International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A NOVEL APPROACH TO STEGANOGRAPHY USING PIXEL-BASED ALGORITHM IN IMAGE HIDING

Dr.V.RADHIKA[1], B.SAI PRAVALLIKA[2], K.E.KALYANRAMAN[3], A.LAVANYA[4], N.VIJAYA KUMAR[5], K.KEERTHI SOWJANYA[6]

[1]Associate Professor, Dept. of ECE, PRAGATI ENGINEERING COLLEGE

[23456]UG Students, Dept. of ECE, PRAGATI ENGINEERING COLLEGE

ABSTRACT

Steganography is the technique of hiding data under image to prevent it from being unintentionally accessed by anyone else. This process involves a hidden image and a cover image file. By looking at the need of steganography we have proposed a new algorithm which will satisfy the aim of steganography. In our algorithm, we will have a cover image file and the secret image. Then the cover image’s pixel will be taken into consideration. In that we will embed each bit of secret image pixels. This will be continued until the last bit of the secret images’ pixels. After this step, the data is hidden under the image. Then we will send this image file to our client and client will have reverse process to retrieve the hidden image from the cover image. We will then compare our algorithm with BLIND HIDE steganography algorithm on the basis of accuracy, precision, recall and f1-score. We will also check for the output image quality generated by both algorithms on structural similarity measure to reach proper consensus.

INTRODUCTION

The recent growth in computational power and technology has propelled the need for highly secured data communication. One of the best techniques for secure communication is Steganography- a covert writing. It is an art of hiding the very existence of communicated message itself. The aim is to design a steganography algorithm which not only hide the message behind the image but also provide more security than others. A new steganography technique for embedding both text or image in cover images by using LSB & Link List method is implemented. This steganography technique is completely a time domain (pixel based) and secret messages are embedded directly into 24- bit color image. Two ways are provided for embedding the secret data inside cover image such as sequential encoding and random encoding for both text & image. For the purpose of security, encryption technique is used with a user defined key. RGB image format is used to improve the quality of the stego image. At last that RGB image will saved as BMP image file so that no lossy compression can occur and the original message do not destroy and can be extract as it is. Aspect ratio for both text and image after hiding in cover image maintains exactly same. Performance of proposed steganography technique is evaluated by calculating values of MSE (Mean square error), PSNR (Peak signal to noise ratio), ET (Elapse time).

Image Steganography is a very important task in real life where the users want to keep data secret. Data is the heart of computer communication and over the years, different methods have been proposed and created to accomplish the goal of using steganography to hide data. The problem occurs when Traditional Text and Image Based Steganography techniques is not plentiful. They are able to carry only small files. So there is a problem, how to get much enough files to hide our message. This becomes a very tedious task for carry large amount of data. Here, comes the need of Image Steganography. The use of image as a carrier cover for the secure message is overcame the capacity problem. Information can be hidden in any frame of image. Image has a large Capacity to store information. Added small enhancement to the security aspects. The integration of Steganography and cryptography techniques provided powerful systems for sharing secure messages.

LITERATURE SURVEY

Now a days, for secret and secure communication image steganography has become a well-liked option. The performance of any steganography algorithm is based on some parameters. In this paper, the author proposed a novel image steganography algorithm based on the KLT tracking algorithm and BCH codes in the wavelet domain. The proposed algorithm encompasses four distinct steps. First, in the encryption process the secret message is preprocessed, and secret message is encoded by applying BCH codes (n, k, t). Second, to identify the facial regions of interest, face detection and face tracking algorithms are applied on the cover images. Third, In the Embedding process embeds the encoded secret message into the high and middle frequency wavelet coefficients of all facial regions are achieved. Forth, In the extraction process, extracting the secret message from the high and middle frequency wavelet coefficients for each RGB components of all facial regions is accomplished.

Experimental results of the proposed image steganography algorithm have demonstrated a more embedding efficiency and a more embedding payload. Present day, Researches are usually focused on Linguistic steganography. This paper proposed a new steganography method with an Indian local language, Malayalam. The proposed method is based on custom Unicode technique with embedding based on indexing, i.e. firstly the original message is encoded to Malayalam text with custom UNICODE values produced for the Malayalam text. The comparison of the proposed method against an existing method depicts that, the proposed steganography methods is more accurate in the encoding as well as in decoding process. [2] Steganography is a technique that is used to hide data and that data is cannot be detected by attacker. Steganography is basically used for data securing applications. Steganography hides the existence of the message so that attacker cannot identify the presence of message and unable to decrypt it. In this paper, multiple color images are hidden into a single-color image using the Discrete Wavelet Transform. The cover image is split up into R, G and B planes. Secret images are embedded into these planes. An Nlevel decomposition of the cover image and the secret images are done and some frequency components of the same are combined. Secret images are then extracted from the stego image. Here, the appearance of both stego image and the original image is almost same with high overall security. In this literature, an image steganography technique is proposed that is used to hide audio signal in image in the transform domain using wavelet transform. The audio signal in any format i.e., MP3 or WAV or any other type is encrypted and carried by the image. Viewer cannot recognize the existence of signal. Whenever the secret information is hidden in the carrier the result is the stego signal. In this paper, the quality of the stego image is measured by some parameters i.e. Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM), Universal Image Quality Index (UIQI). The quality of secret audio signal that is extracted is measured by Signal to Noise Ratio (SNR), Squared Pearson Correlation Coefficient (SPCC). The results describe good values for these parameters. The results show good quality stego signal and the stego signal is analyzed for different attacks.

EXISTING SYSTEM

Image Steganography may be a technique to cover any reasonably files into a carrying image file. The employment of the image primarily based steganography is additional eligible than different transmission files thanks to its size and memory necessities. Images square measure the set of pictures. Image is associate degree electronic medium for the recording, repetition and broadcasting of moving visual pictures. The average number of still images per unit of time of image is twenty- four frames per second.

If a person sends sensitive information over the insecure channels of the system, then there may be a chance of hacking it, they can alter the information and sends it over the net. (Example is military persons sending sensitive information over the net.) This problem has been solved by the proposed system.

HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR IMAGE STEGANOGRAPHY (HLSB):

Image Steganography deals with hiding secret data or information within a image. In this paper, a hash based least significant bit (LSB) technique has been proposed. A spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret information is divided into 3,3,2 and embedded into the RGB pixel values of the cover frames respectively. A hash function is used to select the position of insertion in LSB bits. The proposed method is analyzedin terms of both Peak Signal to Noise Ratio (PSNR) compared to the original cover image as well as the Mean Square Error (MSE) measured between the original and steganographic files averaged over all image frames. Image Fidelity (IF) is also measured and the results show minimal degradation of the steganographic image file. The proposed technique is compared with existing LSB based steganography and the results are found to be encouraging. An estimate of the embedding capacity of the technique in the test image file along with an application of the proposed method has also been presented. Steganography is hiding private or secret data within a carrier in invisible manner. It derives from the Greek word steganos, meaning covered or secret, Androphy (writing or drawing). The medium where the secret data is hidden is called as cover medium, this can be image,

image or an audio file. Any stego algorithm removes the redundant bits in the cover media and inserts the secret data into the space. Higher the quality of image or sound more redundant bits are available for hiding. Application of Steganography varies from military, industrial applications to copyright and Intellectual Property Rights (IPR). Image Steganography is a method for hiding data in a image file and hence it reduces the chance of access by unauthorized user. In steganography various carrier file formats can be used, among which images are popular due their frequent use on internet. Image steganography has a lot more scope of hiding secret data because of the nature of image which has many numbers of redundant bits. As per the requirement of user there are different image steganography technique proposed leading to own positive and negative points. The image steganography techniques are beneficial in application having high security requirements. The paper provides effective review of existing image steganography techniques and some guidelines for the design of image steganography system.

PROPOSED SYSTEM

In the proposed system the above problem has been solved by embedding the data into the image file. Before embedding it into the file, encryption operation will be performed by using the encryption key which is provided by the source. Then this image file will be passed over the network, even if hacker hacks it, can be able to see only an image file. At the destination side this data will be encrypted from image file and performs decryption to get original message. The data is embedded inside the image by embedding each byte of information inside the pixel of image frames without affecting the original quality of the image. By using this concept:

•Large amount of data can be stored because of embedding the information inside image. Hence increases the storage capacity.

•More security will be provided to data since the information is encrypted using Feistel network before embedding it inside the image.

•Quality of cover image will not be affected.

Since Linked List method has been used for embedding information inside image, it will be difficult for the intruders to predict the location of the presence of the information inside each frame.

The process is done by, first converting the images into frames. Then the secrete text should be encrypted using Feistel network and then embedded inside the frames of the cover image to obtain Stego frames. The embedding process is done using Linked List Method. In Linked List method, after embedding the byte of information inside one 3*3 pixel, the address of the location of next byte of information should be embedded next to it. The Stego frames are then combined to get the Stego Image.

STEGANOGRAPHY:

STEGANOGRAPHY is the practice of concealing a file, message, image, or image within another file, message, image, or image.

BLIND HIDE STEGANOGRAPHY

We proposed a data hiding method of steganography which is image-based. We have taken a text file which contains the secret text and an image file which will be act as cover image to hide the data. The process of image-based steganography is very simple. Images are composed of pixels which describes the content of image. Pixels are usually made up of colors. Every pixel is of combination of three colors red, green and blue. We kept the sole aim of maintaining the characteristics of image file. The main aim of the proposed work is to enhance the security of a secret message sent over communication networks by combining several functional points:

1.Concealing the secret message in a grayscale image which is sent over communication channel in order to prevent a potential attack by an adversary.

2.Adding decoy data, in order to confuse the attacker in case the presence of a secret message is detected by some steganalysis tool, and the attacker attempted to uncover the secret message.

3.The embedding process should result in a stego image that is less likely to be detectable by meeting un-detectability criteria such as the visual imperceptibility and the PSNR metric.

4.Adding a checksum to the stego image in the embedding process, and calculating a second checksum during the extraction process. The checksums will be used to detect if any alteration has happened by comparing the two checksums.

5.The recovered secret file should be equal to the original secret file in contents and format if the stego has not been attacked.

6.Apply an attack to produce changes in the stego image that needs to be detected by the extraction process.

7.Extract the secret message and verify its integrity using the checksum comparison.

8.In case an attacked is detected, identify locations of bytes of the secret image that has been changed, by comparing the data bit pair and the decoy bit pair in every byte.

SIMULATION

The general architecture consists of two phases:

1.Hiding data in Image (Encryption)

2.Retrieval of original information (Decryption)

SECURITY

Main intention of the proposed model is to provide security. To assure the correct extraction of the secret message, the same key is used by the sender and receiver. Only the receiver who has a valid key can open the secret message.

MODULE DESCRIPTION

The modules are:

Encryption process

Decryption process

MODULE 1: Encryption Process

The steps involved in encryption process are:

1. Extracting frames from image
2. Encrypting data using Feistel network algorithm
3. Embedding text inside image frames

ENCRYPTING DATA USING STEGANOGRAPHY ALGORITHM: The secret information is encrypted using steganography algorithm. In cryptography, a Feistel cipher is a symmetric structure used in the construction of block ciphers, named after the German IBM cryptographer Horst Feistel; it is also commonly known as a steganography. A large set of block ciphers use the scheme, including the Data Encryption Standard (DES). The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore, the size of the code or circuitry required to implement such a cipher is nearly halved. Feistel construction is iterative in nature which makes implementing the cryptosystem in hardware easier.

CONCLUSION

By comparing results of our proposed method with BLIND HIDE, we reach to following conclusions

•It is clear that our proposed method yields more accuracy, precision, recall and f1-score.

•Also, our proposed method yields output image of about same size as o original image.

•Our proposed method yields steganograted image in PNG (Portable Network Graphics) which is better than BMP (Bitmap) as it is compressed and lossless where BMP is uncompressed and lossless. In future, we aim to provide more optimum speed and the security of the data. The proposed algorithm gives better results for color images in dual-level security. Although the image quality can be preserved with high PSNR, visual quality can hardly be improved.

REFERENCES

1. Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, “Hash Based Least Significant Bit Technique for Image Steganography (HLSB”), International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.1,No2, April 2012.
2. A. Swathi and Dr. S.A.K. Jilani, “Image Steganography by LSB Substitution Using Different Polynomial Equations”, International Journal of Computational Engineering Research (IJCER), Vol. 2, Issue 5, September 2012.
3. Ronak Doshi, Pratik Jain and Lalit Gupta, “Steganography and Its Applications in Security”,International Journal of Modern Engineering Research (IJMER), Vol. 2, Issue 6, November-December 2012.
4. Rohit G Bal and Dr. P. Ezhilarasu, “An Efficient Safe and Secured Image Steganography using Shadow Derivation”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.
5. Vipula Madhukar Wajgade and Dr. Suresh Kumar, “Enhancing Data Security using Image Steganography”, International Journal of Emerging Technology and Advanced Engineering (IJETAC), Vol. 3, Issue 4, April 2013.
6. Ms. Fameela. K. A, Mrs. Najiya. A and Mrs. Reshma. V. K, “Survey on Reversible Data Hiding in Encrypted Images”, International Journal of Science, Engineering and Technology Research (IJSETR), Vol. 3, Issue 4, April 2014.