International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 12 | Dec 2022 www.irjet.net p-ISSN: 2395-0072

MESSAGE TRANSFER USING STEGANOGRAPHY

Hrushikesh Kale[1], Meera Keshattiwar[2], Mrunal Patil[3], Aakanksha Shinde [4]

[1]Hrushikesh Kale
[2]Meera Keshattiwar
[5]Professor P.P.Mahale, Dept. of Information Technology, Aissms IOIT Pune, Maharashtra, India

---

Abstract -Steganography is used to hide information like text, images, videos in other media files like images, videos, music. We can use steganography to transfer messages from one host to another securely. Nowadays we cannot trust the server side to encrypt our messages end to end as the server side knows the keys of both the sender and receiver. Using steganography, we can make sure that the server does not decrypt and store our messages in plain text. We can secure our messages from server side and intruders also. In steganography we store our secret data into the least significant bits of the pixels. Storing data into the least significant bits does not affect the image that much as the values of the pixels change slightly. We can use different techniques to cipher data into images like sequential, prime and equations ciphering. To decipher such an image the intruder has to check for all the combinations of pixels which increases the time complexity of this task to exponential. Using this technique we can protect our messages not just from intruders but also server side proxy attacks. In this method the sender and receiver mutually decide some keys which will be used to cipher and decipher data from images. The user only needs to remember two keys, the starting point and the method used to cipher data into the image.

Key Words: ***Data Hiding. Steganography, Cyber Security, Cryptography, Data Security***

1. INTRODUCTION

In the present situation, secret messages may be conveyed by concealing them in a picture or text so that only the sender and the recipient can read or see them. Data concealing and revealing is referred to as steganography. Because it conceals the secret message, the picture that hides the data in steganography is known as the cover image. After the data has been hidden, the image is known as the stego-image. For embedding data in a cover file, LSB insertion is a highly well-liked and often used technique in steganography. According to the LSB embedding approach, data can be concealed in the LSBs of the cover file so that even the human eye cannot detect the concealed information. It is an approach in the spatial domain. Steganography is a way of hiding text in pictures such that if an intruder finds the secret message, it cannot be read by the intruder. So, using steganography will add an extra degree of protection. Image compression is used to minimise the size of a message so that it may be easily hidden. Image compression is a critical application in the field of Digital Image Processing.. We can secure our messages from server side and intruders also. In steganography we store our secret data into the least significant bits of the pixels. Storing data into the least significant bits does not affect the image that much as the values of the pixels change slightly. We can use different techniques to cipher data into images like sequential, prime and equations ciphering. This is one of the safest way to share confidential information.

1.1 Need of the Topic

It is one of various data hiding techniques, which aims at transmitting a message on a channel where some other kind of information is already being transmitted. This distinguishes steganography from covert channel techniques, which instead of trying to transmit data between two entities that were unconnected before. Steganography is defined by Markus Kahn as follows, “Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity”. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present”.

2. LITERATURE SURVEY

[1]. Osama Fouad Abdel Wahab, Ashraf A. M. Khalaf, Aziza I. Hussein, Hesham F. A. Hamed,“Hiding Data Using Efficient Combination of RSA Cryptography and Compression Steganography Techniques”, IEEE Issue:2021,

Image compression is a useful technology that helps save memory space and time while transferring images over a network. This helps to increase storage capacity as well as transfer speed.

[2]. Nandhini Subramanian ,Omar Elharrouss , Somaya Al-Maadeed, Ahmed Bouridane , “Image Steganography: A Review of the Recent Advances” , IEEE , Issue:2021.

Image steganography is the method used in transmitting secret information by hiding it in plain sight inside a cover image. Deep learning methods are widely used in every field and has been used in the research of steganography. Review of all the related works led to categorizing them into three

groups vastly. Most of the traditional based steganography methods use the LSB substitution and some of its variants.

[3]. Asha Durafe, Rutika Desai, "Steganography for Public Security", IEEE , Issue:2020,

In a nutshell, secure transmission of data is the rising concern with the advancements in technology. Steganography has its own pros and cons but is a better choice for sending secret information from one point to another without getting detected.

3. METHODOLOGY

By exchanging private keys, the two clients may begin communicating with one another. The clients will be able to decode the incoming messages using the key. A client encrypts the private key into an image using a predefined location and ciphering algorithm in order to transfer the private key. The other client may extract the private key from the picture and use it to decode messages using the known location and scheme. Therefore, our technique uses steganography to implement a key exchange. The technique for encoding data into pictures is based on changing a pixel's bits. Alpha, red, green, and blue bytes each contain at least two significant bits, which together make up one byte of information per pixel. One significant drawback of changing only the pixels that contain data is that there will likely be differences in the neighboring pixels, which may make it simpler to analyze the image. A user's private key may be made public due to this flaw, which could lead to message interception. In order to get around this issue, we will also change the random and nearby pixels in images to make steganalysis challenging. For an image to be decoded, a client needs to know the location of the first pixel and the ciphering technique that was used to encrypt the data. Voice messages, hints, or other tangible media can be used to communicate this information between individuals. The benefit of this strategy over the exchange of lengthy, complex keys is that there is less, simpler information to remember.

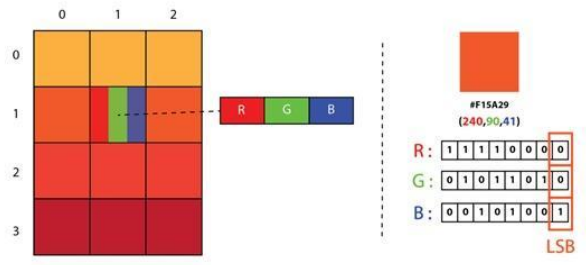

Figure 1 How pixel is represented as an integer

We use bitwise operators like &, —, and! to modify a pixel's bits using bit-wise operations. As a result, the bits in the required position can be changed to match the bit in the data. We may simplify this process by generating a stream of bits from the secret data, which we can then use to determine which bit in the cover picture needs to change next. We use a queue-like data structure to store the pieces of secret data, thus this operation has some overhead. Additionally, large files increase the amount of time needed to distort an image before encrypting it. High security is provided, but at the expense of computing power. The image in the above image has a total of w*h pixels, where w is the image's width and h is its height. With a slight modification to the n-queens solution, we may attempt to decode the image using the information from the n-queens issue. We may choose any of the remaining pixels to be the next data point because this is not a pursuit.

3.1 ALGORITH USED

[1] Data Cipher: The least significant bit algorithm is being used to encrypt data into graphics. In this process, data is transformed into a queue of bits, which are then inserted into the picture at the proper places. The location of the pixel and the chosen scheme dictate the order of the bits where data is ciphered. The user has previously communicated these two things via a vocal channel.

[2] Camouflage Data: There is a chance that someone will be able to detect a change in the adjacent pixels of a picture when we alter its pixels.The key may be taken out of the image using this information. We get around this issue by making random modifications to picture pixels such that the read change blends in with other changes.

[3] Data Decipher: Using the initial pixel's location and the scheme, the information contained in the least significant bits is decoded. Depending on the ciphering system employed, the data are stored in a certain sequence. A 16 bit integer is put at the beginning of the data to indicate the length of the data. In the initial stage, we take the image's first 16 bits and transform them to an integer. The content's length, as ciphered in the picture, is this. We begin to extract the real information from data after extracting the content length. The ciphering algorithm employed determines exactly where the bits and pixels should be placed.

[4] Key Exchange Algorithm: A key exchange algorithm based on steganography is used between two clients to exchange keys. A user creates a public key and a private key, and then sends the public key to another user. Data is encrypted by one user using the public key of another user, who subsequently receives the encrypted data.

Symmetric key cryptography is another tool we may utilise to speed up communication. But compared to symmetric key cryptography, asymmetric key cryptography provides greater security.

4. ARCHITECTURE OF STEGANOGRAPHY

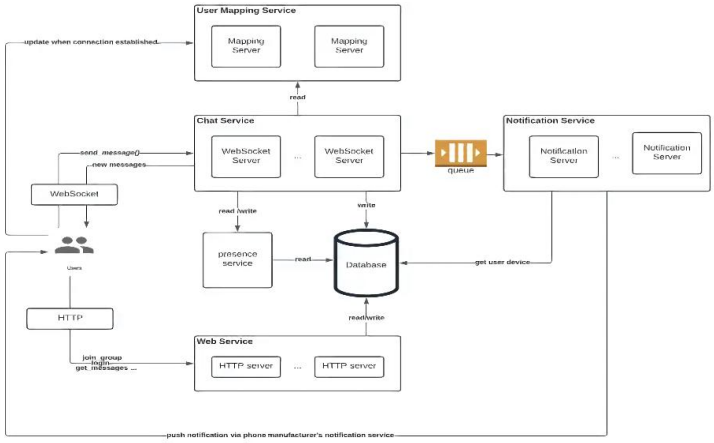

Figure 2. Architecture of web application

The figure above illustrates the processes of encoding secret text as a picture and extracting secret data from the image. It contains the cover picture, the secret data, and the key required for both ciphering and deciphering the data from the image. The architecture of the steganography process may be used to get an overview of the process of encrypting data into images. We first want a cover picture that will conceal data. The size of the cover picture utilised determines how effective the algorithm is. The process of decoding will be extremely difficult and time-consuming if the image is vast since there will be several ways to interpret it. Once data has been concealed in a picture, the image must be sent to the other end over a channel, which may or may not be secure. The message is unaffected by the channel's security since the data is concealed inside the cover picture, making it unclear to attackers whether a message is being sent or not. The user has to know the initial pixel from which the ciphering process began and the technique that was employed to encrypt the data into the image in order to decrypt the image. The attacker is free to test any potential pairing of the message's decoding sites and techniques. To grasp what the text means, this step must be done manually or with the aid of a deep learning neural network. However, in practise this task is all but impossible because there are an infinite number of combinations of places and methods that may be used. An picture with a width and height of 7 pixels, for instance, has 823543 potential permutations. However, in practise, we may utilise photos that are considerably larger. If we use a picture with dimensions of 100 by 100, the number of deciphering combinations is about 1, with 30000 zeroes after that. As was said before, the size of the picture has a significant impact on how strong the algorithm is; as image size rises, algorithm strength increases exponentially.

5. CONCLUSIONS

The Steganography can be used in various applications for securing the identity of data. One way is to use steganography in secure messaging applications in which the keys are transferred using steganography. By using our proposed model for exchanging data we can transfer data secretly not just from external intruders but also server side decryptions. In most messaging applications the server side can easily decrypt messages using decryption keys. Using the system we have proposed any intruder or attacker will have to check all the combinations of keys from the image. The time complexity of deciphering the keys from the image is exponential. Also while deciphering the image the attacker needs to check if his/her decipher is successful or not manually or using some kind of intelligent algorithm. The time complexity of such an operation is quite high. Using very little information from clients we can share large data from one client to another and vice versa . If the size of the image is n*m then the time required for deciphering is exponential to the number of pixels in the image.

REFERENCES

[1] Osama Fouad Abdel Wahab, Ashraf A. M. Khalaf, Aziza I. Hussein, Hesham F. A. Hamed, “Hiding Data Using Efficient Combination of RSA Cryptography and Compression Steganography Techniques”, IEEE, Issue:2021.

[2] Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, Ahmed Bouridan e , “Image Steganography: A Review of the Recent Advances” , IEEE , Issue:2021

[3] Asha Durafe, Rutika Desai, “Steganography for Public Security” , IEEE , Issue:2020.

[4] Ali Salem Ali, Mohammed Sabbih Hamoud Al-Tamimi, Alaa Ahmed Abbood, “Secure Image Steganography Through Multilevel Security”, International Journal of Innovation , Creativity and Change, IJICC , Issue:2020.

[5] manshu Arora, Cheshta Bansal, Sunny Dagar,”Comparative study of image steganography techniques” , International Conference on Advances in Computing, Communication Control and Networking, Issue : 2018

[6] Ammad Ul Islam1 , Faiza Khalid2 , Mohsin Shah2 , Zakir Khan2 , Toqeer Mahmood3 , Adnan Khan2 , Usman Ali2 , Muhammad Naeem4 , “An Improved Image Steganography Technique based on MSB using Bit Differencing” , The Sixth International conference on Innovative computing technology,Issue : 2016

[7] Ravi K Sheth,Rashmi M. Tank , “Image Steganography Technique”, Academia , Issue:2015

[8] Manveer Kaur , Gagandeep Kaur, “Review of Various Steganalysis Techniques”,IJCSIT, Issue:2014

[9] Abdalbasit Mohammed, Nurhayat Varol,"A Review Paper on Cryptography ", Research Gate , Issue: 2019

BIOGRAPHIES

Hrushikesh Kale
BE-IT
AISSMS IOIT,Pune

Meera Keshattiwar
BE-IT
AISSMS IOIT,Pune

Mrunal Patil
BE-IT
AISSMS IOIT,Pune

Aakanksha Shinde
BE-IT
AISSMS IOIT,Pune

Prof. Pragati Mahale
Department of Information Technology
AISSMS IOIT,Pune