Enhancing the Secrecy of the Confidential Message Through Pxi – Lsb Model

Karthikeyan N[1] Joel Franklin J[2] Puvaneshwaran V[3] Jeganeeshwaran S[4] Guhan R [5]

[1]Assistant Professor, Department of CSE, Government College of Engineering, Sengipatti, Thanjavur, Tamilnadu
[2,3,4,5] Third Year CSE, Department of CSE, Government College of Engineering, Sengipatti, Thanjavur, Tamilnadu

Corresponding Author: nkarthikeyan@gcetj.edu.in

ABSTRACT

Communication on the internet involves the global exchange of information, messages, and multimedia content through various online platforms. Ensuring secure communication is paramount, guaranteeing confidentiality, integrity, authenticity, and availability of data. Numerous models have been proposed to safeguard confidential messages, utilizing cryptographic and image steganography techniques. In this study, a novel model is introduced, leveraging image steganography methodologies, particularly the Least Significant Bit (LSB) embedding technique augmented with the Pixel Value Indicator (PXI) method. Initially, PXI identifies the most dominant pixel in the cover image, and secret bits are then embedded into different color components, excluding the dominant color channel indicated by PXI. Through comparative analysis with existing models, our proposed approach enhances security without compromising the quality of the cover image, offering robust protection against unauthorized access and interception.

Keywords: Image Steganography, Least Significant Bit (LSB), Pixel Value Indicator (PXI), Security

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.

However, the true strength of digital security lies in the fusion of cryptography and steganography, leveraging the strengths of both disciplines to create synergistic defence mechanisms[1-4]. Through the integration of encryption with covert communication channels, practitioners can bolster their defences against a wide array of cyber threats, ranging from brute-force attacks to sophisticated surveillance tactics. By offering insightful analyses and case studies, this journal advocates for the amalgamation of cryptographic and steganographic techniques, showcasing their collective efficacy in fortifying the security posture of digital communication infrastructures.

As the digital landscape continues to evolve, the importance of secure communication becomes increasingly apparent. By examining the interconnectedness of cryptography and steganography, this journal seeks to elucidate how their convergence can enhance the resilience of digital communication systems against adversarial exploits[5-9]. Through a comprehensive understanding of these technologies and their practical applications, stakeholders can confidently navigate the complexities of modern cyber security challenges, ensuring the confidentiality, integrity, and availability of sensitive information in an interconnected world.

2. LITERATURE SURVEY

In recent years, there has been a notable exploration into adaptive and reversible steganography schemes, which have garnered considerable attention in contemporary research.

These schemes possess the capability to dynamically adjust embedding strategies based on the content of the image, ensuring a more efficient and tailored approach to hiding information. Moreover, they enable precise data extraction without any loss, addressing the need for accurate retrieval of concealed data while maintaining image quality.

Furthermore, novel approaches in image steganography have emerged, leveraging techniques such as pixel value indicator (PVI) and Least Significant Bit (LSB) embedding. These innovative methods offer enhanced privacy and access control within covert communication channels. PVI techniques, for instance, allow for the identification of specific pixels in an image to embed data, thereby providing a more targeted and secure means of concealing information. Similarly, LSB embedding remains a prevalent method due to its simplicity and effectiveness, enabling the embedding of data in the least significant bit of pixel values without significantly altering the visual appearance of the image.

By incorporating these advanced steganographic techniques into contemporary research, scholars aim to elevate the security and efficiency of covert communication channels. These efforts contribute to the ongoing evolution of steganography, paving the way for more robust and versatile solutions that meet the demands of modern digital communication while safeguarding privacy and ensuring data integrity.

3. PROPOSED MODEL

The proposed model offers a dual-layered security approach for safeguarding secret messages, employing both the pixel indicator technique and the LSB Technique. Initially, the model utilizes the pixel indicator technique to determine the dominant color channel within the cover image by analyzing the frequency count and comparing pixel intensities across various color components. Subsequently, the secret message bits are embedded into the cover image using the LSB Technique, with the exception of the dominant color channel in each pixel. This ensures that the visual integrity of the dominant intensity remains unchanged, making it challenging for intruders to anticipate alterations in the other two components within the same pixel. The resulting updated cover image, referred to as the stego image, can then be securely stored in local storage, cloud storage, or transmitted to the intended recipient.

Upon accessing the stego image either from storage or received from the sender, the authorized recipient proceeds to extract the confidential message embedded within it. The extraction process begins by isolating the dominant color channel present in the cover image within the stego. Subsequently, utilizing the LSB technique, the recipient extracts the confidential messages from the stego image's remaining two color channels, excluding the dominant one. This dual-layered security approach enhances protection against a multitude of attacks, ensuring the confidentiality of the messages without sacrificing the imperceptibility of the cover image. Moreover, this methodology facilitates an increased embedding capacity, further enhancing the security measures in place.

4. RESULTS AND DISCUSSION

The proposed model has been realized utilizing Python 3.10 on the Windows 10 operating system. Extensive testing of the model has been conducted using a diverse range of standard and non-standard images, encompassing different formats and dimensions. The performance evaluation of the proposed model has been carried out through the analysis of various parameters, including imperceptibility, embedding capacity, and security, to ensure its efficacy across different scenarios and image characteristics.

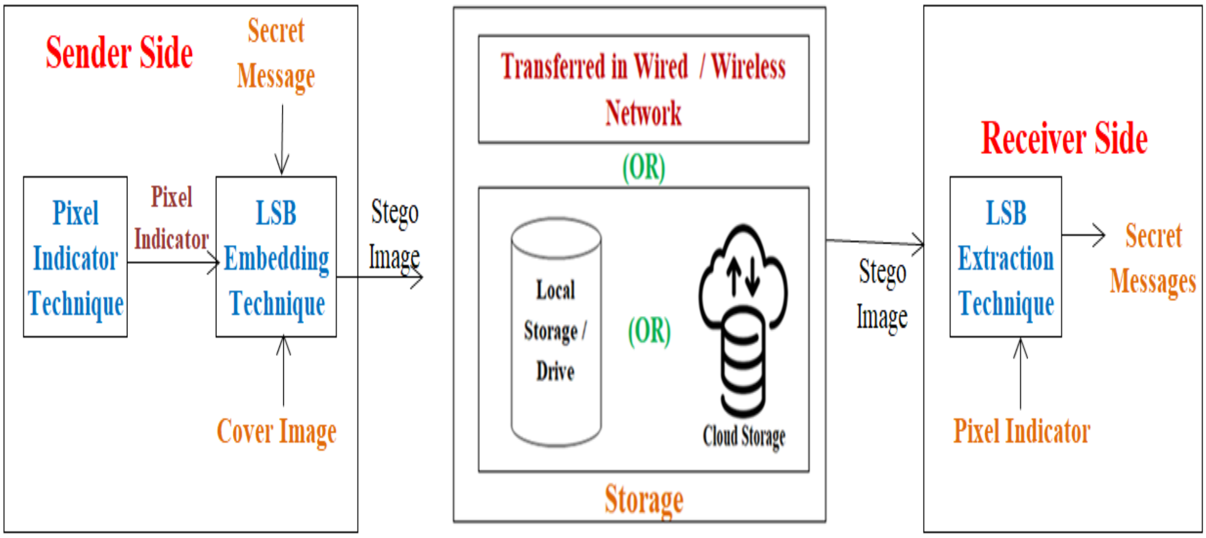

Fig. No. 1Architecture of the proposed Model

Table 1. Analysis of various quality metrics of the proposed Model with fixed input size with execution time

Length of the file = 26838 Characters, Number of Bits Embedded = 214704									
Image Name	Image Dimension	Pixel Indicator	MSE	RMSE	PSNR	SSIM	SC	Embedding Time (in ms)	Extraction Time (in ms)
Nature.jpg	592 x 1024	Red	0.0590	0.2430	60.4192	1.0	0.9999	1.1381	0.7360
pepper.jpg	512 x 512	Red	0.1362	0.3691	56.7891	1.0	0.9999	1.1222	0.7360
parrot.jpg	853 x 1280	Red	0.0329	0.1814	62.9596	1.0	1.0000	1.1720	0.6882
pirate.jpg	512 x 512	Red	0.1366	0.3696	56.3582	1.0	0.9998	1.1101	0.7197
babbon.jpeg	512 x 512	Blue	0.1361	0.3690	56.7908	1.0	0.9999	1.1423	0.7674
camera.jpg	512 x 512	Red	0.1369	0.3700	56.7679	1.0	0.9999	1.1745	0.6896
russel.jpeg	512 x 512	Red	0.1376	0.3709	56.7449	1.0	0.9999	1.1103	0.7039
sun.jpeg	462 x 616	Red	0.1259	0.3549	57.1296	1.0	0.9998	1.1168	0.7694
sun1.jpeg	1092 x 1092	Red	0.0306	0.1750	63.2710	1.0	1.0000	1.1999	0.7225
cat.jpg	512 x 512	Red	0.1366	0.3696	56.6725	1.0	0.9999	1.1281	0.7527

Table 1. Analysis of various quality metrics of the proposed Model with different input size with execution time

Image Name= baboon.jpeg, Dimension = 512 x 512, Pixel Indicator= Blue								
Message Size	Number of bits embedded	MSE	RMSE	PSNR	SSIM	SC	Embedding Time (in ms)	Extraction Time (in ms)
61	488	0.0003	0.017	83.8036	1	1	0.0156	0.0131
131	1048	0.0006	0.025	80.2479	1	1	0.0166	0.0157
2966	23728	0.0151	0.123	66.3393	1	1	0.0937	0.0625
5767	46136	0.0293	0.171	63.4592	1	1	0.1875	0.125
23422	187376	0.1189	0.345	57.3795	1	1	0.7349	0.5162
14207	113656	0.0721	0.269	59.5523	1	1	0.4548	0.3132
48241	385928	0.245	0.495	54.2384	1	1	1.5476	1.0317
36708	293664	0.1865	0.432	55.4231	1	1	1.6468	1.1748
26838	214704	0.1361	0.369	56.7908	1	1	1.1423	0.7674

4.1 Assessment of Quality

During the analysis of results, the image quality is assessed against specific standards to validate its accuracy. Comparison of properties between the quality of the stego image and the original image is facilitated through various metrics such as 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). These metrics serve a pivotal role in evaluating the quality of the stego image, offering valuable insights into the effectiveness of the results obtained.

The results from both table 1 and table 2 demonstrate that our proposed method exhibits low Mean Square Error (MSE) and Root Mean Squared Error (RMSE), suggesting high quality of the cover image. This indicates that intruders would face difficulty in discerning hidden details within the stego image through visual analysis. Additionally, the average Peak Signal to Noise Ratio (PSNR) value ranges between 63.31 to 63.43 across different image dimensions and formats for the same message size, further affirming the effectiveness of our approach in maintaining image quality.

4.2 Assessment of Security

4.2.1 Visual Analysis

A visual assessment was conducted by comparing the quality of the original cover image to that of the stego image, allowing for the detection of concealed messages within the latter. The model achieved an average PSNR of approximately 58.39dB while embedding messages sized at 26.31KB, equivalent to 2,14,704 bits. With the average PSNR exceeding the minimum perceptible threshold of 30dB, the human visual system cannot discern hidden messages within the stego image. Furthermore, the utilization of the LSB technique ensures minimal deviation in intensities, within a range of ±1, thereby impeding intruders' ability to detect alterations in cover image intensities.

4.2.2 Histogram Analysis

Unauthorized individuals often rely on discrepancies in pixel intensities across the red, green, and blue channels of both the original cover image and the stego image to uncover concealed messages. Figure 2 provides a histogram representation of the baboon image's red, blue, and green channels, illustrating a 2D graph where the X-axis represents pixel location and the Y-axis denotes the intensity of the corresponding color channel. By leveraging the LSB technique, alterations in intensity across various color channels in the cover image are minimized, thus hindering intruders' efforts to discern changes in the stego image through histogram analysis.

Image Name= parrot.jpeg, Dimension = 512 x 512, Pixel Indicator= Blue

Before Embedding **After Embedding**

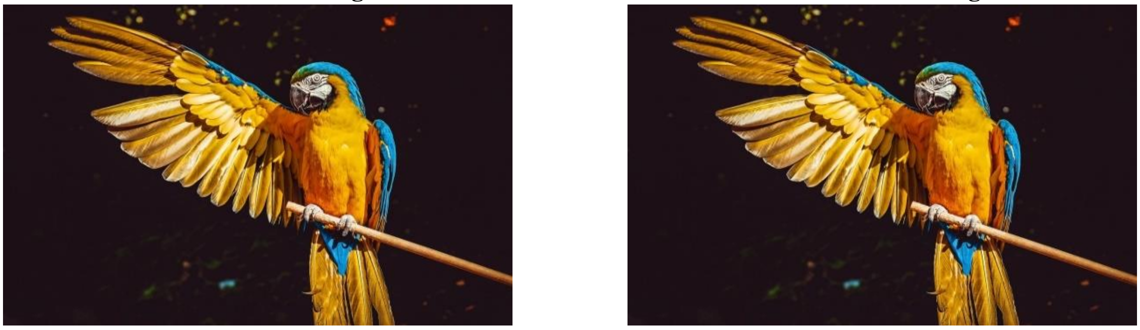

Fig. No. 2.1 (a) Sample Cover image and Stego Image

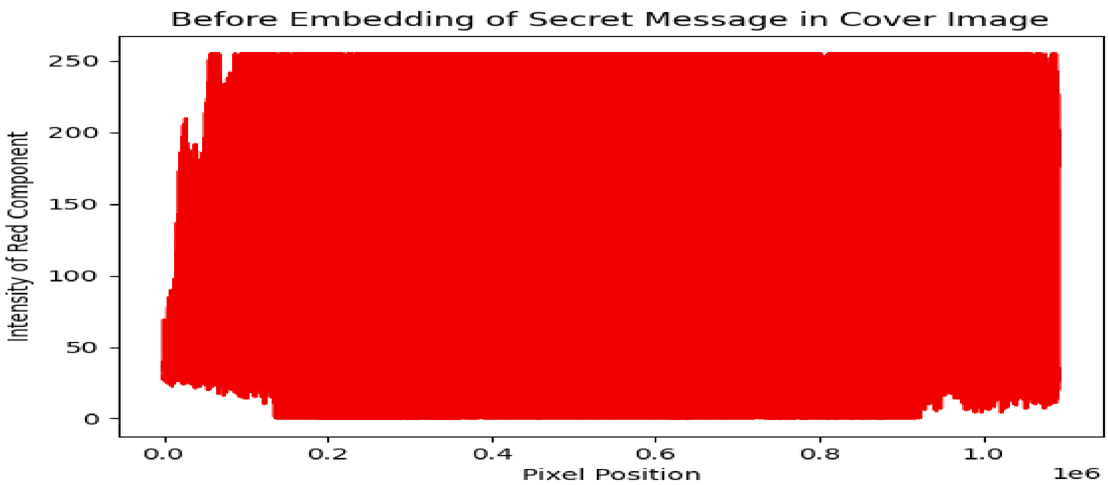

Fig. No. 2.1 (b) Intensity of Red component of the cover image (Before Embedding)

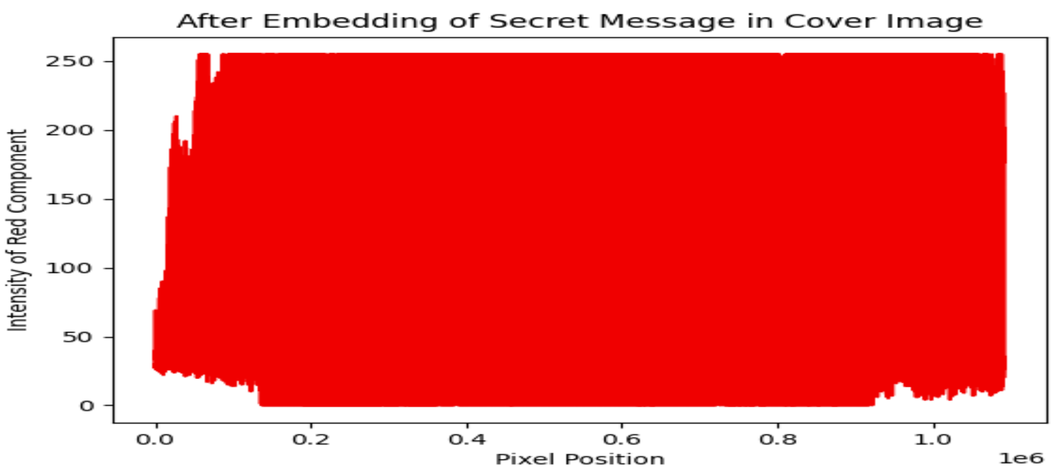

Fig. No. 2.1 (c) Intensity of Red component of the Stego image (After Embedding)

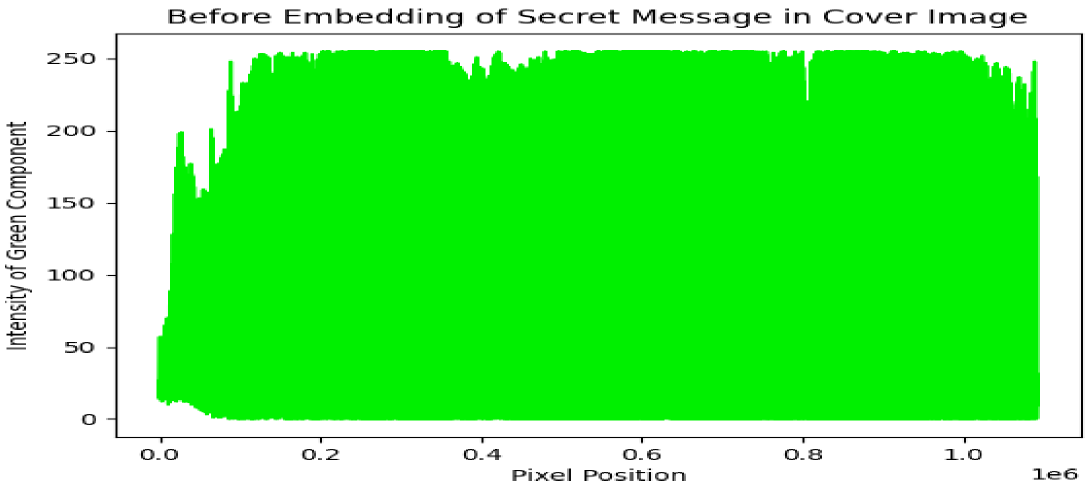

Fig. No. 2.1 (d) Intensity of Green component of the cover image (Before Embedding)

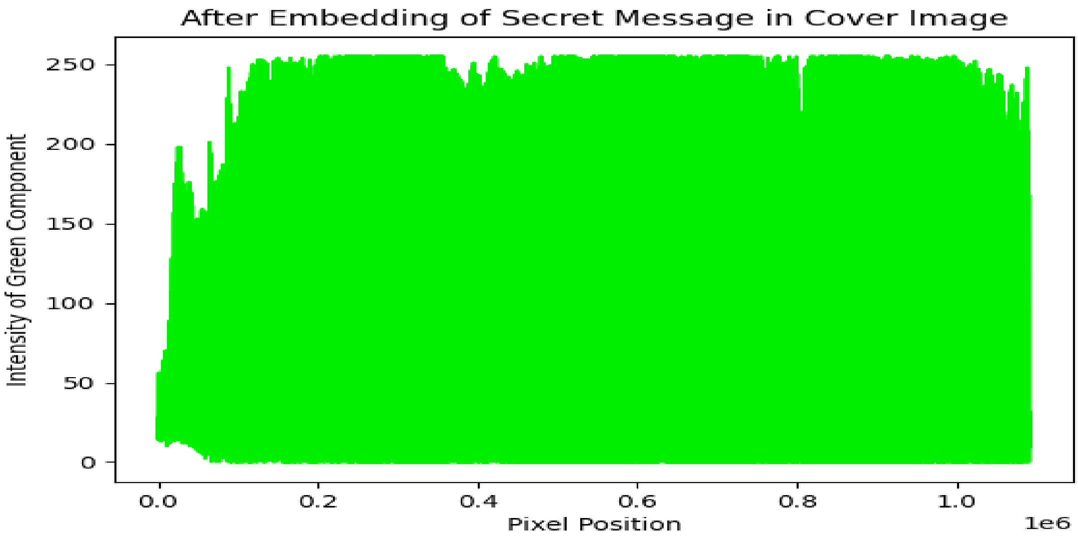

Fig. No. 2.1 (e) Intensity of Green component of the Stego image (After Embedding)

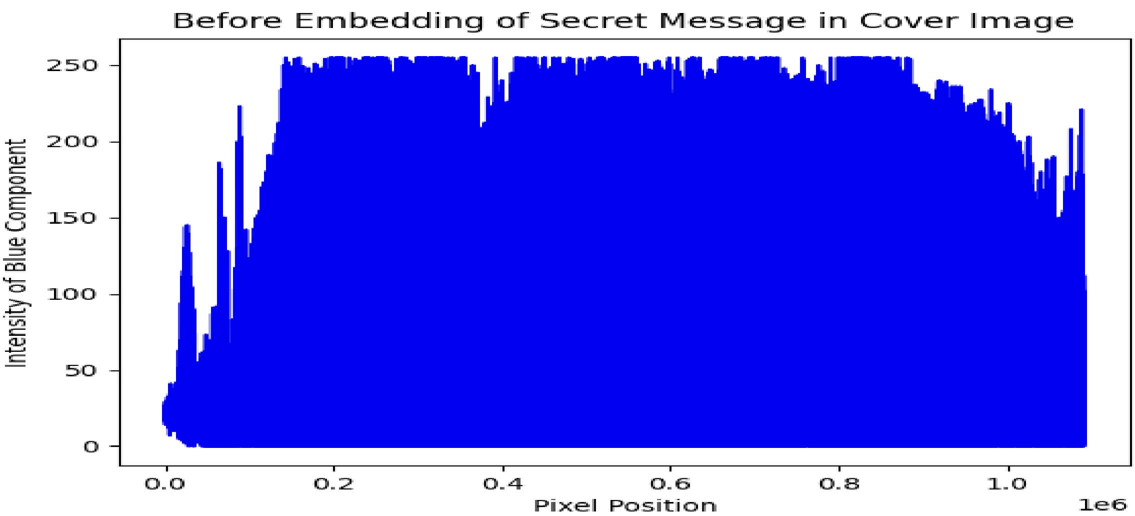

Fig. No. 2.1 (f) Intensity of Blue component of the cover image (Before Embedding)

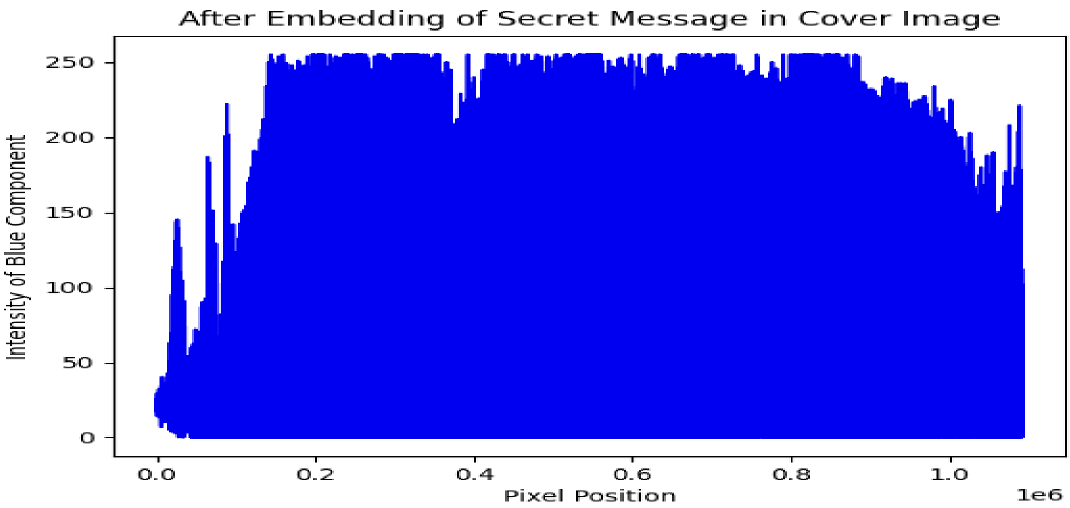

Fig. No. 2.1 (g) Intensity of Blue component of the Stego image (After Embedding)

CONCLUSION

The innovative approach presented in the proposed model provides a dual layer of security for transmitting confidential messages in digital communication, integrating image steganography techniques. Notably, this model ensures maintained image quality despite increased embedding capacity, while simultaneously offering heightened security against diverse residual attacks compared to single-layer security measures. Even in scenarios where intruders may anticipate the LSB technique for extraction, the dual layer of protection affords superior defense compared to a single layer. Looking forward, potential enhancements may involve integrating cryptographic techniques to further elevate the level of protection provided by the model. This forward-looking perspective emphasizes the model's adaptability and potential for continued advancement in safeguarding digital communications.

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.