ISSN 2349-0292
Impact Factor 3.802

GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

SECURITY BY AN IMPROVED MULTI LEVEL IMAGE STEGANOGRAPHY

Kalpana Vijay Mane[1], Arpit Solanki[2]
[1]Student, Dr. A.P.J. Abdul Kalam University, Indore, M.P., India
[2]Assistant Professor, Dr. A.P.J. Abdul Kalam University, Indore, M.P., India

ABSTRACT

Image security is becoming increasingly important among humans as it is shared on various internet social media platforms, and the authenticity of images is one of the primary tasks for which creators have put in significant effort to create or capture, especially if there are copyright laws involved. As a result, distributed and shared photos must be validated with additional information that will never compromise image quality and is difficult to guess or hack. Several techniques were used to improve security levels in image steganography, and multi-level security was also achieved. In the same spirit, this work is also attempting to develop a novel method of integrating information with images that have multiple security levels. The proposed methodology was evaluated on three different photos, with each image treated with a varied text length. The stego images were examined using mean square error (MSE) and peak signal to noise ratio (PSNR) to compare to earlier methods and demonstrate their performance. In this paper, presents a highly secure image steganography technique with multiple levels of encryption.

KEYWORDS: Steganography, encryption, multi-level security, image forensics.

1. INTRODUCTION

In this information age, people transfer information directly using the available communication technologies such as a local area network (LAN), a wide area network (WAN) or the Internet. This information can be very important and strong data security techniques is required for secure transmission of important and confidential data. Therefore, the current channels of communication technology cannot be the exclusive means of conveying reasonable information. Then, we require a strong technique to protect important and confidential data from unauthorized persons.

Steganography is the specialty of disguising sensible data into digital media (i.e., images, sound, and text). It is an instrument that totally contrasts from cryptography. Truth be told, in cryptography the data is altered yet at the same time can be found in this muddled configuration once sent over the systems, while in steganography the data is essentially implanted into a digital support and can't be seen as long as the nature of the carrier is not crumbled [5].

The steganography procedure has been utilized numerous years prior to pass on secret messages. For example, a king in old Greece used to shave the slave's head and inked some secret data on it. At the point when the hair was developed, the slave was sent to disperse the message. The beneficiary then shaved the hair and gets the secret message [6]. In present day life, steganography is utilized for some reasons, for example, implanting copyright [6], installing individual's detail in brilliant IDs and embedding understanding point of interest in medicinal imaging framework. There has been a fast development of enthusiasm on steganography especially with astute service organizations. For example, the US Pentagon has as of late distributed huge assets to lead look into here, as they trust that fear-based oppressors may utilize this philosophy to trade data [6].

Steganography hides data into a digital media called cover object which can be a video clasp, a digital image, a sound document or basically a text. This digital media is called separately a cover image, a cover sound, a cover video, and a cover text. Once the data is implanted in that cover it is known as a stego-protest. On the off chance that the cover is an image or a sound document, then the consequence of installing the data in the cover is referred to as stego-image or stego-sound separately.

One of the most widely recognized reasons that intruders can have the capacity to increase unauthorized access of data and they can utilize this data for their own particular reason, to mischief somebody, change and attack. As the advancements are constantly becoming because of potential outcomes of data to be hacked or unapproved are likewise developing and in current time communication require unique sort of security from interlopers. It's not just restricted up to data or communication, it likewise applies on PC arrange in light of the fact that web is just

ISSN 2349-0292
Impact Factor 3.802

the medium to trade the message. Thus, giving greater security to PC system is more vital in light of the fact that a large portion of the data is exchanged over the web. The primary motivation to give is to keep up the privacy, honesty, accessibility and furthermore to stop the unapproved utilization of data. This must be halted either concealing presence of the data or keeping the data secret. Most normal approaches to stop this are steganography and cryptography. Both are correlative to each other and give better security, secrecy and validness. Image steganography is turning into an essential territory in the field of steganography. As the request of security and protection builds, need of concealing their secret data is going on. On the off chance that a client needs to send their secret data to different people with security and protection he can send it by utilizing image steganography.

2. RELATED STUDY

G. S. Charan, Nithin Kumar S S V, Karthikeyan B, Vaithiyanathan V, and Divya Lakshmi K. [1] Steganography is the practice of concealing the presence of secret data by placing it in a cover, preventing unauthorised access to protected material. This research paper presents a revolutionary method for scrambling plain text into cypher text and embedding it into a colour image. Encryption is done in two stages: first, it is scrambled using the Ceaser cypher process, and then it is encoded using the turbulence hypothesis. The ciphertext obtained after encryption is inserted using the 3, 3, 2 LSB substitution

M. Nayana, B. Karthikeyan, S. Sruti, and M. Gomathymeenakshi [2] To be used as part of a channel medium, information transmission needs to be sufficiently secure to prevent errors and information alteration. Condensed information transmission contributes to the maintenance of the components of secure interaction. In essence, minimisation is achieved through information pressure, which reduces the data's storage space or transmission limit. The most reliable technique for data compression in this study is arithmetic coding. Steganography is used to conceal the packed data within the image, creating a secure medium. In order to increase the mystery of the data, this work provides a stage in between steganography and information pressure.

J. M. Guo and T. N. Le [3] show that the quality calculate of a JPEG image can be an embedding space, and we discuss the ability to install a message to a JPEG image by monitoring JPEG quantisation tables (QTs). Up until now, cryptography has consistently played a decisive role in maintaining the mystery between the sender and the intended recipient. However, steganography techniques are increasingly being used in addition to cryptography to add a more defensive layer to the hidden information.

Qingyun Shi and Pengwei Hao, [4] The foundation of transformation-based lossless source coding is reversible integer mapping. For reversible whole number mapping of invertible straight changes, a generic matrix factorisation hypothesis is generated. Two forms of ERM—triangular ERM (TERM) and single-column ERM (SERM)—are examined, together with concepts of the whole number element and the basic reversible network (ERM) for whole number mapping. Show that if the change is invertible and occurs in a finite dimensional space, there are methods for factorising a lattice into TERMs or SERMs.
J. Fridrich and M. Long,[5] Observe the security of least significant bit (LSB) insertion for hiding communications in high-color-profundity digital photos. Describe a rigorous steganalytic process that enables us to reliably determine the proximity of a pseudorandom binary message that is randomly distributed throughout a colour image.

3. PROBLEM STATEMENT AND PROPOSED METHODOLOGY

In modern era, unauthorized access of information increases day by day due to this we need to secure information and this can be done using cryptography or steganography technique. There are many steganography and cryptography algorithms, including Least Significant Bit (LSB), Random Scattered (RS), and Most Significant Bit (MSB), have already been created. However, LSB is the most commonly used algorithm because it merely inserts the secret message bit with the least significant bit of the image. LSB is very simple due to this detection of secret message is also easy, so we need to develop an improved version of LSB algorithms which is more secure than LSB.

The proposed method employs multilevel image steganography. Level one involves embedding the secret message (text) into a cover image (cover one), which is a colored image (RGB image), using Least Significant Bit (LSB) image steganography. Level one produces a stego image known as an intermediate image, which is then converted into binary text and used as input in level two.

ISSN 2349-0292
Impact Factor 3.802

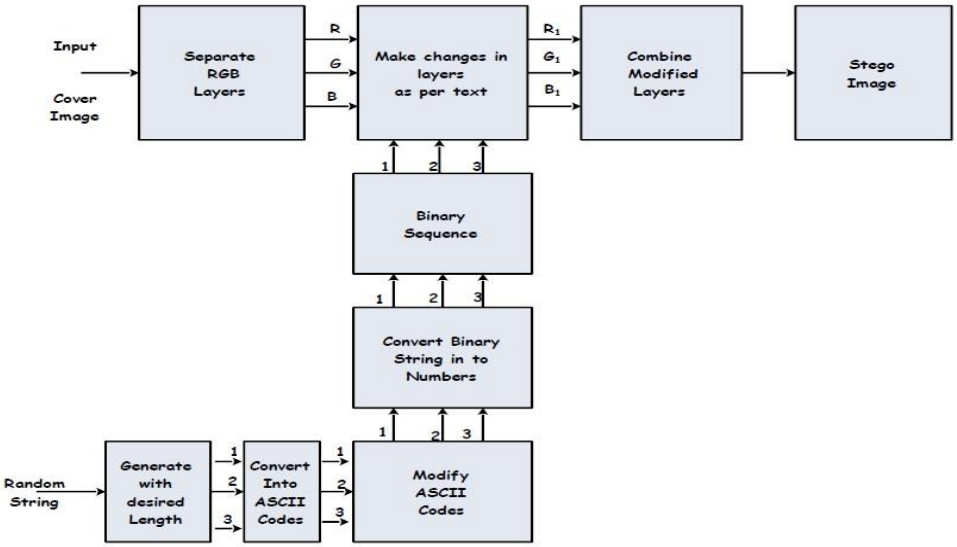

Figure: 1 Proposed System Model

4. RESULTS ANALYSIS

In this section, performance of proposed system evaluated. Additionally, a performance comparison has also been presented.

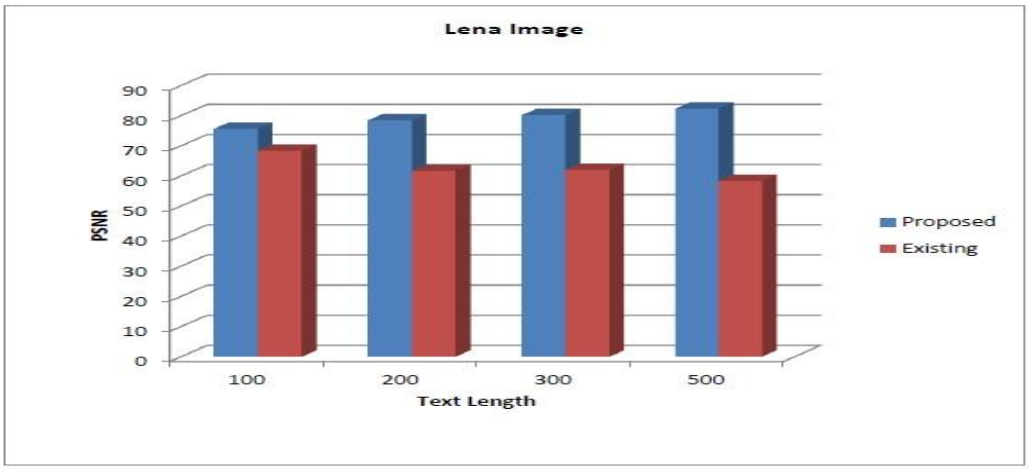

Figure 2 Comparison PSNR of Lena Image with Different Texts Lengths

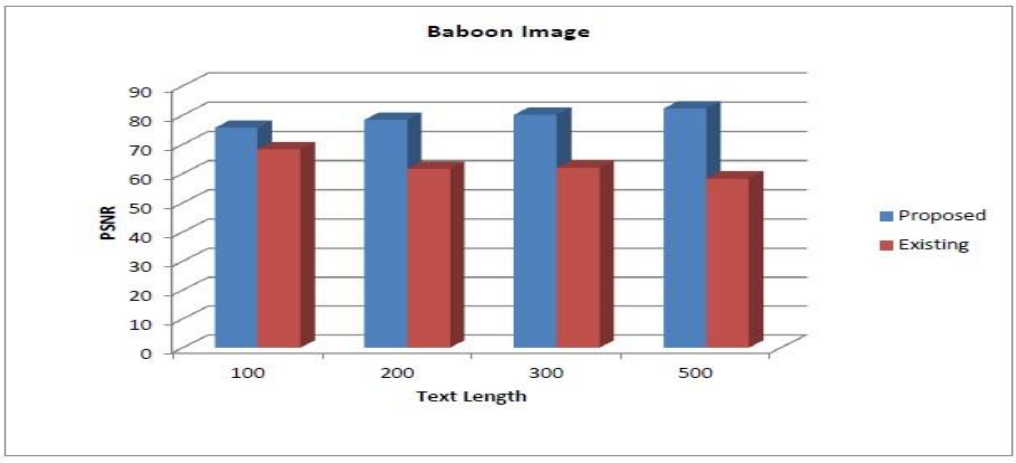

Figure 3 Comparison PSNR of Baboon Image with Different Texts Lengths

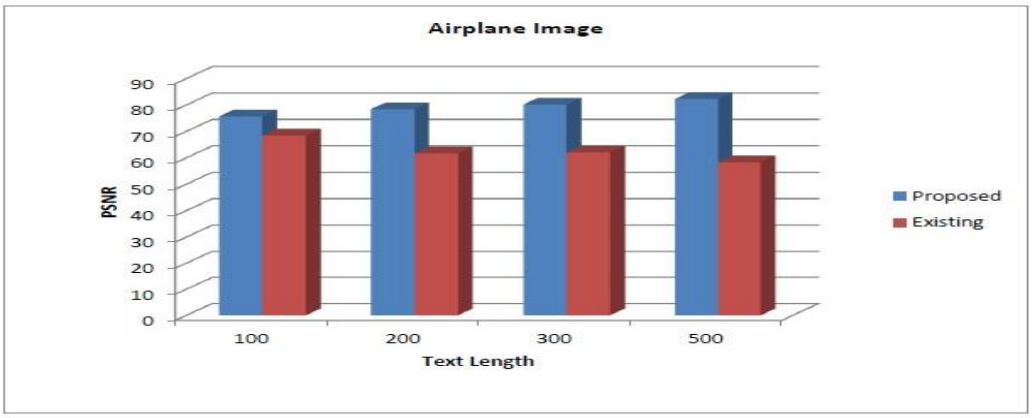

Figure 4 Comparison PSNR of Airplane Image with Different Texts Lengths

5. CONCLUSION

This research work presents a highly secure image steganography technique with multiple levels of encryption. The stego images have been evaluated with mean square error (MSE) and peak signal to noise ratio (PSNR) to compare with previous algorithms and show their performance. The proposed algorithm has added security and improved.

REFERENCES

[1] G. S. Charan, Nithin Kumar S S V, Karthikeyan B, Vaithiyanathan V and Divya Lakshmi K, "A novel LSB based image steganography with multi-level encryption," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-5.

[2] Gomathymeenakshi,M., Sruthi, S .,Karthikeyan,B .,N ayana,M. ”An efficient arithmetic coding data compression with steganography”, in 2013 IEEE International.

[3] Guo,J,-M.,Le,T,-N, “Secret Communication Using JPEG Double Compression”, IEEE Signal Processing Letters, 17(10),5556462,pp.879-882.

[4] Hao,P.,Shi,Q. “Matrix factorizations for reversible integer mapping”, IEEE Transactions on Signal Processing. 49 (I0),pp. 2314-2324.

[5] J. Fridrich and M. Long, "Steganalysis of LSB encoding in color images," 2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No.00TH8532), New York, NY, 2000, pp. 1279-1282 vol.3.

[6] Singla,D., Juneja,M. ”New information hiding technique using Features of image”, Journal of Emerging Technology in Web Intelligence, 6(2),pp.237-242.

[7] Delahaye, J. P. ; “Embeddeed Information, Information Hiding”, Scientific American, pp.142-46, 1996..

[8] Conference on Emerging Trends in Computing and Nanotechnology,ICE-CCN 2013 6528520,pp. 342-345.

[9] Lin, Y.-K. “A data hiding scheme based upon DCT coefficient modification”, Computer Standards and Interfaces 36(5),pp.855- 862.

[10] Hu,Y.,Wang,K.,Z.-M.” An improved VLC-based lossless data hiding scheme for JPEG images” Journals of Systems and Software 86 (8),pp.2166- 2173.

[11] Rasber Dh Rashid and Taban F Majeed. Edge based image steganography: Problems and solution. In 2019 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), pages 1–5 .IEEE, 2019.

[12] Anqi Qiu, Xianyi Chen, Xingming Sun, Shuai Wang, and Wei Guo.Coverless image steganography method based on feature selection. Journal of Information Hiding and Privacy Protection, 1(2):49, 2019.