International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT2063191

Image based Steganography in Cryptography implementing different Encryption-Decryption Algorithm

Pinky Saikia Dutta, Sauvik Chakraborty

Computer Science and Engineering, Girijananda Chowdhury Institute of Management and Technology, Guwahati, Assam, India

ABSTRACT

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. Steganography techniques can be applied to images, a video file or an audio file. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. 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 both with concealing the fact that a secret message is being sent and its contents. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol.

Keywords : Cryptography, Steganography, LSB, RSA Encryption, Decryption

I. INTRODUCTION

Steganography is the technique of hiding private or sensitive information within something that appears to be nothing be a usual image.[1] Steganography involves hiding Text so it appears that to be a normal image or other file. If a person views that object which has hidden information inside, he or she will have no idea that there is any secret information. What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them.[2] What this system does is, it lets user to send text as secrete message inside an image file, user uploads the image and enters the text to send secretly, and gives a key or a pass word to lock the text, what this key does is it encrypts the text, so that even if it is hacked by hacker he will not be able to read the text. You will need the key to decrypt the hidden text. User then sends the image and key to the receiver and receiver first opens the image, and then he enters the key or password for decryption of text, he then press decrypt key to get secret text of the sender.[4] By using this method you can double ensure that your secret message is sent secretly without outside interference of hackers or crackers.[4] If sender sends this image in public others will not know what is it, and it will be received by receiver. In our proposed system we will develop a project where we implement encryption algorithm LSB (Least Significant Bit) to embed a secret message within an image file. Later in the receiving end it will decrypt with the key provided with the Stego object.

II. TYPES OF STEGANOGRAPHY

1. **TEXT STEGANOGRAPHY**:

Hiding important information in a text file is the method of Steganography. The method was to hide a secret message into a text message.[1]

2. **IMAGE STEGANOGRAPHY**:

Images are used as cover medium for steganography. A message is embedded in a digital image using algorithm and the secret key.[1]. The image selected for this purpose is called the **cover-image** and the image obtained after steganography is called the **stego-image.**

3. **AUDIO STEGANOGRAPHY**:

It is used to embedding data in cover speech in a secure and robust manner. An audible, sound can be inaudible in the presence of another louder audible sound.[1]

4. **VIDEO STEGANOGRAPHY**:

Video Steganography is a technique to hide any kind of files in any extension into a carrrying Video file.[1]

III. CRYPTOGRAPHY

The field of cryptography has a rich and important history, ranging from pen and paper methods, to specially built machines, to the mathematical functions that are used today. In this paper only brief discussion that is essential for knowledge transfer has been presented[2]. Cryptography is similar to writing a letter in a secret language: people can read it, but won't understand what it means.[2] However, the existence of a (probably secret) message would be obvious to anyone who sees the letter, and if someone either knows or figures out your secret language, then your message can easily be read.

IV. DIFFERENT CATEGORIES OF ALGORITHMS USED FOR ENCRYPTION AND DECRYPTION IN THE STEGANOGRAPHIC OPERATIONS

There many advanced algorithm proposed among them I image steganography mostly practised algorithm is LSB(Least Significant Bit). And some others are RSA, AES etc.

RSA Algorithm : RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in our PGP and GPG programs.[2] Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You've got your public key, which is what we use to encrypt our message, and a private key to decrypt it. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers quite a bit of time and processing power to break. [2]

AES Algorithm : The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations. Although it is extremely efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy duty encryption purposes. AES is largely considered impervious to all attacks, with the exception of brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher. Still, security experts believe that AES will eventually be hailed the de facto standard for encrypting data in the private sector.

LSB : The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit.[3] As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. LSB (least significant bit) array based image steganographic technique using encryption by RSA algorithm is proposed. LSB stands for Least

Significant Bit. The idea behind LSB embedding is that if we change the last bit value of a pixel, there won't be much visible change in the color.[3] For example, 0 is black. Changing the value to 1 won't make much of a difference since it is still black, just a lighter shade.

IV.I Data encoding procedure

- Convert the image to greyscale.
- Resize the image if needed.
- Convert the message to its binary format.
- Initialize output image same as input image.
- Traverse through each pixel of the image and do the following:
  - Convert the pixel value to binary.
  - Get the next bit of the message to be embedded.
  - Create a variable temp.
  - If the message bit and the LSB of the pixel are same, set temp = 0.
  - If the message bit and the LSB of the pixel are different, set temp = 1.
  - This setting of temp can be done by taking XOR of message bit and the LSB of the pixel.
  - Update the pixel of output image to input image pixel value + temp.
- Keep updating the output image till all the bits in the message are embedded.
- Finally, write the input as well as the output image to local system.

IV.II. Extraction Process (Decryption) :

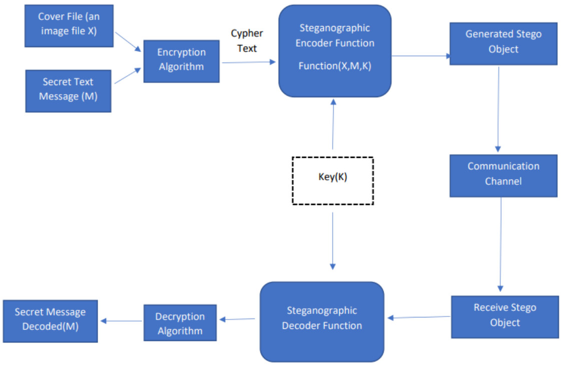
The extraction process is simple. We need to first calculate how many pixels is the text stored in. For example, the text "Secret Message" has 14 characters. Each character is represented in 8 bits. So, the number of pixels in which the text is stored will be 14 * 8 = 112. Now after knowing this, we need to traverse through the image, one pixel at a time. We store the Least Significant Bit (LSB) of each pixel in an array extracted_bits. After extracting the LSBs of the required pixels, we need to take every 8 bits from extracted_bits and convert it to the corresponding character. In this way, the text stored in the stego image can be extracted.

V. OUR APPROACH

After a lot of research, we have find that there are many advanced methods has been used for image steganography. But the mostly used method is LSB(Least Significant Bit) so we have decided to use this method in our project. In this method, it does not directly replace the LSB of cover image with the secret bit instead it check the matching between secret bit and LSB of the cover image.[3] If the secret bit does not match the LSB of the cover image, then +1 or −1 is randomly added to the corresponding pixel value.[3]. As far our research there are various encryption algorithm are there but the mostly used algorithm for encryption is RSA. So we have decided to use this algorithm in our project to encrypt the secret message.

RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. [2]

Here is our model of the Project where it is explained clearly how our system is working:



Cover File : It can be Image , Audio, Video file to cover up the secret message M. The secret message will be hide inside the cover object or image file.

1. **Encoder Function(funct(X, M, K)):** This a process to encode the message (M) inside the cover file X and then this encoder will generate a secret stego Key K which will be send to the receiver end. This embed key through which receiver will extract the message covered inside an image. Key will provide extra security to the message.
2. **Stego Object:** Steganographic embedding process generate Stego Object using kind of Algorithm as LSB and RSA. This stego object as looks exactly like covered object. It is the process of encryption.
3. **Communication Channel :** Stego object send to receiver through a proper secured network channel.
4. **Steganographic Decoder :** From the network the stego object will be received at the end and this decoder will decrypt the stego object and extract the secret message without any distraction.

VI. CONCLUSION

A new approach is proposed which gives good quality of the image after encoding the original image by using the LSB technique and RSA Encryption-Decryption Algorithm. Here we encrypt the data using the RSA algorithm after encryption a stego image is generated if the third party get the stego image it cannot be decrypted without the personal it will show the image in encrypted form. These method helps us to increase the security level of the data that is embedded in the image. After embedding the data in the image the quality of image will not be affected. A normal human being cannot identify that a sensitive data is embedded in the image. This increase the security of the data.

VII. REFERENCES

[1]. Munesh Kuma and Gaurav Yadav(2017) Image Processing using Steganography. International Journal of Engineering Science and Computing(April 2017).

[2]. Rituparna Halder and Susmit Sengupta (2016) A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique. Journal of Computer Engineering. www.iosrjournals.org (Jan-Feb 2016). e-ISSN: 2278-0661,p-ISSN: 2278-8727 DOI: 10.9790/0661-18143943.

[3]. S. Uma Maheswari and D. Jude Hemanth Karunya University(2015) Different methodology for image steganography-based data hiding: Review paper. International Journal of Information and Communication Technology(January 2015).

[4]. Dr. Mahesh Kumar, Munesh Yadav(2014) Image Steganography Using Frequency Domain. International Journal of Scientific & Technology Research www.ijstr.org(September 2014). ISSN 2277-8616.

Cite this article as :

Pinky Saikia Dutta, Sauvik Chakraborty, "Image based Steganography in Cryptography implementing different Encryption – Decryption Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 3, pp.745-748, May-June-2020. Available at

doi : https://doi.org/10.32628/CSEIT2063191

Journal URL : http://ijsrcseit.com/CSEIT2063191