Elevating Network Security Through Synergistic Image Steganography

KARTHIKEYAN N [1]   SHANTHI S[2]   MAHALAKSHMI G[3]

[1,3] *Assistant Professor, Department of CSE, Government College of Engineering, Sengipatti, Thanjavur, Tamilnadu*

[2] *Associate Professor, Department of CSE, Kongu Engineering College, Perundurai, Erode, Tamilnadu*

Corresponding Author: nkarthikeyan@gcetj.edu.in

Abstract

In the contemporary world, secure communication poses significant challenges. Ensuring security between two communicating parties has become increasingly complex. To address this, cryptographic algorithms are combined with steganography to facilitate secure data transmission from sender to receiver. Constant enhancement of Security Architecture is essential to bolster security parameters such as Confidentiality, Integrity, Accountability, and Availability. In this study, the author presents a novel model that integrates cryptographic and image steganographic techniques to enhance the security of confidential messages. Initially, confidential messages are encrypted using symmetric key encryption, followed by embedding the 8-bit binary form of message bits into the cover image using the Least Significant Bit (LSB) technique[8]. The effectiveness of the proposed model's security is evaluated across various parameters, demonstrating superior protection compared to existing models.

Keywords: Image steganography, Least Significant Bit, Security, Cryptography, Pixel value Difference

1. INTRODUCTION

In today's digital age, the paramount importance of security cannot be overstated. With the exponential growth of digital data and the ubiquitous nature of communication networks, ensuring the confidentiality, integrity, and authenticity of information has become a pressing concern. Cryptography stands as a stalwart guardian in this realm, offering techniques to encode data such that only authorized parties can decipher it. However, as technologies advance, so do the methods employed by malicious actors to breach security measures. In this landscape, the fusion of cryptography with image steganography emerges as a potent strategy, leveraging the power of concealment within the visual medium to fortify data protection [1-7].

Within the domain of image steganography, concealing messages within images has long been recognized as an effective means of covert communication. By embedding data within the pixels of an image, steganography provides a clandestine channel for information transmission, often evading detection by casual observers. However, the spatial domain of steganography presents both challenges and opportunities in ensuring robust security [9]. As techniques evolve to conceal information within images, the need for cryptographic safeguards becomes increasingly evident. Combining cryptography with image steganography not only enhances the level of security but also enriches the arsenal of tools available for safeguarding sensitive data in an ever-evolving digital landscape.

2. LITERATURE SURVEY

A comprehensive literature survey on various image steganography and cryptography techniques reveals a rich tapestry of methodologies aimed at fortifying data security in digital communication. In the realm of image steganography, researchers have explored diverse approaches to conceal information within images while preserving their perceptual integrity. Traditional techniques, such as Least Significant Bit (LSB) embedding, remain foundational, offering simplicity and ease of implementation. However, contemporary advancements have led to the development of sophisticated algorithms, including Transform Domain Techniques (TDTs) like Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT), which exploit frequency or spatial domain characteristics to embed data imperceptibly.

Furthermore, recent research has delved into adaptive and reversible steganography schemes, which dynamically adjust embedding strategies based on image content or enable precise extraction of hidden data without any loss. Alongside these developments, the literature showcases a parallel evolution in cryptographic techniques tailored for securing digital imagery. Classical cryptographic primitives such as symmetric and asymmetric encryption play pivotal roles in ensuring confidentiality and integrity, offering robust mechanisms for securing steganographic payloads. Additionally, novel cryptographic protocols like homomorphic encryption and attribute-based encryption have been investigated for their compatibility with image steganography, promising enhanced privacy and access control in clandestine communication channels.

Moreover, the fusion of cryptography with steganography has spurred interdisciplinary research endeavors, yielding hybrid frameworks that synergistically combine the strengths of both discrepancies. the dynamic landscape of image steganography and cryptography, characterized by ongoing innovation and cross-pollination of ideas, aimed at fortifying data security in diverse digital applications.

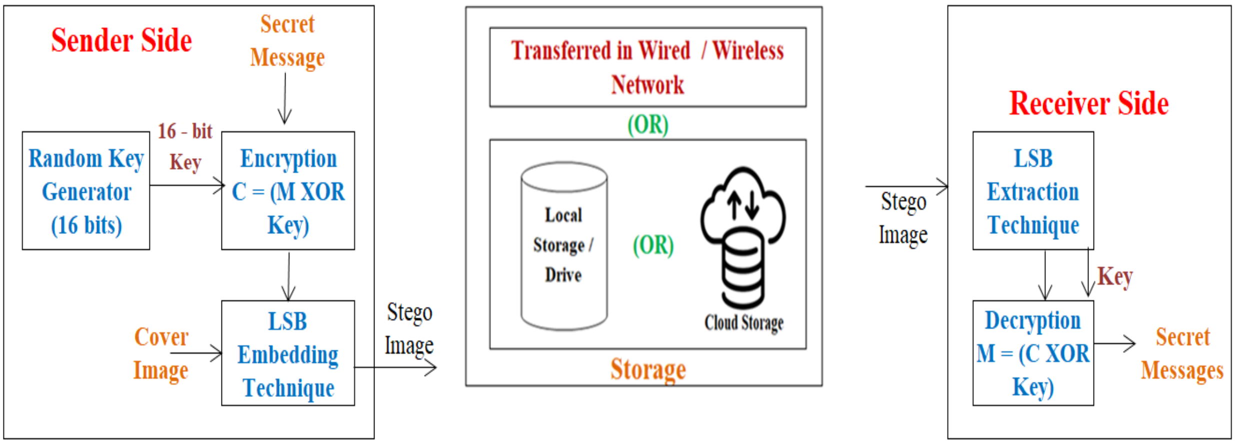


Figure No. 1 Architecture of the Proposed Model

3. PROPOSED MODEL

Ensuring the security of shared messages is paramount in digital communication. The proposed model provides a dual-layer security mechanism for safeguarding secret messages. At the sender's end, the process begins with the generation of a 16-bit random key using a random number generator. Subsequently, the input secret messages are encrypted using the random 16-bit key. Finally, the encrypted secret messages are embedded into the cover image utilizing the LSB Technique, resulting in the creation of a stego image. This stego image can then be stored locally, in cloud storage, or transmitted to the intended recipient. Upon reception of the stego image or retrieval from storage, the recipient employs the LSB technique to extract the encrypted secret messages embedded within. Subsequently, the recipient decrypts the extracted encrypted secret messages using the same random number generated during the sender's process. The framework illustration of the proposed model is depicted in Fig1.

4. RESULTS AND DISCUSSION

The proposed framework has been developed using Python 3.12 on a Windows 10 operating system, with 4GB of RAM size. It underwent rigorous testing with a diverse array of standard and non-standard images, encompassing various formats and sizes. Performance evaluation involved assessing parameters such as stego image quality, embedding capacity, and security, with a particular focus on security assessment for evaluating model efficacy.

4.1 Visual Analysis

Visual analysis was conducted by comparing the quality of the original cover image with that of the stego image, revealing the detection of concealed messages within the latter. This model achieves an average Peak Signal-to-Noise Ratio (PSNR) of approximately 63.44dB while embedding messages sized at 5.93KB, equating to 97,224 bits. With an average PSNR range surpassing the minimum perceptible threshold of 30dB, the human visual system is unable to discern hidden messages within the stego image. Furthermore, employing the Least Significant Bit (LSB) technique ensures minimal deviation in intensities, ±1, thereby thwarting intruders' ability to detect changes in cover image intensities.

4.2 Histogram Analysis

Intruders often rely on deviations in pixel intensities across the red, green, and blue channels of both the original cover image and the stego image to uncover hidden messages. Fig. 2 illustrates the histogram representation of the baboon image's red, blue, and green channels. A 2D graph is plotted where the X-axis denotes pixel location and the Y-axis indicates the intensity of the corresponding color channel. Leveraging the Least Significant Bit (LSB) technique minimizes alterations in intensity across various color channels in the cover image, thereby thwarting intruders' attempts to discern changes in the stego image through histogram analysis.

4.3Execution Time Analysis

Table 1 provides an analysis of the execution time for the proposed model when embedding an input size of 5.93KB across various image dimensions and formats. Table 2, on the other hand, showcases the execution time analysis for different embedding capacities of secret messages within a standard 512 x 512-dimension image. It's evident from Table 1 that the proposed method consistently maintains similar encryption, embedding, execution, and extraction times for identical input sizes. Additionally, Table 2 demonstrates that as embedding capacity increases, the execution time of the proposed model gradually rises without compromising the quality of the stego image. This incremental increase in execution time indicates that even for intruders attempting to detect the secret key, key size, and embedding technique, more time is required to uncover hidden messages.

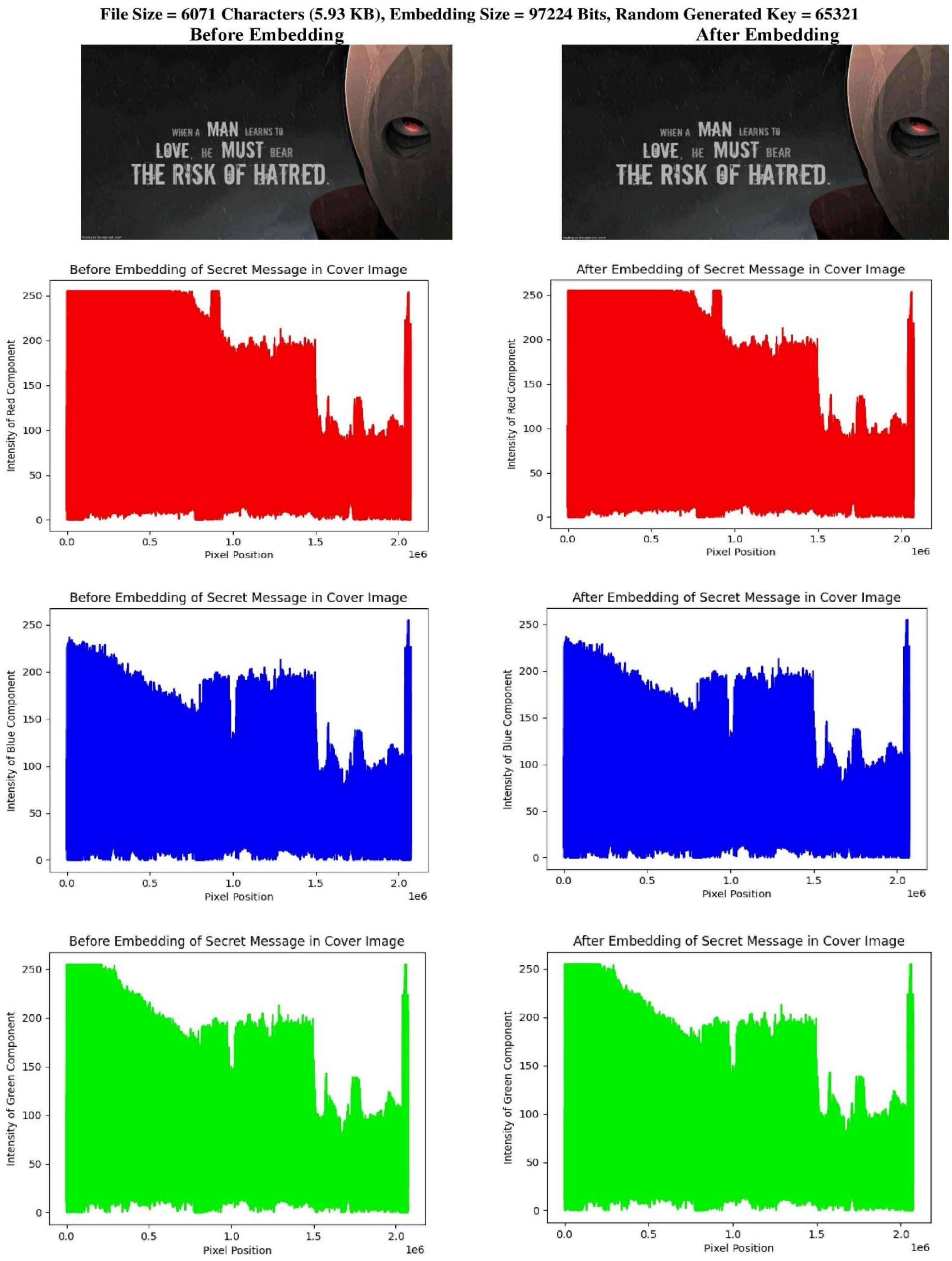


Fig. No. 2 Histogram Analysis of the Red, Blue, and Green Components of the cover and Stego images of the proposed Model.

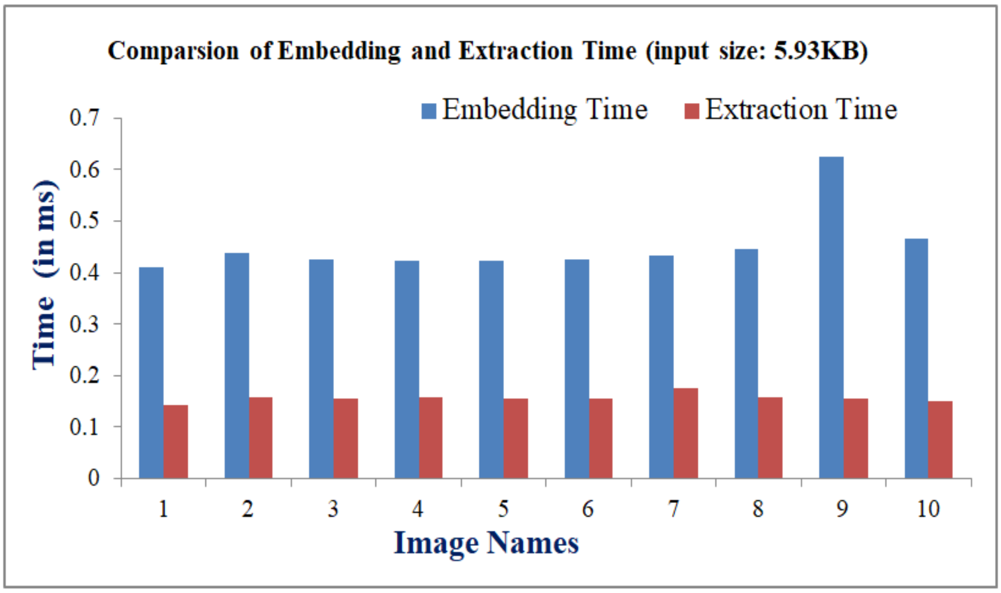
Table 1. Execution Time Analysis of the Proposed Model for the input size of 5.93KB

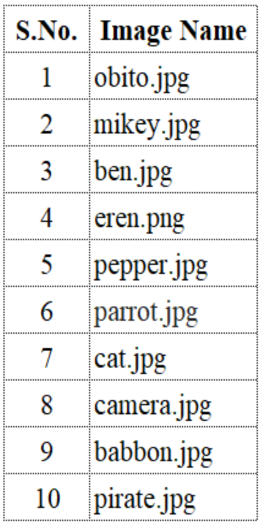
File Size = 6071 Characters (5.93 KB), Embedding Size = 97224 Bits, Random Generated Key = 65321						
Image Name	**Image Size**	**Maximum Embedding Capacity (in bits)**	**Encryption Time (in ms)**	**Embedding Time (in ms)**	**Extraction Time (in ms)**	**Decryption Time (in ms)**
obito.jpg	1080x1920	6220800	0.001063	0.4102	0.1427	0.001073
mikey.jpg	478x850	1218900	0.001082	0.4388	0.1581	0.001089
ben.jpg	720x1280	2764800	0.001058	0.4242	0.1549	0.001073
eren.png	1080x1920	6220800	0.001055	0.4217	0.1588	0.001075
pepper.jpg	512x512	786432	0.001034	0.4240	0.1564	0.001081
parrot.jpg	853x1280	3275520	0.001036	0.4242	0.1542	0.000992
cat.jpg	512x512	786432	0.001001	0.4333	0.1752	0.000997
camera.jpg	512x512	786432	0.001052	0.4451	0.1577	0.001004
babbon.jpg	512x512	786432	0.001068	0.6239	0.1553	0.001001
pirate.jpg	512x512	786432	0.001134	0.4655	0.1503	0.001132

Table 2. Execution Time Analysis of the Proposed Model for various input size

Image Name = pepper.jpg, Image Size = 512 x 512, Maximum Embedding Capacity = 786432 bits, Random Generated Key = 65321				
File Size (in KB)	**Encryption Time (in ms)**	**Embedding Time (in ms)**	**Extraction Time (in ms)**	**Decryption Time (in ms)**
8.54	0.003073	0.4502	0.3413	0.002031
9.77	0.005045	0.5418	0.4211	0.002989
9.81	0.005313	0.5771	0.4541	0.003083
11.6	0.006052	0.689	0.5851	0.004912
12	0.006831	0.7424	0.6219	0.005081
12.6	0.007216	0.7836	0.6834	0.006102
13.2	0.007863	0.8413	0.7291	0.006835
14.3	0.008071	0.8973	0.7834	0.007319
15.2	0.009021	0.9761	0.8512	0.007912
17.1	0.010131	1.0031	0.9828	0.009132

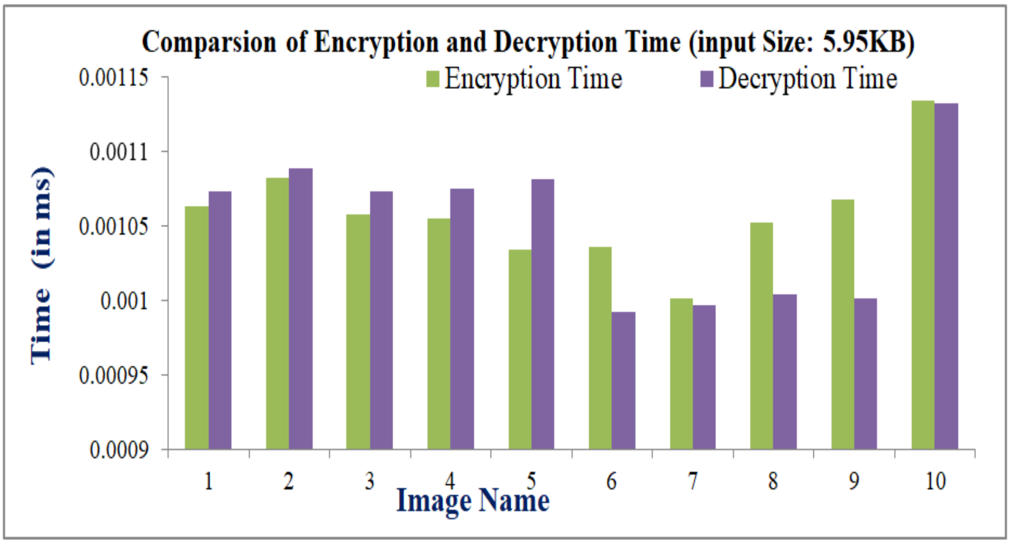
Consequently, intruders face greater challenges and time constraints in uncovering secret messages within the stego image. Fig. 3 depicts the execution time analysis corresponding to the data presented in Tables 1 and 2.





S.No.	Image Name
1	obito.jpg
2	mikey.jpg
3	ben.jpg
4	eren.png
5	pepper.jpg
6	parrot.jpg
7	cat.jpg
8	camera.jpg
9	babbon.jpg
10	pirate.jpg

Fig. No. 3 (a) Comparison of Embedding and Extraction Time for various image for the fixed input size



S.No.	Image Name
1	obito.jpg
2	mikey.jpg
3	ben.jpg
4	eren.png
5	pepper.jpg
6	parrot.jpg
7	cat.jpg
8	camera.jpg
9	babbon.jpg
10	pirate.jpg

Fig. No. 3 (b) Comparison of Encryption and Decryption Time for various image for the fixed input size

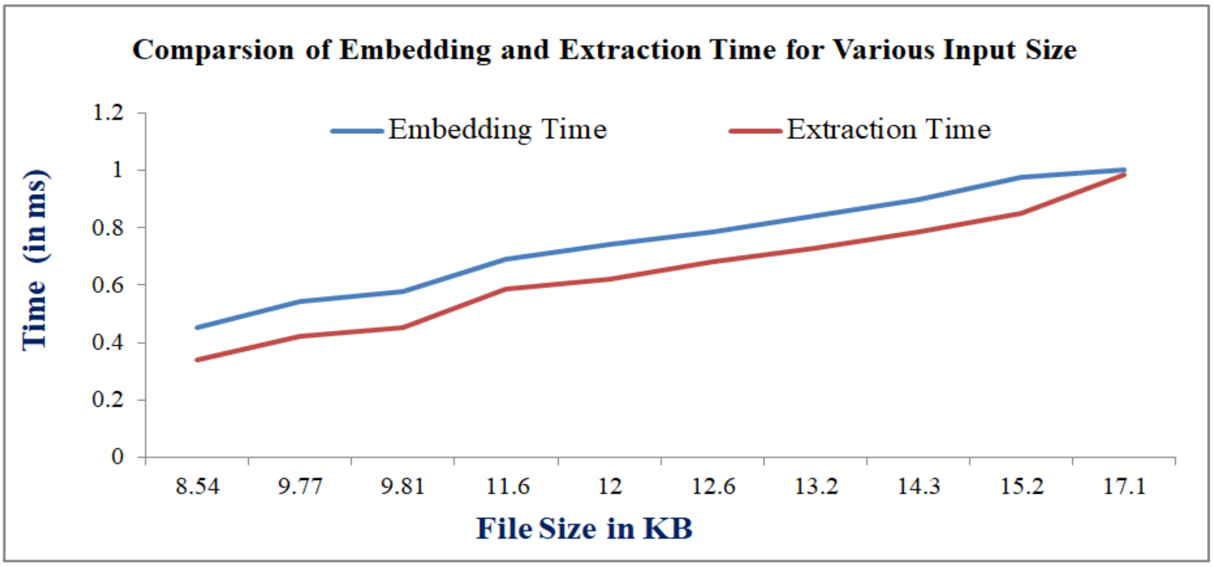


Fig. No. 3 (c) Comparison of Embedding and Extraction Time for various input size.

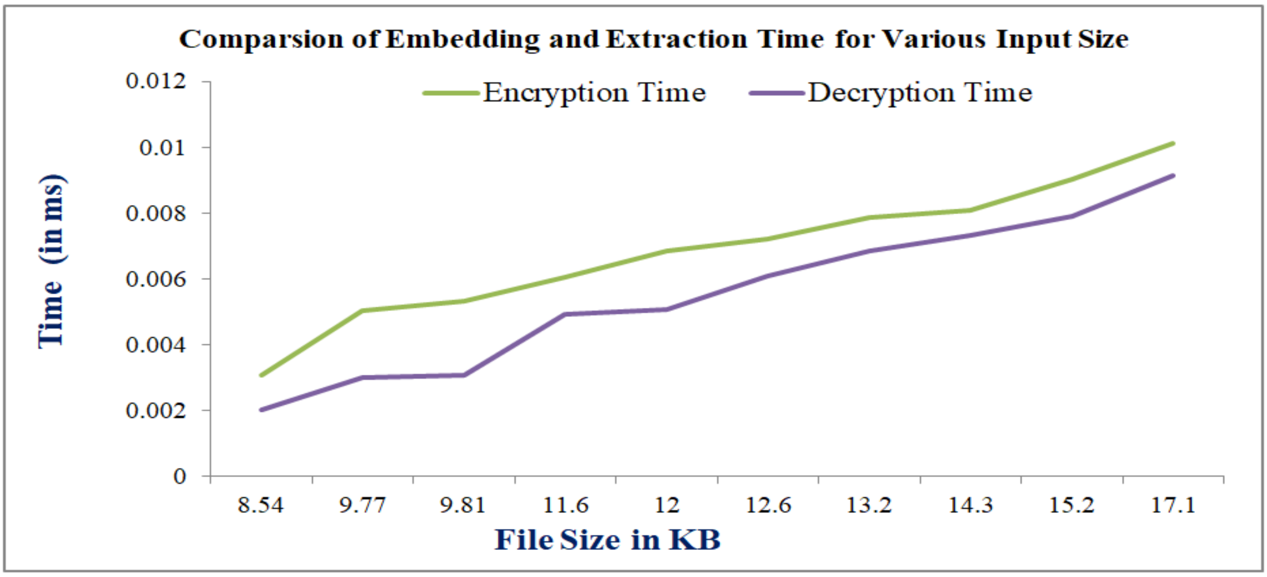


Fig. No. 3 (d) Comparison of Embedding and Extraction Time for various input size.

CONCLUSION

In conclusion, our proposed model introduces a dual-layer security framework by integrating symmetric encryption with the LSB technique, thus bolstering the safeguarding of confidential messages within digital communication channels. Notably, this model demonstrates notable strengths in generating high-quality steganographic images with increased embedding capacity, while concurrently offering enhanced protection against various residual attacks. Through empirical evaluation, it becomes evident that our model exhibits superior resilience against intrusion attempts, as evidenced by both visual and execution time analyses. The findings of this study suggest promising avenues for further research, including the exploration of alternative embedding techniques within the framework of our proposed model. By maintaining a delicate balance between security, embedding capacity, and steganographic quality, this model holds significant potential for advancing data protection measures in digital communication contexts.

REFERENCES

[1] Priyankkumar Sharma, Meet Shitalkumar Patel, Apoorva Rajesh Prasad, “A Systematic Literature Review on Internet of Vehicles Security”, arXiv (2022), DOI: https://doi.org/10.48550/arXiv.2212.08754

[2] Van Huynh Le, Jerry den Hartog, Nicola Zannone,"Security and privacy for innovative automotive applications: A survey", Computer Communications, Volume 132, 2018, Pages 17-41,ISSN 0140-3664, DOI: https://doi.org/10.1016/j.comcom.2018.09.010.

[3] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, ”Digital image steganography: Survey and analysis of current methods”, Signal Processing, Volume 90, Issue 3,2010, Pages 727-752, ISSN 0165-1684, https://doi.org/10.1016/j.sigpro.2009.08.010.

[4] Pratap Chandra Mandal and Imon Mukherjee and Goutam Paul and B.N. Chatterji, “Digital image steganography: A literature survey”, Information Sciences, (2022) Volume. 609, pp. 1451-1488, ISSN 0020-0255, doi: https://doi.org/10.1016/j.ins.2022.07.120.

[5] Hussain, Mehdi, et al. "Image steganography in spatial domain: A survey." Signal Processing: Image Communication 65 (2018): 46-66.

[6] Laishram, Debina, and Themrichon Tuithung. "A survey on digital image steganography: current trends and challenges." proceedings of 3rd international conference on internet of things and connected technologies (ICIoTCT). 2018.

[7] Sachin Dhawan & Rashmi Gupta (2021) Analysis of various data security techniques of steganography: A survey, Information Security Journal: A Global Perspective, 2021, Vol 30:2, 63-87, DOI: 10.1080/19393555.2020.1801911

[8] Solak, Serdar, and U. M. U. T. Altınışık. "LSB Substitution and PVD performance analysis for image steganography." International Journal of Computer Sciences and Engineering 6.10 (2018): 1-4.

[9] K. C. Nunna and R. Marapareddy, "Secure Data Transfer Through Internet Using Cryptography and Image Steganography," *2020 SoutheastCon*, Raleigh, NC, USA, 2020, pp. 1-5, doi: 10.1109/SoutheastCon44009.2020.9368301.