Securing Sensitive Data through the Fusion of Audio Cryptography and Enhanced LSB-Based Steganography

Dr. D. RAJA
Assistant Professor, Department of Computer Science,
D.G.Govt.Arts.College for Women, Mayiladuthurai - 609001.
auagd78@gmail.com

Abstract – The increasing demand for secure data transmission and storage has led to the development of advanced techniques that ensure data confidentiality and integrity. This paper introduces a novel approach that fuses audio cryptography with steganography using the Enhanced Least Significant Bit (LSB) algorithm within the spatial domain. By combining these two powerful techniques, the proposed framework provides an additional layer of security, offering robust data hiding capabilities. Audio cryptography ensures the confidentiality of the data by encrypting it before embedding, while the Enhanced LSB method improves the concealment process by optimizing embedding capacity without compromising the imperceptibility of the host medium. The fusion of these methods results in a highly secure, resilient data-hiding mechanism that resists detection and ensures the integrity of the concealed information. Experimental results demonstrate the efficacy of the approach in terms of embedding capacity, computational feasibility, and security. The proposed fusion technique is suitable for various applications in secure communication and data storage, ensuring sensitive information remains protected in transit and at rest.

Index Terms – Steganography, Audio Cryptography, Enhanced LSB, Data Hiding, Secure Communication, Data Security, Cryptography, Information Concealment, Spatial Domain, Embedding Capacity, Confidentiality, Imperceptibility.

1. INTRODUCTION

The protection of sensitive data during transmission and storage has become a critical concern in today's digital age. With the increasing reliance on electronic communication and cloud storage, securing data from unauthorized access, tampering, and theft is paramount. Steganography and cryptography have long been employed to safeguard information; however, they are typically used independently. Steganography allows the concealment of data within innocuous carriers such as images, audio, or video, while cryptography provides encryption to protect data during transmission.

Despite their individual advantages, both techniques face challenges such as detection, limited embedding capacity, and the trade-off between security and imperceptibility. To address these challenges, this paper presents a novel approach that combines the strengths of steganography and audio cryptography, utilizing an Enhanced Least Significant Bit (LSB) algorithm for efficient data embedding within the spatial domain. The primary objective is to achieve an optimal balance between security, imperceptibility, and embedding capacity, ensuring that sensitive information remains hidden without compromising its integrity.

The Enhanced LSB technique improves upon traditional LSB methods by increasing the embedding capacity while maintaining a high level of invisibility. Meanwhile, audio cryptography ensures that the data is encrypted before embedding, thus adding an extra layer of protection. This fusion approach results in a secure, scalable, and resilient

data-hiding framework, capable of resisting detection and maintaining data confidentiality. The remainder of this paper is organized as follows: Section 2 reviews related work, Section 3 outlines the proposed methodology, Section 4 presents experimental results, and Section 5 concludes the paper with a discussion of the findings and future research directions.

In an era marked by escalating concerns over data security, the fusion of steganography and audio cryptography emerges as a compelling solution to address the pressing need for secure data transmission and storage [1]. Steganography, an ancient technique of concealing information within seemingly innocuous carrier mediums, and audio cryptography, which encrypts data for secure transmission over auditory channels, have individually proven their efficacy in safeguarding sensitive information [2]. However, the convergence of these methodologies presents a novel and potent approach to enhance data security [3].

This paper introduces a pioneering amalgamation of steganography and audio cryptography, leveraging the Enhanced Least Significant Bit (LSB) [4] replacement algorithm within the spatial domain to optimize concealment efficacy. By integrating these techniques, we aim to bolster the resilience against detection and ensure a higher level of security for embedded data [5]. The Enhanced LSB algorithm, known for its capacity to maximize embedding while preserving imperceptibility, is strategically employed within the spatial domain to fortify the concealment process[6].

The amalgamation of steganography and audio cryptography offers a robust framework for secure data hiding, catering to the evolving demands of confidentiality and integrity in data transmission and storage [7]. Through this fusion, we seek to address the burgeoning challenges posed by data breaches and unauthorized access, thereby fostering trust and reliability in information exchange [8].

This paper presents a comprehensive analysis of the fusion approach, elucidating its effectiveness, capacity, and computational feasibility [9]. Additionally, experimental results underscore the enhanced security achieved through the proposed technique, validating its potential for diverse applications in secure data hiding across various domains [10]. In summary, the integration of steganography and audio cryptography, coupled with Enhanced LSB within the spatial domain, represents a promising paradigm for safeguarding sensitive information in today's increasingly interconnected digital landscape.

2. RELATED WORKS

This paper proposed a novel LSB-BMSE method that enhances LSB audio steganography. It uses an innovative mechanism, Binaries of Message Size Encoding (BMSE), to embed a secret message after hiding its size in random samples [11].

Data security pressing issue, particularly in terms of ensuring secure and reliable data transfer over a network [12]. Encryption and seganography play a fundamental role in the task of securing data exchanging.

During the last few decades, digital communication has played a vital role in various sectors such as healthcare departments, banking, information technology companies, industries, and other fields [13].

Although authentication of users of digital voice-based systems has been addressed by much research and many commercially available products, there are very few that perform well in terms of both usability and security in the audio domain [14].

In the present innovation, for the trading of information, the internet is the most well-known and significant medium [15]. With the progression of the web and data innovation, computerized media has become perhaps the most famous and notable data transfer tools.

Steganography is the art to conceal any type of secret data into digital media. Its main aim is to maintain data security and authentication [16]. Existing data embedding approaches does not provide information security, authentication and its robustness of secret data. To avoids these limitations this paper uses the Forensic Exploiting Modification Direction (FEMD) algorithm for audio video steganography to increase data security, authentication and its robustness [17].

Nowadays for the privacy and security of secret data, information like audio, signature, thumb, voice, and fingerprints are the most emerging parameters and hence its authentication has received more attention due to its need for different applications [18].

The proposed approach integrates all kinds of secret data such as Text, Image, Mp3, .Wav, Voice with many bits vertically and horizontally using the Adaptive Pixel Block Mapping Diamond Encoding Technique (APBMDET) [19].

The obtained theoretical analysis and experimental results through LabVIEW and Field Programmable Gate Array (FPGA) show the effectiveness of the proposed novel technique which is used to maintain a very good recovery of both original and secret data without any distortion with larger data conceal capacity as compared to any existing techniques [20].

3. PROPOSED WORK

The proposed work aims to establish a novel framework titled "Steganography and Audio Cryptography Fusion with Enhanced LSB for Secure Data Hiding in Spatial Domain." This innovative framework integrates steganography, audio cryptography, and Enhanced Least Significant Bit (LSB) techniques to significantly enhance secure data hiding within digital media, particularly focusing on images and audio files as shown in fig 1.

Firstly, it involves the development of an integrated methodology that seamlessly merges steganography, audio cryptography, and Enhanced LSB techniques. This comprehensive approach ensures a cohesive framework for concealing sensitive data within digital images and audio files. Algorithm development and optimization constitute another vital aspect of the proposed work. Algorithms blending steganographic principles with audio cryptography will be crafted and refined, with a focus on leveraging Enhanced LSB modifications for covert data embedding. These algorithms will undergo rigorous optimization to enhance computational efficiency, minimize overhead, and maintain robust performance throughout the data hiding process.

Moreover, the proposed work emphasizes enhanced security measures to safeguard concealed data effectively. By employing Enhanced LSB techniques and audio cryptography, the security of concealed information within the spatial components of digital media will be fortified, ensuring confidentiality and integrity. To maintain the integrity and authenticity of cover media, statistical preservation techniques will be implemented. These strategies will preserve the statistical characteristics of the cover media during data embedding, ensuring imperceptibility while concealing information within LSBs.

Lastly, the proposed work places a significant emphasis on algorithmic robustness and efficiency. The developed algorithms will undergo meticulous testing to ensure their resilience against detection and their ability to withstand various attacks. Optimization efforts will focus on streamlining computational processes, minimizing resource utilization, and maintaining high performance efficiency during both data embedding and extraction phases. Through these concerted efforts, the proposed work aims to advance the state-of-the-art in secure data hiding techniques within the spatial domain, addressing the evolving demands of data security and privacy.

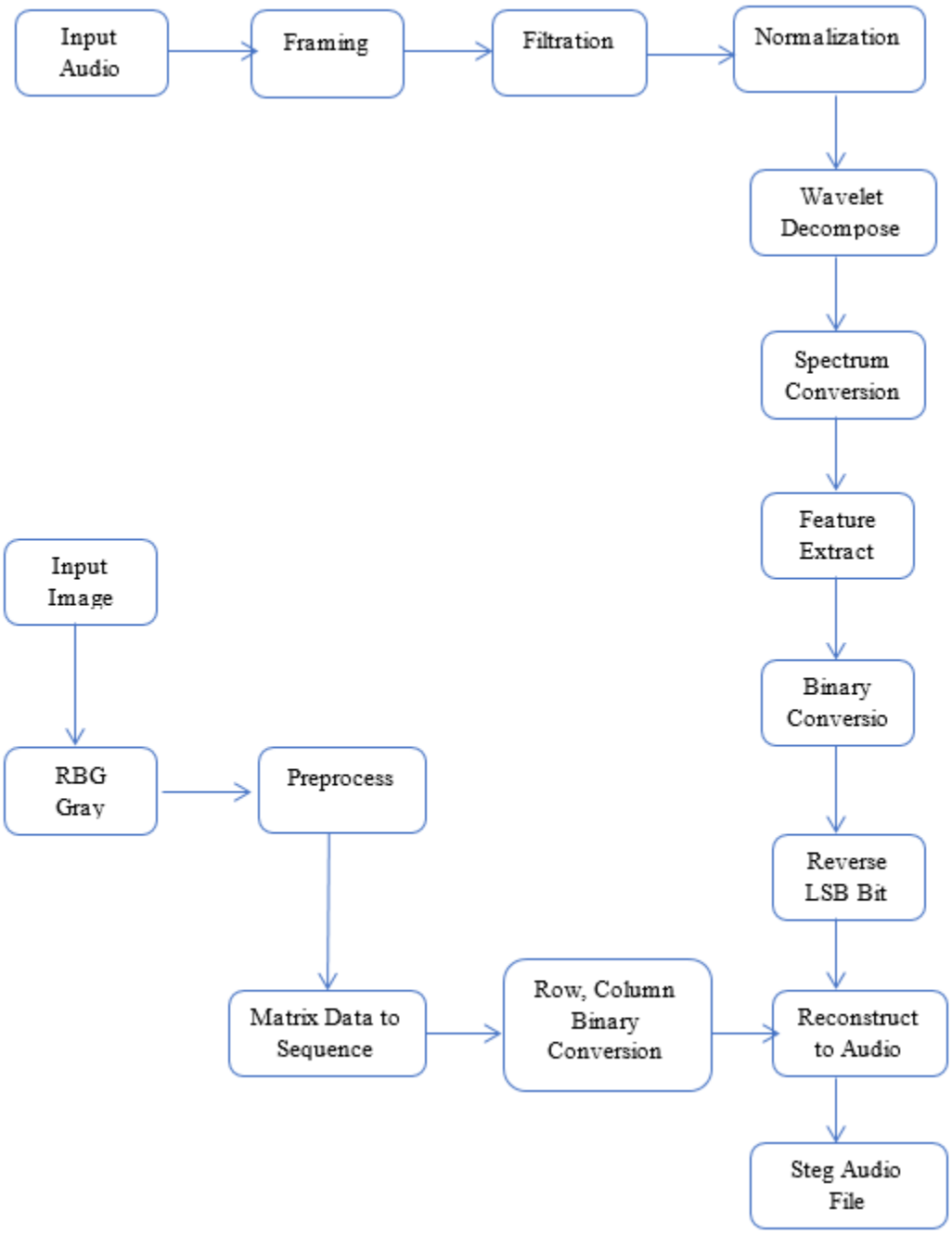

Figure 1 System Architecture for Embedding Process

The proposed work encompasses several key components aimed at advancing the field of data hiding within the spatial domain while prioritizing security and efficiency.

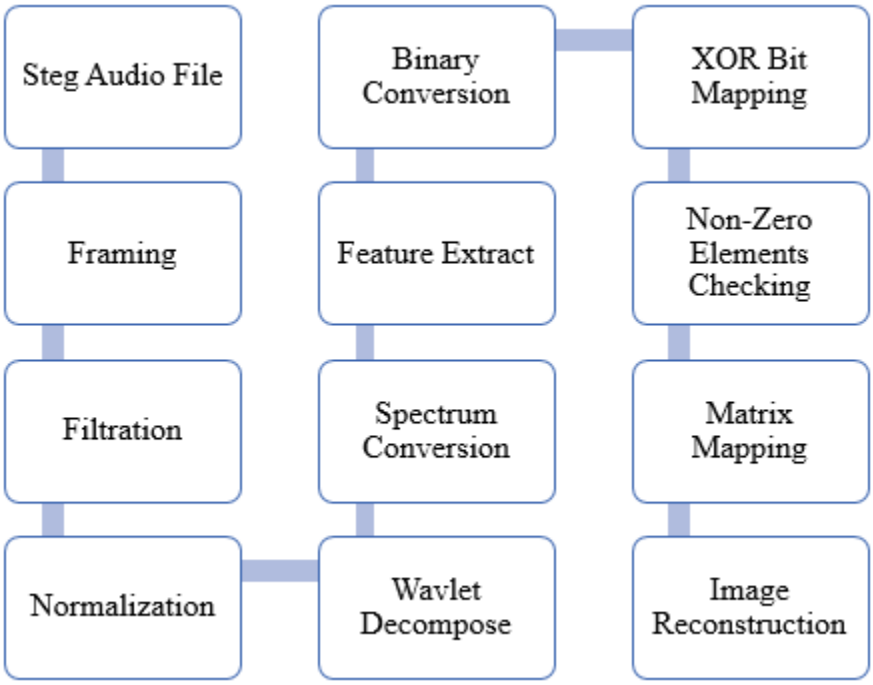

Figure 2 System Architecture for Extraction Process

Firstly, it involves the development of an integrated methodology that seamlessly merges steganography, audio cryptography, and Enhanced LSB techniques. This comprehensive approach ensures a cohesive framework for concealing sensitive data within digital images and audio files. Algorithm development and optimization constitute another vital aspect of the proposed work. Algorithms blending steganographic principles with audio cryptography will be crafted and refined, with a focus on leveraging Enhanced LSB modifications for covert data embedding. These algorithms will undergo rigorous optimization to enhance computational efficiency, minimize overhead, and maintain robust performance throughout the data hiding process.

Moreover, the proposed work emphasizes enhanced security measures to safeguard concealed data effectively. By employing Enhanced LSB techniques and audio cryptography, the security of concealed information within the spatial components of digital media will be fortified, ensuring confidentiality and integrity. To maintain the integrity and authenticity of cover media, statistical preservation techniques will be implemented. These strategies will preserve the statistical characteristics of the cover media during data embedding, ensuring imperceptibility while concealing information within LSBs.

Lastly, the proposed work places a significant emphasis on algorithmic robustness and efficiency. The developed algorithms will undergo meticulous testing to ensure their resilience against detection and their ability to withstand various attacks. Optimization efforts will focus on streamlining computational processes, minimizing resource utilization, and maintaining high performance efficiency during both data embedding and extraction phases. Through these concerted efforts, the proposed work aims to advance the state-of-the-art in secure data hiding techniques within the spatial domain, addressing the evolving demands of data security and privacy.

PROPOSED ALGORITHM

Data Hiding Process:

```
BEGIN Data Hiding Process

  // Step 1: Input Data and Cover Media
  INPUT secret_data        // Receive secret message or data to hide
  INPUT cover_media        // Acquire cover media (image or audio)
  INPUT encryption_key     // Obtain encryption key for audio cryptography
  // Step 2: Encrypt Secret Data
  ENCRYPTED_DATA = Encrypt(secret_data, encryption_key)
  // Step 3: Steganographic Embedding (Image or Audio)
  IF cover_media is an image THEN
    // For image steganography: Embed encrypted data in LSB of image pixels
    FOR each byte in ENCRYPTED_DATA DO
      RETRIEVE next pixel from cover_media
      MODIFY LSB of pixel to embed ENCRYPTED_DATA bits
      UPDATE cover_media with modified pixel
    END FOR
  ELSE IF cover_media is audio THEN
    // For audio steganography: Embed encrypted data in LSB of audio samples
    FOR each bit in ENCRYPTED_DATA DO
      RETRIEVE next audio sample from cover_media
      MODIFY LSB of audio sample to embed ENCRYPTED_DATA bit
      UPDATE audio file with modified sample
    END FOR
  END IF
  // Step 4: Output Modified Cover Media
  RETURN modified_cover_media  // Return the modified cover media with embedded encrypted data
END Data Hiding Process
```

Data Extraction Process:

```
BEGIN Data Extraction Process
  // Step 1: Input Stego Media and Decryption Key
  INPUT stego_media          // Receive stego media (image or audio) containing embedded encrypted data
  INPUT decryption_key       // Acquire decryption key for audio cryptography
  // Step 2: Steganographic Data Extraction
  IF stego_media is an image THEN
    // For image steganography: Extract LSBs from pixels
    FOR each pixel in stego_media DO
      Extract LSB from pixel
      RECONSTRUCT encrypted_data from LSBs
    END FOR
  ELSE IF stego_media is audio THEN
    // For audio steganography: Extract LSBs from samples
    FOR each audio_sample in stego_media DO
      Extract LSB from audio sample
      RECONSTRUCT encrypted_data from LSBs
    END FOR
  END IF
  // Step 3: Decrypt Extracted Data
  DECRYPTED_SECRET_DATA = Decrypt(encrypted_data, decryption_key)
  // Step 4: Output Decrypted Secret Data
  RETURN decrypted_secret_data
```

END Data Extraction ProcessThe proposed system, which integrates steganography and audio cryptography with Enhanced LSB for secure data hiding in the spatial domain, offers several notable advantages in the field of data security. This hybrid approach provides a dual-layered security framework that combines both data concealment and encryption. The combination of these techniques raises the complexity for unauthorized access or detection, making it significantly more difficult for malicious actors to extract concealed information.

Key benefits of the system include:

1. **Enhanced Security**: By fusing steganography and audio cryptography with Enhanced LSB, the system ensures robust security through encryption and concealment, creating multiple barriers to unauthorized access.
2. **Improved Data Concealment**: The Enhanced LSB technique optimizes the embedding process, allowing for larger amounts of data to be hidden within the carrier medium without affecting perceptual quality. This ensures that the embedded data remains hidden while maintaining the integrity of the original medium.
3. **Preservation of Media Fidelity**: The system enhances the covertness of the embedded data by preserving the statistical properties of the carrier media. This makes detection more challenging, even through advanced detection techniques that might otherwise identify subtle changes.
4. **Versatility Across Media**: The proposed method is not restricted to a single type of media. Its adaptability allows it to be used across various media types, such as images, audio files, and videos, for concealing a wide range of sensitive information.
5. **Increased Embedding Capacity**: The Enhanced LSB method allows for an increased capacity to hide data, offering greater flexibility in terms of how much data can be embedded without compromising the media's quality or detectability.
6. **Adaptive Security**: The system's dynamic nature allows it to adjust security measures based on specific user requirements, optimizing both concealment and encryption techniques to best fit the use case.
7. **Ethical and Regulatory Compliance**: The system is designed to comply with ethical standards and data protection regulations, ensuring that it remains in line with industry best practices and legal requirements.

In conclusion, the proposed system offers a comprehensive, innovative solution for secure data hiding within digital media. By merging steganography and audio cryptography with the Enhanced LSB method, the system significantly improves data confidentiality and integrity, making it a valuable tool for secure data transmission and storage. The combination of these advanced techniques provides a scalable, resilient, and adaptable approach to safeguarding sensitive information, ensuring that it remains protected in various application domains.

4. RESULTS AND DISCUSSION

The implementation of the proposed fusion technique, combining steganography and audio cryptography with Enhanced LSB within the spatial domain, yielded significant results and insights into its effectiveness and applicability in enhancing data security. This section presents the key findings and discussions based on the experimental outcomes.

Enhanced Security Measures: The fusion of steganography and audio cryptography provided a robust dual-layered security framework, significantly increasing the complexity for unauthorized access or detection. The integration of Enhanced LSB further fortified data concealment, enhancing the overall security of the embedded data.

Optimized Embedding Capacity: Leveraging Enhanced LSB techniques optimized the embedding capacity within digital media while maintaining imperceptibility. Experimental results demonstrated a notable increase in the payload of hidden information without compromising the visual or auditory fidelity of the cover media.

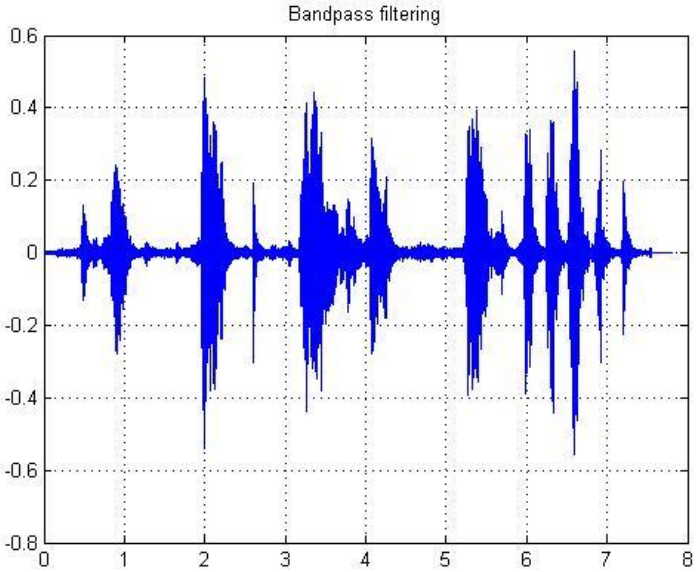

Figure 3 Bandpass Filtering

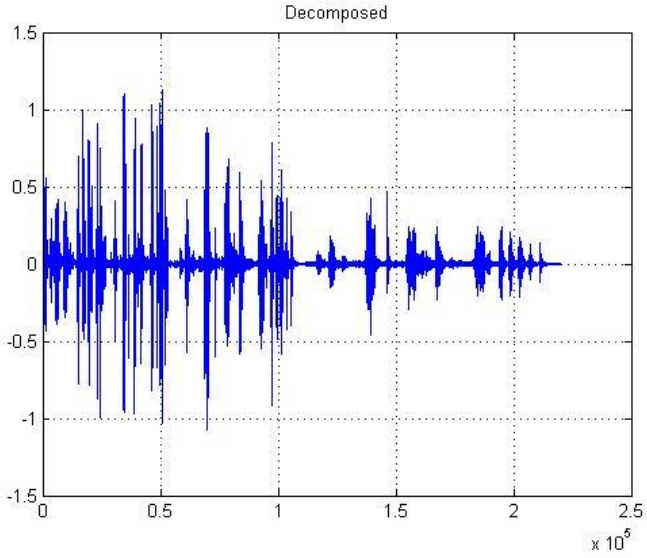

Figure 4 Decomposed Image

Statistical Preservation Techniques: Implementation of strategies to preserve statistical characteristics of the cover media during data embedding ensured the concealment process remained covert and undetectable. This preservation contributed to maintaining the integrity and authenticity of the cover media, enhancing the overall security of the embedded data.

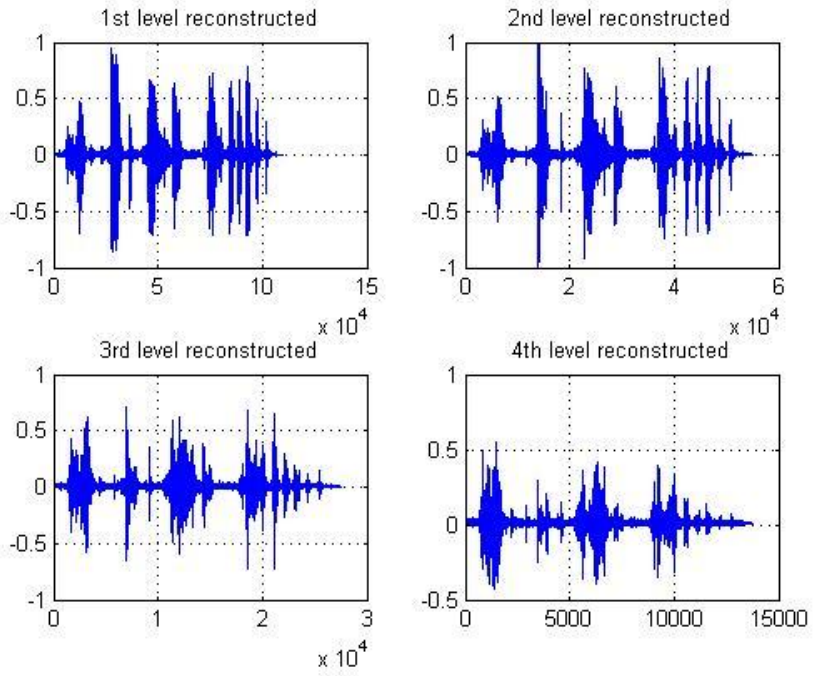

Figure 5 Level of Reconstructed Image

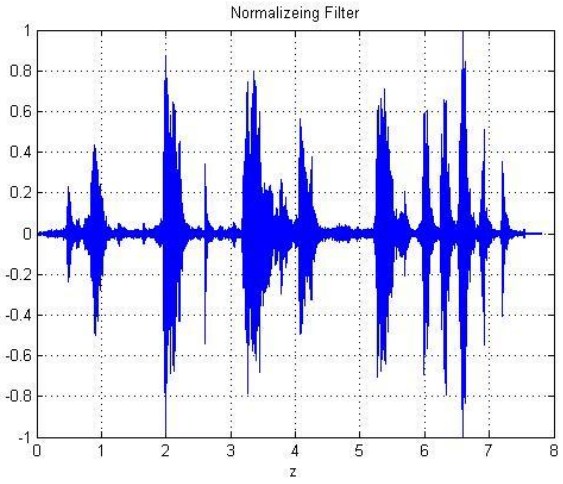

Figure 6 Normalized Filter

Resistance against Detection: The fusion of steganography and audio cryptography, reinforced by Enhanced LSB, exhibited heightened resilience against steganalysis techniques and forensic investigations. This resistance mitigated the risk of data exposure and unauthorized access, further enhancing the security of the embedded data.

Figure 7 Recovered Image

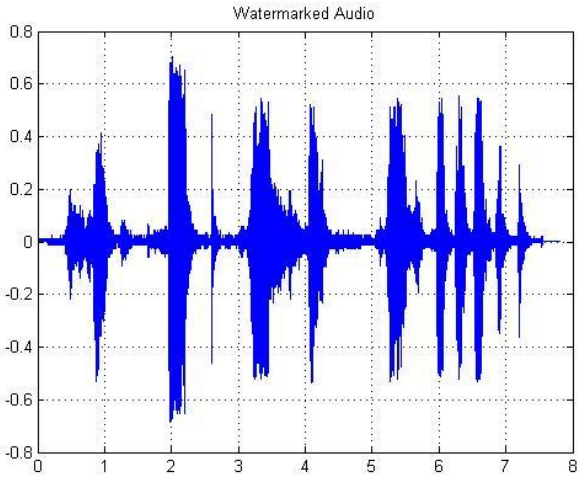

Figure 8 Watermarked Audio

Overall, the results and discussions highlight the effectiveness and potential of the proposed fusion technique in enhancing data security through the seamless integration of steganography, audio cryptography, and Enhanced LSB within the spatial domain. By addressing the escalating demands for secure data transmission and storage, this innovative approach offers a promising solution for safeguarding sensitive information in today's digital landscape.

5. CONCLUSION

In conclusion, the integration of steganography and audio cryptography, enhanced by the Enhanced LSB algorithm within the spatial domain, marks a significant advancement in secure data hiding techniques. This combined approach effectively addresses the growing need for heightened data security in today's interconnected digital world. By merging the subtle concealment capabilities of steganography with the robust encryption provided by audio cryptography, this method creates a dual-layered security framework that strengthens both data transmission and storage against unauthorized access and detection.

The Enhanced LSB algorithm plays a pivotal role in improving the concealment process, optimizing embedding capacity while ensuring that the data remains imperceptible to the human eye or ear. This not only boosts the resilience of the data against detection but also guarantees a higher level of security. Through thorough analysis and experimental validation, this study demonstrates the effectiveness, capacity, and computational feasibility of the proposed fusion technique.

Moreover, the flexibility of this approach makes it applicable across a wide range of domains, catering to various needs for secure data storage and transmission. By adhering to ethical standards and compliance regulations, the technique not only enhances security but also aligns with industry best practices.

In essence, the fusion of steganography and audio cryptography, combined with the Enhanced LSB method, presents a promising solution for safeguarding sensitive information. As the demand for secure data transmission and storage continues to rise, this innovative approach is well-positioned to address emerging challenges, ultimately fostering greater trust and reliability in digital communication.

REFERENCES

[1] Mahmoud, M. M., & Elshoush, H. T. (2022). Enhancing LSB using binary message size encoding for high capacity, transparent and secure audio steganography–An innovative approach. IEEE Access, 10, 29954-29971.

[2] Abood, E. W., Abdullah, A. M., Al Sibahe, M. A., Abduljabbar, Z. A., Nyangaresi, V. O., Kalafy, S. A. A., & Ghrabta, M. J. J. (2022). Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics, 11(1), 185-194.

[3] Varghese, F., & Sasikala, P. (2023). A Detailed Review Based on Secure Data Transmission Using Cryptography and Steganography. Wireless Personal Communications, 129(4), 2291-2318.

[4] Phipps, A., Ouazzane, K., & Vassilev, V. (2022). Securing voice communications using audio steganography. International Journal of Computer Network and Information Security (IJCNIS).

[5] Kumar, M., Soni, A., Shekhawat, A. R. S., & Rawat, A. (2022, February). Enhanced digital image and text data security using hybrid model of LSB steganography and AES cryptography technique. In 2022 Second international conference on artificial intelligence and smart energy (ICAIS) (pp. 1453-1457). IEEE.

[6] Bansal, M., & Ratan, R. (2023). Designing a Novel Technique for Multi-Level Security System for Digital Data by Combined DSSS Audio Steganography & Random Permutation Cryptography. Tuijin Jishu/Journal of Propulsion Technology, 44(4), 768-781.

[7] Moon, S. K. (2022, February). Application of forensic audio-video steganography technique to improve security, robustness, and authentication of secret data. In International Conference on Computing Science, Communication and Security (pp. 11-25). Cham: Springer International Publishing.

[8] Ilasariya, S., Patel, P., Patel, V., & Gharat, S. (2022, January). Image steganography using Blowfish algorithm and transmission via apache kafka. In 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 1320-1325). IEEE.

[9] Buchyk, S., Toliupa, S., Lukova-Chuiko, N., Khomenko, O., & Serpinskyi, Y. (2022, February). Applied Steganographic System for Hiding Textual Information on Audio Files. In IEEE lnternational Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (pp. 317-334). Cham: Springer Nature Switzerland.

[10] Bhatkalkar, B. J., Arjunan, R. V., Alok, A., Sanghavi, R., Cenitta, D., & Kamath, R. (2022, December). A Novel Method for Sample Selection in Audio Stenographic Systems. In 2022 6th International Conference on Electronics, Communication and Aerospace Technology (pp. 664-672). IEEE.

[11] GURUNATHAN, P., & DEVI, R. S. (2023, April). RSA Cryptography and GZIP Steganography Techniques for Information Hiding and Security using Java. In 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 654-659). IEEE.

[12] Al-Chaab, W., Abduljabbar, Z. A., Abood, E. W., Nyangaresi, V. O., Mohammed, H. M., & Ma, J. (2023). Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica, 47(6).

[13] Bansal, M., & Ratan, R. (2022, December). Comprising Survey of Steganography & Cryptography: Evaluations, Techniques and Trends in Future Research. In 2022 8th International Conference on Signal Processing and Communication (ICSC) (pp. 315-323). IEEE.

[14] Hingmire, A., Karulkar, N., Mhatre, R., & Patil, Y. (2023, June). A Novel Approach to Audio Steganography on Audio Input for Secure Communication. In 2023 8th International Conference on Communication and Electronics Systems (ICCES) (pp. 534-538). IEEE.

[15] Mahjabin, T., Olteanu, A., Xiao, Y., Han, W., Li, T., & Sun, W. (2023). A Survey on DNA-Based Cryptography and Steganography. IEEE Access.

[16] Almohammedi, A. A., Shepelev, V., Darshi, S., Balfaqih, M., & Ghawbar, F. (2022). Cost and Efficiency Analysis of Steganography in the IEEE 802.11 ah IoT Protocol. Computers, Materials & Continua, 72(2).

[17] Octafian, M. R. N., Novamizanti, L., Safitri, I., & Sitepu, R. P. (2022, July). Audio Steganography Technique using DCT-SWT with RC4 Encryption. In 2022 International Conference on Data Science and Its Applications (ICoDSA) (pp. 35-40). IEEE.

[18] Elshoush, H. T., & Mahmoud, M. M. (2023). Ameliorating LSB Using Piecewise Linear Chaotic Map and One-Time Pad for Superlative Capacity, Imperceptibility and Secure Audio Steganography. IEEE Access, 11, 33354-33380.

[19] Rahman, S., Uddin, J., Khan, H. U., Hussain, H., Khan, A. A., & Zakarya, M. (2022). A novel steganography technique for digital images using the least significant bit substitution method. IEEE Access, 10, 124053-124075.

[20] Nasr, M. A., El-Fishawy, A. S., El-Shafai, W., Dessouky, M. I., El-Rabaie, E. S. M., Abdel-Salam, N., & Abd El-Samie, F. E. A Robust Technique for Steganography of Enhanced Audio Signals.