Volume: 10 Issue: V Month of publication: May 2022

DOI: https://doi.org/10.22214/ijraset.2022.43647

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 V May 2022- Available at www.ijraset.com

Basic of Secrete Communication System for Military by Using ML and Steganography

Namrata Gawade[1], Aishwarya More[2], Swati Dange[3], Sagar Ingole[4], Shubhra Mathaur[5]
[1, 2, 3, 4]*U.G Student Department of Computer Engineering, Shree Ramchandra College of Engineering, Pune, India*
[5]*Professor Department of Computer Engineering, Shree Ramchandra College of Engineering, Pune,India*

Abstract: Information security is an important factor during transmitting secret information between two objects. Generally, we use cryptography for information hiding and sending secret messages in the form of text. Nowadays, there are several techniques used for hiding information in any medium. One such technique is steganography. In this technique, digital images are used for hiding information and the information is in the form of text, digital image, video or audio file may be used as a secret message. Using LSB Steganography Technique we can implement a high level of information security without any damage to the cover image. In this system we are using the hybrid approach i.e. cryptography and steganography. So, our system has a higher security level than existing systems. With the development of machine learning, face recognition technology based on CNN (Convolutional Neural Network) has become the main method adopted in the field of face recognition security systems to securely access the confidential system.

Keywords: Image data hiding, LSB Steganography, AES cryptography, Face Recognition, Machine Learning CNN technique.

I. INTRODUCTION

Information security is an important facto during transmitting secret information between two objects. As early as in ancient Greece there were attempts to hide a message in trusted media to deliver it across the enemy territory. Generally, we use cryptography for information hiding and sending secret messages in the form of text. In the modern world of digital communication, there are several techniques used for hiding information in any medium. One of such technique is steganography. In which digital media mainly digital images are used as a medium for hiding information and the information in the form text, digital image, video or audio file may be used as secret message. The word steganography derived from two Greek words: steganos means covered and graphos means writing and often refers to secret writing or data hiding. With the development of machine learning, face recognition technology based on CNN (Convolutional Neural Network) has become the main method adopted in the field of face recognition security system securely access the confidential system. Information security plays a major role in any data transfer security can be obtained by information hiding that focuses on hiding the existence of secrete information. In this project we use to provide security and hide information.

II. CRYPTOGRAPHY

The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications. Cryptography: AES is an iterative rather than Feistel cipher. It is based on the ‘substitution–permutation network. It comprises a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix − Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The features of AES are as follows −

1) Symmetric key symmetric block cipher
2) 128-bit data, 128/192/256-bit keys
3) Stronger and faster than Triple-DES
4) Provide full specification and design details
5) Software implementable in C and Java

III.STEGANOGRAPHY VS CRYPTOGRAPHY

Steganography has a critical advantage over cryptography: In cryptography, you know the secret message is there, only its content is concealed; in steganography, the existence of the secret message is often difficult to notice. Threat actors sometimes use the two techniques together, encrypting a message before sneaking it inside a file.

Cryptography is the process used for the conversion of the plain text into cipher text by using the symmetric key and this process is known as the encryption. The main disadvantage of cryptography is that the plaintext can be known and the cipher text is visible but we can‘t read it [4]. Steganography is a method where the plain text is concealed into the digital media .In this process the Trespasser can‘t be able to see the plaintext or the cipher text because it is concealed into the other media. Using LSB Steganography and AES algorithm Technique we can implement a high level of information security without any damage to the cover image. Least Significant Bit (LSB) is a technique in which the last bit of each pixel is modified and replaced with the secret messages data bit. AES has built-in flexibility of key length, which allows a degree of future proofing” against progress in the ability to perform exhaustive key searches. For example, is 128 bits long, meaning, AES is operate on 128 bits of plaintext to produce 128 bits cipher text.

IV.STEGANOGRAPHY PROCESS

Steganography is one way malicious actors fly under the radar. "We often see it being used as the initial entry point, and once the threat actors are in the network, there are more tools and code that they will use to move laterally," Jon Clay, vice president of threat intelligence at Trend Micro, says. Frequently, the secret data is cleverly hidden inside an image by manipulating a few bits. Still, if users look at the original photo and compare it with the altered one, they can't tell the difference. To show this, researchers at Kaspersky camouflaged the first ten chapters of Nabokov's novel Lolita inside the standard image Lenna. The initial photo (Lenna.bmp) and the changed one (Lenna_stego.bmp) look exactly the same to the naked eye. Also, both files are the same size, 786,486 bytes.

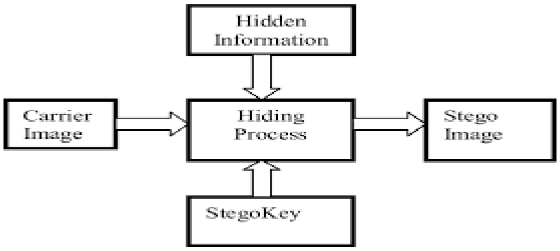


Fig. 1 steganography process

A. Secret Message

The data that you need to insert inside the digital media.. Stego-key: The key used in the Steganography process. Cover Media: The medium utilized in Steganography procedure, for example, picture, video and audio. Sender Algorithm: The technique utilized in this Steganography process. Stego-Media: The media coming about because of including the mystery message into a spread media utilizing Stego-key and encoding calculation. Receiver Algorithm: The technique used to extract the mystery message from Stego-media utilizing stego key.

V. LEAST SIGNIFICANT BIT (LSB)

The well-known strategy that is utilized for steganography is the LSB. And additionally the prominent technique steganography is to utilize LSB of picture‘s pixel data. This investigation is utilized for one piece of the LSB. It inserts each piece of the double content piece with one piece of every pixel in the first picture. This strategy works when the record is longer than the message document and if picture is grayscale, when applying LSB strategies to every bite of a 24 bit picture, three bits can be encoded into every pixel [3] Example: We can use images to hide things if we replace the last bit of every color’s byte with a bit from the message.

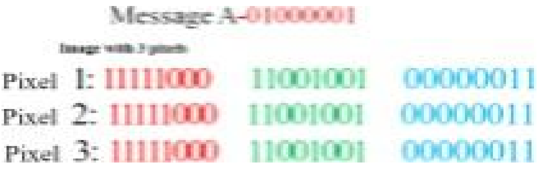
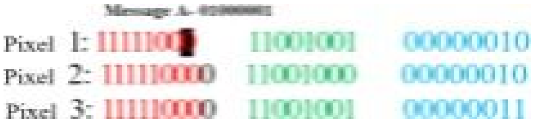

Message A-01000001
Image with 3 pixels
Pixel 1: 11111000 11001001 00000011
Pixel 2: 11111000 11001001 00000011
Pixel 3: 11111000 11001001 00000011

Fig. 2 Message A before encryption

Now we hide our message in the image. Message A- 01000001



Message A- 01000001

Pixel 1:	1111100[illegible]	11001001	00000010
Pixel 2:	11111000	11001000	00000010
Pixel 3:	11111000	11001001	00000011

Fig. 3 Message A after encryption

VI. METHODOLOGY

In this term paper we used the technique that is using the symmetric key between the sender and receiver and by the Least Significant Bit. In this we will also see how the encryption and decryption will be done.
Secure Information Transmission using Steganography and Cryptography using Login Module

A. Sender Side

- Input
- Cover image : Secret Data
- Encryption perform on secret data and divide Encryption perform on secret data and divide encrypted data into two parts
- Two parts of encrypted data is cover by steg image.

B. Receiver Side

- Image extraction perform for un stage the steg image and encrypted
- Merge two encrypted data
- Decryption perform on encrypted message and original message
- It will be displayed to the receiver.

VII. STEGANOGRAPHY USING LSB AND SYMMETRIC KEY

In this framework to the rejection of everything else we need to change over the picture pixels to Binary attributes by utilizing Zigzag Scanning by size=R*S*8 where R is the measure of lines in the picture and S is the count of sections and 8 is the number of bits for each pixel. Eventually to get the last two bits of every pixel where LSB position is 0 and bit before the LSB is 1. While doing this method, meanwhile convert the riddle message (which you need to hide away) into coordinated qualities with size equivalent to1*N where N is the count of bits in the mystery message. Coming about to change over the picture pixels and secret message, straightforwardly we will encourage the mystery message to be two fold bits with the two bits of LSB. There are 3 steps in this process.

- If the confidential message bit equals with 0 th position of the LSB, then the key value will be "0".
- In this process, if the confidential message bit equals with position —1th of the LSB, then the key value will be "1".
- In this process, if the confidential message bit doesn't equals with both position 1 of LSB and position 0 of LSB, by then the key value will be "0".

After this strategy we will get the key. This key will be stego key between the sender and receiver. Without having this stego-key, the receiver won't be able to interpret the confidential data. This stego-key will propose the Position of puzzle data in the stego-picture. This stego-key is basic for this framework. This key is called the Dynamic Symmetric key in light of how the key will be changed subject to the picture. We will utilize the key for this in like manner, the extent of the secret message. By taking this model we will indicate how the encryption and the decryption methods are finished. In the below example I have taken the text as 181 and then I converted the text value 181 into binary value 10110101. Now using this text value I have calculated the key value. This key will be used for the both encoding and decoding processes.

VIII. MACHINE LEARNING: CNN (CONVOLUTIONAL NEURAL NETWORK)

With the development of convolutional neural networks, the achievements made in various competitions are getting better and better, making it the focus of research. In order to improve the training performance of the forward BP algorithm, an effective method is to reduce the number of learning parameters. This can be done by convolution of the spatial relationship of the neural network.

Convolutional neural network, the network structure is proposed, it minimizes the input data pretreatment. In the structure of convolution neural network, the input data is input from the initial input layer, through each layer processing, and then into the other hierarchy, each layer has convolution kernel to obtain the most significant data characteristics. The previously mentioned obvious features such as translation, rotation and the like can be obtained by this method. Convolution neural network basic structure neural network can be divided into two kinds, biological neural network is one of them, and artificial neural network is another kind. Intelligent systems appear more and more in people's lives, and often need to be identified when using intelligent systems. Traditional methods of identification mainly identify individuals with some personal characteristics such as identity documents, such as documents and keys, which have obvious shortcomings. They are easily forgotten, lost or faked. If you use some of the personal characteristics to identify the effect will be quite good, such as: face recognition, fingerprinting and so on. In terms of algorithms, there are sharing parameters between the convolution layer and the convolution layer of CNN.

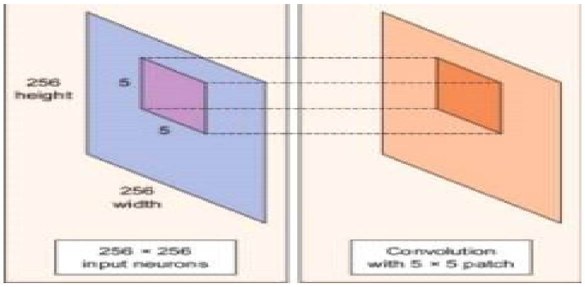


Fig. 4. CNN (CONVOLUTIONAL NEURAL NETWORK)

IX. COMPARATIVE STUDY

Advantages of LSB Steganography

1) Using LSB Technique we can implement high level of information security without any damage to cover image.
2) LSB Steganography has very less MSEvalue(Mean square error) as compared to DWT &Other techniques
3) LSB steganography has high PSNR value as compared with DCT & DWT steganography.
4) As LSB has good performance in terms of MSE& PSNR, it becomes very difficult for hackers tohack the information.

X. CONCLUSION

1) In this project, we are implement high level of information security without any damage to cover image using LSB technique.
2) It will be almost impossible for hackers to attack the stego Image as cover image and stego image looks similar.
3) In this project, with steganography we have also used cryptography i.e. we have first encrypted our text message and divide the cipher text and then embedded it into the image file i.e stego image. This approach helps us to achieve more security, in case anyone intercepts our transmission. Moreover image file is used as a cover medium because we can embed more data into it as compared to other cover mediums.

XI. ACKNOWLEDGMENT

We thank the Management, Principal, Head of Computer Science Department and the Professors of Shree Ramchandra College of Engineering for providing the opportunity. A special thanks to our project Guide and Counsellors for extending a helping hand throughout the process. We would also like to thank our parents and friends for their help and Motivation throughout this project.

REFERENCES

[1] G. Prashanti, K. Sandhyarani, “A New Approach for Data Hiding with LSB Steganography”, Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer 2021, pp. 423- 430.

[2] S. Goel, S. Gupta, N. Kaushik, “Image Steganography – Least Significant Bit with Multiple Progressions”, Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), Springer 2020, pp. 105-112S.

[3] D. Baby, J. Thomas, G. Augustine, E. George, Arseev and L. Mestetsky, "Handwritten Text Recognition Using Reconstructed Pen Trace with Medial Representation," 2020 International Conference on Information Technology and Nanotechnology (ITNT), 2020, pp. 1-4, doi: 10.1109/ITNT49337.2020.9253330.

[4] B. Feng, W. Lu, and W. Sun, “Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture”, IEEE transactions on Information Forensics and Security, Feb. 2020.

[5] M. Nusrati, A. Hanani and R. Karimi, “Steganography in Image Segments Using Genetic Algorithm”, 5th IEEE International Conference on Advanced Computing & Communication Technologies (ACCT), Feb 2019 pp. 102-107.

[6] N. A. Al-Otaibi, and A. A. Gutub, “2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers”, Lecture Notes on Information Theory, June 2019, pp. 151-157.

[7] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain, “An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography”, IEEE International Conference on Informatics, Electronics & Vision (ICIEV), May 2019, pp. 1-6.

[8] K. Qazanfari and R. Safabakhsh, “A new Steganography Method which Preserves Histogram: Generalization of LSB++”, Elsevier International Journal of Information Sciences, Sept. 2019, pp. 90-101.48