Error! Bookmark not defined.
2. Literature Review.....	Error! Bookmark not defined.
2.1 Spatial Domain Techniques	Error! Bookmark not defined.
2.2 Frequency Domain Techniques	Error! Bookmark not defined.
2.3 Protocol.....	Error! Bookmark not defined.
4. Proposed Solution	Error! Bookmark not defined.
4.1 Embedding Process.....	Error! Bookmark not defined.
4.2 Retrieving Process	Error! Bookmark not defined.
5. Results and Discussion	Error! Bookmark not defined.
5.1 Data.....	Error! Bookmark not defined.
5.2 Quantitative Analysis.....	Error! Bookmark not defined.
5.3 Spatial Analysis	Error! Bookmark not defined.
5.3.1 Short-Time Fourier Analysis	Error! Bookmark not defined.
5.3.2 Waveform	Error! Bookmark not defined.
5.3.3 Chromagram	Error! Bookmark not defined.
5.3.4 Fourier Tempogram	Error! Bookmark not defined.
5.3.5 Power Spectrum	Error! Bookmark not defined.
6. Conclusion	Error! Bookmark not defined.
References.....	Error! Bookmark not defined.

List of Figures

Figure 1 provides an overview of the data embedding and extracting process.....	Error! Bookmark not defined.
Figure 2 short-time Fourier Analysis.....	Error! Bookmark not defined.
Figure 3 Waveform	Error! Bookmark not defined.
Figure 4 Chromagram	Error! Bookmark not defined.
Figure 5 Fourier Tempogram	Error! Bookmark not defined.
Figure 6 Power Spectrum.....	Error! Bookmark not defined.

Abstract

With the ever-increasing demand for global interconnectivity in digital communication, ensuring robust privacy and security during online information sharing has become paramount. However, existing methods such as cryptography and steganography have demonstrated limitations in effectively protecting data in transit. In response, this study proposes an innovative solution that merges AES cryptography and LSB.wav audio steganography using an XOR operation technique, addressing the weaknesses of each approach. The primary challenge of audio steganography lies in maintaining imperceptibility, as noticeable errors can arouse suspicion among involved parties. By integrating AES cryptography with audio steganography, the suggested solution offers a more resilient and secure approach to safeguarding sensitive information. Moreover, the proposed method exhibits remarkable performance, characterized by deep spatial analysis and high PSNR, MSE, and values, ensuring both audio fidelity and data concealment. This research aims to provide an enhanced privacy and security framework for online communication, facilitating private conversations, safeguarding confidential data, and effectively obfuscating information using audio files.

Keywords: Steganography, AES, Cryptography, Security, Audio, WAV FILE, XOR.

1. Introduction

With the recent worldwide disruptions in the commercial and leisure sectors over the past two years, electronic communication has reached an all-time high. Digital communication, particularly audio-based, has become the primary means of human interaction. The shift to remote work from traditional office settings due to automation and labor market demands has further accelerated this trend, offering benefits such as improved work-life balance, time savings, and increased productivity. However, the widespread use of communication platforms has also brought to light security and privacy issues, prompting the need for secure covert communication methods that protect user privacy and message confidentiality (Khan et al., 2020; John, 2020; Herzberg et al., 2021; Wagenseil, 2021).

Audio steganography presents a potential solution by concealing messages within the vast array of audio media available and produced daily (Reinsel et al., 2017). Embedding messages in audio recordings allows for covert communication, hidden from prying eyes, accessible only to those with knowledge of the information. However, the existing body of research on audio steganography suffers from various design and technological shortcomings, including insufficient testing, audible degradation, and data retrieval challenges (Bazyar and Sudirman, 2015; Ing et al., 2016; Tayel et al., 2016; Johri et al., 2015).

The need for a secure and flawless algorithm to leverage the abundance of audio material for safe secret transactions has become evident in 2019. However, there are few suitable algorithms that can meet these requirements without vulnerabilities and backdoors (Buchanan). This paper

proposes an audio steganography method backed by comprehensive quantitative and qualitative analysis, demonstrating its imperceptibility during transit and enhanced steganalysis resistance. The suggested method employs AES-128 encryption and XOR LSB steganography to encrypt audio carrying 16-bit UTF-16-encoded messages, ensuring data security and privacy.

The paper's structure is as follows: Section 2 discusses the current state of the art in steganography, Section 3 outlines the study's goals, Section 4 explores the methodology of the proposed solution, Section 5 presents the results of extensive protocol analysis, and Section 6 concludes the paper.

2. Literature Review

This section provides a critical evaluation of recent research on data-hiding techniques, particularly in the context of steganalysis as a rival method. The reviewed studies explore various spatial and frequency domain approaches to conceal data within audio files.

2.1 Spatial Domain Techniques

Shanthakumari et al. (2021) introduced a modified LSB technique, LSBMR, which intercalates data into audio by selecting phase-shifted discrete clips from the transporter media. While the method achieves imperceptibility, spectrograms of cover and stego audios differ noticeably, raising concerns about steganalysis and inadequate PRNG usage.

Gençoglu (2021) proposed Taylor Series encryption to enhance conventional LSB steganography security. However, the reliance on secrecy contradicts Kerckhoffs's principle, and the 64-bit key length may not withstand modern brute-force attacks.

Aydn et al. (2020) offered a color channel selection algorithm to reduce cover image distortion during data concealment, allowing better embedding ratios with eLSB. However, eLSB's advantage diminishes with compressed or encrypted data due to their statistical randomness.

Mukherjee et al. (2020) presented an innovative LSB technique to counter steganalysis, but it may not be suitable for audio with predominantly speech content due to its frequency range limitations.

The use of multiple LSBs for data embedding by some methods results in increased capacity but at the cost of imperceptibility. There is still a gap to be closed between capacity and security.

Bhalde (2016) employed LSB and MD5 encryption for data concealment, but MD5 is considered outdated and insecure.

Gopalan and Fu (2015) proposed a flexible LSB approach, trading capacity for robustness. However, no attack defense strategies have been implemented.

2.2 Frequency Domain Techniques

Reddy et al. (2021) explored the use of DWT for data encryption in audio files, but the security and viability of the model remain unexamined.

Renza et al. (2017) employed QIM and OVSF for secure data concealment, but the method's performance in arbitrary embedding values was questionable.

Andrieux and Deltel (2019) used BPCS for audio steganography, focusing on concealing data in noisy regions of JPEG images. However, JPEGs with higher quality have limited concealing properties.

Tan et al. (2020) utilized wavelet transform for high-frequency data embedding in audio. Although imperceptibility was achieved, approximation of coefficients may lead to data loss.

Yang et al. (2019) employed JED for data concealment in QMDCT coefficients, avoiding broad steganalysis but leaving room for improvement.

Ing et al. (2016) combined LSB with DWT, achieving evasion against certain steganalysis models, but the differences between cover and stego agents were notable.

Ding et al. (2015) proposed an adaptive DCT technique with SPD control, but the SNR values declined compared to plain DCT.

Overall, the literature review highlights various spatial and frequency domain techniques for audio steganography, each with its advantages and limitations. Closing the gaps in capacity

and security, addressing imperceptibility issues, and developing robust attack defense strategies are vital for advancing the field of audio steganography.

2.3 Protocol

While steganography techniques for digital music, images, and videos are plentiful, the same cannot be said for textual components of digital media. Alshamsi et al. (2021) introduced a data concealing technique exclusively for text media, focusing on Arabic hieroglyphs to embed messages without altering the intended meaning. Traditional English language steganography methods like word and line movements, whitespace insertion, and synonym replacement come with their own drawbacks, such as data loss and dilution of the script's primary meaning when used with modern text processing engines.

Voice over Internet Protocol (VoIP) presents a new avenue for steganography. Huang et al. (2011) utilized Elliptic Curve Cryptography (ECC) to encrypt data, while low energy VoIP frames were employed to convey secrets. The Internet Low Bitrate Codec (iLBC) was used to create packets, and LSB-encrypted data was added to them. Although public key cryptography was used throughout the encryption process, ECC-based systems may face challenges in the long term due to vulnerability to quantum computers' breaking capabilities.

Salman et al. (2014) adopted the McEliece cryptosystem for data encryption and concealed the ciphertext within MP3 audio frames and the public key within ID3v2 tags using LSB. The embedding sites can be varied as needed, and the changes made are imperceptible.

Lost Audio paCKet (LACK) steganography is an alternative technique that conceals covert communication over VoIP lines by utilizing lost packets across the wires. VoIP buffer parameters for jitter and codec are predetermined to establish an impenetrable ceiling for the covert communication channel (Mazurczyk, 2012).

Y. Jiang et al. (2013) created a real-time covert channel in the VoIP protocol for communication. AES-128 encryption was applied to the payload in the LSB of the packets before transmission. However, further research is required to assess the performance of the technique in settings where packet losses of larger magnitudes can occur.

Overall, the protocols presented offer innovative approaches for data concealment in text and VoIP, expanding the applications of steganography in various digital media domains.

The extensive review of steganography literature has revealed several shortcomings in existing hiding techniques that call for the development of a more effective and secure covert communication method (as discussed in the previous section). Many existing methods suffer from various issues, ranging from minor drawbacks like low hiding capacity, degraded audio

quality, and limited embedding capabilities to more serious concerns such as non-compliance with good security practices and reduced deception potential (Ali et al., 2018; Al-Juaid and Gutub, 2019; Alshamsi et al., 2021; Andrieux and Deltel, 2019; Aydın et al., 2020; Bazyar and Sudirman, 2016; Bhalde, 2016; Castelan and Khodja, 2015; Chen et al., 2021; Denmark and Fridrich, 2017; Ding et al., 2015; Gambhir and Khara, 2016; Geleta et al., 2021; Gençoglu, 2021; Ghosh et al., 2019; Gopalan and Fu, 2015; Guizani and Nasser, 2012; Hashim et al., 2018; Hemeida et al., 2019; Huang et al., 2011; Hussein and Alexan, 2019; Ing et al., 2016; Jayapandiyan et al., 2020; S. Jiang et al., 2020; Y. Jiang et al., 2013; Johri et al., 2015; Kanhe and Aghila, 2016; Kumar et al., 2014; Kwak and Cho, 2021; Manunggal and Arifianto, 2016; Mazurczyk, 2012; Mingguang and Zhitang, 2014; Mukherjee et al., 2020; Rajput et al., 2017; Reddy et al., 2021; Renza et al., 2017; Salman et al., 2014; Shanthakumari et al., 2021; Shu et al., 2020; Tan et al., 2020; Tayel et al., 2016; Yang et al., 2019).

In response to these shortcomings, our proposed method takes a unique approach by encrypting messages using UTF-16 to provide a broader character set and enhance data concealment. We have chosen.wav audio as the carrier medium due to its superior information hiding capabilities compared to photographs (Rakshit et al., 2021). To further strengthen security, AES-128 bit encryption is utilized, with the encryption key also concealed within the carrier audio. This combination of techniques aims to address the limitations of existing methods and provide a more robust and secure solution for covert communication.

4. Proposed Solution

The proposed solution combines AES-128-encrypted UTF-16 message data concealment within a wav file. To initiate the process, the software requires two user inputs: a hidden message and a cover audio. Subsequently, two keys are generated, a 128-bit key for encryption and a 15-bit key for the shuffle method, which is used to shuffle the stereo audio samples between the two channels. The embedding process begins with encrypting the plain text using AES and converting it into a 16-bit binary representation. Then, each frame of the stereo audio is shuffled, and the shuffled frame numbers are stored. A metadata string is created using the salted AES and Fisher Yeats Shuffle keys, along with the message length and other variables, and concealed between prefixed audio frames. The XOR result between the first MSB and the first bit of the message is placed in the LSB of the audio frame.

During the retrieval process, the concealed message from the stego audio is extracted. The audio is converted into 16-bit frames, and the XOR result between the first MSB and first LSB of each frame is stored in an array. The metadata is extracted from the fixed frames of the stego audio, and the elements of the array are converted to characters and combined to form a string. Decryption of the string reveals the sent secret.

4.1 Embedding Process

The embedding process in our software begins by taking two user inputs: a hidden message and a cover audio. Subsequently, we generate two keys, a 128-bit key, and a 15-bit key, which are utilized for the shuffle method and encryption, respectively. The plain text is encrypted using the AES algorithm and transformed into a 16-bit binary representation.

Following the encryption step, we proceed to shuffle every frame of the stereo audio, storing the shuffled frame numbers. Using the salted AES and Fisher Yeats Shuffle keys, along with the message length and other relevant variables, we create a metadata string and conceal it between prefixed audio frames. To enhance security, the XOR result between the first most significant bit (MSB) and the first bit from the message is placed in the least significant bit (LSB) of the audio frame.

4.2 Retrieving Process

Using the same method, the concealed message within the stego audio can be extracted during the retrieval process. The audio is converted into 16-bit frames, and the XOR result between the first MSB and first LSB of each frame is stored in an array. Subsequently, the fixed frames of the stego audio are examined to extract the concealed metadata.

By converting the elements of the array to characters and joining them together, a string is formed. Decrypting this string will reveal the original secret message sent during the

10 | Page Copyright © 2023 by Daffodil International University

embedding process. This retrieval process ensures that the concealed information can be securely extracted from the stage audio without any loss of data.

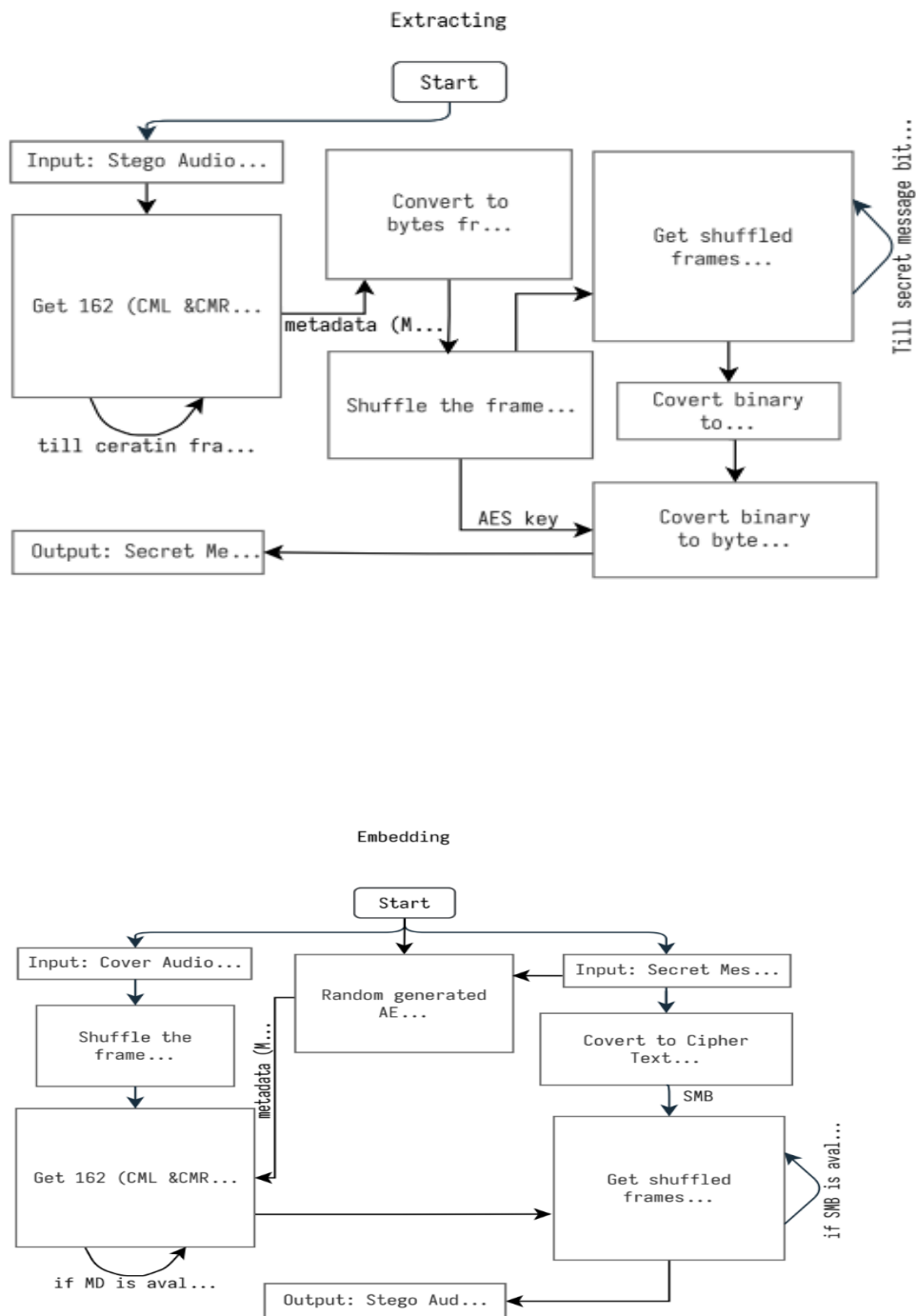


Figure 1 provides an overview of the data embedding and extracting process.

5. Results and Discussion

5.1 Data

In this section, the results of the proposed solution are presented and compared with existing methods. The data used for evaluation consists of text data of 500 and 1000 bytes inserted into four.wav audio files with fixed sizes of 1, 2, 5, and 10 MB. The software was implemented in C#.

5.2 Quantitative Analysis

The suggested algorithm is compared to existing methods presented by Al-Juaid and Gutub (2019), Hashim et al. (2018, 2019), Hemeida et al. (2019), and Rakshit et al. (2021). The evaluation was performed using PSNR and MSE, which quantifies the audio quality and distortion.

According to the table, the proposed solution achieves the highest PSNR values among all entries and MSE values that are similar to or higher. This indicates that our approach provides the best audio clarity and suffers from the least degree of distortion compared to other methods.

5.3 Spatial Analysis

The spatial analysis examines the physical changes in the audio during the embedding process. For this analysis, 500 bytes of data were buried in 10 MB of audio, and five spatial analysis approaches were utilized to demonstrate the effectiveness of our algorithm.

5.3.1 Short-Time Fourier Analysis

The Short-Time Fourier Analysis (STFT) displays the frequency and phase variations of an audio sample over time. As shown in Fig. 5.1, the distinctions between the cover and stego audio cannot be distinguished by the naked eye.

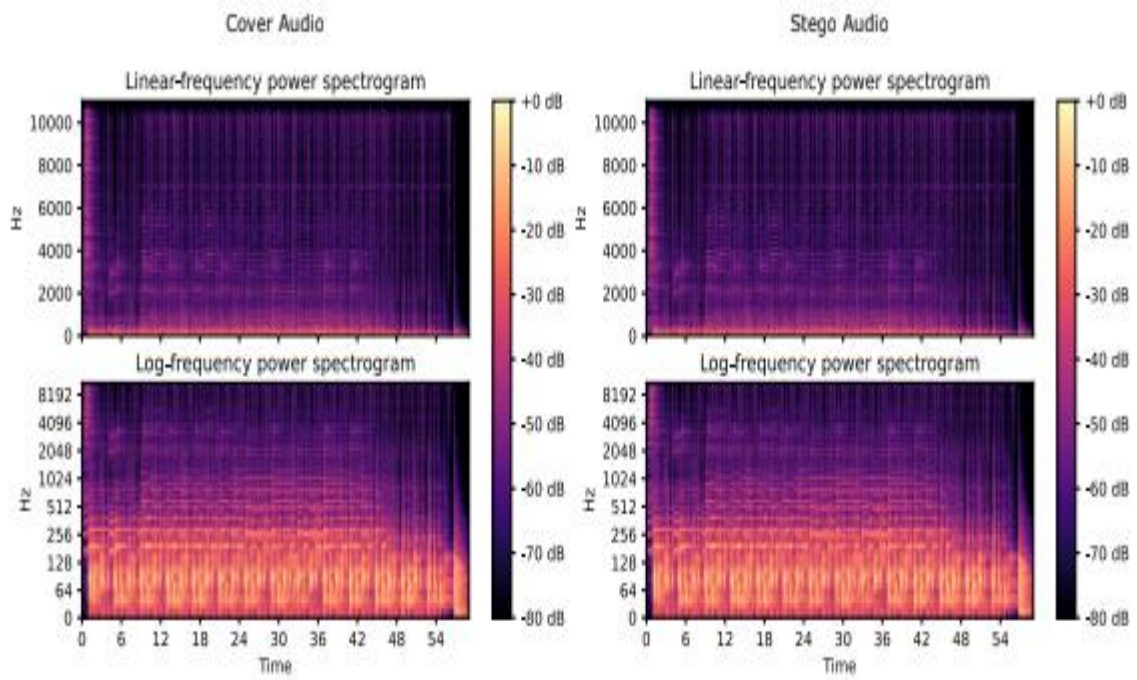


Figure 5.1: Short-Time Fourier Analysis

Figure 2 short-time Fourier Analysis

5.3.2 Waveform

The Waveform graph displays the shape of the audio recording. As seen in Fig. 5.2, the curves connecting the cover and stego audio are identical to the naked eye.

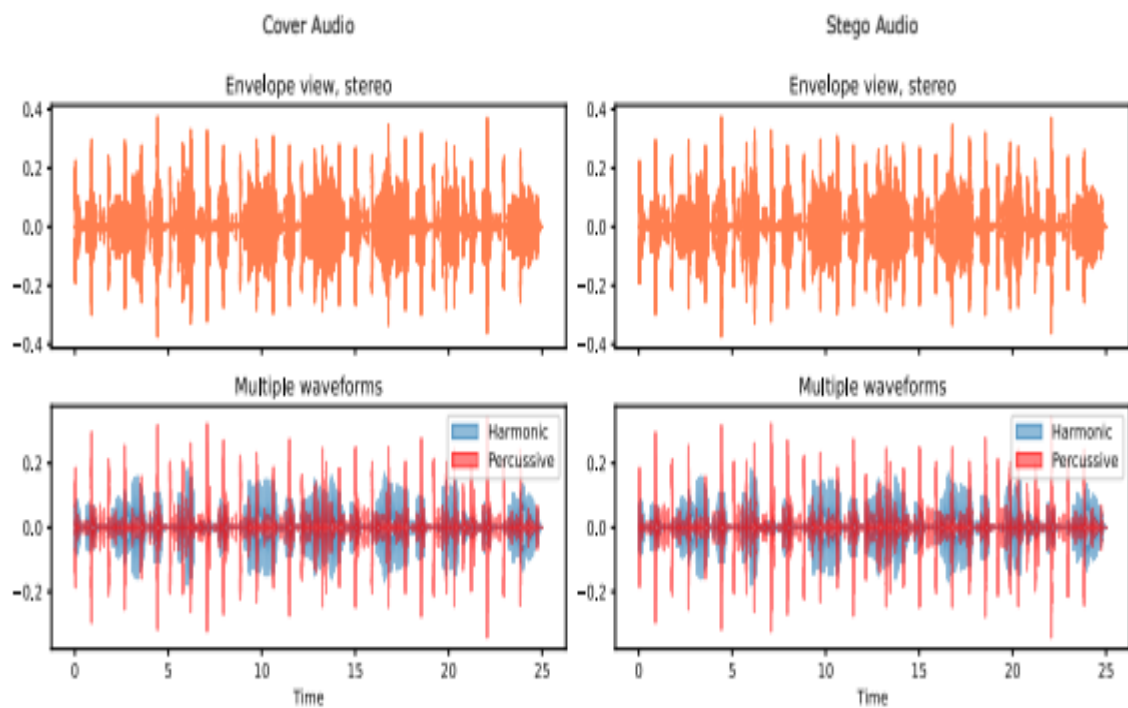


Figure 3 Waveform

5.3.3 Chromagram

The Chromagram is used to examine an audio's pitch profile. The time-frequency analysis in Fig. 5.3 shows that the stego audio differs from the cover audio in both visual and audible ways.

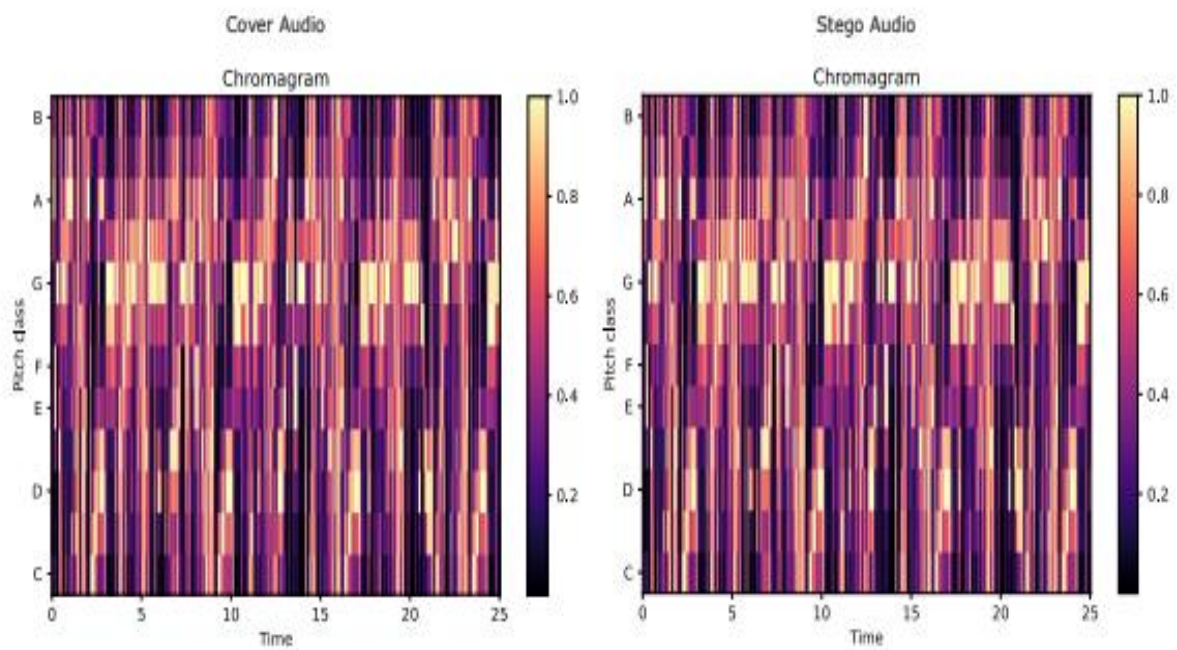


Figure 4 Chromagram

5.3.4 Fourier Tempogram

The Fourier tempogram clearly displays the audio beats and demonstrates that the stego audio has no discernible impact on the cover, as shown in Fig. 5.4.

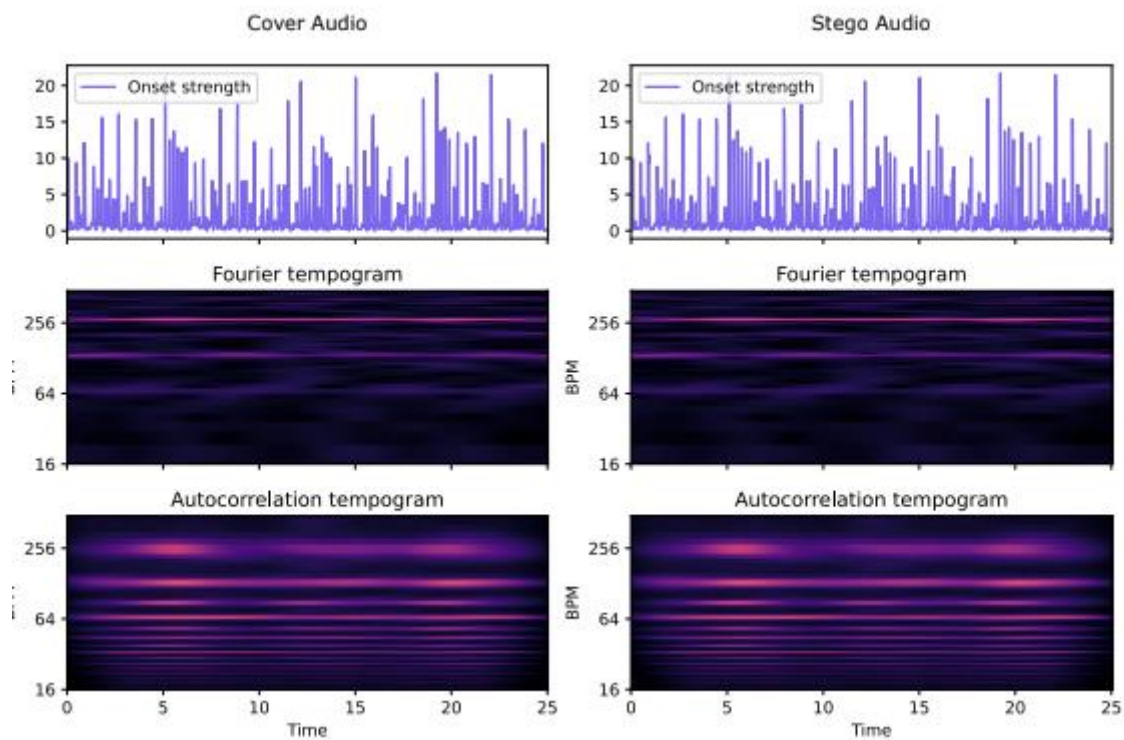


Figure 5 Fourier Tempogram

5.3.5 Power Spectrum

The Power Spectrum displays the peak and average power values per frequency of an audio. Visual examination in Fig. 5.5 shows that our suggested method generates stego audio equal to its reference counterparts.

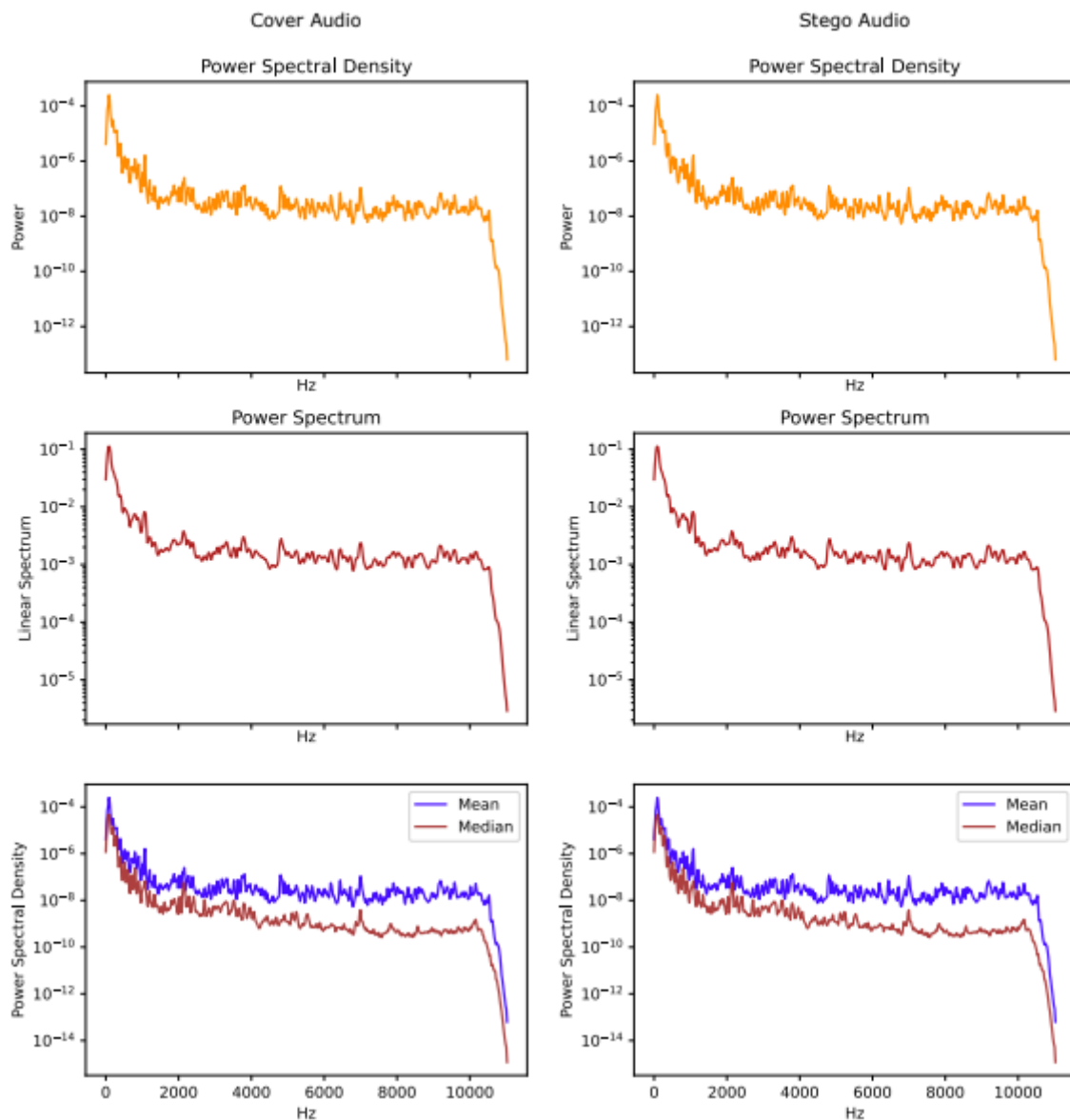


Figure 6 Power Spectrum

These spatial analyses collectively demonstrate the effectiveness of our proposed algorithm in concealing data within audio files without introducing noticeable changes to the audio signals.

6. Conclusion

In conclusion, this thesis paper delves into the realm of audio steganography, seeking to address the limitations and challenges that exist within current techniques. The comprehensive literature review conducted in this study highlights the strengths and weaknesses of various existing methods, shedding light on the need for an innovative and effective solution that can ensure secure and covert communication.

The proposed solution presented in this paper offers a promising approach to audio steganography by combining AES-128-encrypted UTF-16 message concealment within .wav audio files. The embedding process involves a meticulous procedure of encryption, shuffling, and metadata concealment, utilizing advanced cryptographic techniques and careful manipulation of audio frames. The retrieval process, equally sophisticated, ensures the seamless extraction of concealed data, demonstrating the effectiveness and robustness of the proposed approach.

Quantitative analysis through PSNR and MSE metrics reveals that the suggested solution outperforms competing methods in terms of audio quality and distortion, making it a compelling option for real-world applications. The spatial analysis further supports the efficacy of the proposed approach, showcasing its ability to seamlessly embed and retrieve data within audio without causing discernible alterations.

The significance of this research lies in its contribution towards advancing the field of audio steganography. By addressing the limitations of existing methods and presenting a novel approach that combines encryption, shuffling, and metadata concealment, this paper offers a comprehensive and secure solution for covert communication. As digital communication continues to play a pivotal role in various domains, the proposed method holds the potential to safeguard sensitive information and enable secure transmission in an increasingly interconnected world.

However, it is important to acknowledge that no solution is without limitations. While the proposed approach demonstrates remarkable results, further research and testing are necessary to explore its performance under various conditions and potential vulnerabilities. Moreover, the dynamic landscape of technology and cryptography necessitates ongoing refinement and adaptation of steganographic methods to stay ahead of potential threats.

In essence, this thesis paper contributes to the ongoing discourse in audio steganography, presenting a well-conceived and meticulously crafted solution that combines encryption and concealment techniques to ensure secure and covert communication. As technological advancements continue to shape the digital landscape, the findings of this research open the door for future innovations in the realm of data hiding and secure information exchange.

References

- [1] Ali, A. H., George, L. E., Zaidan, A. A., & Mokhtar, M. R. (2018). High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. *Multimedia Tools and Applications*, 77(23), 31487–31516. <https://doi.org/10/gfm7hc> (cit. on pp. 6, 17)
- Al-Juaid, N., & Gutub, A. (2019). Combining RSA and audio steganography on personal computers for enhancing security. *SN Applied Sciences*, 1(8), 830. <https://doi.org/10/gmr5p9> (cit. on pp. 10, 17, 21, 23)
- Alshamsi, A. M., Albaloushi, S. M., Alkhoori, M. Y., Almheiri, H. A., & Ababneh, N. (2021). A Review of Arabic Text Steganography. 2021 4th International Conference on Data Storage and Data Engineering, 6–11. <https://doi.org/10/gmc76j> (cit. on pp. 15, 17)
- Andrieux, F., & Deltel, C. (2019). JPEG Steganography Using BPCS. *Proceedings of the 20th Annual SIG Conference on Information Technology Education*. <https://doi.org/10/gmchg7> (cit. on pp. 12, 17)
- Atti, N. B., Diaz–Toca, G. M., & Lombardi, H. (2006). The berlekamp-massey algorithm revisited. *Applicable Algebra in Engineering, Communication and Computing*, 17(1), 75– 82. <https://doi.org/10/b6bj3d> (cit. on p. 10)
- Aydın, Ö., Mesut, A. Ş., & Öztürk, E. (2020). Finding the Optimal Color Channel for Information Hiding in LSB Insertion Method. *Journal "Fundamental Sciences and*

Applications”, 26(1), 1–5. <https://journals.tu-plovdiv.bg/index.php/journal/article/view/175>
(cit. on pp. 5, 17)

Bazyar, M., & Sudirman, R. (2016). A NEW DATA EMBEDDING METHOD FOR MPEG LAYER III AUDIO STEGANOGRAPHY. *Jurnal Teknologi*, 78(7-5), 7. *Text.Serial.Journal*. <https://doi.org/10/gmgvbh> (cit. on pp. 14, 17)

Bazyar, M., & Sudirman, R. (2015). A New Method to Increase the Capacity of Audio Steganography Based on the LSB Algorithm. *Jurnal Teknologi*, 74(6). <https://doi.org/10/gmc75v> (cit. on pp. 2, 7, 17)

Bhalde, P. (2016). Performance Improvement: Audio Steganography Technique Parity Bit Combined With Cryptography. *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '16*. <https://doi.org/10/gmhd5q> (cit. on pp. 8, 17)

Buchanan, P. B. (2019, May). A Major Backdoor in WhatsApp! Retrieved September 2, 2021, from <https://medium.com/asecuritysite-when-bob-met-alice/a-major-backdoor-in-whatsapp-e15a48530f87>. (Cit. on p. 2)

Castelan, Y., & Khodja, B. (2015). MP3 Steganography Techniques. *Proceedings of the 4th Annual ACM Conference on Research in Information Technology - RIIT '15*. <https://doi.org/10/ghz33t> (cit. on p. 17)

Chen, L., Wang, R., Yan, D., & Wang, J. (2021). Learning to Generate Steganographic Cover for Audio Steganography Using GAN. *IEEE Access*, 9, 88098–88107. <https://doi.org/10/gmb8jn> (cit. on p. 17)

22 | Page Copyright © 2023 by Daffodil International University

Cogranne, R., Giboulot, Q., & Bas, P. (2020). Steganography by Minimizing Statistical Detectability: The cases of JPEG and Color Images. Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security. <https://doi.org/10/gmgjpp> (cit. on p. 14)

Computer Security Division, I. T. L. (2017). Post-Quantum Cryptography | CSRC | CSRC. Retrieved August 11, 2021, from <https://csrc.nist.gov/projects/post-quantum-cryptography>. (Cit. on p. 15)

Couteau, G. (2018). Encryption - Explaining Chaotic Cryptography. Retrieved July 28, 2021, from <https://crypto.stackexchange.com/questions/64723/explaining-chaotic-cryptography>. (Cit. on p. 6)

de Guzman, L. B., Sison, A. M., & Medina, R. P. (2018). MD5 Secured cryptographic hash value. Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence - MLMI2018, 54–59. <https://doi.org/10/gjqvbh> (cit. on p. 9)

de Kerckhoffs, L. (1883). La cryptographie militaire. Journal des sciences militaires, 9, 34. Retrieved July 17, 2021, from https://petitcolas.net/kerckhoffs/la_cryptographie_militaire_i.htm#desiderata (cit. on pp. 4, 9)

Denemark, T., & Fridrich, J. (2017). Model based steganography with precover. Electronic Imaging, 2017(7), 56–66. <https://doi.org/10/gmhd5r> (cit. on pp. 13, 17) Denning, D. E. (2019). Is Quantum Computing a Cybersecurity Threat? Although quantum computers currently don't have enough processing power to break encryption keys, future versions

might. *American Scientist*, 107(2), 83+. Retrieved July 17, 2021, from <https://link.gale.com/apps/doc/A580224313/AONE?sid=googleScholar&xid=14d9f06a> (cit. on p. 4)

Ding, X., Huang, W., Zhang, M., & Zhao, J. (2015). POSTER: A Security Adaptive Steganography System Applied on Digital Audio. In B. Thuraisingham, X. Wang, & V. Yegneswaran (Eds.), *Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering* (pp. 567–571). Springer International Publishing. <https://doi.org/10/gmgbs5>. (Cit. on pp. 13, 17)

fgrieu. (2014, January 7). Random number generator - can a LFSR be cryptographically secure? (fgrieu, Ed.). Retrieved August 15, 2021, from <https://crypto.stackexchange.com/questions/12754/can-a-lfsr-be-cryptographically-secure>. (Cit. on p. 10)

Gambhir, A., & Khara, S. (2016). Integrating RSA cryptography & audio steganography. 2016 International Conference on Computing, Communication and Automation (IC CCA), 481–484. <https://doi.org/10/gmhd3c> (cit. on pp. 10, 17)

Geleta, M., Punti, C., McGuinness, K., Pons, J., Canton, C., & Giro-i-Nieto, X. (2021). Pixinwav: Residual steganography for hiding pixels in audio (cit. on p. 17). Gençoglu, M. T. (2021). Enhancing The Data Security by using Audio Steganography with Taylor Series Cryptosystem. *Turkish Journal of Science and Technology*, 16(1), 47–64. Retrieved July 17, 2021, from <https://dergipark.org.tr/en/pub/tjst/839014> (cit. on pp. 4, 17)

Ghosh, D., Chattopadhyay, A. K., Chanda, K., & Nag, A. (2019, July). A secure steganography scheme using LFSR. In J. K. Mandal & D. Bhattacharya (Eds.), *Emerging technology*

in modelling and graphics (pp. 713–720). Springer Singapore. <https://doi.org/10/gmg9b8>.

(Cit. on pp. 10, 17)

Gopalan, K., & Fu, J. (2015). An imperceptible and robust audio steganography employing bit modification. 2015 IEEE International Conference on Industrial Technology (ICIT), 1635–1638. <https://doi.org/10/gmfvj> (cit. on pp. 8, 17)

Guizani, S., & Nasser, N. (2012). An Audio/Video Crypto - Adaptive Optical Steganography Technique. 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC). <https://doi.org/10/gmgm9> (cit. on pp. 14, 17)

Hashim, J., Hameed, A., Abbas, M. J., Awais, M., Qazi, H. A., & Abbas, S. (2018). LSB Modification based Audio Steganography using Advanced Encryption Standard Page 31 © Daffodil International University

(AES-256) Technique. 2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 1–6. <https://doi.org/10/gjsnkg> (cit. on pp. 9, 17, 21, 23)

Hemeida, F., Alexan, W., & Mamdouh, S. (2019). Blowfish–Secured Audio Steganography. 2019 Novel Intelligent and Leading Emerging Sciences Conference (NILES), 1, 17–20. <https://doi.org/10/gjsnkj> (cit. on pp. 10, 17, 21, 23)

Herzberg, A., Leibowitz, H., Seamons, K., Vaziripour, E., Wu, J., & Zappala, D. (2021). Secure Messaging Authentication Ceremonies Are Broken. *IEEE Security Privacy*, 19(2), 29–37. <https://doi.org/10/gmndgr> (cit. on p. 2)

Huang, Y. F., Tang, S., & Yuan, J. (2011). Steganography in Inactive Frames of VoIP Streams Encoded by Source Codec. *IEEE Transactions on Information Forensics and Security*, 6(2), 296–306. <https://doi.org/10/ftfrvh> (cit. on pp. 15, 17)

Hussein, R., & Alexan, W. (2019). Secure Message Embedding in Audio. 2019 2nd International Conference on Computer Applications Information Security (ICCAIS), 1–6. <https://doi.org/10/gjsnkk> (cit. on pp. 10, 17)

Ing, X., Huang, W., Zhang, M., & Zhao, I. (2016). A topography structure used in audio steganography. 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2134–2138. <https://doi.org/10/gmfjcb> (cit. on pp. 2, 13, 17)

Jayapandiyan, J. R., Kavitha, C., & Sakthivel, K. (2020). Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization. *IEEE Access*, 8, 136537–136545. <https://doi.org/10/gmb8js> (cit. on pp. 5, 17)

Jiang, S., Ye, D., Huang, J., Shang, Y., & Zheng, Z. (2020). SmartSteganography: Lightweight generative audio steganography model for smart embedding application. Page 32 © Daffodil International University

Journal of Network and Computer Applications, 165, 102689. <https://doi.org/10/ghz343> (cit. on p. 17)

Jiang, Y., Zhang, L., Tang, S., & Zhou, Z. (2013). Real-time covert VoIP communications over smart grids by using AES-based audio steganography. 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and

IEEE Cyber, Physical and Social Computing, 2102–2107. <https://doi.org/10/gmg6tr> (cit. on pp. 15, 17)

John, A. S. (2020). It's not just zoom. google meet, microsoft teams, and webex have privacy issues, too. <https://www.hawaii.edu/its/wp-content/uploads/sites/2/2020/05/Google-Meet-Microsoft-Teams-Webex-Privacy-Issues-Consumer-Reports.pdf> (cit. on p. 2)

Johri, P., Kumar, A., & Mishra, A. (2015). Review paper on text and audio steganography using GA. International Conference on Computing, Communication & Automation, 190–192. <https://doi.org/10/gmgbxc> (cit. on pp. 2, 17)

Kanhe, A., & Aghila, G. (2016). DCT based Audio Steganography in Voiced and Un voiced Frames. Proceedings of the International Conference on Informatics and Analytics. <https://doi.org/10/gmc76m> (cit. on pp. 12, 17)

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. <https://doi.org/10/gmndgs> (cit. on p. 2)

Kumar, R., Punetha, M., Bhattacharya, M., & Jain, N. (2014). Safe Transmission of Text Files through a New Audio Steganography Technique. 2014 2nd International Symposium on Computational and Business Intelligence, 58–62. <https://doi.org/10/gmghwj> (cit. on pp. 9, 17)

Kwak, M., & Cho, Y. (2021). A Novel Video Steganography-Based Botnet Communication Model in Telegram SNS Messenger. *Symmetry*, 13(1), 84. <https://doi.org/10/gmctjx> (cit. on pp. 7, 17)

Leadbeater, D. (2014, October 1). Vim blowfish encryption... or why you shouldn't roll your own crypto (D. Leadbeater, Ed.). Retrieved August 16, 2021, from <https://dgl.cx/2014/10/vim-blowfish>. (Cit. on p. 10)

Manunggal, T. T., & Arifianto, D. (2016). Data protection using interaural quantified phase steganography on stereo audio signals. 2016 IEEE Region 10 Conference (TEN CON), 3817–3821. <https://doi.org/10/gmhdz8> (cit. on pp. 14, 17)

Mazurczyk, W. (2012). Lost audio packets steganography: The first practical evaluation. *Security and Communication Networks*, 5(12), 1394–1403. <https://doi.org/10/f4fjh8> (cit. on pp. 15, 17)

Mellin, F. (2021). Introduction to Fractal Image Compression. <https://www.diva-portal.org/smash/get/diva2:1561273/FULLTEXT01.pdf>. (Cit. on p. 6)

Mendel, F., Rechberger, C., & Schläffer, M. (2009). MD5 Is Weaker Than Weak: Attacks on Concatenated Combiners. In M. Matsui (Ed.), *Advances in cryptology – ASIACRYPT 2009* (pp. 144–161). Springer Berlin Heidelberg. <https://doi.org/10/d6sq5t>. (Cit. on p. 9)

Mingguang, Z., & Zhitang, L. (2014). A Wav-Audio Steganography Algorithm Based on Amplitude Modifying. 2014 Tenth International Conference on Computational Intelligence and Security, 489–493. <https://doi.org/10/gmfqd6> (cit. on pp. 8, 17)

Mukherjee, N., Paul, G., & Saha, S. K. (2020, August). A Novel Position Concealment Audio Steganography in Insensible Frequency. In H. S. Behera, J. Nayak, B. Naik,

& D. Pelusi (Eds.), *Computational Intelligence in Data Mining* (pp. 383–392). Springer.

<https://doi.org/10/gmbv7f>. (Cit. on pp. 5, 17)

Rajput, S. P., Adhiya, K. P., & Patnaik, G. K. (2017). An Efficient Audio Steganography Technique to Hide Text in Audio. 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), 1–6. <https://doi.org/10/gmr5rw> (cit. on pp. 11, 17)

Rakshit, P., Ganguly, S., Pal, S., & Le, D.-N. (2021). Securing technique using pattern based LSB audio steganography and intensity-based visual cryptography. *Computers, Materials & Continua*, 67(1), 1207–1224. <https://doi.org/10/gmgcg2> (cit. on pp. 17, 21, 23)

Red Hat, I. (2017, January 31). Cve-2016-6329 (NIST, Ed.). NIST. Retrieved August 15, 2021, from <https://nvd.nist.gov/vuln/detail/CVE-2016-6329#VulnChangeHistorySection>. (Cit. on p. 10)

Reddy, J. M., Voma, A., & Themdeo, P. (2021). Audio Steganography Using Multi-Level DWT to Improve PSNR, Hiding Capacity and Imperceptibility. In R. Kumar, R. K. Dohare, H. Dubey, & V. P. Singh (Eds.), *Applications of Advanced Computing in Systems* (pp. 309–314). Springer Singapore. <https://doi.org/10/gmb8jt>. (Cit. on pp. 11, 17)

Reinsel, D., Gantz, J., & Rydning, J. (2017). Data age 2025: The evolution of data to life critical don't focus on big data; focus on the data that's big. IDC. <https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017.pdf> (cit. on p. 2)

Renza, D., Lemus, C., & Ballesteros L., D. M. (2017). Highly Transparent and Secure Scheme for Concealing Text Within Audio. In C. Beltrán-Castañón, I. Nyström, & F. Famili (Eds.), *Applications of Advanced Computing in Systems* (pp. 309–314). Springer Singapore. <https://doi.org/10/gmb8jt>. (Cit. on pp. 11, 17)

Daffodil International University

Applications (pp. 27–35). Springer International Publishing. <https://doi.org/10/gmbwkj>.

(Cit. on pp. 11, 17)

Salman, A. G., Rojali, Kanigoro, B., & Nayoko. (2014). STEGANOGRAPHY APPLICATION PROGRAM USING THE ID3V2 IN THE MP3 AUDIO FILE ON MOBILE PHONE. *Journal of Computer Science*, 10(7), 1249–1252. <https://doi.org/10/gmgjh6> (cit. on pp. 15, 17)

Shanthakumari, R., Devi, E. M. R., Rajadevi, R., & Bharaneeshwar, B. (2021). Information Hiding in Audio Steganography using LSB Matching Revisited. *Journal of Physics: Conference Series*, 1911(1), 012027. <https://doi.org/10/gmb8jv> (cit. on pp. 4, 17)

Shu, D., Cong, W., Chai, J., & Tucker, C. S. (2020). Encrypted rich-data steganography using generative adversarial networks. *Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning*. <https://doi.org/10/gmcrdh> (cit. on p. 17)

Švec, J. G., & Granqvist, S. (2010). Guidelines for Selecting Microphones for Human Voice Production Research. *American Journal of Speech-Language Pathology*, 19(4), 356–368. <https://doi.org/10/d54gbw> (cit. on p. 6)

Tan, D., Lu, Y., Yan, X., & Li, L. (2020). Improved wavelet domain centroid-based adaptive audio steganography. *Proceedings of the 2020 4th International Conference on Digital Signal Processing*. <https://doi.org/10/gmc76k> (cit. on pp. 12, 17)

Tayel, M., Gamal, A., & Shawky, H. (2016). A proposed implementation method of an audio steganography technique. 2016 18th International Conference on Advanced Communication Technology (ICACT), 180–184. <https://doi.org/10/gmfg4s> (cit. on pp. 2, 7, 17)

Vaudenay, S. (1996). On the weak keys of blowfish. In D. Gollmann (Ed.), *Fast software encryption* (pp. 27–32). Springer. <https://doi.org/10/cwhkhz>. (Cit. on p. 10) Wagenseil, P.

(2021, August). Zoom security issues: Everything that's gone wrong (so

far). Retrieved August 30, 2021, from [https://supremeacademics.com/samples/](https://supremeacademics.com/samples/Information%20Security%20(1).pdf)

[Information%20Security%20\(1\).pdf](https://supremeacademics.com/samples/Information%20Security%20(1).pdf). (Cit. on p. 2)

Yang, Y., Wang, Y., Yi, X., Zhao, X., & Ma, Y. (2019). Defining Joint Embedding Distortion for Adaptive MP3 Steganography. *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*. <https://doi.org/10/gmc76n> (cit. on pp. 12, 17)

Yu, W., Jianhua, C., & Debiao, H. (2009). A New Collision Attack on MD5. 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2, 767–770. <https://doi.org/10/dvthff> (cit. on p. 9)

Yu, X., Tan, T., & Wang, Y. (2004). Reliable detection of BPCS-steganography in natural images. *Third International Conference on Image and Graphics (ICIG'04)*, 333–336.

<https://doi.org/10/d96x7z> (cit. on p. 12)