IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Multi-layered Security System for Secure Transmission of Trade Secrets

T.R. Priyadharshini, N.Saranya

[1] Assistant Professor, Department of Information Technology, Hindusthan College of Engineering and Technology,Coimbatore.

[2] Assistant Professor, Department of Computer Science and Business System ,Bannari Amman Institute of Technology, Erode.

***Abstract*—Image steganography are one of the most powerful and commonly used as well as secure forms of steganography methods available today. A method or process of hiding a secret message within a different media or message is called Steganography. There are plenty of algorithms available to implement image steganography each having certain advantages and few flaws in them. In our paper, a new approach is proposed for bringing in three stages of security to enhance the earlier methods of steganography Based on k-LSB embedding algorithm, a k-LSB-based method that is proposed using fixed k least significant bits to hide the information in an image and also to extract the inserted information from that stego-image. The proposed method ensures that there is very less image quality degradation, working well with different image formats and to provide a better security level.**

***Keywords*—Image Steganography, LSB, Multi-level security, Multiple image formats**

I. INTRODUCTION

The world is growing at a very high pace each day in terms of economy as well as technologies. A human's life is more and more getting attached to data around him. The data is playing the most important and major role in the world of information and technologies. As we get more attached to data there is more and more security issues and data hijacking that we are going to be dealt with. So, it has become a necessity to keep our data safe. Security technologies are needed to get stronger from threats and hacks. Steganography is one such security method to keep our data safe from intruders. Steganography is a method developed under the concept of cryptography to safeguard our important data or information.

The cryptography and steganography are the two faces of a coin where the steganography will hide the traces of communication while cryptography uses technique for encryption to make the message secured. It is a practice where a secret message can be hidden into a normal message. The secret message can be a text, video, audio or image which can hidden into similar format files. We have certain types of the steganography such as Image steganography which is the most commonly used form of steganography. Here a textual message or an image format message can be hidden inside an image. Any person will not be able to read or find what data has been hidden inside the image byseeing with a naked eye. Then there is text steganography, audio steganography and video steganography where message is hidden inside the text, audio or video respectively. In this project we are implementing the image steganography for hiding our textual secret message.

There are various different algorithms developed and being developed to implement the image steganography process. Few of the popular embedding algorithms or methods used are LSB (least significant bit), DWT(Discrete wavelet Transform), DCT(Discrete Cosine Transform**)**, DFT(Discrete Fourier Transform), Pixel value differencing, BPC (binary pattern complexity), Spread spectrum and much more. In this project we are implementing the LSB method for implementing image steganography. Each algorithm or approach have their own pros and cons, few may have better security features, some may have lesser image quality degradation, some may be complex and some may be easy to implement. It depends on what application and what data we are going to work with. In our proposed method we have added two more levels of security in order to ensure the protection of the data from hackers. The proposed system is designed in such a way to accept images with different formats (jpeg, png, bmp, jpg, gif).

We have used substitution cypher which is an algorithm or a method to encrypt an information or a message into cypher text with the help of a key. This will be entry level security feature added in the system before going into the steganography part where we will be hiding our message into an image using the LSB algorithm.

II. EXISTING WORK

There are mainly two common methods for hiding data, which are broadly classified into two types known as spatial-domain and frequency-domain methods. In the spatial domain method complete secret information or message is inserted directly into the last bits or least significant (LSB) bits of image(pixels). On the other hand frequency-domain technique, transformation of image from the spatial domain to a frequency-domain is done initially using common transformation methods like discrete wavelet transform(DWT), discrete cosine transform (DCT) and/or discrete Fourier transform (DFT). These were the earlier methods or algorithms used to implement the image steganography process. After transforming, the message is then embedded or hidden in the coefficients transformed, and finally at the end the data is transformed back from the frequency-domain to the spatial domain.

Even though these methods we successful in implementing the steganography practice, it increased the complexity factor while actually implementing for an application, since it is widely deployed algorithm it is easier for a hacker to gain the knowledge about the algorithm and use that knowledge to decrypt our information. These methods also had certain issues in depleting the image quality and needed some added image quality enhancement algorithm to bring back the image's original quality which brings even more complexity to the system. Even after showing a good performance in certain format images, The algorithm could not hold the same for different formats such as jpg or gif.

There are various different methods to externally encrypt the hidden steganographic secret message or the data, like permutation, a statistical threshold and/or by using some of the cryptographic algorithms.

III. PROPOSED METHOD

In order to provide all the existing advantages of previous implemented methods and some added improvements, we have focused to make the whole system simple to use, provide more security, lesser image quality degradation, and acceptability of various image formats.

The proposed method is built with keeping in mind the security as a major factor. The system consists of three modules or stages to provide to multilevel security feature. The first level of security is by bringing in a cryptographic algorithm to encrypt our plain text (i.e., secret message). This step is going to convert our secret message into a cypher text and will be provided with a key, so that later when the receiver wants to view the message, he can use this key to decrypt the message. For implementing this feature, we have used an cryptographic algorithm called the substitution cypher. This stage can be modified later by replacing the algorithm by a better cryptographic algorithm

based on the security level needed. After getting a cypher text or an embedded message we move into second module or level of the system. This is the core module of the entire system where we will be actually implementing the image steganography method. The embedded message will now be hidden or encrypted into an image. For implementing this process, we use the spatial domain methodology. We used the Least Significant Bit(LSB) algorithm for encrypting the secret message into image. The algorithm proposed works by modifying the least significant bit of the image with the bits of message to be hidden.

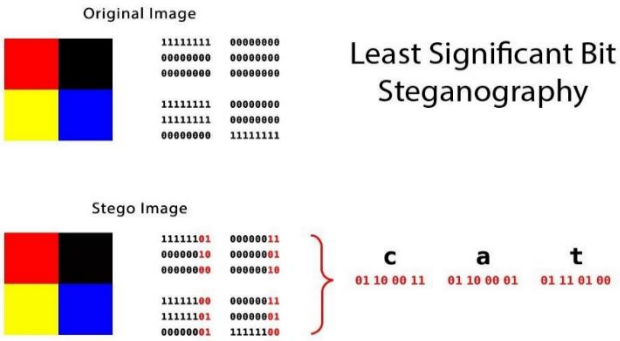

Fig.1 LSB approach

By modifying only, the last bits i.e. most right bit or least significant bit of the image we are embedding our secret message and it also makes the picture unnoticeable, but if the message length is high it starts modifying the second the second least significant bit and so on.

At this stage we will be having a stego-image which contains the secret message in it in a cypher text form. From this stage the stego-image or the encrypted image will move into the final stage of the system. This stage does not consist any algorithm implemented. The stego-image received from stage two is mixed or shuffled with a large number of other images which are not embedded with our desired secret message, but still some images may contain any other duplicate or unwanted message in it for making it hard for the hackers to find which is actually the right message. At the end of this stage, we will be having a folder with a large number of images with our stego-image which has our secret message in it. This folder can be now sent through an private or public channel depending on how important information being transferred. The sender will be sending a key which will be used to decrypt the cypher text into plain text. There is another key which will be already present at the sender and receiver before the communication occurs which can be used to find the right image which will have the desired secret information in it.

The proposed method has added advantages where it can support multiple image formats such as jpeg, jpg, png and gif. It also reduces the complexity in implementation and allows us to bring future modifications at ease. Even though it has a small amount of image quality degradation, it is difficult for a normal human to predict that change.

IV. IMPLEMENTATION

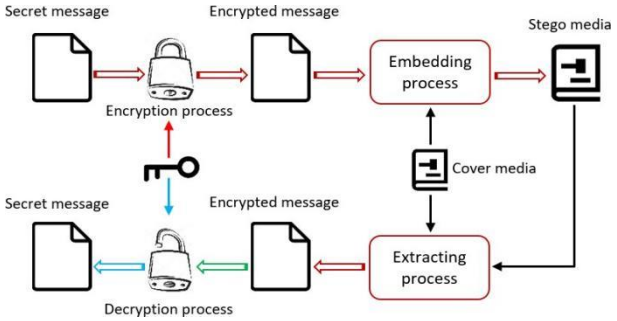

Fig.2 Implementation approach

A. Encoding

For the encoding process we need to input two things. Firstly, the message, which is to be embedded, which in our case is in encrypted form (for additional security) and lastly the cover image in which we will embed our encrypted message.

The application supports all type of image formats (jpeg, png etc.) for the selection of our cover image. (We use a well suited LSB method for embedding the secret encrypted message in our cover image by replacing the lower significant bits of our cover image by the message bits. By using this LSB method for embedding our message the quality of our stego-image is intact as the lower significant bits does not affect the majority of the quality. The output stego-image of our encryption process can be given with any filename and can be stored anywhere in the computer memory. By default, our stego-image is with .png file extension.

B. Decoding

For the decoding process we need to select the stego-image in which we had our encrypted message. After selecting the stego-image the decoding process has similar steps as that in encoding but in reverse order. As a final result of our initial application. Later we provide our obtained encrypted message to the final decoding program which decodes our message and we get our intended original message(or text).

The user interface is going to loos like this:

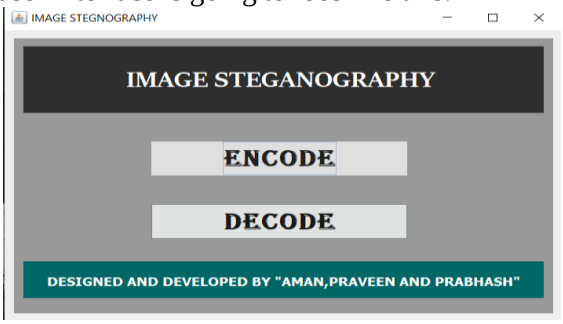

Fig.3 Home Page of the system

We have options listed to perform desired operation, and can type in the secret message and select the image where the secret message will be embedded. After encrypting the message into image we will try to store it in a particular location or a folder where we have a number of already existing images.

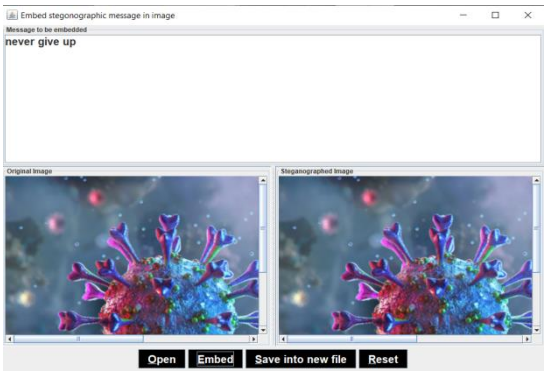

Fig.4 Encoding

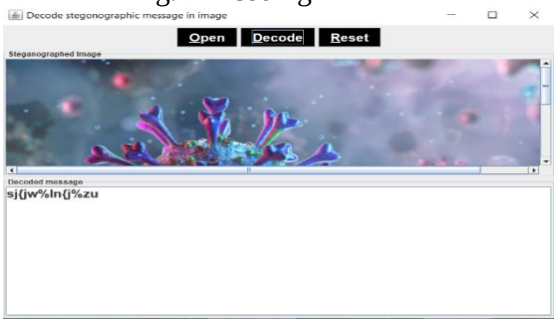

Fig.5 Decoding Encrypted message

For decoding the same steps are following by clicking in the decode button and selecting the image which consists the secret message in it, for this process the receiver will be using a key which already shared by sender to find the right image which has the desired information out of the batch of images. At the end the user will have to use the key shared by the sender to decrypt the cypher text.

V. RESULTS

This paper consists of an image steganography method that is been used for hiding data(mainly text) into an image file. The file format of image that can be used in our application for producing stego-image (encoded image) constrained to 24 bit depth colour space and even the file formats can be *.jpeg, *.jpg, *.gif, *.png. the method of Lossy compression which takes less time to encode and decode comparatively, are been used for file formats like JPEG, whereas the formats of GIF and PNG the lossless compression is used which comparatively takes more time. In our project we tried different file formats like BMP, JPG, GIF, PNG, JPEG, etc. formats. The Table I shows the evaluation of encoding on image with different formats and encoding time has been noted down as observed.

TABLE 1
EFFICIENCY OF ENCODING DIFFERENT FILE FORMATS

FileFormat	Parameters for Simulation		
	File Size (inKilobytes)	*Time for Encoding (innanoseconds)*	*Sizeafterstoring (inKB)*
JPG	32	108358986	33
BMP	483	105029337	483
JPEG	32	108569893	33
GIF	135	174988345	104
PNG	320	159087611	435

The Table 1 shows the result of the program on various colour images of 24-bit depth file formats on the basis of reduction in file size and time for encoding. The Table 1 also includes the size of the file before and after encoding that is, with and with payload respectively.

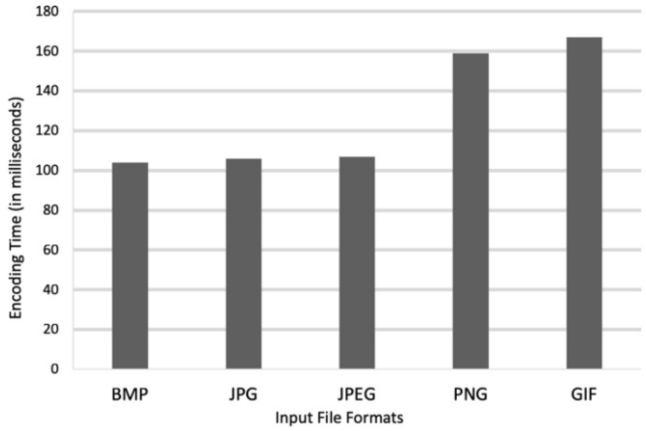

Fig.6 Graph of different file formats of 24-bit depth colour images vs. speed of encoding

When smaller payloads are used , GIF was found as best option because of the reduction in the file size eliminates all the overheads. But the same format does not suite for the large payloads as the delay in its encoding time. Most efficient in the list are JPG and JPEG which could be ideally used for creating cover files.

VI. REFERNCES

[1]Jiayu Den and Zhen Wang. IEEE: https://ieeexplore.ieee.org/document/9064335 , 2019.

[2]S. Sachdeva and A. Kumar. IEEE: https://ieeexplore.ieee.org/document/6168380 , 2015.

[3]Rashad J. Rasras, Ziad A. AlQadi https://www.researchgate.net/publication/331230479_A_Methodology_Based_on_Steganography_and_Cryptography_to_Protect_Highly_Secure_Messages#:~:text=Abstract,data%20hiding%20and%20data%20extracting. , 2019.

[4]Bingwen Feng. IEEE: https://ieeexplore.ieee.org/document/6949122 , 2017.

[5]Arnold Gabriel Benedict. IEEE: https://ieeexplore.ieee.org/document/8816946 ,2019.

[6] Technique of LSB in image steganography: https://www.cybrary.it/blog/0p3n/hide-secret-message-inside-image-using-lsb steganography/#:~:text=LSB%2DSteganography%20is%20a%20steganography,of%20message%20to%20be%20hidden.

[7] Singh and Singh A., Himmat Chauhan, 2015, March. An improved LSB based image steganography technique for RGB images. In 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) (pp. 1-4). IEEE.

[8] K.A. Al-Afandy , O.S. Faragallah, A. ELmhalawy, El-Rabaie, El-Banby, G.M., 2016, October: High security data hiding using image cropping and LSB least significant bit steganography. In 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt) (pp. 400-404).IEEE.

[9] Naveen Patel and Meena Sudha, 2016, November. LSB based image steganography using dynamic key cryptography. In 2016 International Conference on Emerging Trends in Communication Technologies (ETCT) (pp. 1-5). IEEE.

[10] Rama Chandramouli, Nalini Memon, ”Analysis of LSB based image steganography techniques”, Proceedings of International Conference on Image Processing, vol. 3, 2001, pp. 1019-1022.

[11] Walt Bender, Dongo Gruhl, Netin Morimoto, and Ani Lu in 2016 published a research paper on : “Techniques for data hiding ” IBM Systems Journal, vol. 35, no. 3.4, 1996, pp. 313–336.

Archana Bhise and Anjana Rodiges published a research on “Reversible image steganography using cyclic and dynamic cover pixel selection” in 2017in an international conference for wireless communication and signal processing.

[12] Dr H Shaheen, “A Pervasive Multi-Distribution Perceptron and Hidden Markov Model For Context Aware Systems”, “The Journal of Research on the Lepidoptera “. June 2020 ISSN 0022-4324 (print) ISSN 2156-5457 (online) , Volume 51 (2): 818-833