Integrating Quality Analysis Enhancement Through Image Steganography: Fortified Paradigms

KARTHIKEYAN N[1] MOHAMED YASHIN M[2] MANIKANDAN M[3] VASANTH M[4] GANESH S[5]

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

[2,3,4,5] Final Year CSE, Department of CSE, Government College of Engineering, Sengipatti, Thanjavur, Tamilnadu

Corresponding Author: nkarthikeyan@gcetj.edu.in

Abstract

Instances of data breaches and exposure during message transfers across the internet highlight the critical need for securing confidential data. Enhancing security architecture is imperative to bolster parameters such as Confidentiality, Integrity, Accountability, and Availability during data transmission. Various steganography and cryptographic techniques have been proposed to safeguard sensitive information. This study introduces a novel model that integrates cryptographic and image steganography techniques to fortify communication channels. Initially, confidential messages undergo encryption 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. This model provides a dual layer of security for confidential information protection. Performance evaluations of the proposed method demonstrate enhanced security without compromising the quality of the cover image.

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

1. INTRODUCTION

In today's world, where digital communication has become pervasive, the need for security has never been more pressing. With online transactions, sensitive data exchanges, and communication across digital platforms becoming the norm, there is an urgent call for robust protective measures. It sets out to explore the intricate landscape of securing digital communication, highlighting the crucial roles played by cryptography and steganography in maintaining the integrity and confidentiality of information.

Cryptography, an ancient practice of encoding messages to make them incomprehensible to unauthorized individuals, stands as a foundational pillar in the realm of digital security. Its arsenal of techniques, spanning from symmetric and asymmetric encryption to hashing algorithms, serves as a formidable defense against eavesdropping and tampering. Through an in-depth examination of the principles and applications of cryptography, this journal aims to illustrate how these techniques form the backbone of secure digital communication protocols, ensuring confidentiality, authenticity, and integrity in the face of evolving cyber threats.

Yet, as adversaries continue to innovate and devise sophisticated methods to breach cryptographic barriers, the complementary role of steganography emerges as a vital enhancement to traditional security measures. Unlike cryptography, which focuses on obscuring the content of a message, steganography operates by concealing information within seemingly innocuous carriers, such as images or audio files. This covert communication approach introduces an additional layer of complexity, making it significantly more challenging for adversaries to identify concealed data. By exploring the intricacies of steganographic techniques, this journal aims to elucidate how they contribute to the concealment and safeguarding of sensitive information in digital transmissions.

2. LITERATURE SURVEY

A thorough examination of the existing literature on image steganography and cryptography reveals a diverse array of methodologies aimed at bolstering data security in digital communication. In the domain of image steganography, researchers have explored various techniques to conceal information within images while preserving their perceptual integrity. Foundational methods like Least Significant Bit (LSB) embedding continue to be prevalent due to their simplicity and ease of implementation. However, recent advancements have introduced sophisticated algorithms such as Transform Domain Techniques (TDTs) like Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT), which leverage frequency or spatial domain characteristics to embed data imperceptibly.

Furthermore, contemporary research has delved into adaptive and reversible steganography schemes that dynamically adjust embedding strategies based on image content or enable precise data extraction without loss. Concurrently, there has been significant progress in cryptographic techniques tailored for securing digital imagery. Classical cryptographic primitives such as symmetric and asymmetric encryption play vital roles in ensuring confidentiality and integrity, providing robust mechanisms for safeguarding steganographic payloads. Additionally, novel cryptographic protocols like homomorphic encryption and attribute-based encryption are being explored for their compatibility with image steganography, offering improved privacy and access control in covert communication channels.

Moreover, the integration of cryptography with steganography has led to interdisciplinary efforts, resulting in hybrid frameworks that combine the strengths of both disciplines. These hybrid approaches utilize cryptographic keys to bolster the security of steganographic embedding and extraction processes, thereby mitigating risks posed by potential adversaries.

3. PROPOSED MODEL

Ensuring the security of transmitted messages is of utmost importance in digital communication. The proposed model offers a robust dual-layer security approach to protect confidential information. Initially, a 16-bit random key is generated using a random number generator at the sender's end. Following this, the secret messages are encrypted using the generated key. These encrypted messages are then embedded into the cover image using the LSB Technique, resulting in the creation of a stego image. This stego image can be stored locally, in cloud storage, or transmitted to the intended recipient. Upon receiving the stego image or retrieving it from storage, the recipient utilizes the LSB technique to extract the encrypted secret messages. Subsequently, the recipient decrypts the extracted messages using the same randomly generated number employed during the sender's process. A schematic representation of the proposed model is provided in Fig 1.

3.1 Algorithm for implementation of the Proposed Model

The process of embedding involves using a symmetric encryption algorithm and LSB techniques. The steps are as follows:

a. Generate a 16-bit random number.
b. Select the cover image and confidential message.
c. Encrypt the confidential message with the random number using the expression, message XOR random key.
d. Embed the encrypted message into the cover image using LSB technique.

On the receiver side, once the stego image has been received as a part of response from the sender or accessing from either local or cloud storage extraction and decryption process takes place. The steps in receiver side as follows:

a. By using LSB retrieval technique extract the message from the stego image.
b. Decrypt the message using the expression XOR.

3.2 Assessment of Proposed Model

The proposed model's effectiveness is evaluated across various dimensions, including quality, embedding capacity, and security. This paper seeks to demonstrate the model's efficacy by comparing the quality of the stego image with that of the cover image. Several parameters are employed to assess the model's quality, such as Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Matrix (SSIM), Structural Context (SC), Image Fidelity (IF), Absolute Difference, and Normalized Cross-Correlation (NCC). The equations for evaluating these parameters are outlined in Table 1. Here, 'm' and 'n' denote the dimensions of the image, Y_{ij} represents the pixel intensity of the cover image, Y'_{ij} denotes the pixel intensity of the stego image in the ith row in jth column, and 'MAX' represents the maximum pixel value of any color component in the stego image.

4. RESULTS AND DISCUSSION

The image quality is validated using specific standards during the analysis of results. The properties can be compared between the quality of stego image and actual image. Various metrics are Mean Square Error (MSE), Root Mean Squared Error (RMSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Matrix (SSIM), Image Fidelity (IF), Absolute Error (AE), Normalized Cross–Correlation (NCC), and Structural Content (SC) are followed for scaling image quality. These metrics play a crucial role in assessing the quality of the stego image, providing valuable insights into the effectiveness of the results. From Table 1 values for RMSE is 0.18605 which is very low and PSNR value is in the ranges between 63.31 to 63.43 which intimates effective outcome. PSNR value must be above 30 for better outcome and our result satisfies that. NCC and SC achieved the value of 1 which shows resemblance between cover image and stego image. The AE is found to be close to zero which is no difference between the cover image and stego image.

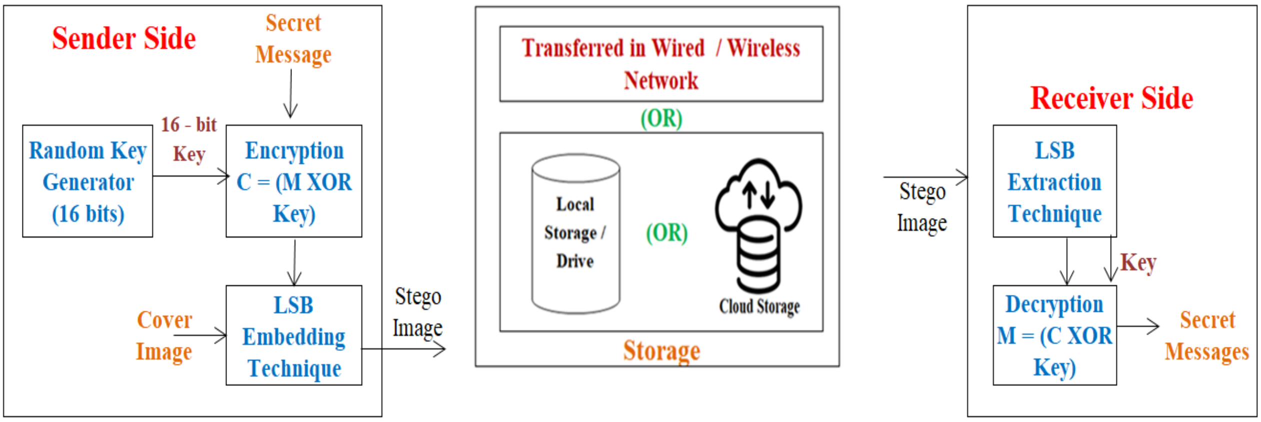


Fig. No. 1 Architecture of the Proposed Model

. From Table 2 the file size is inversely proportional to PSNR values that if the file size is increased the values of PSNR is decreased but in a conventional way. There is no value is below 30dB which states that the result is valid The value of RMSE is 0.33431 which is very low value. NCC and SC achieved the value of 1 which shows resemblance between cover image and stego image. The AE is found to be close to zero which is no difference between the cover image and stego image. From Figure 2(a) illustrates the verification of results for various images, all having a same embedding file size, produces good image quality as indicated by the PSNR results. Figure 2(b) demonstrates that as the file embedding size increases for same image, the PSNR decreases. Since the value remains above 30dB, indicating good quality. In Figure 2(c), multiple images were used with a fixed embedding size and SSIM values near 1 indicate an improvement in image quality. From Figure 2(d) as the file embedding size increases for same image the SSIM values approach 1 indicating good quality.

Table 1 Equation for evaluation of Quality metrics

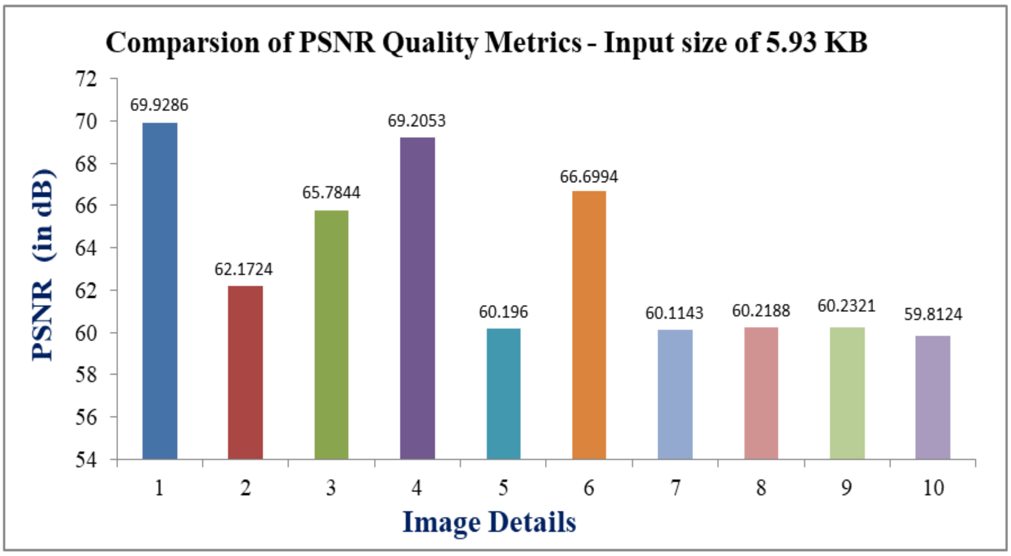
Quality Parameter	Equations
Mean Squared Error (MSE)	$\frac{1}{mn}\sum_{i=0}^{m}\sum_{j=0}^{n}(Y_{ij}-Y'_{ij})^2$
Root Mean Square Error (RMSE)	$\mathrm{MSE}^{\frac{1}{2}}$
Peak Signal to Noise Ratio (PSNR)	$10\log_{10}(MAX^2\,/MSE)$
Image Fidelity (IF)	$1-\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(y(i,j)-Y'^{(ij)})^2}{\sum_{i=1}^{m}\sum_{j=1}^{n}y(i,j)^2}$
Absolute Difference (AE)	$\lvert y(i,j)-y'(i,j)\rvert$
Normalized Cross–Correlation (NCC)	$\sum_{i=1}^{m}\sum_{j=1}^{n}\frac{(y(i,j)y'(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(y(i,j)\right)^2}$
Structural Similarity Index Matrix (SSIM)	$\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_x^2+c_2)}$
Structural Context (SC)	$\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(y(i,j)\right)^2}{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(y'(i,j)\right)^2}$

Table 1 Assessment of Quality Parameters of the Proposed Method for the input size of 5.93KB

<table>
<tr><td colspan="11">File Size = 6071 Characters (5.93 KB), Embedding Size = 97224 Bits, Random Generated Key = 65321</td></tr>
<tr><th>Image Name</th><th>Image Size</th><th>Max. Embedding Capacity (in bits)</th><th>MSE</th><th>RMSE</th><th>PSNR (in dB)</th><th>SSIM</th><th>AE</th><th>NCC</th><th>IF</th><th>SC</th></tr>
<tr><td>obito.jpg</td><td>1080x1920</td><td>6220800</td><td>0.0066</td><td>0.0813</td><td>69.9286</td><td>0.9975</td><td>0.0001</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>mikey.jpg</td><td>478x850</td><td>1218900</td><td>0.0394</td><td>0.1986</td><td>62.1724</td><td>0.9891</td><td>0.0148</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>ben.jpg</td><td>720x1280</td><td>2764800</td><td>0.0172</td><td>0.131</td><td>65.7844</td><td>0.9962</td><td>0.0062</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>eren.png</td><td>1080x1920</td><td>6220800</td><td>0.0078</td><td>0.0884</td><td>69.2053</td><td>0.9971</td><td>0.0032</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>pepper.jpg</td><td>512x512</td><td>786432</td><td>0.0622</td><td>0.2493</td><td>60.196</td><td>0.9821</td><td>0.0249</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>parrot.jpg</td><td>853x1280</td><td>3275520</td><td>0.0139</td><td>0.1179</td><td>66.6994</td><td>0.9971</td><td>0.0034</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>cat.jpg</td><td>512x512</td><td>786432</td><td>0.0619</td><td>0.2487</td><td>60.1143</td><td>0.9831</td><td>0.0244</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>camera.jpg</td><td>512x512</td><td>786432</td><td>0.0618</td><td>0.2487</td><td>60.2188</td><td>0.9842</td><td>0.024</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>babbon.jpg</td><td>512x512</td><td>786432</td><td>0.0616</td><td>0.2483</td><td>60.2321</td><td>0.9847</td><td>0.0247</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>pirate.jpg</td><td>512x512</td><td>786432</td><td>0.0617</td><td>0.2483</td><td>59.8124</td><td>0.9813</td><td>0.0246</td><td>1</td><td>1</td><td>1</td></tr>
</table>

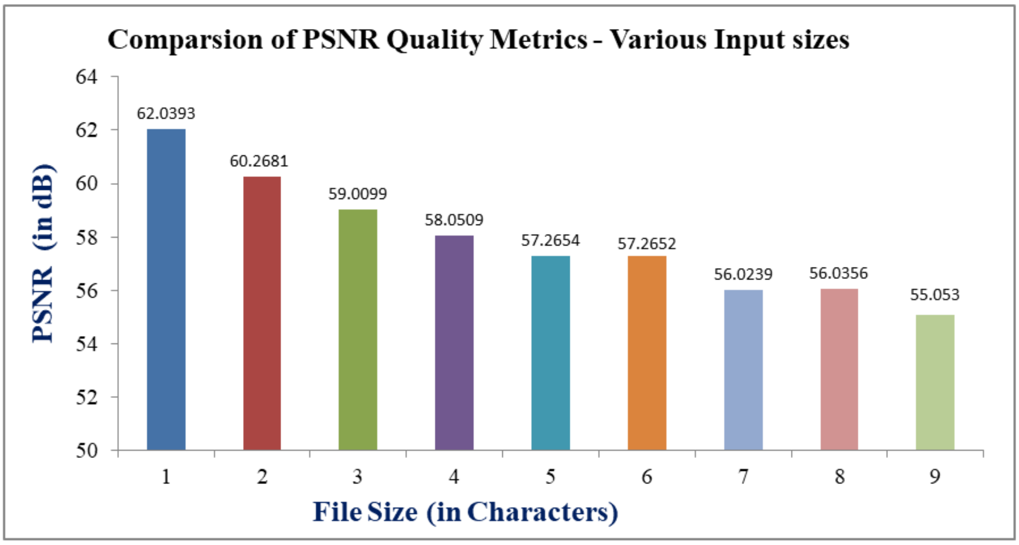
Table 2 Assessment of Quality Parameters of the Proposed Method for various input size

Image Name = camera.jpg, Image Size = 512 x 512, Maximum Embedding Capacity = 786432 bits, Random Generated Key = 65321										
S. No.	**File Size (in characters)**	**Max. Embedding Capacity (in bits)**	**MSE**	**RMSE**	**PSNR (in dB)**	**SSIM**	**AE**	**NCC**	**IF**	**SC**
1	4004	64104	0.0407	0.2016	62.0393	0.9913	0.0407	1	1	1
2	6006	96136	0.0611	0.2472	60.2681	0.9878	0.0611	1	1	1
3	8008	128168	0.0817	0.2858	59.0099	0.9813	0.0817	1	1	1
4	10010	160200	0.1019	0.3192	58.0509	0.9801	0.1019	1	1	1
5	12012	192232	0.1220	0.3494	57.2654	0.9778	0.1220	1	1	1
6	12013	192248	0.1221	0.3494	57.2652	0.9771	0.1221	1	1	1
7	16016	256296	0.1624	0.4030	56.0239	0.9765	0.1624	1	1	1
8	16017	256312	0.1620	0.4025	56.0356	0.9769	0.1620	1	1	1
9	20020	320360	0.2031	0.4507	55.0530	0.9701	0.2031	1	1	1



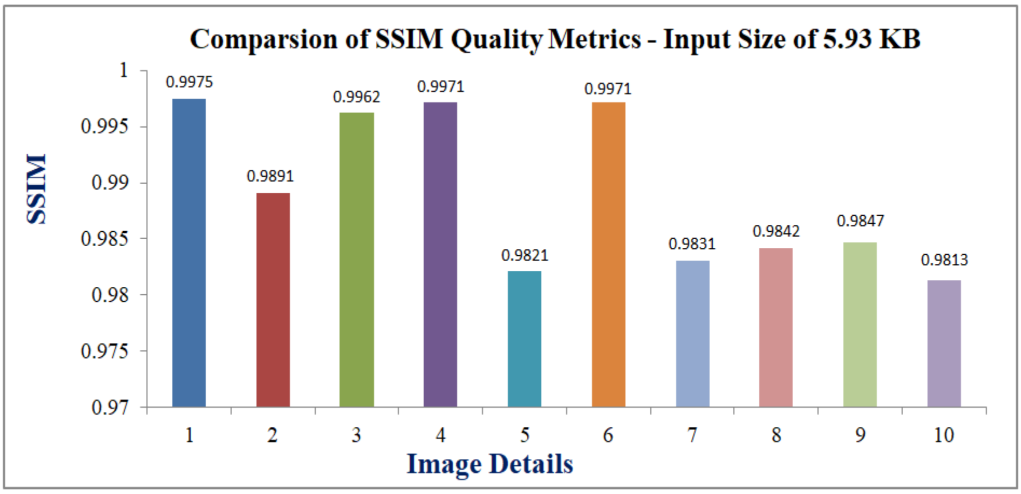
S.No.	Image Name
1	obito.jpg
2	mikey.jpg
3	ben.jpg
4	eren.png
5	pepper.jpg
6	parrot.jpg
7	cat.jpg
8	camera.jpg
9	babbon.jpg
10	pirate.jpg

Figure No. 2 (a) Comparison of PSNR metrics for different images for fixed input Size



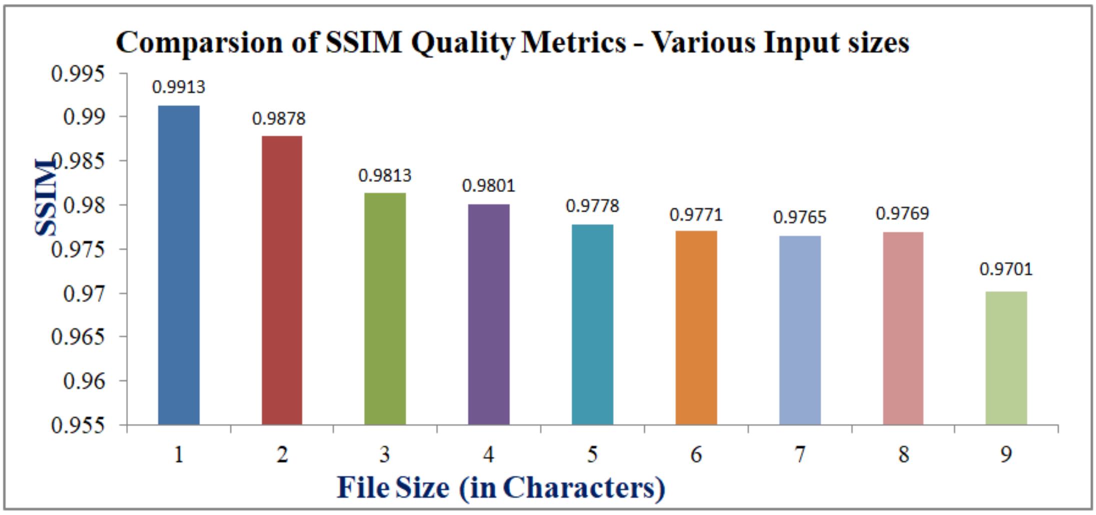
S.No.	File Size
1	4004
2	6006
3	8008
4	10010
5	12012
6	12013
7	16016
8	16017
9	20020

Figure No. 2 (b) Comparison of PSNR metrics for various 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

Figure No. 2 (c) Comparison of SSIM metrics for different images for fixed input Size



S.No.	File Size
1	4004
2	6006
3	8008
4	10010
5	12012
6	12013
7	16016
8	16017
9	20020

Figure No. 2 (d) Comparison of SSIM metrics for various input Size

5. CONCLUSION

Our research concludes by highlighting the importance of image steganography in guaranteeing data security while being transmitted over networks. This technique effectively protects sensitive data by encrypting messages with symmetric encryption algorithms and embedding them using LSB. Our analysis shows promising results in terms of image fidelity and similarity between cover and stego images, based on multiple quality metrics including MSE, RMSE, PSNR, SSIM, AE, NCC, and SC. The results of our experiments are consistently positive, even with different file embedding sizes and image choices. Future work might examine ways to improve on currently used algorithms and expand the use of steganography by implementing additional methods.

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. Alt?n???k. "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.