IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Survey Paper On Data Security Using Image Steganography

Narendra Rane[1], Rishab Khamb[2], Gaurav Mirge[3]
Smt. Kashibai Navale College of Engineering,
Wadgaon, Pune
India

ABSTRACT

Data Security victimization Image Steganography is an Associate in Nursing art of concealing the very fact that communication is taking place, by hiding data in other information. The proposed system uses steganography technique to include more security to the information for the purpose of improving data security. Many different media file formats can be used for image steganography. However, digital images are the most popular because they are widely used on the Internet to hide sensitive data or confidential information in images. There are many steganography techniques, some of which are more effective. They have their own advantages and disadvantages. Different applications have different requirements for the steganography technology used, because, for example, in some applications, secret information may have to be completely invisible, while in other applications, larger secrets must be hidden news. This Project is used to hide the message within the image. For a more secure approach, the project allows the sender or the user to select any BMP cover image with the secret text or the confidential text data and hide it into the image with the bit replacement, it helps to generate a more secure steganographic image. The steganographic image is sent to the destination with the help of a private or public communication network as per the choice of the sender like e-mail, whatsapp or any other medium. On the other side, the receiver downloads the steganographic image and using the software retrieves the secret text hidden in the steganographic image.

General Terms

Image Steganography using LSB Technique

Keywords

Image Steganography, Bitmap, Least Significant Bit Algorithm.

1. INTRODUCTION

Steganography is the art of concealing the actual fact that communication is taking place, by concealing data in different information. Many different carrier file formats may be used, however digital pictures are the most popular as a result of their frequency on the internet. Literature survey is one of the most important steps in any kind of research. Before developing we need to study the previous papers of our domain which we are working on and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers. In this section, we briefly review the related work on Recommendation Systems and their different techniques.

One of the reasons that intruders are also successful is that the foremost of the information they acquire from a system is through a sort that they will browse and comprehend. Intruders may be successful because the most of the knowledge they acquire from a system is during a kind that they'll browse and comprehend. Intruders could reveal the knowledge to others, modify it to misrepresent a private or organization, or use it to launch an associate degree attack. One answer to the current drawback is, through the employment of steganography. Steganography can be used to conceal data in digital media. In distinction to cryptography, it's to not keep others from knowing the hidden information, however it's to stop others from thinking that the knowledge even exists.

Steganography becomes a lot more vital as more people are part of the Net revolution. Steganography is the art of concealing data in ways which prevents the detection of hidden messages. Steganography embraces an associate degree array of secret communication strategies that hide the message from being seen or discovered.

Due to advances in ICT, most data is unbroken electronically. Consequently, the safety of data has become a fundamental issue. Besides cryptography, steganography may be used to secure information. In cryptography, the message or encrypted message is embedded during a digital host before passing it through the network, so the existence of the message is unknown. Besides concealing knowledge for confidentiality, this approach of data concealing may be extended to copyright protection for digital media: audio, video and images.

The growing potential of modern communications would like special means of security particularly on computer networks. Network security is changing a lot because the range of knowledge being changed on the web increases. Therefore, the confidentiality of data increases.

2. Related Work

Literature survey is one of the most important steps in any kind of research. Before developing we need to study the previous papers of our domain which we are working on and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers. In this section, we briefly review the related work on Recommendation Systems and their different techniques.

G. Prashanti and K. Sandhyarani has done a survey on recent achievements of LSB based image steganography. In this survey authors discuss the improvements that enhance the steganographic results such as high robustness, high embedding capacity and un-detectability of hidden information. Along with this survey two new techniques are also proposed. First technique is used to embed data or secret messages into the cover image and in the second technique a secret gray scale image is embedded into another gray scale image. [1]

Savita Goel et al. proposed a new method of embedding secret messages in cover image using LSB method using different progressions. Authors compare the quality of stego image with respect to cover image using number of image quality parameters such as Peak Signal to Noise Ratio(PSNR), Mean Square Error (MSE), histograms and CPU time, Structure Similarity Index Measure (SSIM) and Feature Similarity Index Measure (FSIM). Their study and experimental results showed that their proposed method is fast and highly efficient as compared to basic LSB methods. [2]

Della Baby et al. proposed a “Novel DWT based Image Securing method using Steganography”. In their work a new steganography technique is proposed in which multiple RGB images are embedded into a single RGB image using DWT steganography technique. The cover image is divided into 3 colors i.e. Red, Green and Blue color space. These three color spaces are utilized to hide secret information. [3]

Bingwen Feng, Wei Lu, and Wei Sun in their paper “Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture” proposed a state-of-the-art approach of binary image steganography. This technique is proposed to minimize the distortion on the texture. In this method of steganography firstly the rotation, complement mirroring in variant texture patterns are extracted from the binary image. [4]

M. Nusrati et al. have done study on heuristic genetic algorithm based steganographic methods for hiding secret information in a cover image. This method optimally finds the appropriate locations in the cover image to embed the secret information by focusing on the "before embedding hiding techniques". It tries to make least changes in the bits which lead to minimal modifications in the image histogram. . To convert the LSBs and secret message to a set of blocks, segmentation is done in this genetic algorithm. After this algorithm finds the appropriate locations for embedding, the secret blocks are embedded and it generates the key file which is used during the massage extraction process. [5]

Kazem Qazanfari and Reza Safabakhsh proposed an improved version of LSB++ approach. In this improved LSB++ they make distinction between sensitive pixels and allow protecting them from embedding of extra bits, which results in lower distortion in the co-occurrence matrices. They also extend this method to preserve DCT coefficients of JPEG 3 format images. This improved method results in fewer traces in the co-occurrence matrices than old LSB++ technique.[6]

Based on Huffman Coding, Amitava Nag et al. present a novel steganographic technique of LSB substitution. Their Technique basically focuses on high security, larger embedding capacity and acceptable level of stego image quality. Firstly Huffman tree is produced to encode every 8 bits of secret image. After encoding, they divide the encoded bits into four parts and have 0 to 3 decimal values. Location of embedding a message in the cover image is determined by these decimal values. Experimental results show that it is very difficult for an attacker to extract the secret information because the Huffman table decreases the size of the cover image. [7]

N. Akhtar et al. present and implement the improved version of traditional LSB image steganography technique. Their work enhances the quality of stego image using bit inversion method. They propose and implement two approaches of bit inversion techniques. These both techniques revolve around bit inversion techniques in which LSBs of pixels of a carrier image are inverted only and only if they arise with a specific pattern of pixel's bits. This leads to lesser modification in pixels is compared to traditional LSB method.[8]

P. U. Deshmuk et al. also present the edge adaptive steganography based on LSB substitution. They embed secret information in sharp (edges) regions of the carrier image using an adaptive scheme and difference between two adjacent pixels of the carrier image. Their technique performs better than other LSB and Pixel difference based techniques and maintains the quality of stego image. [9]

E. Dagar and S. Dagar presents the steganography technique for color RGB images to improve the security level of data transfer through the internet. a 24 bit RGB image is utilized as a cover image to embed secret data in red, green and blue pixels. X-Box mapping is used and several boxes contain 16 different values. Here "X" represent any integer number from 0 to 9. After this, values saved in X-Boxes are mapped with LSBs of carrier image. It is very difficult for the attacker to extract the secret information because they make use of mapping. [10]

3. Proposed Algorithm

As we studied the different techniques and went through the projects, we observed that due to the process of encryption the quality of the steganographic image or the resulting image degraded as a result of which the probability of getting caught also increased. So, we can say that the image quality might create much noise and decrease its genuine quality and keeping this in mind we came up with the idea of implementing the Least Significant Bit (L.S.B) algorithm. In a grayscale image every pixel is colored in eight bits. The last bit in a very pixel is named as Least vital bit as its value will have an effect on the pixel worth solely by "1". So, this property is employed to cover the information within the image. If anyone wants to hide more information than in that case we can manipulate the last 2 bits as LSB bits as they'll affect the pixel value only by "3".This helps in storing further data. The Least Vital Bit

Steganography is one such technique during which the least significant little bit of the image is replaced with a data bit. As this methodology is vulnerable to steganalysis thus to build it safer we tend to cipher the raw data before embedding it within the image. Although the secret writing method will increase the time complexity, at a similar time provides higher security also. During this methodology the smallest amount of vital bits of some or all of the bytes within a picture is replaced with a few bits of the key message. The LSB embedding approach has become the idea of the many techniques that hide messages at intervals transmission carrier knowledge. LSB replacement steganography changes the last little bit of every of the element values to mirror the message that must be hidden. Think about associating 8-bit grayscale picture images or we can choose a colored image as well but here we are considering grayscale pictures wherever each pixel is kept as a computer memory unit representing a gray scale color value. Suppose the first eight pixels of the initial images have the subsequent gray color values:

01010010

01001010

10010111

11001100

11010101

01010111

00100110

01000011

To hide the letter Z whose binary value of ASCII [11] code is

10110101, we would replace the LSBs of these pixels to have

the following new values:

01010011

01001010

10010111

11001101

11010100

01010111

00100110

01000011

4.Advantages and Disadvantages

4.1 Advantages

- The main advantage of this system is the security that it provides, security to your messages without knowing to third parties.
- Number of bits has been replaced, therefore the third party cannot guess the password.
- Normal network users can’t guess the image.
- In steganography anyone can't jump on suspects by looking at images.
- It is Reliable.
- Easy to use.

4.2 Disadvantages

- Images can have attacks like diluting, nosing, contrast changes and so on.
- Number bits of pixel should be replaced by equal bits of message.
- If someone is eavesdropping then there is a probability of the message unfolding.
- If more than two people have the same steganography software then hidden messages can be acquired.
- Only unintended users may know the actual working of software.
- Intruders may penetrate suspecting images to get hidden data.

5. Conclusion

It is ascertained that through LSB Substitution Steganography method, the results obtained in data activity are pretty spectacular because it utilizes the easy incontrovertible fact that any image could be happy to individual bit-planes every consisting of various levels of information. Its to be noted that as mentioned earlier, this methodology is only effective for electronic image pictures as these involve lossless compression techniques. But this method can even be extended to be used for color pictures where bit-plane slicing is to be done individually for the highest four bit-planes for every R, G, B of the message image.

6. References

[1]G.Prashanti and K. Sandhyarani - “A New Approach for Data Hiding with LSB Steganography”, 2015.

[2]Savita Goel et al - “Image Steganography – Least Significant Bit with Multiple Progressions”, 2015.

[3]Della Baby et al - “A Novel DWT based Image Securing Method using Steganography”, 2015.

[4]Bingwen Feng et al - “Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture”, 2015.

[5]M.Nusrati et al - “Steganography in image Segments using Genetic Algorithm”, 2015.

[6]K.Qazanfari and R. Safabakhsh - “A new steganography method which preserves histogram: Generalization of LSB++”, 2014.

[7]Amitava Nag et al - “A Huffman Code Based Image Steganography Technique”, 2014.

[8]N. Akhtar et al - “An Improved Inverted LSB Image Steganography”, 2014.

[9]P. U. Deshmukh et al - “A Novel approach for Edge Adaptive Steganography in LSB insertion technique”, 2014.

[10]E.Dager and S. Dagar - “LSB based Image Steganography Using X-Box Mapping”, 2014.

IJCRT