iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XI **Month of publication:** November 2022

DOI: https://doi.org/10.22214/ijraset.2022.47549

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XI Nov 2022- Available at www.ijraset.com

Secret Communication Using Multi-Image Steganography and Face Recognition

Prof. Sakshi Shejole[1], Pratiksha Netke[2], Rohini Jadhav[3], Priya Sawant[4], Jyoti Rajput[5]
Department Of Computer Engineering
Alard College of Engineering, Pune
Savitribai Phule Pune University

Abstract: ***Our Proposed system is to develop a Web Application for hiding information in any image file to ensure the safety of the exchange of data between different military parties and provide better security during message transmission. The scope of the project is the implementation of steganography tools for hiding information including any type of information file and image file and the path where the user wants to save the image and extruded file. We use the LSB technique. The proposed approach is to use a steganography algorithm for embedding data in the image files for military applications. For security purposes we used modules face Recognition technique with AES algorithm for Strong Security purpose. And we use the cover channel technique as an information hiding technique that can be exploited by a process to transfer information in a manner that violates the system security policies. And we use copyright marking techniques. In short, Cover Channels transfer information using non-standard methods against the system design.d. Deep learning techniques used for image steganography can be broadly divided into three categories - traditional methods, Convolutional Neural Network-based and General Adversarial Network-based methods. Along with the methodology, an elaborate summary on the datasets used, experimental set-ups considered and the evaluation metrics commonly used are described in this paper. A table summarizing all the details are also provided for easy reference. This paper aims to help the fellow researchers by compiling the current trends, challenges and some future direction in this field.***

Keywords: AES Algorithm, LSB Algorithm, Steganography, GAN.

I. INTRODUCTION

Designing a system for secret communication using multi-image steganography and face recognition The aim of this project is to provide security for data sent over the network between two or more people. We use advanced technology, which is the OTP system in our project, to enhance the security level of information security. has become a prime issue of worldwide concern. To improve the validity and proficiency of the image data-hiding ap- proach, a cutting-edge secret information concealment transmission scheme based on face recognition is proposed. On the sender and receiver sides, we use the face recognition technique for fetching the sender and receiver secret messages, and the advanced technology we use is OTP technology. This technology can help to pass the secret messages to the receiver without any interference.

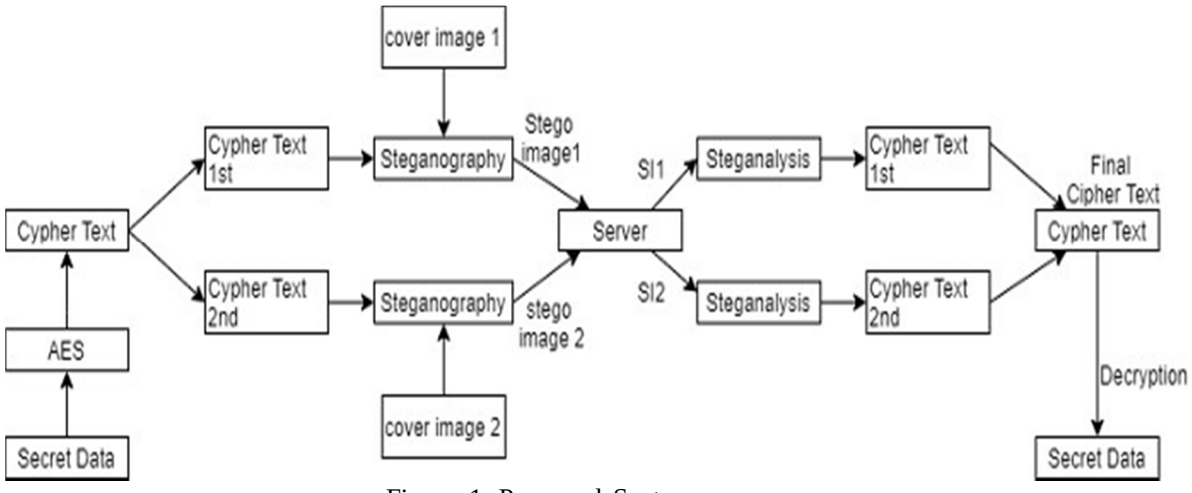


Figure 1: Proposed System

II. LITERATURE SURVEY

1) Covering Image Steganography Using Morphed Face Recognition Based on Convolutional Neural Network Yung-Hui Li1, Ching-Chun Chang2*, Guo-Dong Su3, Kai-Lin Yang1, Muhammad Saqlain Aslam1, and Yanjun Liu3 2022.

a) To improve the validity and proficiency of the image data hiding approach, a piece of state-of-the-art secret A scheme for concealing information transmission based on morphed face recognition is proposed. In our proposed A group of morphed face images is created from an arranged small-scale face image using the data-hiding approach dataset.

b) Then, a morphed face image that is encoded with a secret message is sent to the receiver. The receiver uses powerful and robust deep learning models to recover the secret message by recognizing the parents of the morphed face images. Furthermore, we design two novel convolutional neural networks (CNNs). architectures (e.g., MFR-Net V1 and MFR-Net V2) to perform morphed face recognition and achieved the highest accuracy compared with existing networks.

c) Additionally, the experimental results show that the proposed schema has a higher retrieval capacity and accuracy, and it provides better robustness.

2) Image Steganography: A Review of the Recent Advances

a) Image steganography is the process of hiding information, which can be text, image, or video, inside a cover image.

b) The secret information is hidden in a way that it is not visible to human eyes. Deep learning technology, which has emerged as a powerful tool in various applications, including image steganography, has received increased attention recently.

3) Rateek Kumar Singh, Pratikshit Tripathi, Rohit Kumar, Deepak Kumar, IRJET, Secure Data Transmission, April 2017, Volume 4, Issue 4.

a) Any type of communication over the internet and other network applications needs to be secure due to their increasing utility. For this task, lots of algorithms for security have been implemented and used so far. Up until now, cryptography has been the mainstay for defending secure data transmission. With the increasing threat, steganography has also taken up space for security purposes.

b) In cryptography, we change the natural form of data by using different security algorithms, which leads to increasing the security of the communication process. In steganography, information is kept hidden from the attacker for securely communicating information through the use of images, audio, video, and so on for more We proposed a method for ensuring data transmission security by utilizing both cryptographic techniques, and steganography.

c) In cryptography, we will perform three-level encryption with the use of the AES, DES, and Blowfish algorithms. LSB will be used in steganography to embed the data file in any audio, video, or image. DWT and DCT techniques, and then we will communicate the secure data to the receiver end.

d) In this new research idea, which they explained, the goal was to use the above-mentioned algorithms together to increase the level of security multiple times. The key point of their proposed work is that they can encrypt the data file in any of the desired orders. For eg.

- AES→DES→Blowfish
- DES→AES→Blowfish
- Blowfish→AES→DES, etc. [1]

e) After successfully completing all levels of encryption, they will move on to steganography.

f) In steganography, they will select a video, audio, and image file that is to be merged with the encrypted file. They will now choose the file with the ".blowfish" extension and embed it in the video file. After that, the file will be transferred to the receiver.

4) Dalia Nashat* and Loay Mamdouh, "An efficient steganographic technique for hiding data," 2019.

a) Steganography is a technique for hiding data that aims to hide data in such a way that any eavesdropper cannot detect it. cannot observe any changes in the original media. Image steganography is the most common and widely used method. with reference to other types of steganography least significant bit (LSB) is one of the most public techniques in steganography. The classical technique is LSB substitution.

b) The main idea of this technique is to directly alter some LSB of the cover image with the secret data. The The essential drawback of the available LSB techniques is that increasing the capacity of the stego image leads to decreasing its quality.

Therefore, the goal of the proposed method is to enhance the capacity of high visual quality into consideration.

c) To achieve this goal, some LSBs of the cover image are inverted depending on the secret data for embedding. instead of replacing LSB with secret data. First, the maximum and minimum values in the secret data are determined, then subtract all values of the secret data from this maximum value.

d) The following steps are for hiding secret data (the embedding algorithm) and the steps for retrieving secret data (the extracting algorithm).

In the following, a description of the image used in the proposed method is provided. is given.

- Assume I am any gray image, and consists of a set of pixels $I = P\ 1, ..., PN$. Every pixel is composed of 8 bits:
  $|Pi| = 8$ bits , Pi = b1, ..., b8 , bj g 1, 0
- The image size is computed as
  $$N = H * W$$
- Where H and W are the height and width of the image respectively. Assume M and n are the secret data bits and their length respectively,
  $$M = m1, m2, ..., mn$$
  , where mi g 1, 0 .
- And h is the maximum hiding capacity in image I and computed in terms of bits as
  $$1 \leq h \leq (N * 8).$$

e) Finally, make a division for the results and embed the new results into the cover image to obtain the stego image. The results show that the proposed method gives high capacity and good imperceptibility in comparison with the previous methods.

5) Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, Combination of Steganography and Cryptography: A short Survey, ICSET 2019

a) The establishment of secure communication between two communicating parties is becoming a difficult problem due to the likelihood of attacks and other unintentional changes during active communication over an unsecured network.

b) The security of secret information can be secured using either cryptography or steganography. Steganog- raphy refers to the practice of concealing a message (with no traceability) in a manner that it will make no meaning to anyone else except the intended recipient, while cryptography, on the other hand, refers to the art of converting a plaintext (message) into an unreadable format.

c) Thus, steganography conceals the existence of a secret message while cryptography alters the message format itself. Both steganographic and cryptographic techniques are powerful and robust.

d) Steganography and cryptography have been noted to be individually insufficient for complete information security. Therefore, a more reliable and strong mechanism can be achieved by combining both techniques. Combining these strategies can ensure improved secret information security and will meet the requirements for security and robustness for transmitting important information over open channels.[3]

6) Hussein L. Hussein, Ahmed A. Abbass, Sinan A. Naji, Salam Al-rugby and Jasim H. Lafta, Hiding text in a gray image using mapping technique, IOP Publishing 2018

a) In order to hide the significant and secret message inside a cover object, Steganography is considered one of the most used techniques because of its strength.

b) This paper presents a new steganography technique that is difficult to discover or break by a third party. The ASCII Mapping Technique (AMT) is used to create an encoded table by mapping the text message and matching some bits with that of the cover image.

c) The system saves the character parts matching and the location of which part of the pixels. Then change the related flag from zero to one for matched locations so that they cannot be used again to strengthen the technique and make it more secure.

d) The main idea of the proposed algorithm is to divide each character (8-Bits) of the secret message into two bits and then search the image pixels for the two similar bits in that image (Each pixel in the gray image has 256 gray scales, i.e. in the representation of one pixel in the gray image we need one byte). As an expected result of this method, the probability of finding matching pixels that are in relation to characters of the secret messages.[4]

e) The proposed technique was tested and showed low computational cost with effective performance to be used for multi-purpose applications.

III. METHODOLOGY

Steganography Steganography is the technique for hiding data and aims to hide data in such a way that any eavesdropper cannot observe any changes in the original media. Data hiding has two main branches, steganography and watermarking. The present work focuses on steganography and uses images as the cover for 28 hiding secret data. Steganography conceals the secret data inside the cover image in such a way that no one can even know there is secret data there. Image steganography is common and used most widely in comparison to other types of steganography. This popularity is because images have a large amount of redundant data that can be used to hide secret data easily and because images take into consideration the advantage of the limited power of the human visual system (HVS). In image steganography, the original image is called the cover image, the stego image is the image that results from embedding secret data inside the original image. The cover and stego images should be more similar, so it will be harder for an unauthorized person to know the stego image. – Cryptography Cryptography refers to the act of secret writing through the enciphering and deciphering of encoded messages.

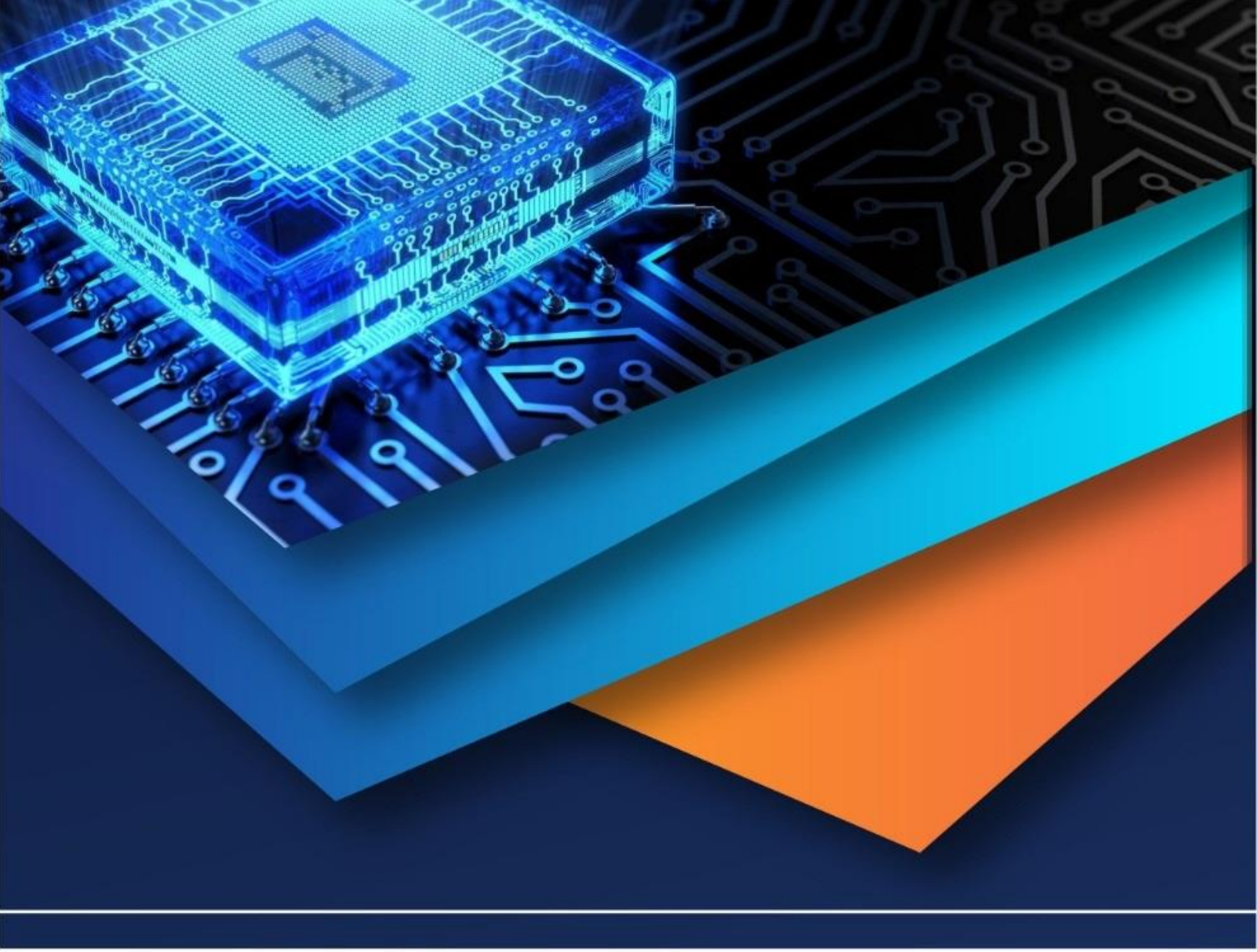
It is evident in situations where two parties establish communication over an insecure medium. a medium that can be easily eavesdropped on. Cryptography is a pool of cryptographic techniques comprising encryp- tion and decryption frameworks, integrity, check functions, and digital signature frameworks. Encryption frameworks alter secret messages into illegible formats for an unauthorized person. while decryption frame- works are used to decode the scrambled message by a person who has authorized to do so. The encryption aspect of cryptography is mainly for the protection of sensitive information and unsolicited alterations. It entails the encryption of stored data information as well as the encryption of the information to ensure secure communication. If an encrypted message is successfully intercepted by an eavesdropper, it will be useless to the attacker because an encrypted message cannot possibly be decrypted. by an authorized per- son. The value of the confidential data obtained from a system is the most essential factor. the thing to the attacker. The data may be compromised, distorted, or even deployed for future attacks by attackers. A perfect way of solving these problems would be to exploit the advantages of cryptographic and stegano- graphic techniques to develop a hybrid system that can be stronger than the individual strengths of the component techniques.

IV. CONCLUSION AND FUTURE WORK

In this project, we are designing a high level of information security without causing any damage to the cover image. using the LSB technique. When we are using the LSB algorithm, there will be fewer chances to lose data. It will be almost impossible for hackers to attack the stego image, as the cover and stego images look similar. In the future, we will be expanding our technique using a generative adversarial network (GAN). came into existence, which helps to generate networks without losing the properties of attributes such as the face. identity and orientation

REFERENCES

[1] Prateek Kumar Singh, Pratikshit Tripathi, Rohit Kumar, Deepak Kumar, IRJET, Secure Data Trans- mission, Volume: 04 Issue: 04 — Apr-2017.
[2] Dalia Nashat* and Loay Mamdouh, An efficient steganographic technique for hiding data.
[3] Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, Combination of Steganography and Cryptography: A short Survey, ICSET 2019
[4] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica ridrich, Ton Kalker," Digital Water- marking and Steganography"
[5] Hussein L. Hussein, Ahmed A. Abbass, Sinan A. Naji, Salam Al-augby and Jasim H. Lafta, Hiding text in gray image using mapping technique, IOP Publishing 2018
[6] Deepesh Rawat and Vijaya Bhandari, Steganography technique for hiding text information in color image using improved LSB method, IJCA 2013. Mehdi Hussain, A survey of image steganography techniques, IJAST 2013
[7] Hamad A. Al-Korbi, Ali Al-Ataby, Majid A. Al-Taee and Waleed Al- Nuaimy, Highly efficient image steganography using Haar DWT for hiding miscellaneous data, JJIT 2016
[8] Nitin Jirwan, Ajay Singh, Dr. Sandip Vijay, Review and analysis of cryptography techniques, IJSER 2013
[9] M. Karolin, Dr. T. Meyyappan, SM. Thamarai, Encryption and decryption of color images using virtual cryptography, IJPAM 2018



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY