An Algorithm for Security Enhancement in Image Transmission Using Steganography

M. Saravanan [1, *], A. Priya [2]

[1] Hindustan Institute of Technology and Science, Department of ECE, Chennai, Tamilnadu, India.
msarawins@gmail.com
[2] B. S. Abdur Rahman Crescent Institute of Science and Technology, Department of ECE, Chennai, Tamilnadu, India.
priyamarish@crescent.education
*Corresponding Author: M.Saravanan, Email: msarawins@gmail.com

How to cite this paper: M. Saravanan and A. Priya (2019) An Algorithm for Security Enhancement in Image Transmission Using Steganography. Journal of the Institute of Electronics and Computer, **1**, 1-8. https://doi.org/10.33969/JIEC.2019.11001

Received: October 7, 2019
Accepted: October 28, 2019
Published: November 5, 2019

Abstract

Data communication through the public communication channels is insecure due to advanced technology available for interception of third party users. Therefore, an efficient data hiding technology is vital for secure data transmission especially when the system is connected with internet services. Audio steganography is one of the promising solutions for where the information is hidden over audio file. In this paper, a novel method for the hiding of image information by converting into another format thereby reduces the computational complexity.

Keywords

Image enhancement, Image restoration, Image Scaling, Steganography, Steganalysis.

1. Introduction

In last few decades, steganography plays a vital role in securing data transmission. A lot of research has been carried in this field of steganography to improve the level of security. Hiding images or other information in the audio file has attracted many researchers nowadays due to its less computational complexity. In some approaches, the information is embedded in positions of pixels in the image based on pseudorandom number generator which is independent of image content and secret content. This degrades the visual quality of the image, especially in smooth regions. In order to mitigate this problem a new approach shown in [1], selects embedding regions which are dependent on the size of secret information and also the difference in consecutive pixels. In [2], the secret message is modified to a particular direction to have (2n+1) notations carried by n cover pixels. This utilizes the direction of modification and hence improves embedding efficiency. In [3], a clustering modification direction (CMDs) strategy is used which works by splitting the original images into various sub-images and embedded with a message with well-known schemes. In some approaches [4], a binary image steganographic scheme is introduced to reduce the embedding distortion on the texture. A statistical model is used to calculate the variation of coefficients in the image and it is used to determine the embedding modifications in the image as in [5]. In contrast to modifying the secret information and embedded in images, there are many types of research emerging nowadays to embed information in audio signal [6]. The presence of hidden image in the audio signal can be detected by steganalysis techniques and the same is used to extract the hidden data from it. In [7], artificial neural network algorithm is used to detect and extract the hidden information from the image. The estimate of secure payload that the image can handle and the level of secret data detected from the image is calculated in [8].

In the approaches discussed above, the secret information is embedded in the image with or without modifying the secret data. This requires an algorithm to select the embedded position in the image which increases the computational complexity especially when the secret data is of huge size. Hence the proposed algorithm avoids the necessity of an additional image or audio for packing the secret data by converting the secret data into an audio file. This reduces the device complexity and still attains the optimum performance.

2. Proposed Model

Figure 1 shows the proposed model for encoding of image input inside the audio file and decoding the same at the receiver side. Initially, the information which has to be secured is taken and is given to the proposed model. In this case, a lena.jpg image of size 512 x 512 is taken and is given to the proposed model as the input image. The primary objective of the model is to convert the image into an audio signal which is a one-dimensional vector quantity. The input image is a two-dimensional array and hence the two-dimensional input image taken is converted into one-dimensional quantity. The most common audio file format used in most of the system is .wav file format and hence the same format is considered in this model. The .wav format has audio information in terms of a one-dimensional vector having values between 0 and 1. However, the converted 1D image file has values between 0 and 255 and this makes the converted image file to be unsuitable for formatting in terms of .wav format. Therefore the converted file has to be normalized in such a way that it suits for conversion into .wav format. Once the file is converted to the audio format, it is transmitted over a free space. Since the transmitted information is in form of audio signal, the third party persons cannot eavesdrop using the traditional gadget which senses only electromagnetic signal, not the audio signals. At the receiver side, the audio signal is received and is decoded by de-normalizing the data and then reshaping the 1D vector into a 2D array to extract the original image.

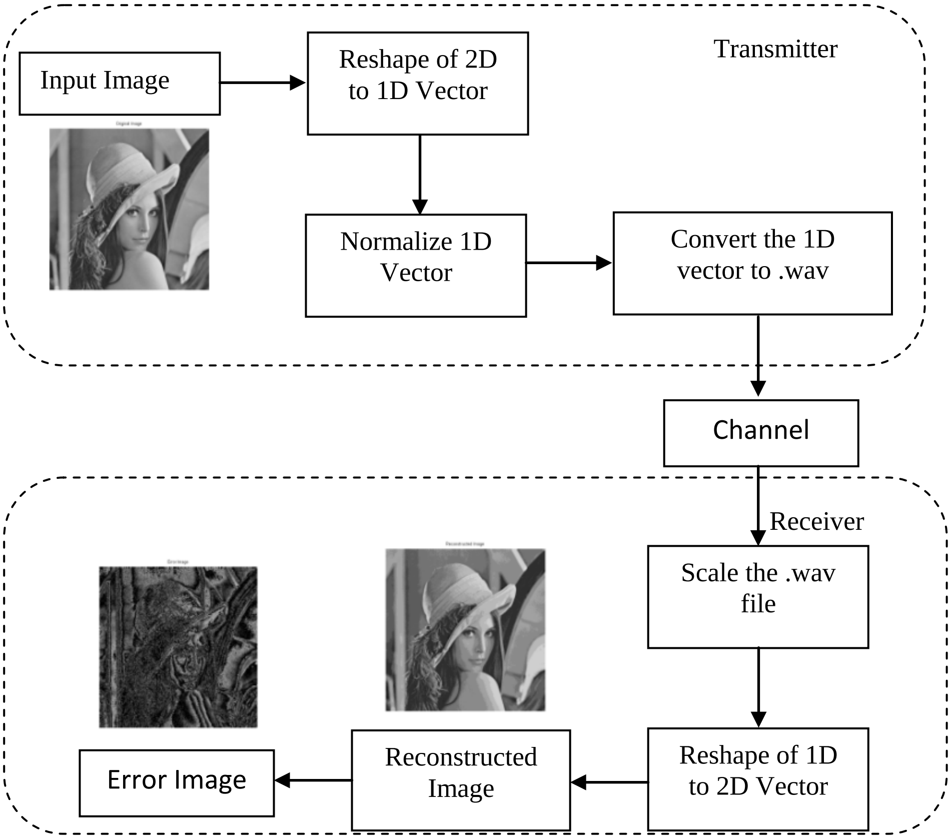

Figure 1. Input Image

2.1 Algorithm 1

```
//Encode of original image to audio file //
Initialize I, k←1;                  //Input Image that has to be secured//
[r , c]← Size (I)                   //Find Size of Input//
Length←Multiply(r,c)      // Find Length of image input//
// Reshape the 2D Image file in 1D vector //
for i=1 to r
for j=1 to c
```

```
            IV(k)←I(i , j)
            j←j+1; k←k+1;
end
i←i+1
end
//Normalization Algorithm//
for k=1 to Length
IN(k)← IV(k)/(min(IV));
k←k+1;
end
//Convert the Normalized image to .wav format //
Aud←wavwrite(IN) //wavwrite is matlab predefined function to convert a vector to .wav format
```

2.2 Algorithm 2

```
//Decode of original image from received audio file //

//Scale the .wav file back to original scale factor//
Scale_Factor←mean(IV)/mean(Aud);
    IO←Aud*scale_factor;
// Reconstruct the input image from scaled audio signal
Initialize k←1;
for i=1 to r
for j=1 to c
            IR(i,j)←IO(k)
            j←j+1; k←k+1;
end
i←i+1
end
```

3. Results and Discussions

In this proposed model a grayscale image of size 512 x 512 having pixel values from 0 to 255 is taken as input as shown in Figure 2. The input is represented in 2D form and hence has to be converted to 1D form. Hence a predefined function named ‘reshape.m’ in Matlab tool is used to convert 2D form to 1D form and the resultant signal is shown in Figure. 3.

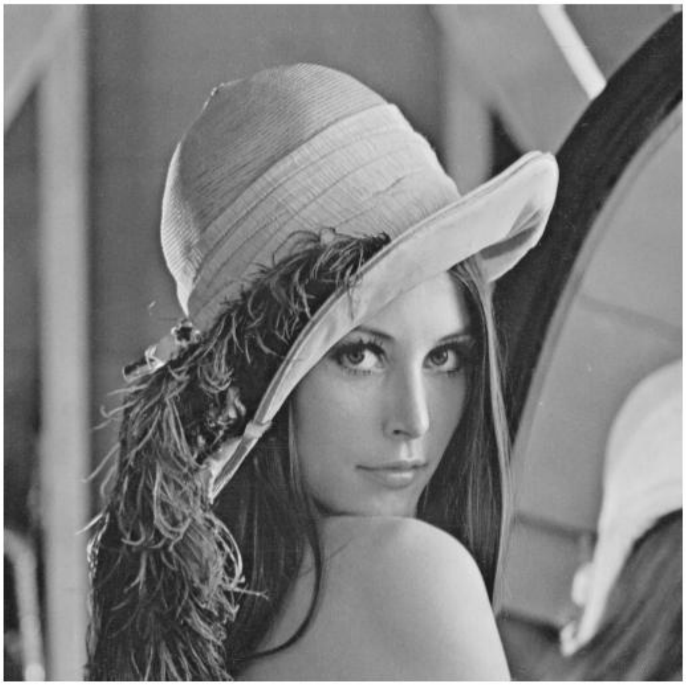

Figure 2. Original input image

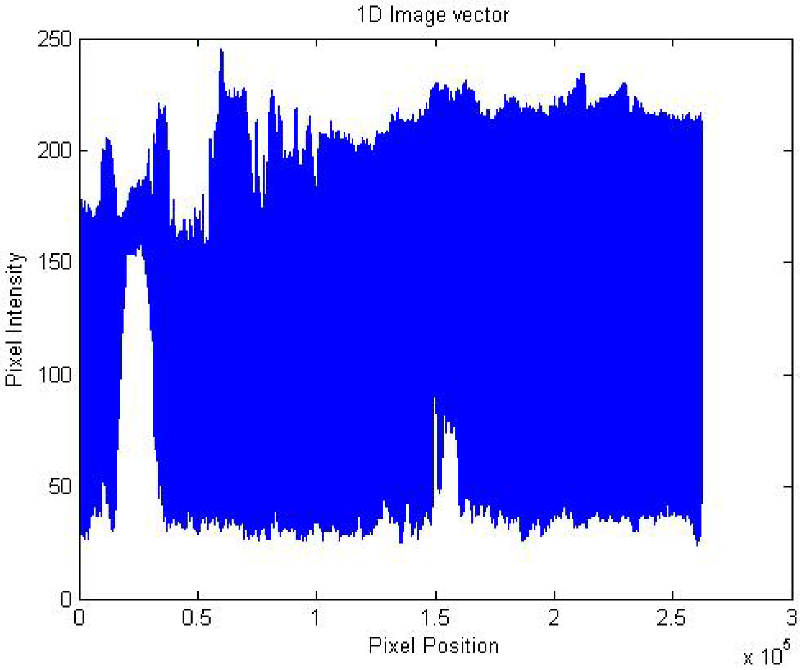

Figure 3. 1D Representation of image

In Figure 3 it is observed that the signal level span between 0 and 255 for a length of

262144 which is obtained by multiplying a number of row elements (512) with column elements (512) in the input image. However, the signal level is shown in Figure. 3 is much higher to convert to audio (.wav) format and hence the resultant signal has to be normalized. Figure. 4 shows equivalent audio file for the input image whose levels is normalized between 0 to 1 and are transmitted in free space. Since the image information is in the form of an audio file, the attackers cannot receive or track it since the attackers don't have knowledge about the nature of data transmitted. This improves the security level of information with reduced computational complexity.

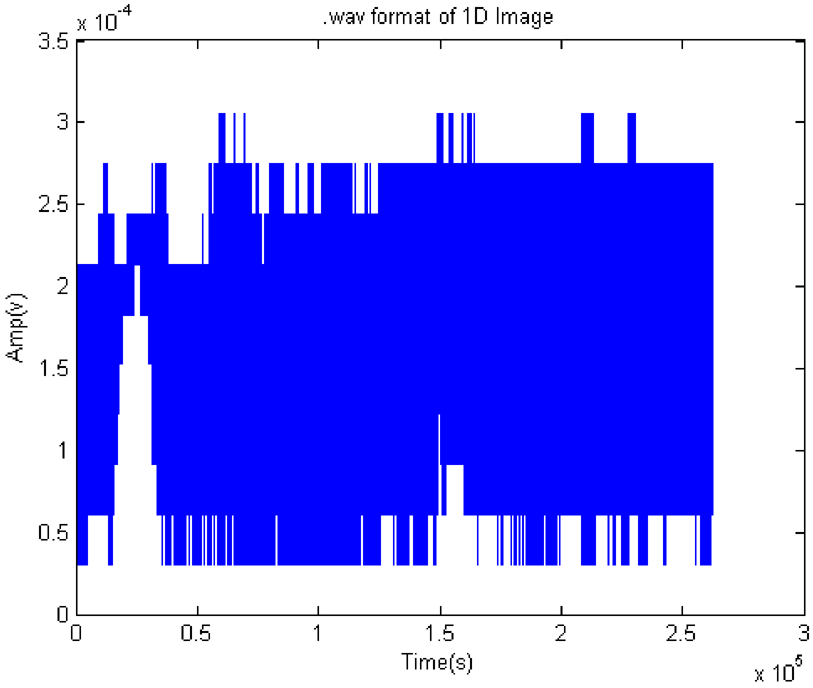

Figure 4. Equivalent audio signal

Figure 5 shows the reconstructed image from the audio signal. In order to reconstruct the image, the audio file has to be de-normalized by the same scaling factor used in transmitter side and then converting the 1D audio file back to the 2D array to extract the image information.

Figure 6 shows the difference or error in pixel values between the input image and the reconstructed image. Though the reconstructed image has some noises in the pixel intensity, it gives sufficient information about the input image.

4. Conclusion

A novel algorithm for improving the level of security in image transmission is proposed. Here instead of encrypting the image directly, the input image is scaled and converted into audio format and the transmitted as an audio file. At the receiver side the audio file is once again scaled back to restore the input image. Since the information is in the form of audio signal, it is much difficult to recognize the data hidden in the audio signal. Thus the image information is hidden in the audio medium which makes it more robust and secures especially when the transmission takes place in public communication.

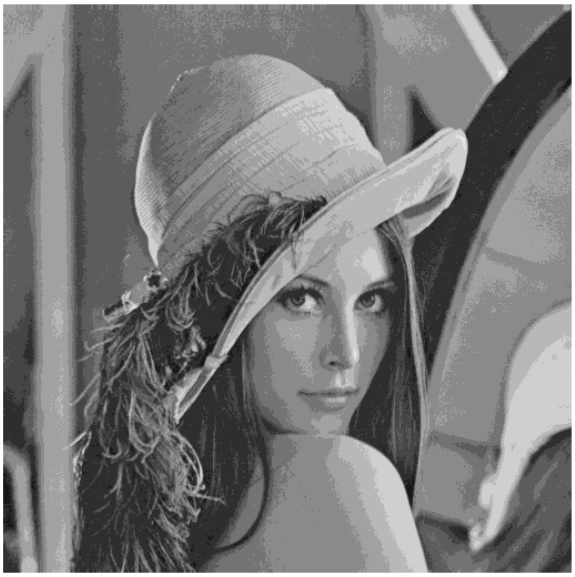

Figure 5. Reconstructed Image

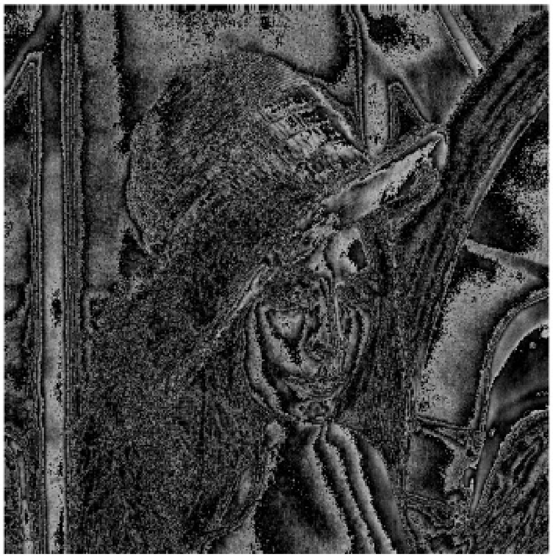

Figure 6. Error Image

Acknowledgements

We are grateful to Hindustan Institute of Technology and Science and B. S. Abdur Rahman Crescent Institute of Science and Technology for providing HTRF fund and research lab facilities.

Conflicts of Interest

There is no conflict of interest.

References

[1] Weiqi Luo, Fangjun Huang, Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", in IEEE Transactions on Information Forensics and Security, Volume: 5, Issue: 2, pp. 201-214, 2010, DOI: 10.1109/TIFS.2010.2041812.

[2] Xinpeng Zhang, Shuozhong Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction", in IEEE Communications Letters,Volume:10,Issue:11,November2006,DOI: 10.1109/LCOMM.2006.060863.

[3] Bin Li; Ming Wang, Xiaolong Li, Shunquan Tan, Jiwu Huang, "A Strategy of Clustering Modification Directions in Spatial Image Steganography", in IEEE Transactions on Information Forensics and Security, Volume: 10, Issue: 9, pp. 1905-1917, 2015, DOI: 10.1109/TIFS.2015.2434600.

[4] Bingwen Feng, Wei Lu, Wei Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", in IEEE Transactions on Information Forensics and Security, Volume: 10, Issue: 2, pp. 243-255, 2015, DOI: 10.1109/ TIFS.2014.2368364.

[5] Linjie Guo, Jiangqun Ni, Wenkang Su, Chengpei Tang, Yun-Qing Shi, "Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited", in IEEE Transactions on Information Forensics and Security, Volume: 10, Issue: 12, pp: 2669 – 2680, 2015, DOI: 10.1109/TIFS.2015.2473815.

[6] Debnath Bhattacharyya, Tai-hoon Kim & Poulami Dutta, "A method of data hiding in audio signal", in Journal of the Chinese Institute of Engineers, Vol 35, Issue 5, pp. 523-528, 2012, DOI: 10.1080/02533839.2012.679054.

[7] Alexandre Santos Brandao, David Calhau Jorge, "Artificial Neural Networks Applied to Image Steganography", in IEEE Journals & Magazines, Volume: 14, Issue: 3, pp.1361- 1366, 2016, DOI: 10.1109/TLA.2016.7459621.

[8] Vahid Sedighi, Rémi Cogranne, Jessica Fridrich, "Content-Adaptive Steganography by Minimizing Statistical Detectability", in IEEE Transactions on Information Forensics and Security, Volume: 11, Issue: 2, pp: 221 - 234, 2016, DOI: 10.1109/TIFS.2015.2486744.