An Steganography-based Triple Layered Image Data Hiding Using Visual Cryptography

PROF. RAJENDRA ARAKH[1], AYUSHI SHRIVASTAVA[2], AYUSH BAKODE[3], KARTIK MISHRA[4]
[1] *Dept. of Computer Science & Engineering, Shri Ram Institute of Technology Jabalpur*
[2, 3, 4] *B. Tech (Computer Science & Engineering), Shri Ram Institute of Technology, Jabalpur*

***Abstract*— Steganography is the practice of representing information within another message or physical object, in such a manner that the presence of the information is not evident to human inspection. The advantages of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and many in themselves are incriminating in countries in which encryption is illegal. Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent and its contents. Through the concept of steganography, this project wishes to hide the text message in the cover files like image files.**

***Index Terms*— Steganography**

I. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means “concealed writing” from the Greek words steganos meaning “cover or protected”, and graphy meaning “writing”. The first recorded use of the term was in 1499 by Johannes Trichinisin his “Steganographia”, a treatise cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: image, articles, shopping lists or some other converted text and classically, the hiding message may be in invisible ink between the visible lines of a private letter.

The advantage of steganography over cryptography alone is that messages don't attract attention to themselves. Plainly visible encrypted messages, no matter how unbreakable, will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties. Through the concept of steganography, this project wishes to hide the text message in the cover files like audio, video, text, image files. The purpose in doing so is to create a fine multi-purpose Steganography Tool to increase the security of confidential messages across a network when only sender and receiver knows the trick behind the steganographic message.

II. EASE OF USE

A. User Interface: The user interface of steganography and cryptography tools plays a critical role in ease of use. Intuitive interfaces and clear instructions can make the process more straightforward.
B. Complexity vs Usability: Combining cryptography with steganography adds an extra layer of complexity to the process of hiding and revealing data. This complexity can affect ease of use.
C. Security: Combining steganography and cryptography enhances security by hiding the existence of secret communication and protecting the content with encryption.
D. Performance: Depending on the size of the carrier file and the amount of data to be hidden, performance considerations such as processing time and file size may come into play.
E. Legal and Ethical Consideration: The use of steganography and cryptography tools for hiding data should comply with legal and ethical guidelines. Misuse or unauthorized use can lead to legal consequences.
F. Documentation & Support: The Comprehensive documentation and user support resources accompany the system, equipping user with the necessary guidance and assistance for seamless deployment and

operation. User manuals, troubleshooting guides, and online support channels ensure users have access to timely assistance and resources for resolving issues effectively.

G. Key Management: The management of encryption keys is crucial. Users must securely exchange or store decryption keys to ensure that intended recipients can access the hidden data.

H. Scalability and Interoperability: Built with scalability and interoperability in mind, the system accommodates future expansion and integration with existing infrastructure seamlessly. Modular architecture and standardized interfaces facilitate interoperability with third-party systems and enable seamless scalability to meet evolving needs and requirements.

I. Feedback Mechanisms: Continuous feedback mechanisms enable users to provide input and suggestions for system enhancements and optimizations. User feedback is systematically collected, analysed, and incorporated into future system updates and iterations, ensuring ongoing improvement and user satisfaction.

J. Compliance and Standards: Adherence to industry standards and regulatory requirements is paramount in ensuring the system's reliability and compliance. The system is designed and tested to meet applicable standards and regulations, providing users with confidence in its performance and legal compliance.

The ease-of-use section outlines the user-centric design principles and features incorporated into the system to simplify deployment, operation, and maintenance while maximizing user satisfaction and system effectiveness.

III. METHODOLOGY

- Splitting Of the program We have splatted the program into two parts:
- Steganography.py (The main file)
- libs (A folder that contains the individual files as library) image steganography.py Creating “image_steganography.py” This file contains a function called:
- Image steganography (file): with parameters: “file” - which takes the file name as argument. “n” - which takes an integer i.e.: 0 or 1 as argument, which acts as an flag, means 0 for encode and 1 for decode.

The Sub-functions:

- Encode ():
- Decode ():
- Encode (): Modified LSB Algorithm where we overwrite the LSB bit of actual image with the bit of text message character. At the end of the text message, we push a checkpoint to the message string as a checkpoint useful in the decoding function. We encode data in order of red, green and blue pixel for the entire message.
- Decode (): In the decode part, we take all LSB bits of each pixel until we get a checkpoint and then we split them by 8 bits and convert them to characters data type and print the string (i.e., the secret text message) without delimiter.

IV. LITERATURE REVIEW

In this chapter, we are going to focus on discussing the results or endings based on the article, journals or any other related reference material. Some original words from the reference material may be cited in order to enhance the review. Basically, it is divided into a few sub-sections as well. Those sub-section include some little explanation of basic concepts of the selected project, research of some already existing similar problem or solution done by others and the hardware, technique or method which will be applied or used in the selected project. This review will do research and describe the existing problem or solution done by other parties. It will also study other systems which are related to the selected project. This chapter explains in detail the techniques /method/hardware technologies which are suitable to be adapted into the project. A few techniques have high payload cut-off points and incredible delicate quality and fogginess rely upon the picked cover for disguised or obscure data, hiding (Spatial space) however more powerless against attacks (Noise throwing, rotation, disturbance, resize Plagiarised Unique Total Words: 967 Total Characters: 6300 Plagiarized Sentences: 0 Unique Sentences: 47 (100%) 0% 100% Page1of2 Ing, etc). This infers there is dependably a trade-off between the three main criteria of steganography (Payload, Imperceptibility& Robustness).

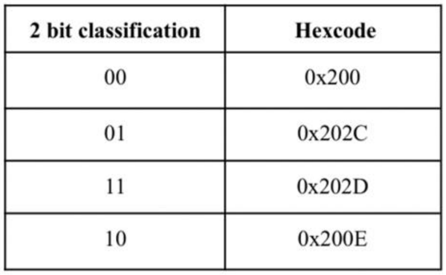
V. UNITS

Packets or Frames: In steganography involving network traffic, units can be packets (in packet-switched networks) or frames (in data link layer networks). Information can be hidden by subtly altering certain fields or properties within these packets or frames.

Bytes: In some cases, steganography operates at the byte level, where each byte represents a color channel value for a pixel. Manipulating these bytes allows for hiding information in the image data.

Image size (width x height): The dimensions of an image, typically measured in pixels. For example, an image might have a size of 640x480 VI.

Table no: 1



2 bit classification	Hexcode
00	0x200
01	0x202C
11	0x202D
10	0x200E

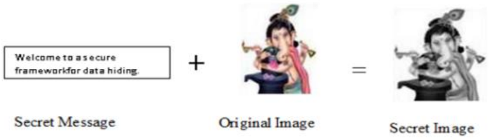


Fig no: 1

Pixels: Images are composed of pixels, which are the smallest units of a digital image. Each pixel contains colour information, typically represented by values for red, green, and blue (RGB).

ACKNOWLEDGEMENT

The completion of this research would not have been possible without the support and contributions of several individuals and organizations. We would like to express our sincere gratitude to SHRI RAM GROUP, JABALPUR for providing access to the necessary resources and facilities essential for conducting experiments and analysis.

We extend our heartfelt appreciation to Mr. Rajendra Arakh for their invaluable guidance, encouragement, and expertise throughout the duration of this project. Their insightful feedback and constructive criticism significantly enriched the quality of this research.

Furthermore, we acknowledge the contributions of our colleagues and peers who provided valuable insights and suggestions during discussions and presentations. Finally, we would like to express our gratitude to our families and friends for their unwavering support and understanding during the challenging phases of this endeavour...

REFERENCES

[1] Steganography, 2020, [online] Available: https://en.wikipedia.org/wiki/Steganography.

[2] H. Shi, X.-Y. Zhang, S. Wang, G. Fu and J. Tang, "Synchronized detection and recovery of steganographic messages with adversarial learning", Proc. Int. Conf. Comput. Sci, pp. 31-43, 2019.

[3] N. F. Hordri, S. S. Yuhaniz and S. M. Shamsuddin, "Deep learning and its applications: A review", Proc. Conf. Postgraduate Annu. Res. In format. Seminar, pp. 1-6, 2016.

[4] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen", Computer, vol. 31, no. 2, pp. 26-34, Feb. 1998.

[5] S. Gupta, G. Gujral and N. Aggarwal, "Enhanced least significant bit algorithm for image steganography", Int. J. Comput. Eng. Manage., vol. 15, no. 4, pp. 40-42, 2012.

[6] R. J. Mstafa, K. M. Elleithy and E. Abdelfattah, "A robust and secure video steganography method in DWT-DCT domains based on multiple objects tracking and ECC", IEEE Access, vol. 5, pp. 5354-5365, 2017.