IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 5, April 2025

Impact Factor: 7.67

Audio Steganography: Image Embedding in Audio

Ch. Rambabu[1], P. Threenadh Reddy[2], R. Ambika Soni[3], Y. Sandeep Kumar[4]

Associate Professor Department of Electronics and Communication Engineering[1]

Under Graduate Student, Department of Electronics and Communication Engineering[2,3,4,5]

Seshadri Rao Gudlavalleru Engineering College, Andhra Pradesh, India

Abstract: *Steganography is an advanced technique used for secure data communication by concealing information within digital media. This research explores the process of embedding images within audio signals, analyzing the effectiveness of various encoding techniques, including Least Significant Bit (LSB) substitution, and cryptographic methods such as Advanced Encryption Standard (AES). The study evaluates imperceptibility, fidelity, payload capacity, and robustness to determine the feasibility of audio steganography for secure digital communication. Experimental results indicate that efficient encryption and compression techniques enhance the security and usability of audio steganography*

Keywords*:* LSB, AES, Steganography, Cryptography, Histogram, Entropy, PSNR.

I. INTRODUCTION

With the rise of digital communication, securing information has become a critical aspect of modern technology. Various security techniques, such as cryptography and steganography, are used to protect sensitive data from unauthorized access and cyber threats. While cryptography transforms data into an unreadable format to prevent unauthorized interpretation, steganography hides the existence of data within another medium, making it difficult for attackers to detect. This makes steganography an effective approach for covert communication.

Among the different forms of steganography, audio steganography has emerged as a powerful technique due to its high data-hiding capacity and robustness. Unlike image steganography, where data is embedded within pixel values, audio steganography exploits the properties of sound signals to hide data. Various encoding methods, including Least Significant Bit (LSB) substitution, phase coding, spread spectrum, and echo hiding, allow for effective data embedding without significant alterations to the audio signal. Each of these methods presents unique advantages in terms of imperceptibility, robustness, and payload capacity.

This research explores a novel approach to embedding images within audio signals, leveraging cryptographic techniques and compression methods to enhance security and efficiency. By using encryption techniques such as AES, the security of the embedded image is strengthened, ensuring protection against unauthorized extraction.

The primary objective of this study is to evaluate the trade-offs between security, imperceptibility, and robustness in audio steganography. By analyzing the effectiveness of different encoding mechanisms and their impact on audio quality, this research aims to provide insights into the feasibility of using audio steganography for secure digital communication.

Steganography has numerous real-world applications, including secure military communications, watermarking digital content to prevent piracy, and embedding medical records within patient audio files for secure healthcare data transmission. With the growing concerns over data privacy, steganography provides an additional layer of security by ensuring that sensitive information is transmitted without raising suspicion. The combination of encryption and steganography further enhances security by preventing unauthorized decryption even if the hidden message is detected.

The study also explores the impact of audio file formats (WAV) on steganographic efficiency. Lossless formats such as WAV provide better fidelity but require larger storage capacity. Understanding these trade-offs allows for the selection of the most suitable format based on the intended application.

Furthermore, advancements in artificial intelligence and machine learning have introduced new methods for detecting steganographic content, making it essential to continuously improve embedding techniques. This research contributes to the development of resilient steganographic systems capable of withstanding modern steganalysis methods. By

DOI: 10.48175/IJARSCT-25230

addressing challenges such as detection resistance and payload optimization, this study aims to advance the field of audio steganography and promote its application in secure digital communication.

II. METHODOLOGY

The proposed system for embedding images into audio signals follows a structured process:

Pre-processing the Image:

- The image is resized and converted into a binary format for embedding.

Image Encryption:

- To enhance security, the binary image is encrypted using AES.
- AES offers strong encryption but requires more computational power.

Compression:

- The encrypted image is compressed using PNG's default DEFLATE compression (via zlib) through OpenCV's imencode() function
- Compression ensures that the audio signal remains unaffected while maximizing storage efficiency.

Encoding in Audio:

- The compressed and encrypted image is embedded into the audio signal using LSB substitution.
- Base64 encoding is used to enhance compatibility and maintain data integrity.
- The embedding process ensures that imperceptibility is maintained so that the modifications in the audio remain undetectable by human ears.

Extraction and Decoding:

- The embedded image is extracted from the audio using an inverse LSB algorithm.
- The extracted data is then decompressed and decrypted using the corresponding cryptographic key.
- The final output is reconstructed to retrieve the original image with minimal distortion.

Analysis of Different Audio Formats:

- The methodology evaluates WAV format.
- Lossless formats (e.g., WAV) provide better fidelity.
- By following this structured approach, the research aims to balance security, efficiency, and imperceptibility while ensuring that the embedded image can be securely transmitted and retrieved without degradation.

Evaluation Metrics:

To assess the performance of the proposed steganographic method, the following metrics are used:

- **Imperceptibility:** Spectral analysis of the audio signal ensures that the embedded data does not cause significant distortion.
- **Fidelity:** The Peak Signal-to-Noise Ratio (PSNR) is measured to evaluate the quality of the audio after embedding the image.
- **Robustness:** The system's resilience against noise, compression, and other signal modifications is tested to ensure reliability.

Encryption and Embedding Process

The first step is to input the image file as a message and the audio file as the cover media. After that, the audio and image files will be validated. The allowed image file extensions are (.jpg, .png, .bmp), and the allowed audio file extension is (.wav); otherwise, they will be rejected. If the two files match, then both files will be converted into byte streams to compare and measure the capacity of picture messages that can be inserted into audio files. If the image file size is larger than the audio file size, the image file cannot be inserted.

After the image file is inputted according to the size of the audio file, the image encryption process will then be carried out. In this study, encryption is performed using the AES encryption algorithm. The result of the encryption process is in the form of encrypted bytes, which will then be compressed using PNG's default DEFLATE compression (via zlib)

DOI: 10.48175/IJARSCT-25230

through OpenCV's imencode() function. Then the encrypted binary information is converted into bit stream. Furthermore, the insertion process using the LSB method is carried out into the audio file by replacing LSB of each audio sample with image bits, so that the stego-audio file is obtained.

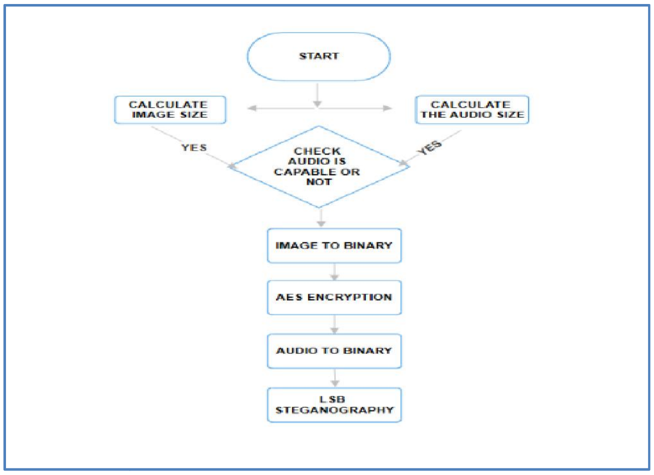


Fig. 1.Encryption and Embedding Process

Extraction and Decryption Process

The first step is to input an audio stego file containing confidential information, the audio file will be converted to a byte stream. Then each LSB byte will be taken from the audio byte stream using the LSB technique.Raw bytes are extracted from audio LSBs and directly decrypted using AES-CBC. The decrypted PNG data is then decompressed and saved as an image file.

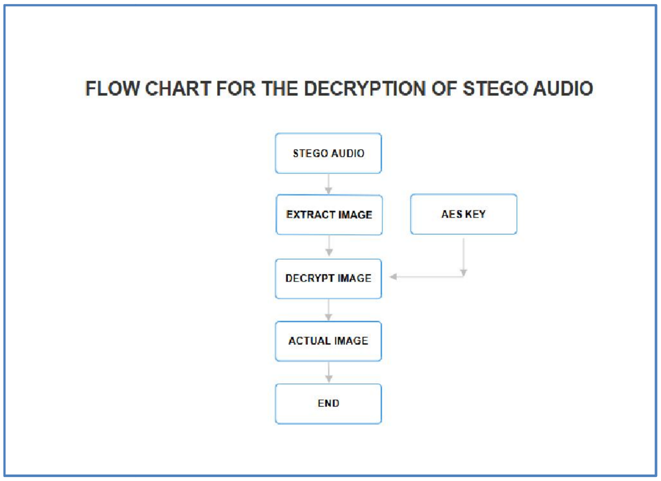


Fig. 2.Extraction and Decryption Process

Validation Process:

The can_embed function checks if an audio file can store an image by comparing the required number of bits (image size * 8) to the available audio samples. If the image fits within the audio capacity, it returns true.

```
def can_embed(audio_samples, image_binary):
    return len(image_binary) * 8 <= len(audio_samples)
```

Capacity=Audio Size × Bits per Sample × Channels × Embedding Rate
Where:
Audio Size: Total number of samples in the audio.
Bits per Sample: Usually 16 for high-quality WAV files.
Number of Channels: 1 (mono) or 2 (stereo).
Embedding Rate: Number of Least Significant Bits (LSBs) used for embedding per sample (usually 1 or 2).
Requirement=Image Size × 8

III. RESULT AND DISCUSSION

Result and Discussion The quality of the steganography file is measured using following parameters: imperceptibility, robustness, recovery, and fidelity. The measurement of these steganographic parameters can be done both subjectively and objectively. Imperceptibility is evaluated through subjective observation by analyzing the histogram of the image and the audio spectrum of the steganographic file, as well as comparing the size of the audio file before and after the message insertion. Objective measurement involves assessing fidelity and recovery parameters through computational analysis. The technical details of testing these parameters will be further described in the following sections.

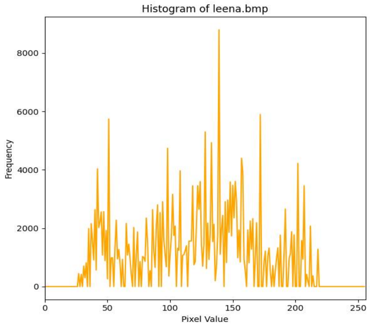
Imperceptibility

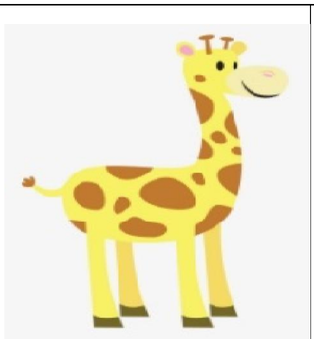
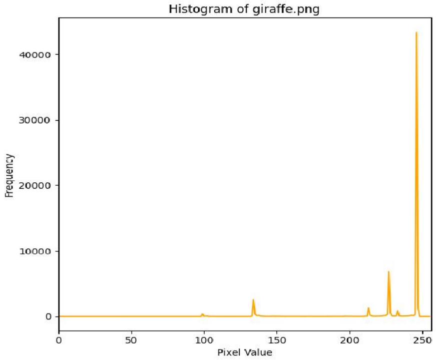
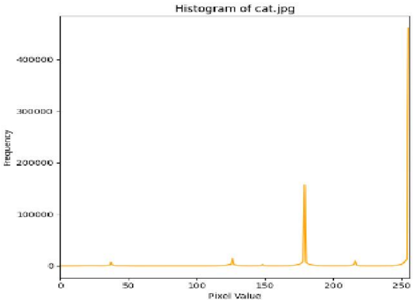
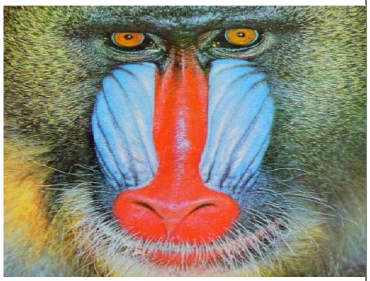
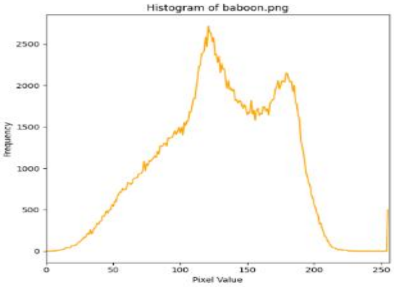
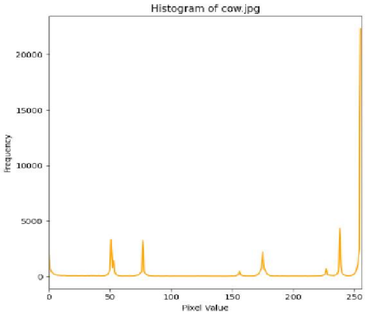
Imperceptibility testing ensures that the audio quality of steganography is not much different from before and after the image message is inserted. In this test, the quality of steganographic audio files will be compared before inserting image messages (JPEG, PNG, and BMP) with after inserting image messages of various sizes, both before being compressed and after being compressed using the PNG's default DEFLATE compression algorithm and encryption algorithm (AES and RC4). Observation of imperceptibility by looking at the color image histogram before inserting it into the cover audio file and after extracting it from the steganography audio file, besides that, visualization of the spectrum of the initial audio file (before inserting the message) and after inserting the image message will also be seen. The test results on the imperceptibility aspect can be seen in tables 3 to 4.

Input Images and Histogram Analysis

The analysis of input images and their histograms reveals interesting patterns. The histogram of the 'lenna.bmp' image shows a uniform distribution with minor variations after the steganography process. The 'Giraffe.png' and 'Cat.jpg' images exhibit slight intensity changes due to embedding, primarily affecting the lower intensity values. In contrast, 'Baboon.png' has a high-contrast nature, making the histogram variations more noticeable. The 'Cow.jpg' image experiences minimal changes, indicating that the embedding process has a limited impact on its pixel distribution. Comparison will be made between the visualization of the original image histogram and after it is compressed and encrypted using AES

Table1. Visualization of original Image files and Audio Files

Input image	histogram of input images
 lenna.bmp(769kb)	

 Girafee.png(23kb)	
 Cat.jpg(27kb)	
 Baboon.png(550kb)	
 Cow.jpg(20kb)	

DOI: 10.48175/IJARSCT-25230

Table 2. Visualization of image and audio files before and after compression and encryption

Audio Spectrum Analysis After Embedding

When analysing the audio spectrum after embedding images, minor distortions appear in the high-frequency range, suggesting slight modifications. Silent parts of the audio show slight amplitude changes, which could indicate embedding activity. These changes indicate that while the embedding process does not drastically alter the audio file, it does introduce small fluctuations that may be detectable under careful scrutiny.

Table 3. Visualization of image and audio files before and after compression and encryption

Extracted Image Quality

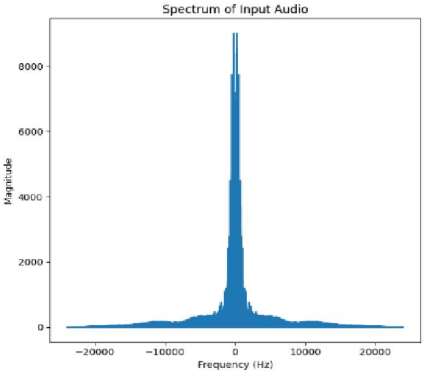
The extracted images retain most of their features with minimal degradation. However, some images exhibit slight deterioration, possibly due to compression artifacts or minor data loss during the embedding and extraction process. The clarity and accuracy of the extracted images suggest that the embedding method preserves most of the original information while introducing only negligible distortions.

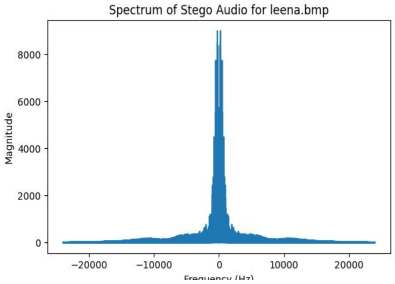
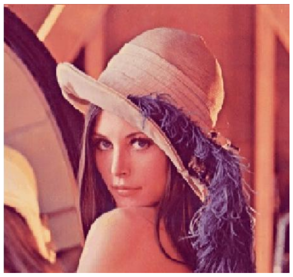
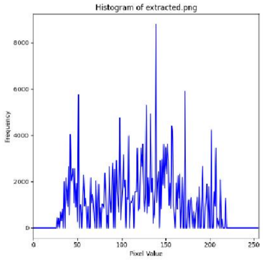
Title: ancient Egyptian goddess amuzium

Size: 14.1 mbps

Length: 00:01:23

Item type: WAV



Spectrum of audio after embedding image	Extracted image	histogram of extracted image
	 lenna.bmp(769kb)	

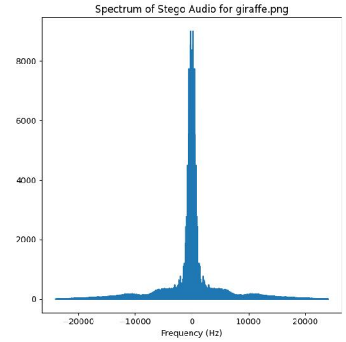
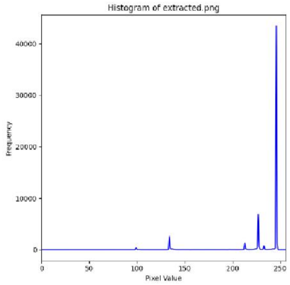
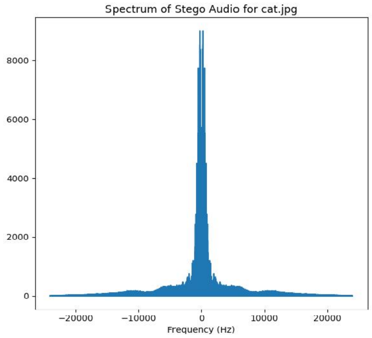
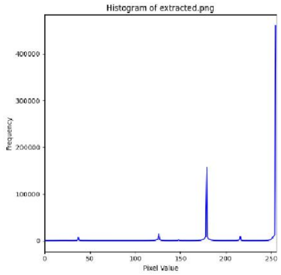
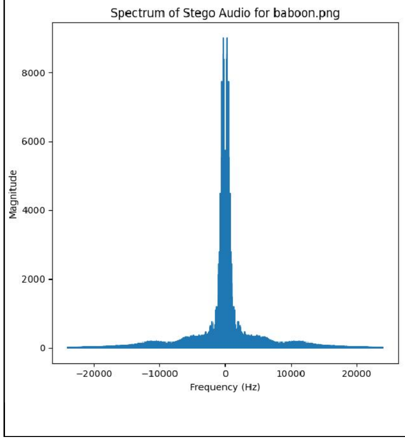
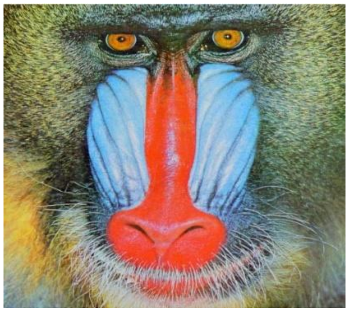
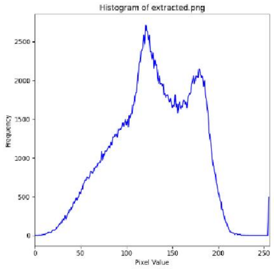
DOI: 10.48175/IJARSCT-25230

IJARSCT

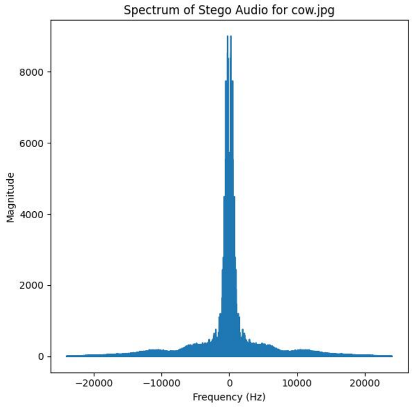
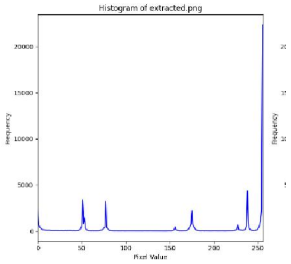
International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429 Volume 5, Issue 5, April 2025 Impact Factor: 7.67

	Girafee.png(23kb)	
	Cat,jpg(27kb)	
	 Baboon.png(550kb)	

DOI: 10.48175/IJARSCT-25230

	 Cow.jpg(20kb)	

Fidelity

Measurement of fidelity aspect using SNR and PSNR. The measurement ofthe fidelity aspect is to ensure that the quality or quality of the steganography audio file after being inserted can be measured and assessed objectively [28]. The standard to show the quality of a good audio steganography file is with a PSNR value greater than 30 dB, assuming that with a minimum value of 30 dB the message cannot be perceived as being in the steganography file and the steganographic audio quality does not cause much noise.

The histogram of the extracted images remains similar to the original, with negligible loss in details. There are minor variations in pixel intensity distribution, which may indicate slight modifications due to the embedding and extraction processes. However, the overall structure and frequency of pixel values are largely preserved, showing that the method maintains a high level of integrity for the hidden data.

Parameter	Cat.jpg	Leena.bmp	Girafee.png	Cow.jpg	Baboon.png
Audio PSNR	66.1934	66.0123	73.3113	69.6069	**60.9242**
Audio SNR	37.2326	37.0515	47.6915	43.9871	**35.30435**
Error rate of audio	0.00781	0.00814	0.000197	0.00058	**0.00330**
Entropy of original audio	4.7131	4.7131	4.7131	4.7131	**4.7131**
Entropy of stego audio	4.7136	4.7136	4.7131	4.7132	**4.7137**
Entropy of original image	2.9183	6.8730	2.1922	5.0247	**7.3531**
Entropy of extracted image	**2.9183**	**6.8730**	**2.1925**	**5.0247**	**7.3531**

Table 4. The results of testing the fidelity aspect by comparing the aspects of the AES

IV. CONCLUSION

Upon analysing the data from the PDF, it is evident that the steganographic techniques used in the experiment effectively embed and extract hidden information while maintaining a high level of integrity in both audio and image domains. The histogram analysis of the input images reveals that while some modifications occur due to the embedding process, they are minimal and often imperceptible to the human eye. High-contrast images like 'Baboon.png' show more noticeable changes, but overall, the alterations remain within acceptable limits.

The audio spectrum analysis indicates that while minor distortions occur, they do not significantly impact the audio quality. Changes are mostly limited to high-frequency regions and silent parts of the audio file, suggesting that the embedding process is subtle enough to avoid detection through casual listening. However, advanced forensic techniques may still be able to detect these modifications under close examination.

DOI: 10.48175/IJARSCT-25230

The quality of the extracted images further supports the effectiveness of the steganographic technique. Most extracted images retain their original features with only slight degradation, indicating that the embedding process does not introduce significant losses. This highlights the efficiency of the method in preserving hidden information while keeping visual quality intact.

The histogram analysis of extracted images shows that the pixel intensity distribution remains largely unchanged. While slight variations exist, they do not significantly impact the overall image structure. This demonstrates that the embedding and extraction processes are well-optimized to ensure minimal disruption to the original data.

In conclusion, the study confirms that steganographic methods can successfully hide information within audio and image files without introducing significant perceptible changes. The effectiveness of the approach depends on factors such as image contrast, audio frequency distribution, and compression artifacts. While minor distortions occur, they remain within acceptable limits, making the method viable for secure communication and data hiding purposes. However, further research may be necessary to enhance the robustness of these techniques against forensic detection methods. Overall, the experiment highlights the potential of steganography as a valuable tool for secure data transmission while maintaining media integrity.

REFERENCES

[1]. F. Ashari, “Graph Steganography Based On Multimedia Cover To Improve Security and Capacity,” in *2018 International Conference on Applied Information Technology and Innovation (ICAITI)*, 2018, no. April 2019, pp. 194–201.

[2]. F. Ashari, “Implementation of Cyber-Physical-Social System Based on Service Oriented Architecture in Smart Tourism,” *J. Appl. InformaticsComput.*, vol. 4, no. 1, pp. 66–73, 2020, doi: 10.30871/jaic.v4i1.2077.

[3]. N. I. Munawar, Zen and Putri, “KeamananJaringanKomputer Pada Era Big Data,” *J-SIKA| J. Sist. Inf. Karya Anak Bangsa*, vol. 02, no. 01, pp. 14–20, 2020.

[4]. Sebbar, K. Zkik, Y. Baddi, M. Boulmalf, and M. D. E. C. El Kettani, “MitM detection and defense mechanism CBNA-RF based on machine learning for large-scale SDN context,” *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 12, pp.5875–5894,2020,doi:10.1007/s12652-020-02099-4.

[5]. A Mallik, A. Ahsan, M. M. Z. Shahadat, and J. C. Tsou, “Man-in-the-middle-attack:Understandinginsimplewords,”*Int.J.DataNetw.Sci.*,vol.3,no.2, pp.77–92,2019,doi: 10.5267/j.ijdns.2019.1.001.

[6]. F. Ashari, M. Alfarizi, M. N. K, and M. A. H, “Vulnerability Analysis and Proven On The neonime . co Website Using OWASP ZAP 4 and XSpear,” *J. Teknol. Komput. dan Sist. Inf.*, vol. 5, no. 2, pp. 75–81, 2022.

[7]. F. Ashari and V. Adhelia, “Expert System and IoT for Diagnose of Feline Panleukopenia Virus Using Certainty Factor,” *Matrik J. Manajemen, Tek. Inform. dan RekayasaKomput.*, vol. 21, no. 2, pp. 451–462, 2022, doi: 10.30812/matrik.v21i2.1517.

[8]. C. Biswas, U. Das Gupta, and M. M. Haque, “An Efficient Algorithm for Confidentiality,IntegrityandAuthenticationUsingHybridCryptographyand Steganography,” *2nd Int. Conf. Electr. Comput. Commun. Eng. ECCE 2019*, pp. 1–5, 2019, doi: 10.1109/ECACE.2019.8679136.

[9]. F. Ashari, A. J. Aryani, and A. M. Ardhi, “DESIGN AND BUILD INVENTORY MANAGEMENT INFORMATION SYSTEM,” vol. 9, no. 1, pp. 27–35, 2022.

[10]. V. Reshma, S. Joseph Gladwin, and C. Thiruvenkatesan, “Pairing-free CP-ABE based cryptography combined with steganography for multimedia applications,” *Proc. 2019 IEEE Int. Conf. Commun. Signal Process. ICCSP 2019*,pp.501–505,2019,doi: 10.1109/ICCSP.2019.8698053.

[11]. V. Verma, S. K. Muttoo, and V. B. Singh, “Enhanced payload and trade-off for image steganography via a novel pixel digits alteration,” *Multimed. Tools Appl.*,vol.79,no.11–12,pp.7471–7490,2020,doi:10.1007/s11042-019-08283-9.

[12]. M. H. N. Azam, F. Ridzuan, M. N. S. M. Sayuti, and A. A. Alsabhany, “Balancing the Trade-Off betweenCapacity and Imperceptibility for LeastSignificant Bit Audio Steganography Method: A New Parameter,” *2019 IEEE Conf. Appl. Inf.* 10.1109/AINS47559.2019.8968707.

[13]. D. H. Zulfikar, "Quality Factor terhadapKapasitas Pesan Rahasia pada Steganografi Citra JPEG dan Kualitas Citra Stego," *JUSIFO (Jurnal Sist. Informasi)*, vol. 6, no. 2, pp. 89–100, 2020, doi: 10.19109/jusifo.v6i2.6608.

[14]. B. Sinha, "Comparison of PNG & JPEG Format for LSB Steganography," *Int. J. Sci. Res.*, vol. 4, no. 4, pp. 198–201, 2015.

[15]. B. D. Raharja and P. Harsadi, "ImplementasiKompresi Citra Digital DenganMengaturKualitas Citra Digital," *J. Ilm. SINUS*, vol. 16, no. 2, pp. 71–77, 2018, doi: 10.30646/sinus.v16i2.363.

[16]. H. Antonio, P. W. C. Prasad, and A. Alsadoon, "Implementation of cryptography in steganography for enhanced security," *Multimed. ToolsAppl.*,vol.78,no.23,pp.32721–32734,2019,doi:10.1007/s11042-019-7559-7.

[17]. S. H. WE Pangesti, GWidagdo, DRiana, "ImplementasiKompresi Citra Digital DenganMembandingkan Metode Lossy dan Lossless Compression MenggunakanMatlab," *J. KHATULISTIWA Inform.*, vol. 8, no. 1, pp. 53–58, 2020.

[18]. A.D.PutriAriyanto,E.H.Rachmawanto,D.R.IgnatiusMosesSetiadi,andC. Sari, "Performance Analysis of LSB Image Steganography Combined with Blowfish-RC4 Encryption in Various File Extensions," *Proc. 2019 4th Int.Conf. Informatics Comput. ICIC 2019*, pp. 0–5, 2019, doi: 10.1109/ICIC47613.2019.8985848.

[19]. I.F.Ashari, "Aplikasisteganografipesanteks pada media audio mp3 menggunakanmetodepenyisipan least significant bit dan advanced encryption standard skripsi," pp. 1–114, 2015.

DOI: 10.48175/IJARSCT-25230