ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW ON VARIOUS TECHNIQUES OF STEGANOGRAPHY TO HIDE THE DATA INTO DIGITAL IMAGES

Arshpreet Sidhu*, Er.Rajbhupinder Kaur
Student,Yadavindra College of Engg.Punjabi University Patiala
Assistant Prof. Yadavindra College of Engg.Punjabi University Patiala

ABSTRACT

Steganography could be a technique of concealing secret messages in a very cowl object whereas communication takes place between sender and receiver. Security of wind has forever been a serious issue from the interests to the current time. it's forever been the interested topic for researchers to develop secure techniques to send knowledge while not revealing it to anyone apart from the receiver. thus from time to time researchers have developed several techniques to satisfy secure transfer of information and steganography is one in every of them. during this paper we've got projected a replacement technique of image steganography i.e. Hash-LSB with RSA formula for providing additional security to knowledge furthermore as our knowledge concealing technique. The projected technique uses a hash operate to come up with a pattern for concealing knowledge bits into LSB of RGB pel values of the duvet image. this system makes certain that the message has been encrypted before concealing it into a canopy image. If in any case the cipher text got unconcealed from the duvet image, the intermediate person apart from receiver cannot access the message because it is in encrypted type.

KEYWORDS: Cryptography, Steganography, LSB, Hash-LSB, RSA Encryption –Decryption .

INTRODUCTION

Digital steganography is the art and science of hiding communications; a steganographic system thus embeds secret data in public cover media so as not to arouse an eavesdropper's suspicion. A steganographic system has two main aspects: steganographic capacity and imperceptibility. However, these two characteristics are at odds with each other. Furthermore, it is quite difficult to increase the steganographic capacity and simultaneously maintain the imperceptibility of a steganographic system. Additionally, there are still very limited methods of steganography to be used with communication protocols, which represent unconventional but promising steganography mediums. Digital image steganography, as a method of secret communication, aims to convey a large amount of secret data, relatively to the size of cover image, between communicating parties. Additionally, it aims to avoid the suspicion of non-communicating parties to this kind of communication. Thus, this research addresses and proposes some methods to improve these fundamental aspects of digital image steganography. Hence, some characteristics and properties of digital images have been employed to increase the steganographic capacity and enhance the stego image quality (imperceptibility). This chapter provides a general introduction to the research by first explaining the research background. Then, the main motivations of this study and the research problem are defined and discussed. Next, the research aim is identified based on the established definition of the research problem and motivations.

Steganography and Cryptography

Cryptography and steganography achieve separate goals. Cryptography conceals only the meaning or contents of a secret message from an eavesdropper. However, steganography conceals even the existence of this message (Lou and Liu, 2002). Furthermore, steganography provides more confidentiality and information security than cryptography since it conceals the mere existence of secret message rather than only protecting the message contents. Therefore, one of the major weaknesses of cryptosystems is that even though the message has been encrypted, it still exists.
Even though both cryptographic and steganographic systems provide secret communications, they have different definitions in terms of system breaking. A cryptographic system is considered broken if an attacker can read the secret message. However, a steganographic system is considered broken if an attacker can detect the existence or read the contents of the hidden message. Moreover, a steganographic system will be considered to have failed if an attacker suspects a specific file or steganography method even without decoding the message. As a result, this consideration

makes steganographic systems more fragile than cryptography systems in terms of system failure. Additionally, steganographic systems must avoid all kinds of suspicion in order to achieve security and not be considered failed systems. Since steganography adds an extra layer of protection to cryptography, combining steganography and encryption gives the ultimate in private communication. Therefore, the purpose of steganography is to complement cryptography and to avoid raising the suspicion of system attackers but not to replace cryptography.

Steganography and Watermarking

Steganography aims to hide the very existence of communication by embedding messages within other cover objects. However, watermarking aims to protect the rights of the owners of digital media such as images, music, video and software. Even if people copy or make minor modification to the watermarked file, the owner can still prove it is his or her file. Thus, both of steganography and watermarking are forms of data hiding and share some common characteristics. Nevertheless, the goal of steganography is the embedded message while the goal of watermarking is the cover object itself. Watermarking is a data hiding technique that protects digital documents, files, or images against removal of copyright information. Even if someone knows that a watermark is exist (i.e. visible watermarking) in a given object, it should be impossible to remove the watermark from the watermarked object without causing a distortion or destroying the original (watermarked) object. This aspect or feature of watermarking is known as "robustness". According to the kind of embedded information, two techniques of document marking can be distinguished: watermarking and fingerprinting. Watermarking is the process of embedding a specific copyright mark into digital documents in the same way. On the other hand, in order to detect any break of licensing agreement, a serial number is embedded in every copy of this digital document. This process is known as "fingerprinting". Even if these markings are detected, it should be practically impossible to remove them.

LITERATURE

K.Thangadurai and G.Sudha Devi, An analysis of LSB Based Image Steganography Techniques [1] Steganography refers to information or a file that has been concealed inside a digital picture, video or audio file. If a person views the object in which the information is hidden inside, he or she will have no indication that there is any hidden information. So the person will not try to decrypt the information. Steganography can be divided into Text Steganography, Image Steganography, Audio/Video Steganography. Image Steganography is one of the common methods used for hiding the information in the cover image. LSB is very efficient algorithm used to embed the information in a cover file. This paper presents the detail knowledge about the LSB based image steganography and its applications to various file formats. In this paper authors also analyze the available image based steganography along with cryptography technique to achieve security.

Rashi Singh ,Gaurav Chawla ,A Review on Image Steganography [2] This paper gives a review of steganography, its various techniques, its advantages and disadvantages, applications, it's merging with cryptography techniques .Today's the rise of the internet become the most important factor of information technology and communication but along with this the threat of information security increases. It's become very important to give security to your data so that no unauthorized person can access it. The steganography is a powerful security tool with which we can hide a secret message inside an object. The object can be text, image, audio or video.

Shikha Sharda, Sumit Budhiraja, Image Steganography: A Review [3] Steganography can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. If it is achieved successfully, the message does not attract attention from eavesdroppers and attackers. The main objectives of steganography are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data. These are the main factors which make it different from other techniques watermarking and cryptography. This paper includes the important steganography methods and the main focus is on the review of steganography in digital images.

Vipul Sharma, Sunny Kumar , A New Approach to Hide Text in Images Using Steganography [4] In this paper, authors have proposed a new steganographic algorithm that is used to hide text file inside an image. In order to increase/ maximize the storage capacity we have used a compression algorithm that compresses the data to be embedded. The compression algorithm we have used works in a range of 1bit to 8 bits per pixel ratio. By applying this algorithm we have developed an application that would help users to efficiently hide the data.

EXISTING TECHNIQUES

There are a large number of cryptographic and steganographic methods that most of us are familiar with. The most widely used two techniques are:

- RSA Algorithm

- LSB Insertion Method

A. RSA Algorithm

The algorithm was given by three MIT's Rivest, Shamir & Adleman and published in year 1977. 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. The RSA algorithm could be used in combination with Hash-LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm we are increasing the security to a level above. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure. RSA algorithm procedure can be illustrated in brief as in following steps:

(i) Select two large strong prime numbers, p and q. Let n = p q.
(ii) Compute Euler's totient value for n: f (n) = (p - 1) (q - 1).
(iii) Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (n)) = 1.
(iv) Calculate a number d such that d = e-1 mod f (n).
(v) Encryption: Given a plain text m satisfying m < n, then the Cipher text c = me mod n.
(vi) Decryption: The cipher text is decrypted by m = cd mod n.

Least Significant Bit (LSB) Insertion Method

One of the most common techniques used in steganography today is called least significant bit (LSB) insertion. Also called LSB (Least Significant Bit) substitution and it is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. In this method some information from the pixel of the carrier image is replaced with the message information so that it can't be observed by the human visual system, therefore it exploits some limitations of the human visual system. The Least Significant Bit insertion varies according to number of bits in an image. For an 8-bit image, the least significant bit i.e. the 8th bit of each byte of the image will be changed by the 1-bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) will be changed. LSB steganography involves the operation on least significant bits of cover image, audio or video. The least significant bit is the lowest bit in a series of binary numbe. In LSB substitution the least significant bits of the pixels are displaced by the bits of the secret message which gives rise to an image with a secret message embedded in it. The method of embedding differs according to the number of bits in an image (different in 8 bit and 24 bit images).

Data Embedding Algorithm in LSB

Step 1: Extract the pixels of the cover image.
Step 2: Extract the characters of the text file.
Step 3: Extract the characters from the Stego key.
Step 4: Choose first pixel and pick characters of the Stego key and place it in first component of pixel.
Step 5: Place some terminating symbol to indicate end of the key. 0 can be used as a terminating symbol in this algorithm.
Step 6: Insert characters of text file in each first component of next pixels by replacing it.
Step 7: Repeat step 6 till all the characters has been embedded.
Step 8: Again place some terminating symbol to indicate end of data.
Step 9: Obtained stego image.

Data Extraction Algorithm in LSB

Step 1: Extract the pixels of the stego image.
Step 2: Now, start from first pixel and extract stego key characters from first component of the pixels. Follow Step3 up to terminating symbol, otherwise follow step 4.
Step 4: If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program.
Step 5: If the key is correct, then go to next pixels and extract secret message characters from first component of next pixels. Follow Step 5 till up to terminating symbol, otherwise follow step 6.
Step 6: Extract secret message

CONCLUSION & FUTURE SCOPE

In this paper we have presented the review of various techniques of stegnography. Work of various authors has been discussed in this paper. It is concluded that a existing techniques does not provide the security to the hidden data. Anyone can decode the data by extracting LSB of every byte in the colored image. The future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly

the steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.

REFERENCES

1. K.Thangadurai and G.Sudha Devi, An analysis of LSB Based Image Steganography Techniques
2. Vijay Kumar Sharma ,vishal Shrivastavaa "Steganography Algorithm For Hiding Image In Image By Improved Lsb Substitution By Minimize Detection"
3. Gurpreet Kaur, Kamaljeet Kaur ,Image Watermarking Using LSB (Least Significant Bit)
4. Amit Singh, Susheel Jain, Anurag Jain, Digital watermarking method using replacement of second Least significant Bit(LSB) with inverse of LSB
5. Nayan K. Dey ,Suman K. Mitra ,Ashish N. Jadhav , Hybrid Scheme for Robust Digital Image Watermarking Using Dirty Paper Trellis Codes ,
6. Lahouari Ghouti, Ahmed Bouridane, Mohammad K. Ibrahim, and Said Boussakta, Digital Image Watermarking Using Balanced Multiwavelets
7. Amir Houmansadr,Shahrokh Ghaemmaghami ,A Digital Image Watermarking Scheme Based on Visual Cryptography
8. Neil F. Johnson2, Zoran Duric1, and Sushil Jajodia2 "Recovery of Watermarks from Distorted Images"
9. Henri Bruno Razafindradina and Attoumani Mohamed Karim , BLIND AND ROBUST IMAGES WATERMARKING BASED ON WAVELET AND EDGE INSERTION
10. Prabhishek Singh, R S Chadha, A Survey of Digital Watermarking Techniques, Applications and Attacks