A Literature Review on Secure Multimedia Communication Using Encryption and Steganography Technique

Mrs. Rashmi V, Samruddhi S Prabhu , Sanjay M Uttangi , Sanya S , Sharan K G

***Abstract*—In the digital era, safeguarding confidential data causes major concern as cyber threats and data leaks increase. This paper presents a comprehensive literature review on various hybrid approaches that combine cryptography and steganography to RSA, ECC and DES, along with steganographic techniques such as LSB, DWT, DCT and innovative methods to alter images,audio and video. The examined systems aim to achieve high imperceptibility minimal distortion, and robust security by employing multi-layer protection and sophisticated embedding techniques. We examine performance indicators like 2222 PSNR, MSE,SSIM,entropy and BER to evaluate the effectiveness of each method. Researchers also use tools such as MATLAB Python and Java in implementations to demonstrate their functionality. The review concludes that while existing solutions show potential for secure data concealment, a need exists for new models that can operate in real time, scale with demand,and resist attacks.**

***keywords*—**Cryptography, Steganography, AES, RSA LSB, Secure Communication, Hybrid Encryption

I. INTRODUCTION

In the modern environment of technologies, the relevance of preventative and confidential interacting with people was never higher.Both in personal talks, business confidentiality information or in the case of government vital information; it has become important to have the messages hidden and not just encrypted. Although cryptography has proved quite effective in ensuring that the content of a message is secure, cryptography does not keep secret truth is communication is being passed across. Conversely, the steganographic approach is concerned rather with hiding the fact that there is a message in the first place and with no or minimal encryption.

That is where our project comes to play. It is a cross between cryptography and steganography systems in that it incorporates in itself the positive attributes of both systems in giving rise to a more secure way of communication. As far as this system is concerned, by means of AES (Advanced Encryption Standard) we have the ability of encrypting the message and guaranteeing that the content will be secured. So as to safely share the encryption key, we trust RSA, the asymmetric method of encryption. The encrypted data is lastly hidden into a carrier file, e.g. image, audio, video or text, using LSB (Least Significant Bit) steganography to ensure that the existence of the data is almost undetectable.

The flexibility of the system makes it special. As opposed to the majority of the systems being more specific, engaging mainly with the files of a single type, a user with our project is free to conceal the information of any type, having more options at their disposal due to such flexibility. Not only do these multi layered approaches juice up the security of the data but it also hides the communication process away from the prying eyes of the attackers.

Advanced Encryption Standard (AES) is a symmetric key algorithm. It takes data to encrypt at fixed rates of 128 bits and uses a key of 128 bits, 192 bits or 256 bits. AES uses repetitive processes of substitution, permutation and mixing in several rounds and offers good encryptions and immunity to a majority of the cryptographic attacks. It doesn't take long and performance because they both use the same key in encryption and decryption. In this system, a person won't be able to interpret the original message without the key code although he/she may suspect the use of hidden data.

A commonly used public-key cryptosystem algorithm **Rivest Shamir Adleman (RSA),** is an algorithm of cryptography, which is founded on the mathematical challenge of factoring a large composite number. It involves the usage of two keys, which are the public one, used in encryption, and private one, applied in decryption. In contrast to AES, RSA is an asymmetric encryption scheme and it is primarily applicable to exchange secret keys or encrypt small portions of data. In this system, RSA is important in transmission of the AES key securely. Instead of, the AES key is not sent in plain text, but it is encrypted with the RSA receiver, using his or her public key. The system has the benefit of performance and high security of data communications because of the combination of RSA and AES.

Least Significant Bit (LSB) steganography, this is the technique of hiding data in within the smallest bits of digital media files. The encryption of the message takes place in this method; the smallest bits of each sound sample or pixel image are altered and do not yield visible effects on the base media. This is what makes LSB a perfect method of data invisibility hiding.

To ensure that the system is secure, we tested it to give maximum efficiency. It encrypts messages with high strength (AES-256 and RSA-2048) to prevent the efforts of hackers. Having the PSNR and histogram analysis helped us verify whether the hidden files still appeared normal or not. Bit Error

Rate (BER) was also used to check the accuracy of reception of the message. The tests reveal that the project is safe, correct and consistent.

II. LITERATURE SURVEY

In this section, different writers have introduced different ideas cryptography and steganography techniques.

Badhan and Malhi [1] suggested a series of hybrid data security algorithms incorporating AES and ECC with the inverted LSB steganography and WebP compression in images. AES ciphers the information effectively and ECC protects AES key on lesser keys and smaller computations. Inverted LSB layer encrypts a file and inserts it into pictures, and WebP compresses pictures to improve size and integrity. The PSNR of the model was 68.90 dB, which is high, whereas the MSE was 0.0083, which signifies low distortion.

Al-Rekaby et al. [2] have suggested a hybrid security based system by combining a multi-level chaotic map, AES encryption, and LSB steganography to inset the encrypted text on video frames. The AES encrypted data is concealed in the red channel red of video frames via LSB with high imperceptibility and well data concealment. The system delivered excellent results having PSNR of over 76 dB, SSIM of 1.0000, MSE of 0.0012 and entropy of about 7.98. Its performance has 0.005% or less effect on the quality of videos and has high security without affecting integrity.

Chandra Sekhar Reddy et al. [3] presented a two-layer security architecture in which the pairing of cryptography (AES, RSA, or ECC) with steganography (JISB, DWT, DCT, and PVD) algorithms to preserve the privacy of the digital communication messages. The model introduces an additional layer of concealment, concealing one image in another. An encryption software facilitates an encrypting and embedding application and its decryption. Findings exhibit the high protection to unauthorized accesses, and proposals to be implemented in future using tools like machine learning and deep learning and blockchain.

Munmun Islam Mitu et al. [4] came up with a hybrid data security system where the steganography benefit of DWT was combined with the confidentiality characteristics of AES-128 and the data concealment of SHA-256 hashing. DWT encrypts the data in the images preserving their visual quality. The method demonstrated high levels of security, small distortion, high levels of invisibility, as tested using PSNR, MSE, and SSIM in MATLAB. It is especially applicable to safe communication within such spheres as care and computer forensics.

Balhaf et al. [5] suggested the hybrid security system, encrypting data using RSA in first stage and then steganography of LSB the picture comes next stage to provide protection or confidentiality and integrity of data. It proposes security at two levels by encryption of plaintext with RSA and concealing of ciphertext within images through LSB. MSE, PSNR, and SNR measurement determined how little the image has been distorted and that no visual degradation has been experienced. It turned out to be both grayscale and color-image-concerned, which means that such an approach is applicable in situations of secure and discreet communication.

K. Bhanu Rajesh Naidu et al. [6] have suggested a secure file-sharing system, which encrypts documents with AES and hides the encrypted information into pictures using LSB steganography. They have an approach that carries out XOR operations to ensure an extra level of security and preserves the clarity of the picture. The system allows embedding and extraction using a Java tool (IMStego) hence is effective at securing sensitive information in PNG and BMP images as both the confidentiality and the privacy of the data is ensured.

Gift Nwatuzie et al. [7] suggested a mixed encryption structure to optimize the protection of the data in the cloud with the use of AES, DES, and RC6 encryption algorithms. It stores the data using file splitting and steganographic key management on multi-tenant cloud settings. The data that is encrypted is dissected and dispersed in various servers and the encryption keys will be concealed in the pictures utilizing steganography. This is because it enhances confidentiality, integrity and availability. Based on simulation findings, performance, scalability, and attack resistance are superior to the traditional methods of encryption, which qualifies it to handle sensitive cloud-based applications.

Olawale Surajudeen Adebayo et al. [8] introduced the system of data privacy (a combination of the RSA cryptography and MSB steganography). The system encrypts the secret messages in form of RSA (secret) after which the encrypted data is embedded in images by using Most Significant Bit method. It was coded in Python and was supposed to keep the image's size exactly the same, be highly vast (38.5 percent) and save little memory capacity. The results indicate that it is more secure, the key management is efficient as well as the protection against the unauthorized parties was good meaning that it is better off compared to most of the current ways that employ symmetric encryption. It works only with BMP files and with text messages though.

K. Lokeswari et al. [9] have presented a safe method to hide data built on RSA cryptographic algorithm and steganography on LSB Image. The RSA used to perform encryption text and incorporate the text in an picture using LSB guaranteeing confidentiality. The system was designed and tested in MATLAB and it was tested on the quality and distortion of images. It also recorded an impressive PSNR of 52.71 dB and a low MSE value of 0.0696 meaning that it has visual distortion

which is close to none. Such approach is useful when some confidential data need to be transmitted securely and in a hidden manner.

Allasasmh, Omar et al. [10] suggested an integrated data hiding mechanism, which hides the static text into audio, image, and text format with the help of altered LSB steganography methods. The system applies special techniques like the XOR operations, the zero-width characters, and the changing the pixel of RGB in order to conceal information between different media. It has been realized in Python with GUI, which has provided a user-friendly interface in encoding and decoding the messages. The strategy is very discreet and capable of ensuring message extraction devoid of distortion.

Athira Varma Jayakumar [11] developed a safe image steganography framework called STEGASHIELD, which involves AES encryption, random sewer, and the distraction of an imaginary image as countermeasures in building more confidentiality and imperceptibility of the information. The mechanism takes advantage of pixel wise distortion and histogram essentially to prevent detection and to preserve the image quality. When applied in Java, it has PSNR of more than 50 dB, which is very low in terms of distortion. Such multiple layering outlines its appropriateness in safe and sneaky transmission of image based data.

Soundrapandiyan et al.[12] screened the topic of digital video steganography in terms of its capacity to safely conceal volumes of data within the motion media. They classified techniques as spatial/frequency method and compressed domain techniques such as LSB, DCT, DWT and manipulation of motion vectors. Such performance indicators as imperceptibility, robustness, and payload were mentioned.

Jebur et al. [13] suggested two variants of LSB steganography 1-LSB and 4-LSB, used to conceal information in color and grayscale pictures. Pre-embedding of secret image is done by XORing with a bitstream derived out of the secret key. The 1-LSB approach has ameliorated imperceptibility and image quality (PSNR 42.75 dB), reduced capacity. The 4-LSB scheme has a larger capacity (4bits/byte), but poor image quality (PSNR 29.28 dB).

Sani and Nujjaid [14], the authors offered a combined strategy of LSB steganography with RSA, and AES combined with DiffieHellman, as a form of secure data transfer. The combi of AES + Diffie-Hellman did better as compared to LSB + RSA in terms of PSNR (81.38% vs 81.35%) and MSE (0.004135 vs 0.0010495) and the hiding time was 0.2160s and 0.3335s respectively. This is improved security, efficiency and usability in real-time.

Mushtaq et al. [15] suggested secure video steganography approach by using deepmidt learning in TensorFlow The system employs Discrete Wavelet Transform (DWT), video downsampling along with Mersenne Twister randomization to efficiently embed. In tests on YUV datasets it demonstrated very high throughput, low distorsion, and zero bit error rate (BER). It has better performance compared to the traditional LSB & DCT based methods in PSNR & SSIM and hence, it is suitable for the real time multimedia communication.

This survey reveals that the mix of cryptography and steganography can keep the information safe and concealed. Ciphers such as AES, RSA, and LSB are friendly to file, images, audio as well as video. They have good quality and low distortion. However, more is required to be used in real-time and more secured against smart attacks.

III. SUMMARY

In this project a system designed to hide data that uses a combination of cryptography and steganography to obtain confidentiality of sensitive details together with their invisibility is used. It applies steganography of **LSB** used to conceal the encrypted message in images, audio, video, or text files and **AES** to encrypt the messages and **RSA** to facilitating secure key exchange. As a test of the system, measurements of **PSNR, BER,** and **histogram** were used to test the strength in encryption, accuracy of the messages received, and quality of media. It was revealed that the system has high level of data security, less visual audio distortion and correct extraction of messages across the various file types.

IV. CONCLUSION

This review of the literature demonstrates that using both cryptography and steganography together is a good way to send secure data over different types of media, such as images, audio, and video. AES, RSA, ECC with LSB, DWT, DCT, and MSB have all been shown to be very hard to notice, have little distortion, and protect data very well. Metrics to measure performance such as PSNR, MSE, and SSIM show that the visual quality of the stego-media stays mostly the same.Many people used tools like MATLAB, Java, and Python to do the work. Even though the results are promising, more research is needed to make the system work better in real time, scale up, and be more resistant to modern cyberattacks.

REFERENCES

[1] A.Badhan and S. S. Malhi, “Enhancing Data Security and Efficiency: A Hybrid Cryptography Approach (AES + ECC) Integrated with Steganography and Compression Algorithm,” *Proc. 3rd Int. Conf. on Intelligent Data Communication Technologies and Internet of Things (IDCIoT-2025)*, 2025, pp. 450–456, doi: 10.1109/IDCIoT64235.2025.10914830.

[2] S. N. Al-Rekaby, M. A. A. Khodher and L. K. Adday, "A Hybrid Security System for Text Encryption and Steganography in Video Using Multi-Level Chaotic Maps," *Int. J. Saf. Secur. Eng.*, vol. 15, no. 3, pp. 521–532, Mar. 2025, doi: 10.18280/ijsse.150311.

[3] K. Balhaf, N. A. Munassar, A. A. Bagmeel, M. S. AL Hafeez, F. M. AL Gaafari, and A. Swailem, "Digital Steganography and Cryptography Hybrid System Combining LSB and RSA Algorithms," *Engineering and Technology Journal*, vol. 10, no. 4, pp. 4424–4428, Apr. 2025, doi: 10.47191/etj/v10i04.07

[4] M. I. Mitu, S. Sweety, and S. Waheed, "An Encryption Approach with Steganography for Enhanced Data Security," in *Proc. 2024 IEEE Int. Conf. on Computing, Applications and Systems (COMPAS)*, Bangladesh, Sep. 2024, doi: 10.1109/COMPAS60761.2024.10796556.

[5] S. K. S. Chamarthy, I. Khan, H. S. Sengar, S. Krishnamurthy, O. Goel, and M. Al-Farouni, "Hybrid Data Security Solutions Using Combined Encryption and Steganography in Communication Systems," in *Proc. 2024 3rd Int. Conf. on Computing, Communication, Perception and Quantum Technology (CCPQT)*, IEEE, 2024, pp. 387–393, doi: 10.1109/CCPQT64497.2024.00081.

[6] K. B. Naidu, J. Manikanta, S. M. D. Vaseem, S. M. D. Adnan, and C. N. Kumar, "Secure file sharing system using image steganography and cryptography techniques," in *Challenges in Information, Communication and Computing Technology, Volume 2*, V. Sharmila et al., Eds. London: Taylor & Francis, 2025, pp. 120–124, doi: 10.1201/9781003559092-21.

[7] G. A. Nwatuzie, L. A. Enyejo, and C. Umeaku, "Enhancing Cloud Data Security Using a Hybrid Encryption Framework Integrating AES, DES, and RC6 with File Splitting and Steganographic Key Management," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 1, pp. 1555–1569, Jan. 2025, doi: 10.5281/zenodo.14792173.

[8] O. S. Adebayo, S. O. Ganiyu, F. B. Osang, S. S. Ajiboye, K. M. Olamilekan, and L. Abdulazeez, "Data Privacy System Using Steganography and Cryptography," *Int. J. Math. Sci. Comput. (IJMSC)*, vol. 8, no. 2, pp. 37–45, Jun. 2022, doi: 10.5815/ijmsc.2022.02.04

[9] Keerthy, G., et al. "Enhancing product authentication and counterfeit detection using qr codes and blockchain technology." 2023 2nd International Conference on Edge Computing and Applications (ICECAA). IEEE, 2023.

[10] O. Allasasmh, A. Alsarhan, D. Abu Laila, G. Samara, and M. Aljaidi, "Integrated Approaches to Steganography: Embedding Static Information Across Audio, Visual, and Textual Formats," in *Proc. 2024 Int. Joint Conf. on Computing (IJCC)*, Dec.2024,doi:10.1109/IJCC64742.2024.10847286

[11] A. V. Jayakumar, "STEGASHIELD – A Multi-Technique using image Steganography to Strengthen Security and Undetectability," *Int. J. Comput. Appl.*, vol. 186, no. 73, pp. 49–56, Mar. 2025, doi: 10.5120/ijca2025924603.

[12] **Rajkumar Soundrapandiyan** and **Jayaraman Venkatesan**, *Digital Video Steganography: An Overview*, in *Advances in Computing and Data Sciences*,Springer,2022. https://doi.org/10.1007/978-981-19-3015-7_42

[13] S. A. Jebur, A. K. Nawar, L. E. Kadhim, and M. M. Jahefer, "Hiding data in pictures with LSB Steganography Technique," Int. J. Interact. Mob. Technol., vol. 17, no. 07, pp. 167–178, Apr. 2023, doi: 10.3991/ijim.v17i07.38737.

[14] M. M. M. Kadhim, L. A. L. Ibrahim, and H. N. Husain, "A Proposed Model of Data Encryption and Decryption Using RSA Algorithm and LSB Steganography," Indonesian Journal of Electrical Engineering and Computer Science, vol. 32, no. 1, pp. 267–275, Apr. 2023

[15] D. Mushtaq, K. H. Baig, and S. M. Santosh, "Robust video Data Hiding Using Steganography." International Journal to Conduct Multidisciplinary Research(IJFMR), vol. 7, no. 3, pp. 1–6, May–June 2025