e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

STEGANOGRAPHY USING LSB TECHNIQUE: IMPLEMENTATION, ANALYSIS, AND FUTURE PERSPECTIVES

Chirag Sanghvi*1, Siddhant Sarve*2, Sulabh Jha*3

*1,2,3B.Tech 4th Year, Dept, Of Computer Engineering, DYPSOEA, Pune, Maharashtra, India.

DOI : https://www.doi.org/10.56726/IRJMETS39744

ABSTRACT

Steganography, the usage of codes, is cryptography's sin- ister relative. Steganography is meant to provide secrecy while cryptography offers privacy. Steganography is a secret communication technique. Steganography is the practise of concealing a message in a suitable carrier, such as an image or an audio file. The carrier can then be delivered to a recipient without letting on to its secret message. In this page, we've attempted to clarify the many methods for im- plementing steganography utilising "multimedia" files (text, still images, and audio). Steganalysis is a freshly developed area of data processing that aims to recognise steganographic coverings and, if possible, extract messages from them. It resembles cryptanalysis in the field of cryptography. The method is an age-old rising monster that has come to ev- eryone's attention due to its recent intrusion into the field of digital communication security. The goal is to conceal the message's existence in addition to preventing it from being read. Keywords: Steganography, least significant bit, Multimedia steganography, Steganalysis.

I. INTRODUCTION

A steganography is the practice of hiding information or a file within a digital photograph, video, or audio file. It will not be obvious to a person observing the object that the information is hidden inside if he or she views it. This will prevent the person from decrypting the information. A steganography can be divided into text steganography, image steganography, audio steganography, and video steganog- raphy. Steganography is one of the most common ways to conceal information in cover images. Cover files are embed- ded with information using the LSB algorithm, which is a very efficient algorithm. In this project, we present detailed information about LSB-based image steganography and the applications to different file formats.

Different methods that render the modifications imper- ceptible to the human eye have been devised to conceal messages in photographs. They may statistically provide photos that are equivalent to unaltered images while not hav- ing been thoroughly reviewed. In this project, we examine a few distinct image-based steganography approaches and demonstrate that a viewer can tell the difference between Work supported by photos that include a concealed message and images that do not. In terms of the quantity of hidden bits, we construct a closed form expression for the chance of detection and false alarm. This brings up the idea of steganographic ca- pacity, or, more specifically, the question of how many bits we can conceal in a message without changing it statistically significantly.

II. METHODS AND MATERIAL

The methodologies are essentially divided into three types after a review of all the ones that are currently used: traditional image steganography methods, image-to-image steganography methods, and audio steganography methods. The LSB approach is the foundation of conventional meth- ods. Data collecting: To perform steganography using the LSB technique, the data collection phase entails gathering the necessary materials and tools. A computer system with the necessary software, digital images or audio files that can be used as cover objects, and a text message or other image to serve as the secret data to be implanted are the materials needed for this project.

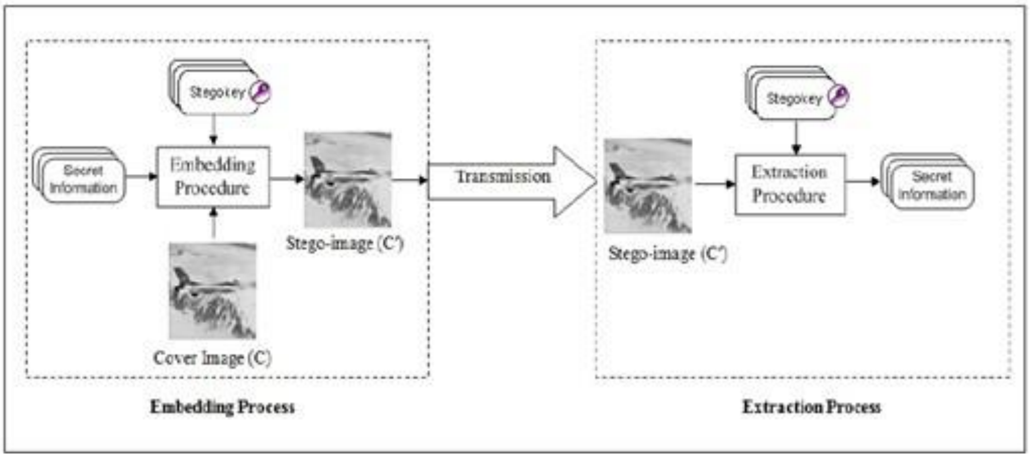

Figure 1: The underlying principle of how steganography and steganalysis operate. Using the cover picture and the secret information, the embedding algorithm builds the stego image, and the extraction method extracts the secret from the stego image.

Algorithms for LSB-Based Steganography LSB-based steganography can be implemented using a variety of algorithms. The selection of an algorithm is based on the partic- ular needs of the application. Some common algorithms are:

a) LSB Replacement: This algorithm substitutes the secret message bits for the LSB of selected cover object pixels.

b) LSB Matching: Using the correlation between neighbouring pixel values and secret message bits, this algorithm alters the LSBs of cover object pixels.

c) LSB Flipping: In order to encode the secret message bits, this technique flips the LSBs of cover object pixels.

Implementation of Steganography method: A appropriate programming language or steganography tool should be used to carry out the LSB-based steganography method selected for the research. The embedding procedure, in which the secret message bits are placed into the LSBs of the cover object pixels, should be handled by the algorithm. The imple- mentation should guarantee data integrity, reduce perceptual distortions, and preserve the cover object’s quality.

Technology Selection: Due to its extensive end-to-end capabilities, suitability for web application development, integration with Python libraries, and effective frontend and backend technology integration, the Django framework was chosen as the basis for the web application performing steganography.

Backend Development: Using the Django framework to implement the web application’s backend A View function that can be used for steganography, message encryp- tion, decryption, and other features was created. Integrated steganography using libraries like "PIL" and "wave" for au- dio data manipulation and image processing and manipu- lation. Integrated AES encryption for additional security using "Cryptodome" libraries, which support asymmetric encryption algorithms.

UI/UX Development: JavaScript was used to create the user interface together with CSS. Components for the encryption page, decryption, and other interactive aspects were designed and implemented.

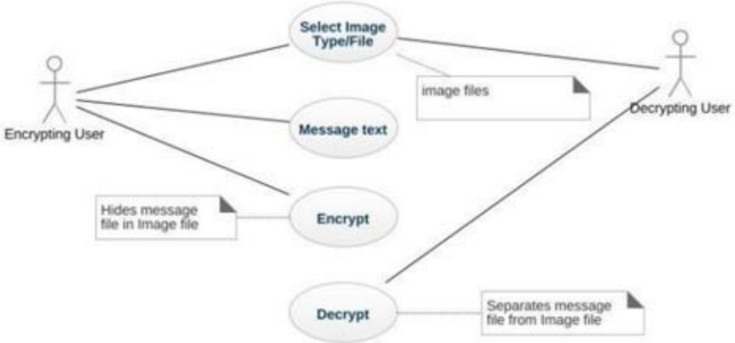

Figure 2: Use case Diagram

III. RESULT

This section presents the findings from the develop- ment and implementation of Steganography, a website built with the Django framework that uses LSB substitution for steganography. The application's efficiency in enabling user- to-user covert communication and hidden media sharing was evaluated based on its performance, usability, and security features.

- Performance Evaluation

Due to the high embedding capacity of the LSB steganography technique, a sizable amount of confiden- tial information could be concealed within the cover media. The number of LSBs modified in the cover me- dia had a direct correlation with the embedding capacity. The embedding capacity increased as the number of modified LSBs increased.

The impact of using the LSB steganography technique on image quality was discovered. The visual quality of the cover media slightly declined as the number of modified LSBs increased.The loss in image quality was negligible and often invisible to the human eye, especially when only a small number of LSBs were altered.

The LSB steganography technique was found to have relatively low computational requirements. The amount of time needed for embedding and extracting the hidden information relied on the size of the cover media and the quantity of modified LSBs. For the ma- jority of real-world applications, the processing time was still acceptable.

- Usability Evaluation

In order to evaluate how intuitive and user-friendly steganographic features are, a thorough usability evalu- ation was done. According to user reviews, the appli- cation's interface seamlessly integrated the steganog- raphy functionalities. Users found it simple to insert and remove hidden media or secret messages into their cover media. Participants praised the application's re- sponsiveness, simplicity, and overall user experience as reasons for their satisfaction.

- Security evaluation

To ensure the confidentiality and integrity of hidden information, the security of steganography techniques was carefully reviewed. Steganalysis techniques were used to evaluate the hidden information's resistance to detection. The analysis showed that the covert nature of the communication was maintained by the fact that the media files and hidden messages remained unde- tectable.

To find potential security holes in the steganographic implementation, vulnerability analyses and penetra- tion testing were carried out. The LSB steganography method exposed its susceptibility to a number of ste- ganalysis techniques and standard image processing operations.

Mechanisms based on the Advanced Encryption Stan- dard were used to protect the message and guarantee the privacy of the steganographic communication.

The evaluation of steganography's effectiveness at en- abling covert communication and secret media shar- ing yielded positive results. During steganographic communication, the application performed effectively while maintaining a seamless user experience. The us- ability evaluation supported the positive user feedback regarding the application's interface's incorporation of steganography features. Additionally, the security anal- ysis demonstrated how well the steganographic tech- niques resisted detection and how precautions were taken to safeguard user identities and the confidential- ity of the concealed data.

IV. DISCUSSION

This research paper's discussion section focuses on inter- preting the LSB steganography technique's findings and of- fering a more thorough analysis of their implications. Along with discussing the technique's benefits, drawbacks, and potential applications, it also discusses future research priorities. With its high embedding capacity, LSB steganography enables the concealment of a sizable amount of confidential information within digital media. This qualifies it for applications that call for the transmission of significant amounts of secret data. Implementing the method only requires a small amount of computational power. It doesn't require major changes to be integrated into already-existing applications or systems. As the concealed information is invisible to the human eye and requires specialised knowledge or algorithms to detect and extract, LSB steganography offers security through obscurity.

LSB steganography, however, is susceptible to steganal- ysis techniques that look for the presence of concealed in- formation. Advanced statistical analysis methods can spot statistical outliers brought on by the embedding procedure, possibly resulting in the discovery and disclosure of the concealed data. The method's resistance to common image processing operations like compression and resizing isn't very strong. The hidden message may be damaged or de- stroyed during these operations, rendering it unrecoverable.

Potential Applications and Future Work:

Numerous potential applications for LSB steganography exist in a variety of fields. It can be used for digital forensics, covert communication, digital watermarking, and intellec- tual property protection.

The goal of future research should be to strengthen LSB steganography's resistance to steganalysis techniques. In- vestigating cutting-edge methods like deep learning, genetic algorithms, or machine learning might improve security and resistance to detection.

Data hiding schemes that use LSB steganography in con- junction with other steganographic techniques tend to be more effective and secure. Future research should look into combining LSB steganography with frequency domain meth- ods (such as discrete cosine transform) or other data hiding techniques (such as spread spectrum) to take advantage of the advantages of various strategies and improve overall performance and security.

New research directions can be explored by examining the applicability and limitations of LSB techniques in cutting- edge technologies like virtual reality, augmented reality, and 3D printing. The applications of LSB steganography could be expanded by creating specialised techniques suitable for these technologies.

Further research is needed to determine how to increase the capacity and robustness of LSB techniques while main- taining acceptable image quality. More effective and secure solutions might be found by investigating complex encoding schemes or by combining LSB with other steganographic techniques.

V. CONCLUSION

LSB-based steganography in particular offers an effective way to conceal sensitive information in digital media, in- cluding photos and audio files. In addition to examining the tools and methods used in LSB steganography, this study also looked at its importance and potential uses.

The enormous embedding capacity of LSB-based steganography enables the concealing of significant amounts of sensitive information. The method can be easily inte- grated into current applications and systems and is com- putationally effective. It offers security through obscurity because the concealed information is concealed from view. LSB steganography does have some restrictions, though.

It is vulnerable to steganalysis methods, which check for the presence of hidden data. The technique might potentially be susceptible to picture processing processes that could harm the hidden message, like compression and resizing. LSB steganography has uses in a variety of disciplines despite these shortcomings. It can be applied to covert com- munication for encrypted messaging, digital watermarking for copyright protection, and intellectual property protection in digital forensics to conceal evidence. Future research should concentrate on creating sophisti- cated approaches that can withstand steganalysis methods in order to increase the security and resilience of LSB steganog- raphy. Exploring how LSB steganography can be combined with other approaches, like spread spectrum or frequency domain methods, may result in more efficient and secure data hiding systems. The use of LSB techniques in cutting-edge technologies like virtual reality, augmented reality, and 3D printing also calls for more research. By applying LSB steganography to these fields, new opportunities for safe information conceal- ing might be created. Finally, LSB steganography is a useful method for secret communication and protecting sensitive data. The potential for LSB steganography to advance the realm of digital com- munication can be realised by overcoming its drawbacks and looking into new research avenues.

VI. REFERENCES

[1] Y. P. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto and C. A. Sari, "Simple and secure image steganography using LSB and triple XOR operation on MSB," 2018 International Conference on Information and Communications Technology (ICOIACT), 2018, pp. 191-195, doi: 10.1109/ICOIACT.2018.8350661.

[2] A. Bose, A. Kumar, M. K. Hota and S. Sherki, "Steganography Method Using Effective Combination of RSA Cryptography and Data Compression," 2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), 2022, pp. 1-5,

doi: 10.1109/ICEE-ICT53079.2022.976840

[3] H. -t. Wu and J. Huang, "Secure JPEG steganography by LSB+ matching and multiband embedding," 2011 18th IEEE Interna- tional Conference on Image Processing, 2011, pp. 2737-2740,

doi: 10.1109/ICIP.2011.6116235.

[4] P. A. Shofro, K. Widia, D. D. A. P. Astuti, E. H. Rachmawanto,

[5] D. R. I. M. Setiadi and C. A. Sari, "Improved Message Payload and Security of Image Steganography using 3-3-2 LSB and Dual Encryption," 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2018, pp. 158-162, doi: 10.1109/ISRITI.2018.8864285.

[6] Xin Peng Zhang and Shuozhong Wang, "Steganography using multiple-base notational system and human vision sensitivity," in IEEE Signal Processing Letters, vol. 12, no. 1, pp. 67-70, Jan. 2005, doi: 10.1109/LSP.2004.838214.

[7] Fridrich, J. (2012). Steganography in Digital Media: Prin- ciples, Algorithms, and Applications. Cambridge University Press.

[8] Singh, D., & Kaur, H. (2017). Steganography Techniques: A Review Paper. International Journal of Computer Applications, 158(2), 1-6.

[9] Huang, J., Zhang, J., & Wang, C. (2020). A Review of Image Steganography Techniques. Journal of Information Hiding and Multimedia Signal Processing, 11(2), 282-305.