SECURE COMMUNICATION USING IMAGE STEGANOGRAPHY

[1]Prerna Laxman Kote, [2]Swapnil Krishna Kadam, [3]Dhanashri Sanjay Hire, [4]Trisha Manik Jadhav, [5]Dr. M. A. Chaudhari

Information Technology
Amrutvahini College of Engineering, Sangamner.

***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 our proposed system we are creating a feature where user will be asked to select the image & add secret message, user will also select the receiver for decryption & enter the key for captcha,then receiver will enter the key and decrypt the secret msg.**

Key Words: **Image steganography, DCT (Discrete Cosine Transform), AES.**

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 Tritheism in his Steganographic, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messagesappear 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 thatlack a shared secret are forms of security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoffs's principle. 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.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 steganographictransmission because of their large size. Forexample, 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

Our system consists of objective like a scalable approach system which will allow system to extends better features in future. System is built with great user interface so that user can able to usethe system easily.

In our proposed system we are creating a feature where user will ask to select the image & add secret message, user will also select the receiver fordecryption & enter the key, then receiver will enter the key and decrypt the secret msg.

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.

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

LITERATURE 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

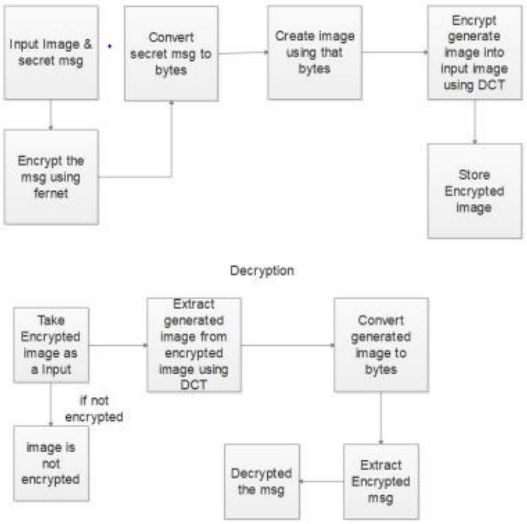


Fig -1: System Architecture Diagram

APPLICATION

- Banking
- Organization
- Personal

ALGORITHM

1. Start
2. Enter User's Email Address and password.
3. Select cover image.
4. Enter Secret Message.
5. System will generate Random Key Automatically.
6. Encrypt the Secret Message and Random Generated Key using AES Algorithm.
7. Generate the Cipher Text using Encrypted Secret Message and EncryptedRandom Generated Key.
8. Convert encrypted text to byte array and generate image.
9. Embed generated image into the cover image and generate stego image.
10. Send that Stego-File with any Communication Medium to the Receiver.
11. Receiver upload that File to the System.
12. If Receiver is Authenticated, then he have the Access of Decrypt the Message, Otherwise System gives "Access Denied" message.
13. If the receiver is Authenticated then, The RandomGenerated Key get Decrypted.
14. Then receiver got the access to show the Decrypted Message orActual Message send by the Sender.

IMPLEMENTATION AND ANALYSIS

INPUT:

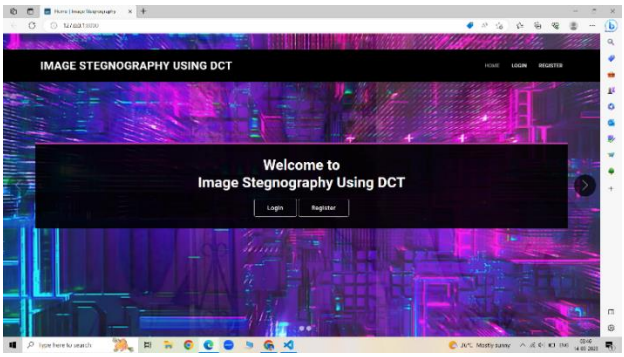


IMAGE STEGNOGRAPHY USING DCT
HOME
LOGIN
REGISTER
Welcome to
Image Stegnography Using DCT
Login
Register

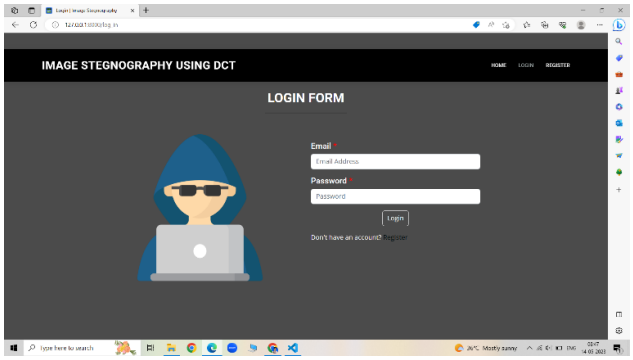


IMAGE STEGNOGRAPHY USING DCT
HOME
LOGIN
REGISTER
LOGIN FORM
Email *
Email Address
Password *
Password
Login
Don't have an account? Register

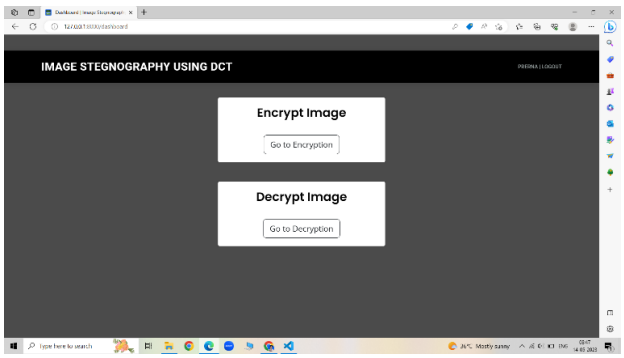


IMAGE STEGNOGRAPHY USING DCT
Encrypt Image
Go to Encryption
Decrypt Image
Go to Decryption

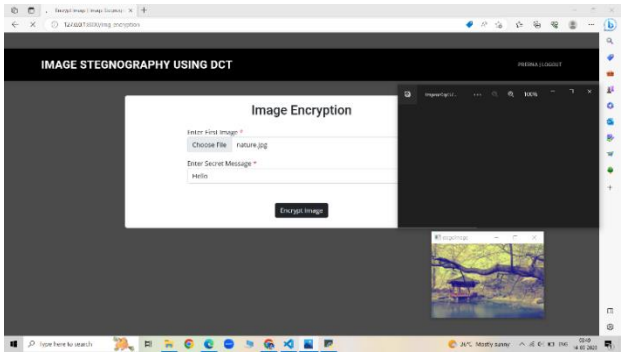


IMAGE STEGNOGRAPHY USING DCT
Image Encryption
Choose File
nature.jpg
Enter Secret Message *
Hello
Encrypt Image

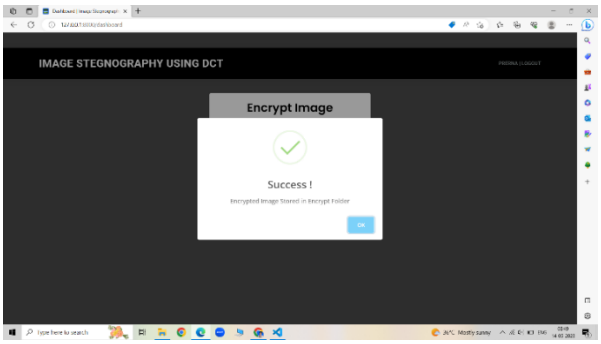
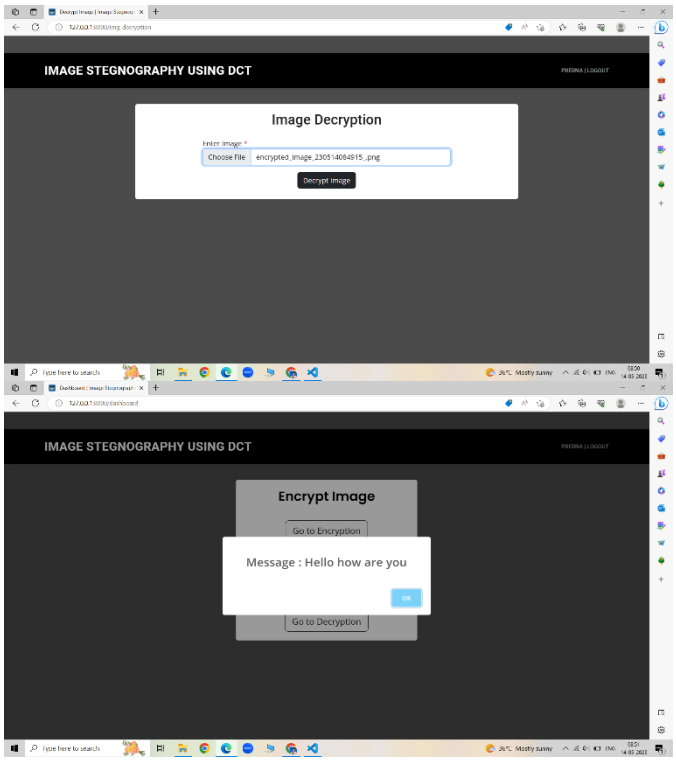


IMAGE STEGNOGRAPHY USING DCT
Encrypt Image
Success !
OK



ANALYSIS TABLE:

Sr. No.	Text File Size	Word Count	Image Size Before Encryption	Image Size After Encryption
1	12.3 kb	1	86 kb	521 kb
2	15 kb	180	115 kb	756 kb
3	22.5 kb	1472	162 kb	1.11 mb
4	30.8 kb	3093	219 kb	1.60 mb
5	40.5 kb	5225	379 kb	3.12 mb
6	49.8kb	4278	70.9kb	748kb
7	60.6kb	5570	127kb	1.3mb
8	72.2kb	6967	340kb	3.45mb
0	80.8kb	8022	917kb	9.14mb
10	90.8kb	9329	978kb	9.96mb

CONCLUSION

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 have triedachieved more accuracy using DCT algorithm with lowest falsepositive rate, so that the reconstructed image will be more similar to the cover image.

REFERENCES

[1] N. Manohar; Peetla Vijay Kumar., Data Encryption & Decryption Using Steganography, 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS).

[2] Mehdi Sharifzadeh., Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography, IEEE Transactions on Information Forensics and Security PP(99):1-1 DOI:10.1109/TIFS.2019.2929441

[3] Catrin Burrows; Pooneh Bagheri Zadeh, A mobile forensic investigation into steganography, 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security).

[4] Mohammed Baziyad; Tamer Rabie; Ibrahim Kamel, Directional Pixogram: A New Approach for Video Steganography, 2020 Advances in Science and Engineering Technology International Conferences (ASET)

[5] Jawwad A R. Kazi, Gunjan N. Kiratka., A novel approach to Steganography using pixel-based algorithm in image hiding, 2020 International Conference on Computer Communication and Informatics (ICCCI).

[6] Jayeeta Majumder et al., "High Capacity Image Steganography using Pixel Value DifferencingMethod with Data Compression using Neural Network", International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 12, October 2019, ISSN 2278 - 3075.
[7] Y. Huo, Y. Qiao and W Gao, "High Capacity Steganography on Float-Point Number with Single Precision", 2020 2nd International Conference on Video Signal and Image Processing, pp. 48-54, 2020, December, [online]
[8] H. A. Al-Korbi, A. Al-Ataby, M. A. Al-Taee and W. Al-Nuaimy, "High-capacity image steganography based on Haar DWT for hiding miscellaneous data", 2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), pp. 1-6, 2015,
[9] S.K. Muttoo et al., "A Multilayered Secure Robust and High Capacity Image Steganographic Algorithm", World of Computer Science and Information Technology Journal (WCSIT), vol. 1, no. 6, pp. 239-246, 2011, ISSN 2221-0741.
[10] Liu and Lee, "High-capacity reversible image steganography based on pixel value ordering EURASIP", Journal on Image and Video Processing, 2019.
[11] I.J. Kadhim et al., "High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform",Cognitive system research, vol. 60, pp. 20-32, May 2020.