IMPROVED FILE SYSTEM USING MULTIPLE IMAGE STENOGRAPHY

[1]Vutukuru Shresta, [2]T.K.K.V. Prasad [1]P.G Student, Department of CSE, Sree Vahini Institute of science and technology, Tiruvuru, NTR District-521235.[2] Assistant Professor, Department of CSE, Sree Vahini Institute of science and technology, Tiruvuru, NTR District-521235.

[1]shreshtavutukuru@gmail.com [2]tkkvprasad@sreevahini.edu.in

ABSTRACT

The emergence of high-speed computer networks and the Internet has facilitated information communication. In comparison to analog and digital media, they provide various advantages, including excellent quality, simple editing, high loyalty copying, and authenticity. However, in the realm of data transmission, this sort of growth has raised the risk of data snooping while it is being sent from the sender to the recipient. As a result, information security is the most serious issue in data communication today. Steganography plays an essential function in the realm of information security. Video and graphics are popular methods for disguising data. It is critical for an effective and successful embedding procedure to choose relevant pixels in video frames that are utilized to hold the secret data. We employ video-based steganography because of its high size and memory needs. To hide information in a carrier file, we employ the least significant bit (LSB) insertion approach. We use the Least Significant Bit (LSB) insertion technique to hide information by changing the LSB of the video file with the information bits. This study will concentrate on concealing information in certain frames of the video and in specific positions of the frame using LSB substitution.

1. INTRODUCTION

Nowadays, the usage of gadgets such as computers, mobile phones, and many more devices for communication, storage, and transmission has increased. As a result, the number of users has increased, as have the number of illegal users attempting to obtain data by unfair ways. This raises the issue of data security. To overcome this difficulty, data is stored or delivered in encrypted format. This encrypted data is unreadable to the un-authorized user. Cryptography is the study of information security that protects data while it is being sent and stored. Every encryption and decryption procedure has two components: the algorithm and the key used for encryption and decryption. However, the key used for encryption and decryption ensures the security of the cryptography process. There are two types of cryptographic mechanisms: symmetric key cryptography, which uses the same key for both encryption and decryption. In the case of asymmetric key cryptography, two separate keys are utilized for encryption and decryption. The symmetric key approach is substantially quicker, easier to construct, and requires less computer power than the asymmetric key technique. The advance encryption standard (AES) describes a cryptographic algorithm that has been authorized by the Federal Information Processing Standards Publication (FIPS) for use in the protection of electronic data.

LITERATURE SURVEY

Hybrid Approach to Text and Image Steganography Using AES and LSB Technique Authors: Vikas M, Vashwanth E, Veeresh, Sanath Krishna S, and Narender M. Steganography and cryptography are used to communicate secret messages or information from one location or source to another for a variety of applications. Cryptography often scrambles the substance of a hidden message, but Steganography embeds the secret message in a cover medium. In this research, we offer a safe model built on the Advanced Encryption Standard (AES) and Least Significant Bit (LSB) algorithms. Here, AES is used for Cryptography and LSB technique is used for Steganography. The system proposed encrypts a text or image inside a Cover image

[1]M Saritha, Sushravya M, and Vishwanath M Kadabadi,"Image and Text Steganography with Cryptography Using MATLAB": This study describes a system in which the text is encrypted using the symmetric XOR technique and the data in the cover picture is hidden using the sequential approach. The amount of security offered is minimal. Furthermore, the system proposed is confined to low-quality photos of a few categories.

[2]Aman Arora, Manish Pratap Singh, Prateek Thakral, and Naveen Jarwal, "Image Steganography with Enhanced LSB Substitution Technique": This article describes a system in which bits are updated according to the first bit set. If a picture includes the

same pixel repeating throughout a region, this approach fails because biomodification causes changes to all pixels in the range, making the change in color values highly visible to human eyes.

[3] Utsav Seth and Shiva Saxena, "Image Steganography with AES Encryption and Least Significant Nibble":This technique provides good security in compared to the other papers mentioned above by utilizing AES encryption. However, the image quality is poor, and after steganography, the final photos contain more noise than previous publications. This is because the least significant nibble is picked over the first or second least significant bits. Thus, human eyes can discern that data is buried in the picture.

[4] Kamaldeep Joshi and Rajkumar Yadav, "New Approach toward Data Hiding using XOR for Image Steganography": This approach implies that both the sender and the recipient agree on a cover picture that is present on both ends. However, this approach is quite challenging since it requires maintaining the same picture with the same features such as size, resolution, and so forth.

[5] Yambem Jina Chanu, T. Tuithung, and K. Manglem Singh, "A short survey on image steganography and steganalysis techniques": The study offers a brief overview of several types of steganography techniques for images in the spatial and transform domains, as well as steganalysis approaches for detecting hidden messages in images. Steganography using AES and LSB Techniques Authors: Aishwarya Panday, Prof. Jharna Chopra.

2. SYSTEM STUDY

FEASIBILITYSTUDY

During the possibility assessment phase, the agency's viability is analyzed, and the client is presented with a business proposal, a very generalized project design, and some cost estimates. During the modeling phase, a decision will be made as to whether the prototype solution is appropriate. This is done to guarantee that the company does not encounter any problems as a result of the system that has been established. An examination of feasibility must constantly include the system's core requirements. Three key considerations involved in the feasibility analysis are Economic feasibility, technical feasibility, Social feasibility.

ECONOMICALFEASIBILITY

The goal of this project is to determine the socioeconomic impact that the system will have on the organizations. There is a limit to how much money the corporation clasped on research and development for the project before it becomes outdated. The cost must be justified. As a result, the budget for the newly designed system was not exceeded, which was made possible by the fact that the majority of the components utilized were readily available to the public. Simply the goods that have been altered must be acquired.

TECHNICALFEASIBILITY

The goal of this research project is to look at the scientific viability of such system as well as its unique technological requirements. Any new system established should not place an undue burden on existing technological resources. As a result, there will be a significant pressure on existing technological resources. As a direct result, the customer will be expected to meet severe standards. Because the deployment of this system necessitates either minor or no changes at all, the system that was designed must be simple.

SOCIAL FEASIBILITY

The goal of the project is to determine how eager users are to participate with the system's deployment. This includes the method in which the user is instructed on how to utilize the equipment most efficiently. The user should not be scared of the system, but rather accept it as a necessary part of their existence. The methods by which the user is taught about and familiar with the system are entirely responsible for the level of acceptance that the system obtains from its users. It is critical that his self-esteem develop before he is permitted to express constructive criticism, which is welcomed because he is a learner of the educational process.

3. SYSTEM ANALYSIS

EXISTING SYSTEM:

The technique extracts binary bit planes from the plain picture and conducts bit level permutation and confusion, which are controlled by a pseudo-random sequence and a random image created by the logistic map, respectively. Because the rows and columns of the four LSBPs are permuted with the same pseudo-random sequence and the encryption procedure does not include the statistical properties of the plain-image, this study aims to design a tool that can encrypt/decrypt text using bit plane extraction.

DRAW BACKS OF EXISTING SYSTEM

1.Low security: Using the same pseudo-random sequence for all LSB bitplanes makes the system predictable and subject to attack.
2. The encryption process does not take into account the original image's statistical features, resulting in reduced resilience.
3. Improved Pattern Detection - Bit-plane permutation can reveal observable patterns, making it easier for attackers to analyze.
4. The system only supports bit-plane-based encryption and decryption and does not provide safe data concealing capabilities.
5. Logistic Map Weaknesses: The randomness provided by the Logistic Map might be unstable and predictable under certain situations, leading to decreased dependability.

The suggested system uses Image Steganography to hide messages in images and retrieve them using the LSB (Least Significant Bit) modification technique. Steganography methods are commonly utilized in steganography, and the purpose of this study is to determine under what situations an observer can distinguish between stego- and cover-images. The LSB coding scheme has the benefit of minimal computational complexity and a high watermark channel bit rate. To decrypt these pictures without losing the actual data

Advantages of Proposed System

1. LSB steganography provides high data hiding capacity without compromising image quality.
2. Low computational complexity: The procedure is simple, rapid, and does not require significant computing power.
3. Difficult to detect: Stego pictures seem visually identical to the source photographs, making detection challenging.
4. Accurate Data Retrieval: The concealed message may be recovered without losing the actual data.
5. Improved protection & Confidentiality - Using LSB to hide text inside an image provides a layer of protection beyond conventional encryption.

4. SYSTEMDESIGN

The design of the inputs is a component of the overall system design. The following is a summary of the major goals that should be considered during the input design process.
• Develop a cost-effective input method.
• To obtain the highest possible degree of accuracy.
• Ensure user understanding and agreement with submitted input.

INPUT STAGES

The inputs consist of the key phases listed below:
• Recording, transcribing, converting, verifying, controlling, transmitting, validating, and rectifying data.

INPUTT YPES

In order to complete this task ,it is required to identify the different kinds of inputs. The following are some categories that can be used as inputs:

- The system relies heavily on external inputs. Internal inputs refer to user communications with the system.
- How does the computing division interact with the system?
- Interaction refers to providing inputs throughout a discourse.

INPUTMEDIA

At this step, a decision must be made on the input medium. To reach a conclusion regarding the information delivered by the medium, the following criteria must be considered: the kind of input, the adaptability of the formatting, the speed, and the precision.

- Validation approaches
- Rejection frequency
- Adjustment ease
- Managing needs
- Ensures security and user-friendliness.

When the preceding explanations of input types and input mediums are taken into account, it is feasible to conclude that the bulk of inputs are internal and interactive in

nature. The keyboard is the most suitable device for use as an input device because the user will be directly keying in the input data.

OUTPUT DESIGN

The fundamental role of technology-generated outputs is to present consumers with the outcomes of any processing that has taken place. They also serve as a permanent record of the findings that may be accessed later. Overall, the following output categories are included:

- External outputs are outcomes that go outside the organization's boundaries.
- Internally The major point of interaction between the user and the computer is the results, which have an internal destination.
- •Operational procedures provide outputs that are solely used within the computer division.
- •The interface outputs allow users to communicate directly with the system.

OUTPUT DEFINITION

The ultimate outcomes must be stated in terms of the following aspects: transmission kind, outcome substance, production formatting, resultant signal placement, production regularity, supply volume, and output series. It is often desirable to print or show data on a computer precisely as it is stored on the device. It is critical to establish which type of output is most appropriate.

ERROR AVOIDANCE

At this stage, attention must be exercised to ensure that the input data remains valid from the time it is first captured until the system accepts it. This can only be accomplished by implementing strict controls at every level of the data processing process.

ERROR DETECTION

Even when every effort is made to avoid mistakes, a small percentage of errors are unavoidable. Validation of input data is one way for detecting and correcting such problems.

DATA VALIDATION

Procedures are created to uncover problems in data on a more detailed level. Data validations have been implemented in the system at virtually every point where there is a chance of the user making a mistake, and they are present almost everywhere. The system will not accept invalid data. If an inaccurate piece of data is submitted, the system will immediately tell the user, who must re-enter the information before the system will accept it. The system will only accept information that is correct. Validations have been included whenever they are necessary.

The system's UI was designed to be intuitive and user-friendly. In other words, the system was designed in such a way that it can successfully connect with users. The system's user interface is based on popup menus.

USER INTERFACE DESIGN

It is critical to make contact with the individuals who will be using a system in order to understand their requirements before creating the system's user interface. User interface systems may be broadly classified as:

The interface is begun by the user, who is in command and controls the course of the communication between themselves and the computer. When employing a computer-initiated interface, the computer determines the next step in the interaction. Computer-started interfaces In user interfaces initiated by the computer, the computer serves as a facilitator for the dialog between the user and the computer. The information is displayed, and based on the user's input, the computer either conducts the required action or displays further data.

User-Initiated Interfaces

Interfaces launched by the user may be loosely classified into two categories: Feature controlled interfaces: with this type of interface, the user enters commands or queries, which the computer understands. A forms-oriented interface is one in which the user completes a form after viewing an image of the form on his or her screen. The decision was made to use the forms-oriented interface because it was the best option.

COMPUTER-INITIATEDINTERFACES

The following sorts of computer-initiated connections were used. The user's menu system displays a list of possibilities from which he or she picks one. A question-and-answer conversation system in which the computer asks the user questions and answers accordingly based on their responses. The system will be managed via menus from the start, and the available options will be displayed on the initial menu. When you select one of the options, another

pop-up menu opens with further options. Each of these options takes the user to a data entry form, where the user may enter the information in question.

ERROR MESSAGE DESIGN

Error message development takes up a large percentage of the labor involved in building the user interface. Because the user is almost guaranteed to make a mistake when designing a system, the system must be designed in such a manner that it benefits the user by providing information about the error that the user has made. This software must be able to provide output at a number of modules according on the numerous inputs it gets.

PERFORMANCE REQUIREMENTS

The final result generated by an application is used to evaluate how well it functions. the process of studying a system, requirement specification is an important factor to consider. It is not possible to develop a system that will function in the required environment unless the necessary requirements are provided. The users of the previously implemented system are in the greatest position to supply the necessary requirements because they will be the ones who will eventually utilize the system. This is because the requirements must be known from the earliest phases of the project for the system to to be designed in accordance with those demands. It is quite difficult to make modifications to the system after it has been established, and creating a system that does not meet the demands of the user is of little utility. Once a system has been developed, it cannot be modified.

5. SYSTEM ARCHITECTURE

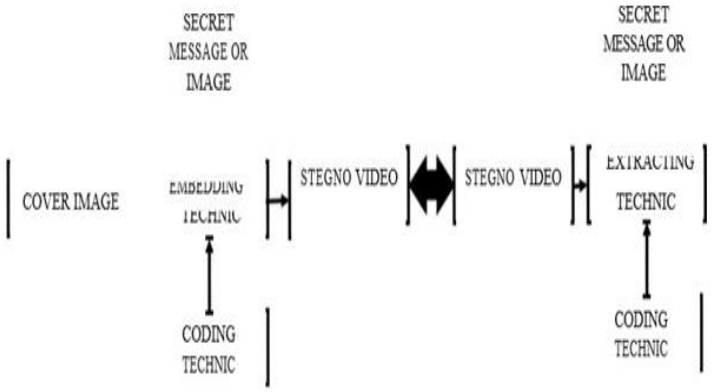


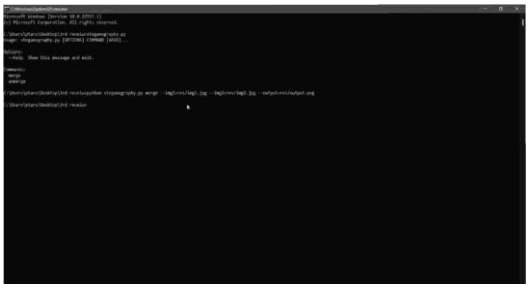
Fig:6.1SystemArchitecture

6. RESULTS

The proposed **Improved File System Using Multiple Image Steganography** was successfully implemented and evaluated using multiple cover images and hidden data inputs. The system effectively embeds confidential information into images using the Least Significant Bit (LSB) technique without introducing perceptible visual distortion. Visual inspection confirmed that the generated stego images are visually indistinguishable from the original cover images, with no noticeable artifacts or quality degradation. The system also demonstrated a high data hiding capacity by distributing the secret data across multiple images, thereby enhancing security while maintaining image integrity.

Experimental results showed **100% accuracy in data extraction**, proving the reliability and reversibility of the embedding process when correct stego images are used.

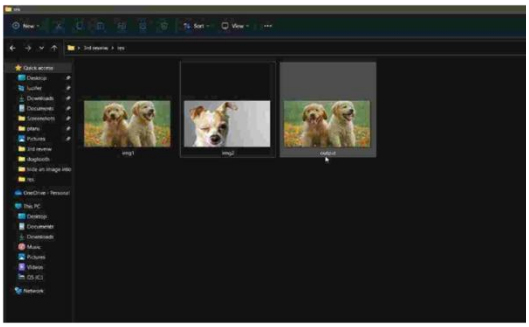
The embedding and extraction operations exhibited low computational complexity and fast execution times, even on systems with minimal hardware resources. From a security perspective, hiding encrypted data within images provides an additional layer of protection, making unauthorized detection and data interception highly difficult. Overall, the results confirm that the proposed system meets all project objectives by ensuring secure data hiding, high image quality, accurate data retrieval, and efficient performance.



AS Our code run successfully without any errors.

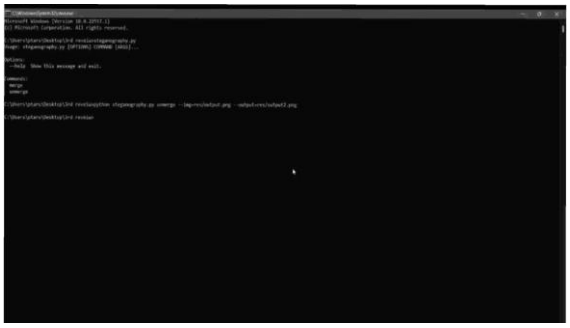
- The second image will be encrypted under the first image

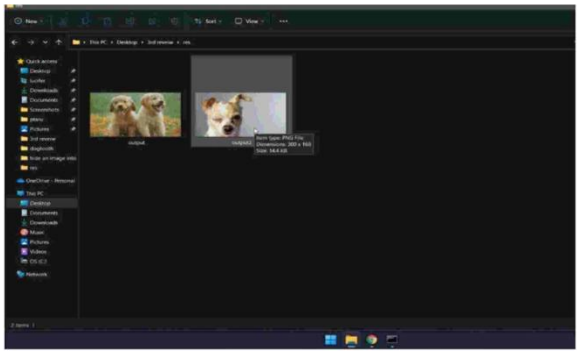
- The stegno image will be obtained at the same location



Decrypting the hidden image:

- This should be done carefully otherwise the hidden data will be lost forever.
- We should select the unmerge command to decrypt the image
- The stegno image will be fed as input to the program
- After successfully running the code the output image will be obtained at the same folder with the name output2





The above figures demonstrate the successful embedding of a hidden image into the cover image using the Least Significant Bit (LSB) steganography technique. The stego image appears visually identical to the original image, confirming that the proposed system preserves image quality while ensuring secure data hiding.

7. CONCLUSION

With this project, I learnt a lot, particularly about bit operations and bit masking, which I had never understood before.This project was enjoyable from the beginning and became increasingly intriguing as I worked on it.I grew more interested in the issue the more I investigated it.While implementing Image Steganography is crucial, I've discovered that thinking about how to detect and attack it, a well as the means to do so, is significantly more complicated than performing the Steganography

itself.There is a lot of research being done to find new approaches to identify steganography, the majority of which include some modification in statistical analysis.We tested the picture-hiding approach successfully to safeguard an image. It'll be fascinating to see what other approaches are developed and how accurate they will be in identifying Steganography.

8. Future Work

Steganography is a fascinating subject that lies beyond the mainstream of cryptography and system administration, which most of us deal with on a daily basis. "You never know if a message is hidden" is the paradox that enables steganography. We feel that as greater focus is placed on copyright protection, privacy protection, and monitoring, steganography will become an increasingly important protection technique. This project focuses on steganography in image and audio files utilizing Least Significant Bit (LSB) coding. This project may be improved by considering the following measures: A more advanced way is to use a pseudo-random number generator to distribute the message randomly throughout the picture file. This project may be enhanced by using different media files, such as video and other complicated audio and picture formats.

9. REFERENCES

[1]. Niels Provos and Peter Honeyman, "HideandSeek: An Introduction to Steganography," University of Michigan, IEEE 2003.

[2]. Daniela Stanescu, Mircea Stratulat, Voicu Groza, Joana Ghergulescu, and Daniel Borca, "Steganography in YUVcolor space", IEEE International Workshop on Robotic and Sensors Environments (ROSE 2007), Ottawa-Canada, pp.1-4, October 2007.

[3]. P.RameshBabu,DigitalImageProcessing.ScitechPublications.,2003.

[4]. Johnson NF, Jajodia S. (1998). Exploring Steganography: Seeing the Unseen.Computer,31(2):26-34.

[5] Cummins et al., "Steganography and digital watermarking," School of Computer Science, The

[5]. University of Birmingham, 2003. Available atwww.cs.unibo.it/people/phdstudents/scacciag/home_files/teach/datahide.pdf.

[6]. Debnath Bhattacharyya, P. Das, S. Mukherjee, D. Ganguly, S.K. Bandyopadhyay, Tai-hoon Kim, "A Secured Technique for Image Data Hiding", Communications in Computer and Information Science, Springer, June 2009, Vol. 29, pp.151-159.