Journal of Positive School Psychology http://journalppw.com
2022, Vol.6, No.4, 4234-4241

Data Hiding in Images using Steganography for Speech Signal and Its Intelligibility and Psychology of Perception after Restoration

[1]Vaibhav Thakur, [2]Rajesh Kumar Dubey

[1]Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Noida (India)-201309

[2]Department of Electrical Engineering, School of Engineering & Technology, Central University of Haryana, Mahendergarh (India)-123031

Email: [1]rajesh.dubey@cuh.ac.in

[2]thakurvaibhav789@gmail.com

Abstract:

Steganography is the discipline of enclosing any form of data message inside another data file in such a fashion that it hides the essence of the hidden data at all. It can be exercised to image, speech, text, and video files. In this paper, a modified version of the Least Significant Bit (LSB) approach has been used and then image segmentation is applied to it to hide and then to recover the speech signal. The experimental result shows that the proposed method produces excellent quality stego-images that can easily combat optical and analytical attacks. The work of hiding speechsignals in an image and then restoration of the speech signal without losing the intelligibility of the speechand its psychology of perception has been presented in this paper.

Keywords: *Image Processing, Image Segmentation, Least Significant Bit, Stego-Image, Steganalysis, Data Hiding, Stegnographic Technique.*

I. INTRODUCTION

The interconnected networks play an important role in our work and normal day-to-day life. Network equips us with a fast shipment of the data from opne node to another in a proficient manner. We all relish the integrity of it in sending and receiving process. But, in certain instances, we may wish to keep our data classified, so various technologies have been recognized in commencing the safe transfer of data. The most common technologies are Cryptography, Steganography, and Watermarking. Steganography and Watermarking are sometimes believed to be the same which is not true as they have the same goal but the way data is administrated is distinct in both techniques. On the elementary level, steganography is the process of concealed scripting. The aim of steganography is to conceal the presence of existing communication. The stenographic techniques can be classified into two types firstly, according to the character of cover (Text, Speech, Image or Video steganography) and secondly in the way manipulation of data during the embedding process (Substitution, Injection, and Generation Steganography). This paper presents a modified LSB method (Zig-Zag Substitution) incorporated along with the image segmentation technique. The cover file is an image and the secret data to be embedded can be text, image, speech, or form of the data file. The input image, text, and speech must be converted to 24 bits in order to be ready for the embedding process into the host medium. The dimensions of the host image will be used to determine the segments that are to be engaged in the covered procedure of embedding and then in extraction. The area is used to selectsegments and for the construction of the area, a segment key is made. The master key must be interpolated during the extraction process by the user in order to generate the other handling keys. The length of the secret message, type of file, or its extension, and the selected

© 2021 JPPW. All rights reserved

segment information must be available to the user for its extraction.

1.1 Steganography

Steganography is currently a field of extensive studies and every day new research works are carried out. There are so many methods and algorithms, which are used for different types of data files. Categorizing on the bases of the cover file used, steganography is broadly classified into the following five categories [1]- [3]:

1) Text Steganography: It has been practiced for a very long time like using the Morse code etc. It includes capital letters, spaces & numbers for data hiding.

2) Image Steganography: when the cover object is the image the type of steganography is called image steganography. Generally, in its routine redundant values of a pixel are used to embed the secret information.

3) Speech Steganography: When aspeech file is used as a bearer of secret information it is known as speech steganography. It has become very popular because it uses large digital speech formats such as AVI, WAVE, MIDI, MPEG, and other formats for steganography.

4) Video Steganography: Video Steganography is a technique to hide any sort of data in any digital video format. Here video is used as a host for transmission. Using the Discrete Cosine Transform (DST), the values are removed to create room for the secret message in particular images of the digital video. Video steganography uses a range of formats such as MPEG, H.264, Mp4, 3gp, or other video formats.

5) Network Steganography: When network protocols such as TCP, UDP, ICMP, IP, etc. are used as cover objects this is network protocol steganography. This can be achieved by using the unused header bits of the TCP/IP field.

1.2 Image Steganography

With the advent of the Internet and other Network technologies, trillions of bytes of data are being transferred every day. Out of which most of the files are in the form of digital images. These images may contain some secrets of great importance embedded into them. A simple JPEG file may be used by the different defense institutions to camouflage their secrets over the network. So, it won't be wrong to say that digital image steganography is a matter of concern for us. Image steganography is a success because the changes in a digital image go unnoticed by the human visual system. It cannot determine random patterns changes or any sort of color changes on a small scale. This vulnerability of the human eye is exploited and data is easily hidden into the host image without anyone noticing it. Every digital image whether it is grayscale or a color image is made up of pixels. In a grayscale image, each pixel has 8 bits and for the color image, it has 24 bits, 8 each for red, green, and blue. The numerical value of the pixel which ranges between 0 to 255 determines the color of the respective pixel.

The rest of the organization of the paper is as follows: Section II gives the details of the proposed structure including embedding and extracting module. Section III presents the data description and results with interpretation. Section IV concludes the paper.

II. THE PROPOSED STRUCTURE

The designed system has the ambition to develop an improved steganography approach that is using the Zig-Zag LSB Method and then segmenting the dimensions of the host image and attaining high quality and large accommodating stego-images which are durable to different types of attacks. The proposed structure is composed of two components:

1) Embedding Module

2) Extracting Module

2.1 Embedding Module

The approach used in masking the data into a cover image is the LSB. It's one of the most common and highly used embedding methods. The method is based on replacing the LSBs of a given byte from the host image pixels. LSB method is very efficient as it is quick and simple to implement, but when the replacement is made for more than three bits per pixel this can cause distortion in the cover image. In this work, it is decided that the target pixels that will be used to store the hidden message bits are selected randomly from different sections areas by the Zig-Zag LSB Substitution. In the Zig-Zag LSB substitution, the first LSB bit of the pixel is replaced and then two bits are removed followed by three bits of the pixel and each bit requires one pixel from the cover image, so each byte in

© 2021 JPPW. All rights reserved

the pixel will be used to stock the bits of secrete message in the similar form. Then for the next pixel values, one can now randomly remove one, two, or three LSB bits. Choosing randomness over a sequential embedding procedure has two benefits; firstly, the security of data is improved as it will be spread all across the cover image rather than all of the data being embedded at the top left corner of the cover. Secondly, it makes the event of substituting relatively less superficial as the replaced pixels may not be contiguous [2]-[3]. Then the cover image chosen can be of any format such as the BMP, JPEG, or PNG. It is converted to 24 bits format in the case of the RGB image and 8 bits in the case of the grayscale. This is the Image conversion. After the image conversion process is completed, the system now deals with the cover image in the form of a two-dimensional array and the image segmentation process is started. It uses the width and height of the image in order to address them towards the segmentation process [4-5]. Inside this process, all desirable segmentations will be analyzed and assigned a proper index for each one. The final computations of each segment are made according to height and width [6]-[8].The selection of the segment will find an area for the embedding process. The secret message could be of any format text, image, PDF, speech, video, etc. The message is converted into a stream of bytes. For the speech and video file formats the only difficulty in the embedding process is that sometimes the size of the cover image is not enough to occupy the bits of the video or the speech file, for this either the cover image should be of large size or the video and speech should be transferred in small segments. The key can be generated randomly using a specific multiplier or following a specific pattern. A master key is necessary for the extraction process.

2.2 Extraction Module

In order to extract the hidden data from the stego-image, four important things are needed; firstly, the length of the secret message, which means one should know the number of bytes that were hidden. Secondly, one should know about the master key that was used during data hiding. Thirdly, one should know the segmentation details that were utilized in data hiding. And finally, one should know the file extension of a secret message like it is an image, text, speech, or video. After processing all this information, one can extract the hidden data from the cover image [9].The segment to be used is determined and the area boundaries are computed as well the area segments are computed as well. The key is initialized and the stego-image is loaded. The numbers of bytes in the hidden data are used to set the loop counter and the segments are used to determine the places where data is hidden. After this, the loop is incremented and bit by bit the data is removed and replaced by original bits removed earlier during the process of embedding. Finally, the data is retrieved and the cover image as well [10-11].

III. DATA DESCRIPTION, RESULTS, AND INTERPRETATION

The Image Steganography has been performed using the MATLAB platform. This application has been divided into two main modules-the first application module contains the components including the operations of the application to input the data for hiding that can be text, image, speech& video, and the second module consists of the background process of steganography which uses the LSB substitution and the Image segmentation to hide secret data and then generate the key that is used for the successful retrieving of the data at the receiver's side.The cover image chosen was the Lena and was in jpeg format [12-14]. When the data was hidden to maximum capacity the results are shown in Figure 1. The Human Visionary System (HVS) is unable to spot any differences between the two images but when analyzing the pixels of the image in the form of a histogram. It is observed that when a difference of pixel intensity vs a number of pixels in the original and embedded image are plotted as in Figure 2, at some places the pixels in the embedded image are missing and replaced with that of the secret message.

© 2021 JPPW. All rights reserved

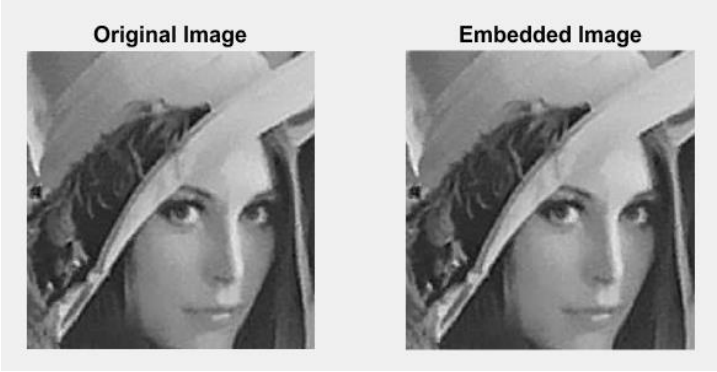

Figure 1: The original image and embedded image with maximum embedded data size

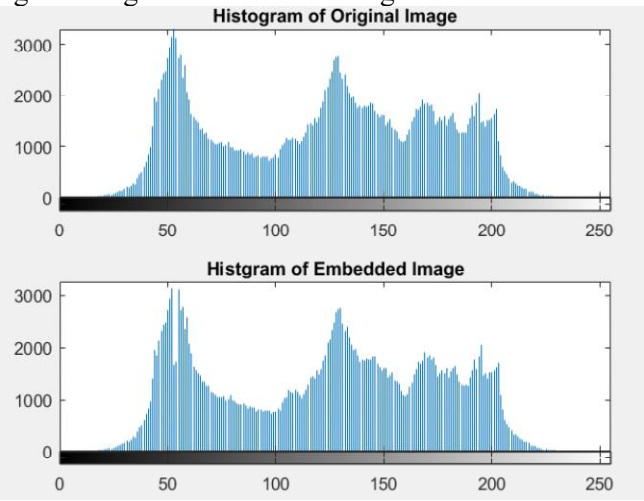

Figure 2: The difference of pixel intensity vs number of pixels in the original and embedded image

The difference that will be visible to our eyes can be noticed in Figure3 when a new image is created that displays the number of free places in the image. The white area in the image determines the area selected for LSB substitution and then segmentation after which the secret data was hidden into it. The black area determines that their no difference between the original and the embedded image in that particular spot. Hence data is not hidden in these spaces.The above results were for the embedding process. The extraction has an opposite cyclic process to the embedding process. After the embedding process, the embedded image or the stego-image is generated. When stego-image, key, segmentation factors, and the length of the secret message are generated, the process of the extraction is commenced. After the process of the extraction, the comparison between the stego and the extracted image as in Figure4 reveals that there is no difference visible to the eye.

© 2021 JPPW. All rights reserved

Figure 3: The difference between original and embedded image

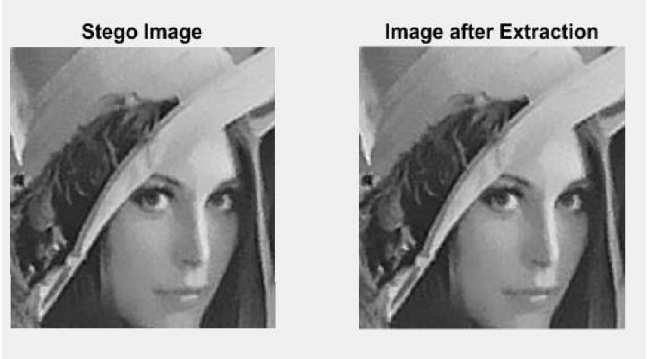

Figure 4: The stego image and extracted image with maximum embedded data size

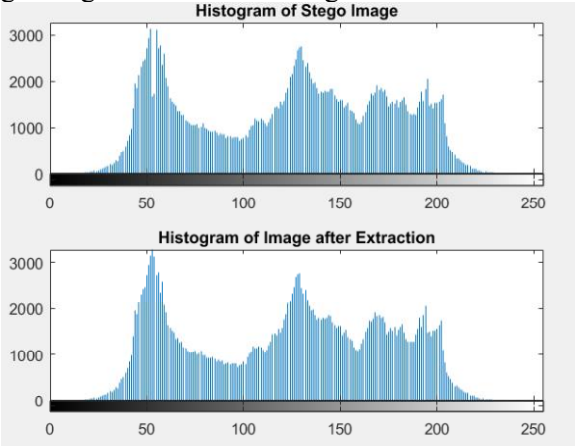

Figure 5: The difference of pixel intensity vs number of pixels in stego and extracted image

Figure5 determines that the extracted image has the same amount of pixel intensity as that of the original cover image. The extracted image has been produced by removing the secret data and using the key to produce the removed bits and putting them to their places to reproduce the cover image. Actually, the cover image's condition is not a concern at the receiver as the only important piece of information is the secret data and its reception not the cover image.The difference between the original and the extracted image as shown in Figure 6 is very less (unnoticeable), the black area shows the patches that display the area of similarity of the bits and the white patches of the changes in the bits. Using the Zig-Zag LSB and the Image segmentation techniques on the cover image the extracted image has almost no difference from the original one.

© 2021 JPPW. All rights reserved

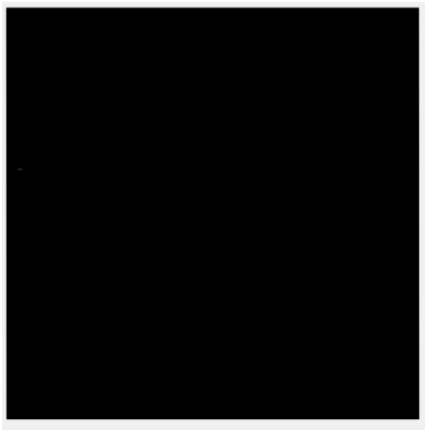

Figure. 6: The difference between original and extracted image

This system was also used to test data such as speech files and videos as well. When the cover image of the right size is chosen, the process of embedding the bits of the speech was achieved and the cover image as shown in Figure7 could incorporate all the bits of the speech file without facing any changes in it.After the embedding process, the extraction was completed and the spectrum of the speech file was analyzed as in Figure. 8 and noticed that the speech has the same features and intelligibility as it did before embedding. Although the Human Auditory System (HAS) is better than the Human Visionary System (HVS) still no difference between the two speech files was recognized by it.

Figure. 7: The cover image before and after incorporating the speech file

For the statistical analysis of the steganographic system, it is decided to take the PSNR of the original cover, stego-image, and the extracted image, when the hidden data is text and image. The results in Figure. 9 show that when noise is added into the image, which in this case is salt and pepper noise, the effect of embedding LSBs and applying Image segmentation on the cover and extraction of the same have no effect on the PSNR of the cover image. It is observed that the difference between the original and the stego is very small in the order of 0.04 for the image and 0.007 for the text which is almost unnoticeable. The results for the original cover and extracted image were determined to be 0.1383 and 0.011 for image and text respectively. These analyses determine that the designed system is noise tolerant.

© 2021 JPPW. All rights reserved

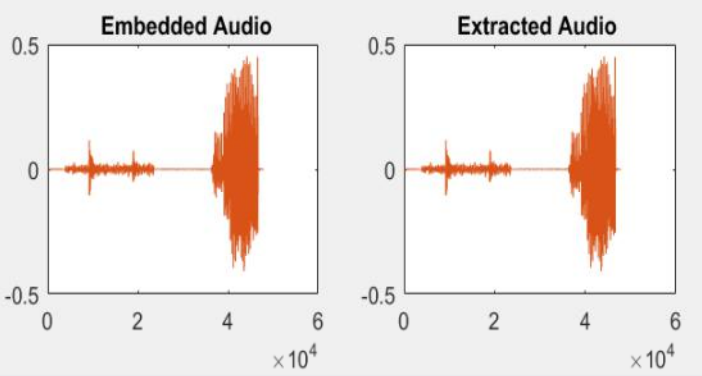

Figure 8: The spectrum of the original speech file and the recovered speech file

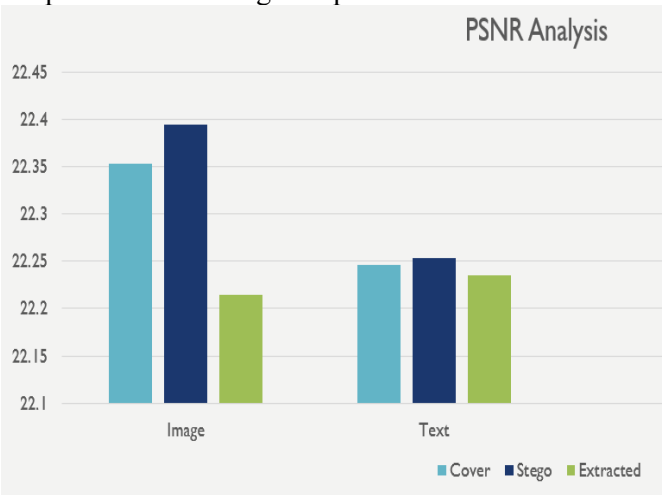

Figure 9: The PSNR Analysis of the cover, stego, and extracted images

IV. CONCLUSION

This work presented a technique for image steganography that is very useful for information surveillance. It combines the existing methods like LSB substitution and Image segmentation to provide additional security to the secret data. For LSB substitution, the Zig-Zag approach has been used, which then gets empowered by image segmentation to determine a random area across the cover to hide data. The main goal of this work is to compose a solution that generates sturdy stego images which are not affected by any attack and it is very difficult to identify the existence of a secret message in it. Experimental results show that the presented technique has satisfied most of the security criteria whether it is its visual appearance, un-detectability, or its security to the hidden data. The cover image was made more adaptable to host a larger amount of data by exploiting every pixel value. The restoration of the speech signal from stego imagesand its intelligibility and psychology of perception areprsented.

Received: May 12, 2021
Accepted: July 28, 2021
Published Online: August 14, 2021

REFERENCES

[1] BawanehMJand ObeidatAA (2016) A Secure robust grayscale image steganography using image segmentation:Journal of Information Security, 1-10.

[2] FarrajiAl-OII (2017)New technique of steganography based on locations of LSB: International Journal of Information Research and Review,1-5.

[3] Al-Omari ZY and Taani AT-Al (2017) Secure LSB steganography for colored images using character-color mapping: International Conference on Information and Communication Systems (ICICS), 1-4.

© 2021 JPPW. All rights reserved

[4] Provos N and Honeyman P (2003) Hide and seek: An introduction to steganography:IEEE Security and Privacy,1 (3), 32-44.
[5] Anderson, Ross J and Fabien AP Petitcolas (1998) On the limits of steganography: IEEE Journal on selected areas in communications, 16 (4), 474-481.
[6] Huang, ZhongFY and Huang J (2014) Improved algorithm of edge adaptive image steganography based on LSB matching revisited algorithm:Digital-Forensics and Watermarking, 19-31.
[7] Mamta J and Lenka SK (2015) Secret data transmission using vital image steganography over transposition cipher: In Green Computing and Internet of Things 2015 International Conference on IEEE, 1026-1029.
[8] Chen WJ, Chang CC and Le T(2010) High payload steganography mechanism using hybrid edge detector, 37, 3292-3301.
[9] Patel H and Dave P (2012) Steganography technique based on DCT coefficients:International Journal of Engineering Research and Applications, 2, 713-717.
[10] Maiti C, Baksi D, Zamider I, Gorai P and Kisku DR (2011) Data hiding in images using some efficient steganography techniques: International Conference on Signal Processing, Image Processing, and Pattern Recognition, 195-203.
[11] Singh AK, Singh J and Singh HV (2015) Steganography in images using LSB technique: International Journal of Latest Trends in Engineering and Technology, 5 (1), 426-430.
[12] Yadav K and Rajput S (2016) Data hiding in image using LSB with DES cryptography: International Journal of Engineering Applied Sciences and Technology, 1 (3), 80-85.
[13] Al-Afandy KA, Faragallah OS, Elmhalawy A, El-Rabaie E-SM. and El-Banby GM (2016) High-security data hiding using image cropping and LSB least significant bit steganography: 4th IEEE International Colloquium on Information Science and Technology, *400-404.*
[14] Nashat D, Mamdouh L (2019) An efficient steganographic technique for hidingdata. Journal of the Egyptian Mathematical Society,27 (57), 1-14.

© 2021 JPPW. All rights reserved