International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Crypto-Stego: A Hybrid Method for Encrypting Text Messages or Text Files within Images Using AES and LSB Algorithms

Mr. Harshal V. Patil[1], Dr. Vaibhav P. Sonaje[2]

Submitted: 28/10/2024 **Revised:** 02/12/2024 **Accepted:** 10/12/2024

Abstract: In recent times, the volume of data transferred over the internet has expanded globally, resulting in increased data security concerns. The security of data is of paramount importance to both individuals and business owners. Cryptography and steganography are two primary data security techniques. Cryptography is used to encrypt secret messages, while steganography conceals secret messages within digital media and images. The present paper implements a secure model that integrates the Advanced Encryption Standard (AES) and Least Significant Bit (LSB) algorithms in instruction to deliver enhanced safety, data protection, and user-friendliness. AES is utilized in cryptography, while LSB is utilized in steganography. The combination of both algorithms guarantees that data remains completely secure and protected. The proposed solution entails a comprehensive analysis of various encryption techniques, which enables a more effective and secure encryption method. By incorporating different encryption mechanisms, the paper presents a thorough analysis that demonstrates its suitability and effectiveness. In conclusion, the paper's contribution to the field of encryption is substantial, and it provides a valuable framework for future research.

Keywords: *Cryptography, Steganography, Cover-Image, Stego-Image, Plain-Text, Cipher Text, AES, LSB, PSNR, MSE, SNR.*

I Introduction

In recent times, the Internet and communication applications have provided numerous benefits, including real-time data and information transfer, as well as virtual conferences [1;2]. The growing prevalence of available applications across many arenas, such as finance, government, and social media, has underscored the importance of securing the networks through which data is transmitted over the internet network [3;4].

Hence, these applications are crucial for enhancing business operations across various sectors. Nevertheless, data and information security emerges as a significant challenge for organizations that transmit sensitive or private information online. As per [5, 6, 7], the number of cybercriminals or digital data thieves has proliferated at an alarming rate in recent times. These malicious actors concentrate on pilfering sensitive data, such as credit card details and confidential corporate information. Consequently, organizations grapple with the uncertainty of data-transferring channels' security levels.

The use of cryptography in network applications is crucial for securing online data transfers [8, 9]. Cryptography employs encryption techniques that provide confidentiality, integrity, and authenticity of electronic transactions, ensuring that messages are sent without modification and received in their original form [10]. Cryptography is widely used in various communication mediums, such as email, e-commerce, ATM machines, cellular phones, and other electronic devices. The increasing use of electronic communication has led to the need for cryptography and its verification, making it an essential component of modern technology [11].

The key limitation of cryptography technology is that hackers can decrypt the communications that have been encrypted using various encryption algorithms. These

Research Scholar, Sandip University Nashik India
Department of Computer Science & Application, SOCSE, Sandip University, Nashik, India

messages have been subjected to numerous attacks, and hackers have attempted to decrypt them using self-contained countermeasures, as well as mathematical techniques based on arithmetic [12]. Insecure security exists because it lacks comprehensive deployment, which makes it vulnerable to attack. Therefore, the importance of cryptography in ensuring online data security is crucial. According to cryptography experts, steganography is an appropriate method to enhance cryptographic security. It is not possible to improve the security of cryptography using other methods. Steganography is a highly suitable tool for enhancing the cryptographic security. Cryptography and steganography must be recycled together to provide high-level online data safety [13].

StrategoGraphy is a system that consists of a dashboard, audio files, and video files that store data and information of all media files. The primary objective of StrategoGraphy is to simplify the complexity of encrypted data in online disseminated research [14, 15].

In order to obtain complete data, the encrypted data can be decrypted by placing the data online through an application. The data can be encrypted again using the same key and uploaded as a media file [16]. The data can be downloaded from the media file using the same key, and it can be decrypted using the same secret key. Therefore, the encrypted data that is published online is significant for the purpose of research.

Cryptography and steganography are two fundamental concepts that are widely used in the field of information security. These techniques are employed to ensure the privacy and reliability of data and to protect it from unofficial access. Cryptography contains the usage of scientific algorithms to convert plaintext into ciphertext, which can only be deciphered using a key [17]. Steganography, on the other hand, involves the concealment of information within other data, such as images or audio files, to prevent its detection. Both cryptography and steganography are essential tools for maintaining the security of sensitive information, and both are widely used in numerous applications, such as military and government communications, financial transactions, and personal privacy. The two techniques are also complementary, as cryptography provides confidentiality and steganography provides secrecy. While cryptography relies on mathematical algorithms and key management, steganography relies on the use of cover data and the properties of the media used to conceal the information. Therefore, it is important to understand the principles and limitations of both techniques to effectively use them in the field of information security [18].

Cryptography and steganography are both highly secure systems. The AES algorithm is widely used to provide a secure encryption standard, whereas steganography is a less secure method of utilizing the least significant bits of encoded data to embed hidden information. However, to ensure that the data are completely secure, they must be encrypted and decrypted multiple times using different algorithms and the data must be stored in a secure environment. The key objective of steganography is to ensure that the transmission of files is unnoticed by hiding it within another file, and the encryption of the data provides an additional layer of security. Cryptography and steganography are combined to create a secure security system that ensures the privacy, reliability, and accessibility of data. The data were encrypted using the AES algorithm, and the image file was encrypted using the LSB steganography algorithm. The data are then transmitted online and the encryption key is kept secure to prevent unauthorized access.

II. Literature Review

International academic networks and multimedia systems have made significant progress in recent years, as evidenced by their increasing use of secure data transmission channels and their ability to adapt to a variety of purposes. This has resulted in the development of a

communication infrastructure that is capable of sending messages within containers, thanks to the collaboration between sampling devices and analytical software. This infrastructure is vital in the field of data processing, as it has enabled the implementation of important concepts such as data encoding and encryption. The trend in information security is to encrypt messages in order to protect them, which is reflected in the increasing use of secret strategies, such as steganography, as well as the use of multimedia, such as images, videos, and audio [19-22].

The strategy for preserving specialized information in digital format involves an extended use of ontologies, which establish a hierarchical classification of the data. With this approach, various types of data can be integrated into a unified system, allowing for the annotation and retrieval of information from digital multimedia content. This process, known as digital watermarking, can be used for both research and educational purposes. The use of ontologies is bound and governed by various constraints and factors, which may include legal, ethical, privacy, and security considerations. The concept of representativeness, as described by the LSB [23;24] perspective, can be applied here, where humans cannot distinguish between the original and the copied content and therefore the importance of the distinction decreases.

Steganographic and cryptographic systems are both powerful and robust. However, cryptographic systems are designed to provide security through secrecy and authentication, while steganographic systems rely on confidentiality and integrity. While cryptographic systems ensure data confidentiality, integrity, and non-repudiation, steganographic systems ensure confidentiality and integrity but not data authenticity. Therefore, several improvements have been made to integrate cryptographic and steganographic systems into a more robust and trustworthy system. This integration of cryptographic and steganographic systems is known as cryptostegano-graphic systems, which provide a more secure and reliable solution. These systems offer greater security and reliability than either system alone, and they are designed to protect information and maintain its authenticity[25,26].

Riya Das and Indrajit Das[27] have proposed a secure data transmission protocol for the IoT system. They have applied cryptography and steganography, which make IoT devices and home and cloud servers both secure data transmission facilitators. IoT devices use cryptography to securely transmit data and receive encrypted messages, while home servers store encrypted data. A comparison of the hash function of the data and the SIFERTEXT message digest was used to confirm the reliability and reality of the transmitted data. This process ensures data confidentiality and privacy, and is performed by both home and cloud servers.

Ankit Gambhir et al. [28] proposed method combines RSA cryptography and audiovisual steganography. The audiovisual steganography is based on the RSA algorithm, which uses the top-secret message to modify the LSBs of the audiovisual signal. The modified audiovisual signal is then securely transmitted. The authors have demonstrated that the proposed method ensures secure data transmission by using the combination of both encryption algorithms.

Moresh Mukhedkar et al. [29] is a renowned and highly credible individual, known for ensuring the secure transformation of the hazardous and environmentally destructive lead-acid battery industry. The author has employed BlofiSh algorithm to create a secure image of the statue, which is the result of the transformation. Additionally, the encrypted statue was embedded into the ELSB (LSB) matrix, which was then converted into an image using the Quantization technique. The BlofiSh algorithm is highly reliable and secure encapsulation technology, which was enhanced by the modification made by the corrective expert.

The researchers, including Irfan Pratama et al. [30], presented Cryptography and Steganography were combined to ensure data transmission security. This process involves an Mp3 file being covertly encoded using a media player and MD5 function, then encrypted using AES for secure communication. The author's proposed concept aims to enhance data protection by ensuring data hashing and encryption to prevent data tampering.

Nikhil Patel, Shweta Mein, and their associates proposed a new hypothesis [31] using a space domain strategy that involves a secret code and a hidden message. In this context, the glyphs are of the same size. Both glyphs have a secret-whisper channel prepared, which is not visible in the background. The author has given the secret-whisper channel (R, G, or B) the same size as the hidden message and the glyphs are divided into 16 pixels each, with the size of each pixel based on the script. In addition, the hidden message is in SI units and is divided into pixels according to the sequence of 16 pixels. After that, the pixels were linked to the hidden message in a way that is incomprehensible to others. The pixels were then embedded in the hidden message in a way that is not visible by using the second glyph. The pixels were linked to the hidden message using the second glyph, which was divided into 16 pixels each, and the pixels were embedded in the hidden message without changing their size.

Researchers S. H. Gawanda et al. [32] projected the usage of AES algorithm for improving the security and reliability of e-commerce and M-commerce. The authors implemented the AES algorithm using an LSB-based approach to enhance its security and performance. Through experiments, the model was able to process 16-bit and 128-bit keys, which are in compliance with the DIVH security requirements and the underlying process. The model's performance was enhanced through the integration of strategies and cryptographic techniques, resulting in better data security and denial of service resistance. The authors reached a conclusion that this approach is the most suitable for achieving the desired result.

Nouf A. Al-Otaibi et al.[33] introduced a novel technique for ensuring the security of data on personal computers by integrating steganography and cryptography. This approach incorporates two layers of security: a steganography cover and a cryptography cover. The LSB algorithm is utilized in the steganography layer, while DES is implemented in the cryptography layer. The researchers also investigated methods to enhance the capacity for hiding secret data. However, a limitation of this approach is that DES is not completely secure, which may compromise the confidentiality of the private data.

Kamaldeep Joshi, Rajkumar Yadav, et al. [34] proposed a new perspective on image and cryptography by integrating image steganography into cryptography. In this method, top-secret data is inserted in text using the vernacular of a self-learner, and this text is then encrypted using standard cryptography techniques. The encrypted text is then placed in an image, and the resulting steganographic image is encoded using LSBs. The sender and receiver communicate securely using a shared one-time pad. The proposed method enhances the privacy of communication, as the message's quality remains high even when transmitted through a noisy channel.

Morresh Mukhedkar and his colleagues[35] proposed a hybrid encryption technique to ensure image security with high quality They used a Blowfish algorithm to create a private image, which is a secure and efficient encryption method. In contrast, the LSB algorithm was used to embed the encrypted image in the LSB of the cover image, resulting in a tamper-proof and secure method. Blowfish algorithm is a fault-tolerant and highly secure encryption technique.

III. Proposed Work

A. Proposed Methodology:

Data security is a primary concern for many organizations. Our proposed method, "Crypto-Stego: A Hybrid Method for Encrypting Text Messages or Text Files with Images Using AES and LSB Algorithms," aims to provide a secure means of communication for sensitive messages or files. We incorporate both cryptography and steganography into our approach. Our method involves a combination of two techniques: first, we use AES encryption to secure the message or file, and second, we use LSB steganography to embed the encrypted data within an image. Our expertise in both fields allows us to provide a comprehensive solution for data security.

Phase – I Embedding process using cryptography and steganography

The use of cryptography leads to the encryption of messages and the generation of encrypted messages based on the underlying steganography. The AES encryption algorithm is utilized for this purpose. As a result, the message's carrier text is encrypted using AES. The encrypted message's carrier text is then embedded in the cover image. The encryption time, decryption time, MSE, PSNR, and SNR are all computed using various cryptographic techniques that are based on the LSB algorithm. The resulting encrypted message can be decrypted using the same cryptographic algorithm and the same cryptographic key that was used for encryption.

The final output is a stego-image that contains the encrypted message. By combining encryption and steganography, an additional layer of security is provided, making it challenging for unauthorized parties to intercept and decipher the message. The specifics of the first phase of the suggested algorithm are depicted in Figure-1 below.

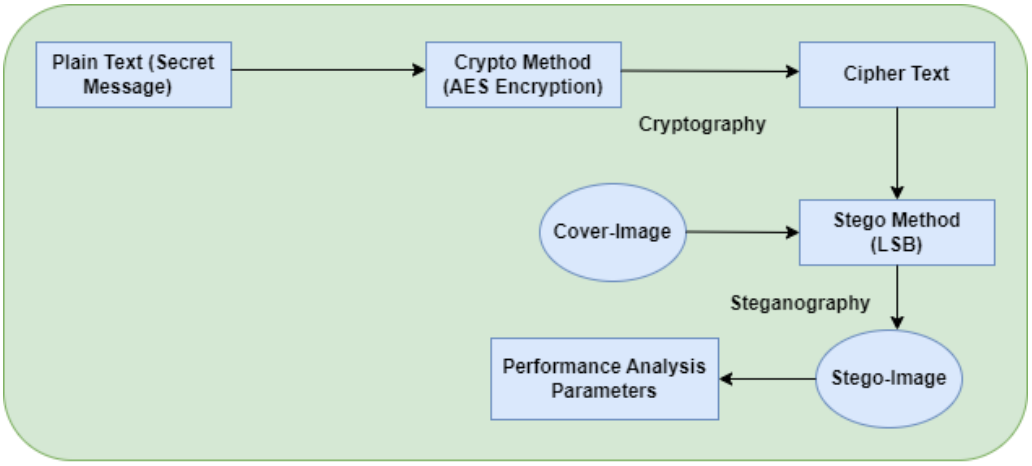

Figure-1 Crypto-Stego Encryption and Embedding Model

Phase – II Extracting process

The process of extracting a message involves reversing the steps taken during the embedding process. To achieve this, a LSB steganography algorithm is employed that has been selected during the inserting process. The resulting stego-image, which contains the concealed cipher text, is then submitted to the decoding method. This produces the cipher text, which is subsequently passed over the AES decryption method to retrieve the top-secret or plain text. The specifics of the second phase of the suggested algorithm are depicted in Figure-2 below.

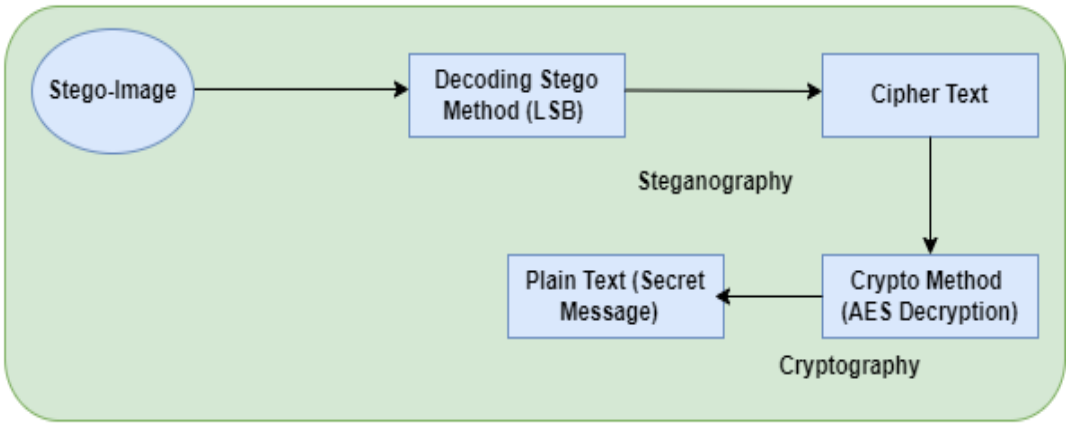

Figure-2 Crypto-Stego Extraction and Decryption Model

B. Proposed Crypto-Stego Algorithm:

Embedding Algorithm

Input: A concealed message or text file and a cover-image

Output: A stego-image

Steps:

1) Examine the cover-image and the confidential message that is intended to be incorporated within the cover-image.

2) Employ the Advanced Encryption Standard (AES) algorithm on the confidential message, transforming plain-text into cipher-text.

3) Convert the cipher-text into binary format.

4) Identify the LSBs of each pixel in the cover-image.

5) Integrate the bits comprising the confidential message into the LSBs of the pixels within the cover-image.

6) Recursively apply this process until the entire confidential message is successfully embedded within the cover-image.

7) The resulting steganographic image, or stego-image, is then created.

Retrieval Algorithm

Input: Stego-image

Output: A confidential message

Steps:

1) Choose the steganographic image or stego-image.

2) Extract the LSBs of each pixel in the stego-image.

3) Recover and retrieve the LSBs of each pixel in the stego-image.

4) Repeat the procedure until the encrypted message is take out from the stego-image.

5) Employ the Advanced Encryption Standard (AES) algorithm on the encrypted message to decipher it and convert it into plain text.

6) Obtain the confidential message.

IV. Implementation and Experimental Result

A. Implementation

Our system incorporates Crypto-Stego algorithms based on the proposed algorithm. Using Visual Studio 2010, we have successfully implemented the Crypto-Stego system that combines AES and LSB. Our primary goal is to thoroughly examine the Crypto-Stego system and evaluate various scenarios to enhance its relevance in both academic and industrial research domains. The implementation details of the proposed algorithm for text messages and text files

are illustrated in Figures 3, 4, 5, and 6 below.

- **Encryption and Embedding Procedure for Text Message**

The accompanying illustrations in Figure 3 depict the graphical representation of the dual layer data security system's implementation interface. The system consists of four functional components, namely Select Cover-Image, Encrypt Original Text Message, Hide Encrypted Text into Image, and Save Stego-Image. The Select Cover-Image feature utilizes the original image and encrypts the Original Message using the AES encryption algorithm with a password or key to generate Cipher-Text. The Cipher-Text is then inserted into the Cover-Image using the LSB technique, resulting in a Stego-Image. Finally, the Stego-Image is saved. Although the Cover-Image and Stego-Image appear visually identical, the latter contains the concealed Cipher-Text.

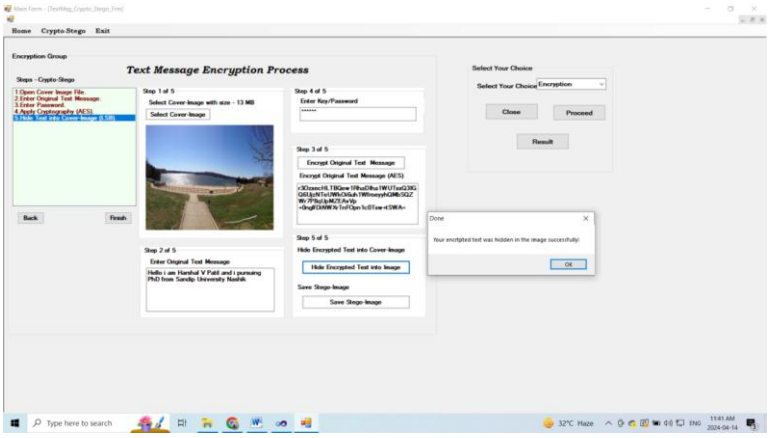

Figure-3 Text Message Encryption and Embedding Procedure

- **Extracting and Decryption Procedure for Text Message**

Three buttons are accessible for completing the process: Select Stego-Image, Get Encrypted Text from Stego-Image, and Decrypt Original Text Message. These buttons are illustrated in Figure 4, where the input supplied to this layer consists of Stego-Image and password/encryption key. The encrypted Text Message is generated using the LSB technique, and it can be decrypted into the Original Message by clicking the Decrypt Original Text Message button, which employs the AES method.

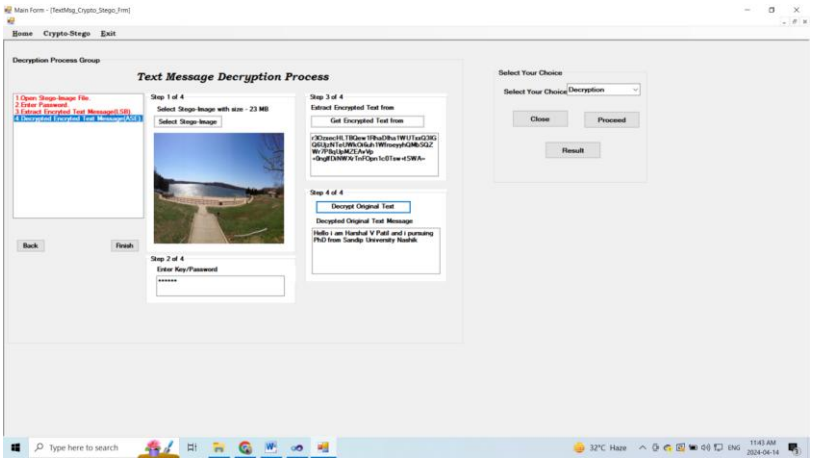

Figure-4 Text Message Extracting and Decryption Procedure

- **Encryption and Embedding Procedure for Text File**

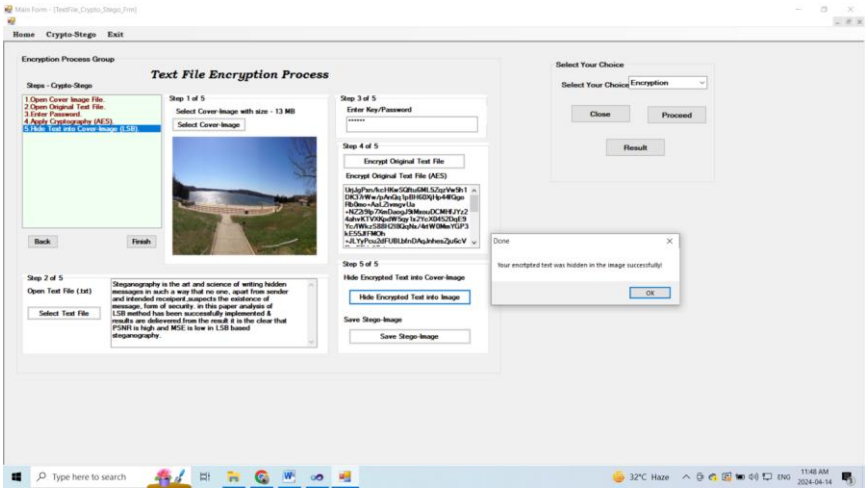

Figure-5 Text File Encryption and Embedding Procedure

- **Extracting and Decryption Procedure for Text File**

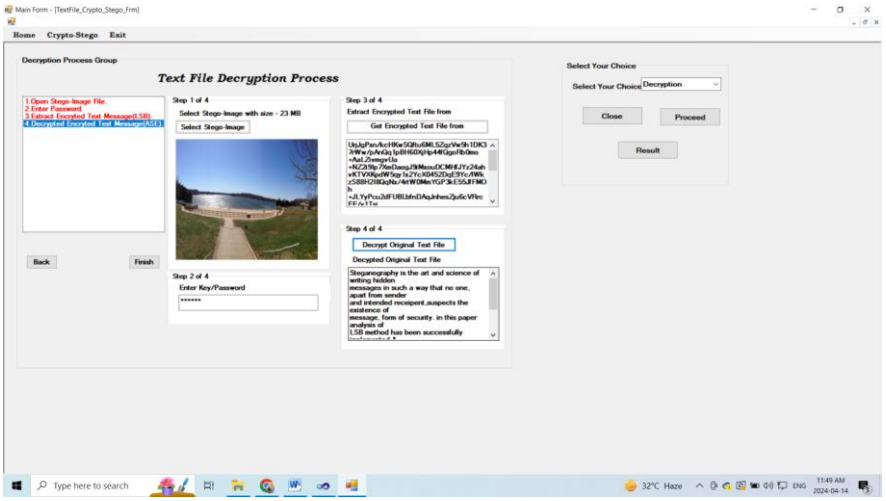

Figure-6 Text File Extracting and Decryption Procedure

B. Experimental Result

To assess the performance of the proposed algorithm, we have utilized various metrics, such as Encryption Time, Decryption Time, PSNR, MSE, and SNR values, which are presented in Tables 1 and 2. Moreover, Figures 7, 8, 9, and 10 provide a graphical representation of the performance evaluation of the proposed algorithm.

- **Experimental Result for Text Message:**

Table-1 Efficiency Parameter of Proposed Method for Text Message.

Sr. No	Cover Image Size in MB	Stego-Image Size in MB	Secret Test Message	Encrypted Message	Encryption Time in Millisecond	Decryption Time in Millisecond	MSE	PSNR in db	SNR in db
1	10	23	Hello i am Harshal V Patil and i pursuing PhD from Sandip University Nashik	r3OzxecHLTBQew1RhaDIha1WUTxxQ3IGQ6UjzNTeUWkZ50G5RiB2ZI2JH/ORZueMUj/ipvR2G1PH/wPaqyaxQO5YrsBxraRGNW8iO1AVHsw=	10.32	12.52	10.02	87.91	93.55
2	15	51			12.14	14.30	9.87	88.18	94.86
3	20	64			12.66	15.81	5.25	90.18	96.53
4	30	79			15.49	16.06	3.48	92.71	98.56
5	40	85			15.89	16.89	3.24	92.97	98.89
6	50	92			16.26	18.72	2.68	93.58	99.73

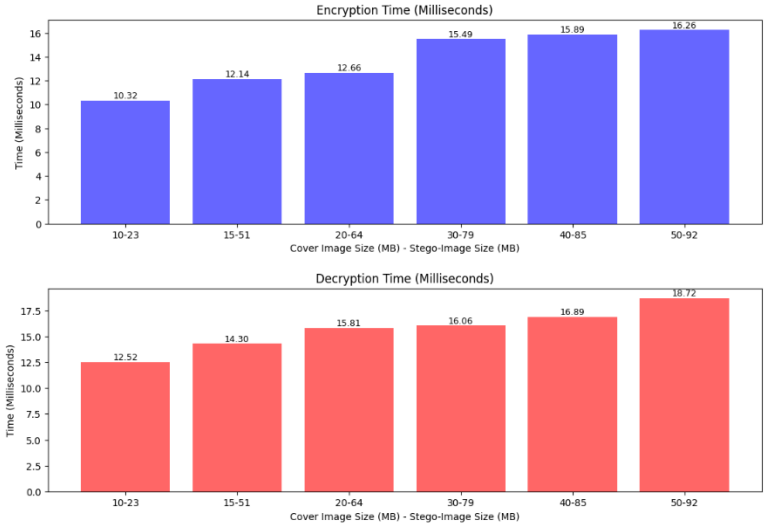

Figure-7 Encryption and Decryption Time of Proposed Method for Text Message

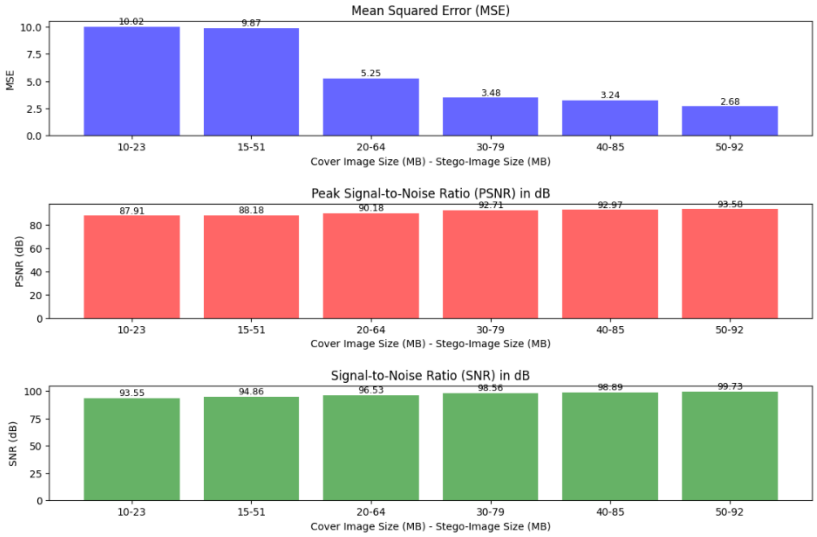

Figure-8 MSE, PSNR and SNR of Proposed Method for Text Message

- **Experimental Result For Text File:**

Table-2 Efficiency Parameter of Proposed Method for Text File.

Sr. No	Cover Image Size in MB	Secret Text File in KB	Stego-Image Size in MB	Encryption Time in Millisecond	Decryption Time in Millisecond	MSE	PSNR in db	SNR in db
1	10	1	23	16.46	19.57	0.00062	80.15	85.06
2		2	23	12.2	41.45	0.0012	77.11	82.27
3		5	23	12.72	56.7	0.0042	71.85	76.81
4		10	23	11.73	65.52	0.0093	68.43	73.51
5	20	1	51	14.22	25.59	0.00028	83.51	88.65
6		2	51	13.34	44.4	0.00057	80.52	85.49
7		5	51	12.04	52.45	0.0022	75.25	80.32
8		10	51	11.06	59.2	0.0042	71.83	76.8
9	30	1	79	15.41	18.94	0.00018	85.45	90.2
10		2	79	12.42	36.22	0.00036	82.49	87.43
11		5	79	11.86	46.52	0.0012	77.17	82.12
12		10	79	10.32	58.26	0.0027	73.74	78.71

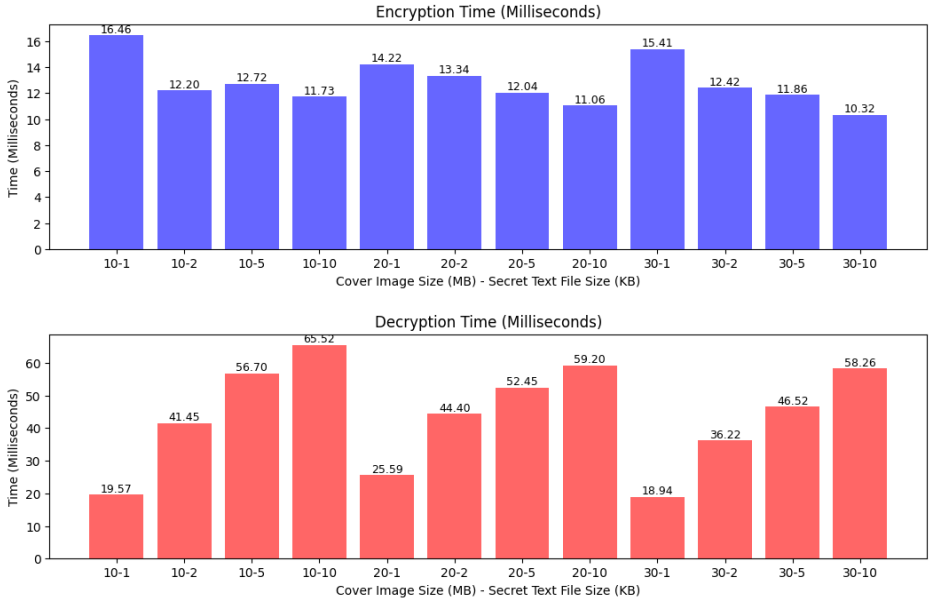

Figure-9 Encryption and Decryption Time of Proposed Method for Text File

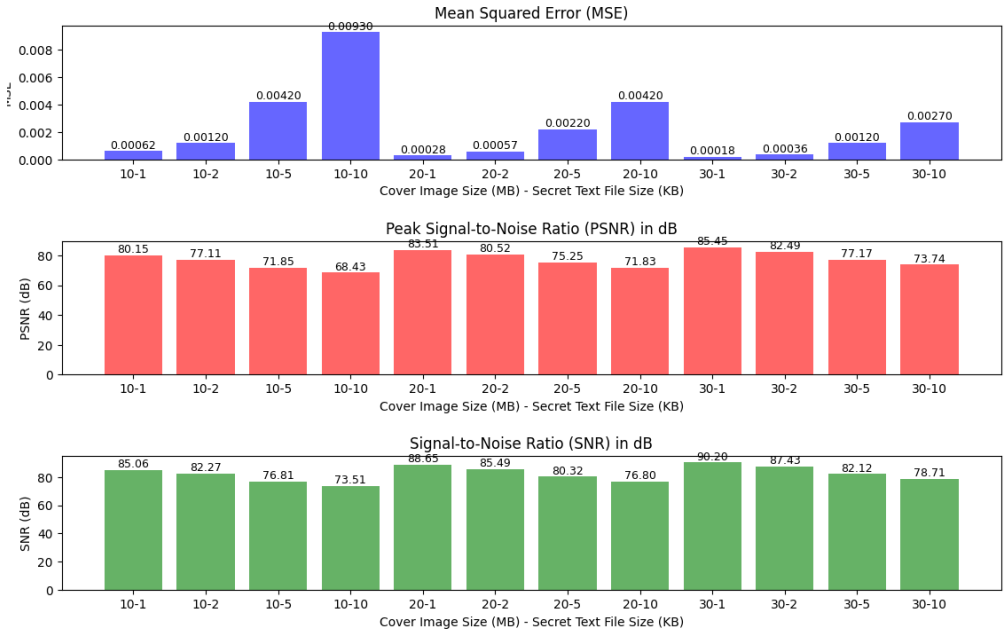

Figure-10 MSE, PSNR and SNR of Proposed Method for Text File

C. Comparative analysis with other CRYPTO-STEGNO model

In comparison with our proposed model and following authors in his research for the same model but used algorithms are different, the following table shows some comparison between both models.

Table-3 Shows the comparative analysis with other CRYPTO-STEGNO model

Compare using	**Proposed CRYPTO-STEGNO Model**	**Saleh Saraiech Model (2013)**	**Manju Bala 2017**	**Ali Ahmed† and Abdelmotalib Ahmed 2020**	**Aljahdali AO, Al-Harbi OA. 2023**
Average PSNR	90.92	62.53	62.6362	41.6	66.28528
Average MSE	5.75	Null	0.1426	30.78	0.022833
Average Encryption Time in MS	13.79	10.40	Null	Null	Null
Average Decryption Time in MS	15.71	10.90	Null	Null	Null

Conclusion:

Our study has revealed a method that provides twofold security for confidential information. By integrating steganography and cryptography, we aim to accomplish the intended objectives. Our system, built using Visual Studio 2010 IDE, is designed to minimize the likelihood of security breaches during the transmission of sensitive data over a network. The proposed system is user-friendly, making it accessible to anyone with basic computer expertise. For image steganography, we have utilized the LSB algorithm, which is a simple yet powerful method. For the encryption and decryption layer, we have employed the AES algorithm, which is a flawless encryption technique.

The performance of proposed algorithm on different mediums has been

assessed using measures such as MSE, PSNR and SNR. The LSB algorithm has been extensively tested using data embedded using the algorithm and the PSNR and SNR values serve as an indicator of the excellence of the stego-object. This proposed method will assist in minimizing the risk of security while transferring sensitive information over the network. The proposed system is user-friendly, allowing anyone with basic computer knowledge to use the system without any difficulty.

References:

[1] Guo, L., B. Yan & Y. Shen 2010. Study on Secure System Architecture of IOT. Information Security and Communications Privacy 12: 042.

[2] Saraireh, S., Al-Saraireh, J. A. A. F. E. R., Al-Sbou, Y. A. Z. E. E. D., & Saraireh, M.(2018). A Hybrid Text-Image Security Technique. Journal of Theoretical & Applied Information Technology, 96(9).

[3] Zmudzinski, S., B. Munir & M. Steinebach 2012. Digital audio authentication by robust feature embedding. IS&T/SPIE Electronic Imaging. pp. 83030I-83030I-7.

[4] Rainie, L., S. Kiesler, R. Kang, M. Madden, M. Duggan, S. Brown & L. Dabbish 2013. Anonymity, privacy, and security online. Pew Research Center.

[5] Kothmayr, T., C. Schmitt, W. Hu, M. Brünig & G. Carle 2013. DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Networks 11(8): 2710-2723.

[6] Sreekutty, M. S., & Baiju, P. S. (2017, April). Security enhancement in image steganography for medical integrity verification system. In Circuit, Power and Computing Technologies (ICCPCT), 2017 International Conference on (pp. 1-5). IEEE.

[7] Al-Saraireh, J. A. (2017). Hvm: A Method For Improving The Performance Of Executing Sql-Query Over Encrypted Database. Journal Of Theoretical & Applied Information Technology, 95(14).

[8] Tirthani, N. & R. Ganesan 2014. Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography. IACR Cryptology ePrint Archive 2014:49

[9] Al Hasib, A. & A. A. M. M. Haque 2008. A comparative study of the performance and security issues of AES and RSA cryptography. Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on. 2 pp. 505-510.

[10] Inzunza-González, E., C. Cruz-Hernández, R. López-Gutiérrez, E. García-Guerrero, L. Cardoza-Avendaño & H. Serrano-Guerrero 2009. Software to Encrypt Messages Using Public-Key Cryptography. World Academy of Science, Engineering and Technology 54.

[11] Goshwe, N. Y. (2013). "Data Encryption and Decryption Using RSA Algorithm in a Network Environment." IJCSNS 13(7): 10.

[12] Chang, C.-C. & C.-Y. Lee 2013. A Smart Card-based Authentication Scheme Using User Identify Cryptography. IJ Network Security 15(2): 139-147.

[13] Dhillon.J 2014. Symmetric and Asymmetric Cryptography Algorithm for Improving Data Security. International Journal of Scientific Engineering and Technology Volume No.3 (Issue No.8): 1123-1125.

[14] Adale, D. A. 2011. Hybrid Information Security Models: Crypto-Steg And Steg-Crypto Systems.Tesis HOWARD UNIVERSITY.Washington.

[15] Rahim, R., Nurdiyanto, H., Hidayat, R., Ahmar, A. S., Siregar, D., Siahaan, A. P. U., Zamsuri, A. (2018). Combination Base64 Algorithm and EOF Technique for Steganography. Paper presented at the Journal of Physics: Conference Series.

[16] Abood, M. H. (2017, March). An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. In New Trends in Information & Communications Technology Applications (NTICT), 2017 Annual Conference on (pp. 86-90). IEEE.

[17] Parah, S. A., Sheikh, J. A., Akhoon, J.

A., Loan, N. A., & Bhat, G. M. (2018). Information hiding in edges: a high capacity information hiding technique using hybrid edge detection. Multimedia Tools and Applications, 77(1), 185-207.
[18] Saraireh S. S., Saraireh M. S., Saraireh S. S., and Saraireh M. S. (2017, Feb), "Filter Bank Block Cipher and LSB Based Steganography for Secure Data Exchange," Int. J. Commun. Antenna Propag., vol. 7, no. 1, p. 1
[19] Taha M S, et al. "Combination of Steganography and Cryptography: A short Survey", 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019), IOP Conf. Series: Materials Science and Engineering, 518 (2019), doi:10.1088/1757-899X/518/5/05200.
[20] Douglas M, Bailey K, Leeney M and Curran K, "An overview of steganography techniques applied to the protection of biometric data", Multimedia Tools and Applications, July 2018, Volume 77, Issue 13, pp 17333–17373.
[21] AL-Shaaby A and AlKharobi T, "Cryptography and Steganography: New Approach", Transactions on Networks and Communications. Volume 5 No. 6, December (2017); pp: 25-38.
[22] Arya A and Soni S, "A Literature Review on Various Recent Steganography Techniques", International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-4248 Volume: 4 Issue: 1, January 2018 pp: 143 – 149.
[23] KASAPBAS M and ELMASRY W, "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check", Sådhanå, (2018), 43:68 Indian Academy of Sciences, https://doi.org/10.1007/s12046-018-0848-4.
[24] Pelosi M, Poudel N, Lamichhane P, and Soomro D, "Steganography System with Application to Crypto-Currency Cold Storage and Secure Transfer", Advances in Science, Technology and Engineering Systems Journal, Vol. 3, No. 2, 271-282 (2018), ISSN: 2415-6698.
[25] Rahmani K, et al., "A Crypto-Steganography: A Survey", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014, pp 149-155, www.ijacsa.thesai.org.
[26] Aung P P and Naing T M, "A novel secure combination technique of steganography and cryptography", International Journal of Information Technology, Modeling and Computing (IJITMC), 2014, 2, pp: 55-62.
[27]. Ria Das, Indrajit Das (2016). Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques. IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN).
[28]. Ankit Gambhir and Sibaram Khara (2016). Integrating RSA Cryptography & Audio Steganography. IEEE ICCCA.
[29]. Moresh Mukhedkar, Prajkta Powar and Peter Gaikwad (2015.). Secure non real time image encryption algorithm development using cryptography & Steganography. IEEE INDICON.
[30]. Irfan Pratama (2016). Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function". International Conference on Science and Technology-Computer. (ICST), IEEE.
[31]. Nikhil Patel, ShwetaMeena (2016). LSB Based Image Steganography Using Dynamic Key Cryptography. International Conference on Emerging Trends in Communication Technologies (ETCT).
[32]. S. H. Gawanda and P. Y. Pawar, (2012). M-Commerce Security Using random LSB Steganography and Cryptography." International Journal od Machine Learning and Computing, vol. 2(4).
[33] N. A. Al-Otaibi and A. A. Gutub, "2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers", Lecture Notes on Information Theory, vol. 2, no. 2, (2014).
[34] Kamaldeep Joshi, RajkumarYadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", IEEE ICIIP,

2015.
[35] Moresh Mukhedkar, Prajkta Powar and Peter Gaikwad, “Secure non real time image encryption algorithm development using cryptography & Steganography”, IEEE INDICON, 2015
[36] Saleh Saraireh, “A secure data communication system using cryptography and Steganography” , International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, pp. 125-137 May 2013.
[37] Manju Bala, Secure Data Transmission techniques using AES cryptography along with Image Steganographic analysis, International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 4, Issue 4, pp. 21-24 Dec 2017.
[38] Ali Ahmed and Abdelmotalib Ahmed, A Secure Image Steganography using LSB and Double XOR Operations IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.5, May 2020
[39] Aljahdali AO, Al-Harbi OA. Double layer steganography technique using DNA sequences and images. PeerJ Comput. Sci. 9:e1379 http://doi.org/10.7717/peerj-cs.1379 (2023).