"Image Steganography"

[1]Ujwal Nikam, [2]Vishal Ahire, [3]Tejas Nikam, [4]Saurav Khairnar

MET Bhujbal Knowledge City
Nashik, Maharashtra, India.

***Abstract*- Nowadays, computer-based communications are at the threshold of making life easier for everyone in the world; from sharing information, to communicating with each other, to exchanging electronic documents, and to checking bank balances and paying bills. Nonetheless, information security is an essential factor, which must be taken into consideration to ensure secure communications. There are significant interests in security approaches that aim to protect information and digital data, since the growing increase in uses of the internet and multimedia, have raised the interests in image steganography in order to secure and protect them. In this paper, a detailed literature review on a variety of different methods, algorithms, and schemes in image steganography is conducted in order to analyses and investigate them. In addition, this research summarized a com- parative literature review for these researches and presented into a table, which involves a research name, broad domain, research methodology, advantages, disadvantages, and the evaluation method.**

***Key Words*: machine learning, image processing, e- commerce, shopping.**

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 11, Issue 3, May-June 2023

INTRODUCTION

The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages appear to be (or to be part of) something else: im- ages, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography that lack a shared secret are forms of security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoffs's principle.[2] The advantage 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 may in themselves be incriminating in countries in which encryption is illegal.[3] 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. Steganography includes the concealment of information within computer files. In dig- ital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change

LITURATURE SURVEY

1. Data Encryption & Decryption Using Steganography, N. Manohar etal.**,[1]** This paper studied that Video steganography is a method that processes secure communication. When we see the history of steganography, it was hidden in many ways such as tablets covered with wax, & written on the stomachs of rabbits. Here in this paper, considering the video steganography methods to perform secure steganography communication. Many methods have been proposed for video steganography but they're no more different types of formats, secured, quality, of the results. So here propose secure steganography methods i.e. Secure

base LSB method, Neural Networks & Fuzzy logic, and check their using PSNR and MSE data of the methods. That data-set has collected is from video streams. And the result was seen with the more formats, more security, quality of outputs, & accuracy values of PSNR & MSE which is better than other proposed methods.

2. Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography, Mehdi Sharifzadeh etal.,[2] This paper shows that, In digital image steganography, the statistical model of an image is essential for hiding data in less detectable regions and achieving better security. This has been addressed in the literature where different cost-based and statistical model-based approaches were proposed. However, due to the usage of heuristically defined distortions and non-constrained message models, resulting in numerically solvable equations, there is no closed-form expression for security as a function of payload. The closed-form expression is crucial for a better insight into image steganography problem and also improving performance of batch steganography algorithms. Here, we develop a statistical framework for image steganography in which the cover and the stego messages are modeled as multivariate Gaussian random variables. We propose a novel Gaussian embedding model by maximizing the detection error of the most common optimal detectors within the adopted statistical model. Furthermore, we extend the formulation to cost-based steganography, resulting in a universal embedding scheme that improves empirical results of current cost-based and statistical model-based approaches. This methodology and its presented solution, by reason of assuming a continuous hidden message, remains the same for any embedding scenario. Afterward, the closed-form detection error is derived within the adopted model for image steganography and it is extended to batch steganography. Thus, we introduce Adaptive Batch size Image Merging steganographer, AdaBIM, and mathematically prove it outperforms the state-of-the-art batch steganography method and further verify its superiority by experiments.

3. A mobile forensic investigation into steganography, Catrin Burrows etal.,[3] This paper studied that, Mobile devices are becoming a more popular tool to use in day-to-day life; this means that they can accumulate a sizeable amount of information, which can be used as evidence if the device is involved in a crime. Steganography is one way to conceal data, as it obscures the data as well as concealing that there is hidden content. This paper will investigate different steganography techniques, steganography artefacts created and the forensic investigation tools used in detecting and extracting steganography in mobile devices. A number of steganography techniques will be used to generate different artefacts on two main mobile device platforms, Android and Apple. Furthermore, Forensic investigation tools will be employed to detect and possibly reveal the hidden data. Finally, a set of mobile forensic investigation policy and guidelines will be developed.

4. Directional Pixogram: A New Approach for Video Steganography, Mohammed Baziyad etal.,[4] This paper explain that, A video signal can be expressed as a 3D signal where the rows and columns of pixels represent the first and the second dimension, while the third dimension is the time. The 3D nature of video signals has produced an additional source of data redundancy; that is, the temporal redundancy. Utilizing signal redundancy is the fundamental driving force for steganography techniques. In this paper, the Directional Pixogram is proposed to optimally exploit the redundancy in a video segment. The Directional Pixogram is a 1D vector that starts from a certain initial position and then grows in the direction of the motion vector associated with that initial position. It is expected that this temporal vector will contain highly correlated pixels. Therefore, the Discrete Cosine Transform (DCT) can express this vector within few significant DCT coefficients leaving a large amount of insignificant DCT coefficients. Thus, experimental results have shown that the proposed Directional Pixogram is able to obtain outstanding stego quality while hiding with very high hiding capacities.

5. A novel approach to Steganography using pixel-based algorithm in image hiding, Jawwad A R. Kazi etal[5] This paper studied the Steganography is the technique of hiding data under image to prevent it from being unintentionally accessed by anyone else. This process involves a plain text and an image file. By looking at the need of steganography we have proposed a new algorithm which will satisfy the aim of steganography. In our algorithm, we will have a cover image file and the message. Then the cover image's pixel will be taken into consideration. In that we will embed each bit of secret text. This process will be continued until the last bit of secret text. After this step, the data is hidden under the image. Then we will send this image file to our client and client will have reverse process to retrieve original text from the image. We will then compare our algorithm with BLIND HIDE steganography algorithm on the basis of accuracy, precision, recall and f1-

score. We will also check for the output image quality generated by both algorithms on structural similarity measure to reach proper consensus

AIM & OBJECTIVES

- System provides best user experience as compare to existing system.
- Scalable system
- High Security
- Less cost
- Easy to use system

MOTIVATION

The internet plays a key role in transferring information or data from one organization to another organization. But anyone can modify and misuse the valuable information through hacking at the time. Steganography plays a very important role in hiding the secret data or information inside the digitally covered information

SYSTEM ARCHITECTURE

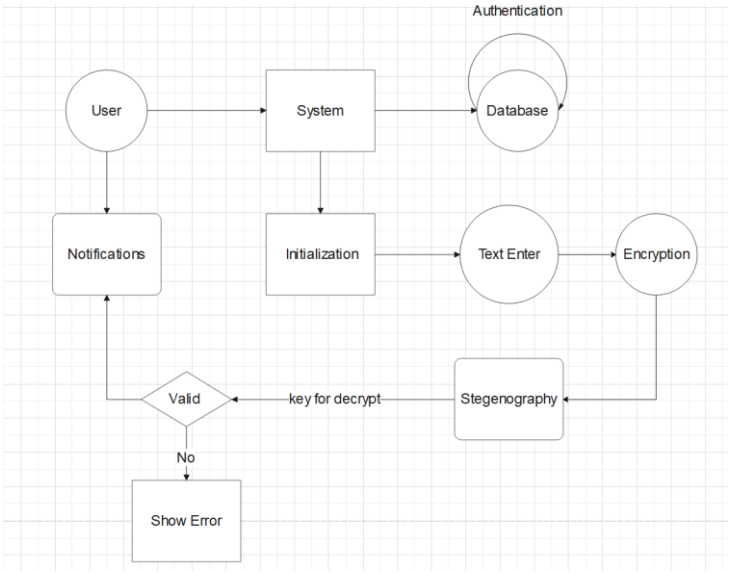

Fig -1: System Architecture Diagram

APPLICATION:

- Banking
- Organization
- Personal

FUNCTIONAL & NON-FUNCTIONAL REQUIREMENTS

Functional requirements: may involve calculations, technical details, data manipulation and processing and other specific functionality that define what a system is supposed to accomplish. Behavioral requirements describe all the cases where the system uses the functional requirements; these are captured in use cases.

Nonfunctional Requirements: (NFRs) define system attributes such as security, reliability, performance, maintainability, scalability, and usability. They serve as constraints or restrictions on the design of the system across the different backlogs.

Functional requirements

- Registration
- User Login
- Creation of database: Users Mandatory Information

Design Constraints:

1. Database

2. Operating System
3. Web-Based Non-functional Requirements

Security:

1. User Identification
2. Login ID
3. Modification

Performance Requirement:

1. Response Time
2. Capacity
3. User Interface
4. Maintainability
5. Availability

SYSTEM REQUIREMENTS

Hardware:

RAM 3 GB or Above
Hard Disk 250 GB or Above
Processor i3 or above

Technology:

MySQL 3.2 or Above
Python
Windows Operating System 7

Tools:

Notepad ++ / VS Code
Pycharm / Jupiter
Browser

CONCLUSION

Hence, we are overcoming the drawback of existing system, and providing a smart system that will not only monitor and control our data with security but also supply it too whenever necessary. We are trying achieved more than 90% detection accuracy using image processing algorithm with lowest false positive rate.

REFERENCES:

1. Bender W., Butera W., Gruhl D., Hwang R., Paiz F.J., Pogreb S., Techniques for data hiding, IBM Systems Journal 39(3-4) (2000), 547– 568.
2. Jayaram P., Ranganatha H.R., Anupama H.S., Information Hiding Using Audio Steganography–A Survey, The International Journal of Multimedia & Its Applications 3(3) (2011).
3. Pal D., Ghashol N., A robust audio steganography scheme in time domain, International Journal of computer Applications 80(15) (2013).
4. Cvejic N., Seppanen T., Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding, Journal of Universal Computer Science 11 (2005).
5. Gopalan K., Audio Steganography Using BIT Modification, International Conference Multimedia and Expo (2003).
6. Jain M.P., Trivedi P.V., Effective Audio Steganography by using Coefficient Comparison in DCT Domain, International Journal of Engineering Research & Technology 2(8) (2013).
7. Santosa R.A., Bao P., Audio-to-Image Wavelet Transform based Audio Steganography, 47th