International Journal of Research in Engineering, Science and Management
Volume-2, Issue-2, February-2019
www.ijresm.com | ISSN (Online): 2581-5792

Data Hiding in Grayscale Images using Least Significant Bit Technique

V. Thamizharasi
Senior Grade Lecturer, Department of ECE, Government Polytechnic College, Trichy, India

***Abstract*: Among all digital file formats available nowadays image files are the most popular cover objects because they are easy to find and have higher degree of distortion tolerance over other types of files with high hiding capacity due to the redundancy of digital information representation of an image data. There are a number of steganographic schemes that hide secret message in an image file; these schemes can be classified according to the format of the cover image or the method of hiding. Steganography attempts to hide the very existence of the message and make communication undetectable. It has many technical challenges such as high hiding capacity and imperceptibility. In this project, a technique for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the wavelet coefficients of the cover image with the key generation. Least significant bit technique is to increase the security of the hidden data. The proposed system showed high hiding rates with reasonable imperceptibility compared to other steganographic systems.**

***Keywords*: Hiding, key generation, secret data, steganography, wavelet.**

1. Introduction

The technologies have advanced so much in the current trends of the world that the most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via e-mails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the 'security threat'. It poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time.

A. Data hiding techniques

In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography and Watermarking. Cryptography is the art of science used to achieve security by encoding the data to transform them into non readable formats so that unauthorized users cannot gain access to it. The encoded text is known as 'Cipher text' and this technique is known as encryption and this process is reversed with authorized access using the decryption technique, in which the encoded data is decoded into readable format. Steganography is the art of hiding and transmitting data through apparently innocuous carriers to conceal the existence of data. The level of visibility is decreased using many hiding techniques in 'Image Modeling' like 'LSB manipulation', 'Masking and filtering'. These techniques are performed by different steganographic algorithms like F5, LSB, JSteg etc, and the act of detecting the information hidden through these algorithms is called 'Steganalysis'. It provides further security by hiding the cipher text into a seemingly invisible image or other formats. Digital watermarking is described as one of the possibilities to close the gap between copyright issues and digital distribution of data. It is mainly based on steganographic techniques and enables useful safety mechanisms. It acts as a very good medium for copyright issues as it embeds a symbol or a logo in the form of a watermark, which cannot be altered manually.

B. Uses of steganography

Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted. It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside. It can also be used to implement watermarking. Although concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information.

C. LSB based image steganography

Digital image has a large amount of redundant data and therefore it is possible to hide data into the image file. An image is the collection of numbers which constitute different light intensities in different areas of an image. This type of numeric representation forms a grid and individual points are called as pixels. If we see any specific color closely it will be observed that single digit modification to the contribution level that are imperceptible to our eye in RGB color representation.

1) Grayscale images

A grayscale or gray level image is simply one in which the only colors are shades of gray. The reason for differentiating such images from any other sort of color image is that less information needs to be provided for each pixel. In fact, a 'gray' color is one in which the red, green and blue components that all have equal intensity in RGB space and so it is only necessary to specify a single intensity value for each pixel, as opposed to the three intensities needed to specify each pixel in a full color image. Often, the grayscale intensity is stored as an 8-bit integer giving 256 possible different shades of gray from black to white. If the levels are evenly spaced then the difference between successive gray levels is significantly better than the gray level resolving power of the human eye. Grayscale images are very common, because much of today's display and image capture hardware can only support 8-bit images. In addition, grayscale images are entirely sufficient for many tasks and so there is no need to use more complicated and harder-to-process color images. In this paper, the image size is taken as 512*512. The color images can also be used for data hiding, which are converted to grayscale for the process. To convert any color image to grayscale representation, first obtain the values for its red, green, and blue(RGB) of each pixel. Then add together 30% of red value, 59% of green value, and 11% of the blue value, that produce the single gray value in the scale 0 to 255 for every pixel of the color image.

2) LSB technique

Least significant bit is the most common type of insertion scheme used currently in digital steganography. This is probably easy way of hiding data in an image, and yet it is surprisingly effective. The secret information is hidden by altering least significant bit in the image file. If we change the MSBs in an image, it will produce a noticeable impact. However, changing the LSBs will not be noticeable to the human eye. The image formats used in the LSB substitution are lossless and secret data can be directly manipulated and recovered. In grayscale images, every pixel is represented by using 8-bits, in which 11111111(=255) represents white and 00000000(=0) represents black. So there are 256 different grayscale shades between black and white. Consider an 8-bit grayscale image in which each pixel is stored as a byte that represents a grayscale value. If the first 8 pixels of the cover image have the following grayscale values:

10011000 01100100 10101101 10010110
00111011 01010101 00010110 01000101

If the letter C is used to hide, first it is converted into binary value as 10000011, then it will replace the LSBs of these pixels to have the following new grayscale values:

10011001 01100100 10101100 10010110
00111010 01010100 00010111 01000101

Note that, on average, only few LSBs need to change. So there is no visible difference between cover and stego image.

LSB insertion has the following advantages.

- Quick and easy
- Works well with gray-scale images
- There is no theoretical outstanding mark of LSB insertion, if not a little increase of background noise.
- It's very easy, instead, to extract LSBs even with simple programs, and to check them later to find if they mean something or not.

2. Proposed work

To transmit the data very securely, it is hidden into the image using steganography. The data embedding and extracting are done by least significant bit technique. Discrete wavelet transform is used to help the data hiding and reconstruction of image.

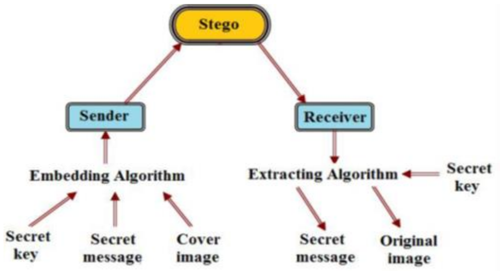


Fig. 1. Proposed method

A. Discrete wavelet transform

Wavelets (i.e. small waves) are mathematical functions that represent scaled and translated (shifted) copies of a finite-length wavelet called mother wavelet. A wavelet transform(WT) is based on wavelets. It is used to analyze a signal(image) into different frequency components at different resolution scales. This allows revealing image's spatial and frequency attributes simultaneously. The Discrete Wavelet Transform(DWT) provides a compact representation of a signal's frequency components with strong spatial support. DWT decomposes a signal into frequency sub bands at different scales from which it can be perfectly reconstructed. Any wavelet-based image processing approach has the following steps:

- Compute the 2D-DWT of an image
- Alter the transform coefficients (i.e. sub bands)
- Compute the inverse transform

To apply DWT on images, first apply a one level discrete wavelet to each row and column of the resulting 'image' of the first operation. The resulted image is decomposed into four sub bands: LL, HL, LH, HH sub bands (L=Low, H-High). The LL-sub band contains an approximation of the original image while the other sub bands contain the missing details. The LL-sub band output from any stage can be decomposed further. In this paper, single level decomposition is enough for data hiding process.

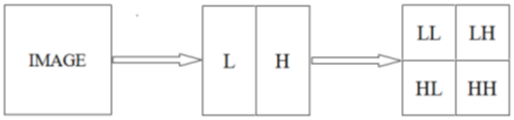


Fig. 2. Single level decomposition

Discrete wavelet transformed images can be perfectly reconstructed with four sub bands by using the inverse discrete wavelet transform.

B. Secret key

The key is a secret code, which is something the sender and recipient agree on beforehand. That is, shared for both embedding and extraction process, used to hide the secret message into the image. In this paper, the secret key is taken as 4-bit integer value.

C. Embedding process

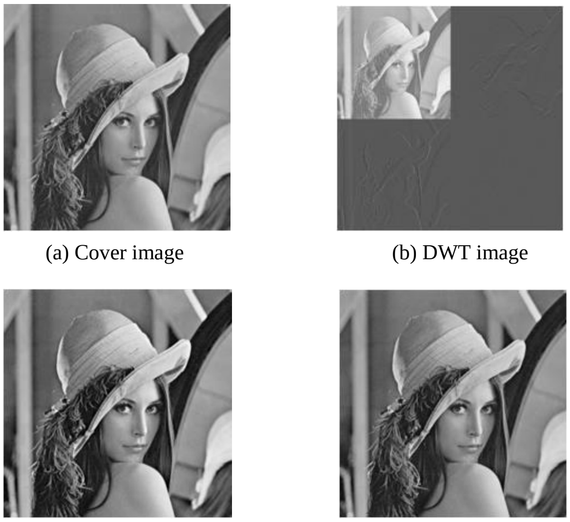
This section has the inputs like cover image and secret data with secret key and the output of this process is text embedded image. First, discrete wavelet transform is applied to the cover image. So the image is converted into 4 sub bands, 3 high pass channels corresponding to vertical, horizontal and diagonal, and one approximation image. Therefore, the data hiding is done only on the low pass channel. All the pixels in the LL-band are extracted and it is stored in the array called pixel array which contains 8 binary bits for each pixel. Then all the characters in the text file are extracted, which are converted into their ASCII equivalent characters and subsequently into binary digits. The last bit of first letter of text is replaced in the LSB of first pixel of LL band by using Least Significant Bit technique. After that second last bit of first letter is embedded into the LSB of second pixel.

This process is continued up to all bits of secret data should be embedded into pixels of the LL-band. Then the technique for combining embedded LL-band with other 3 sub bands is called inverse wavelet transform which gives perfect reconstruction. Finally, it produces the stego image. This image can be transmitted to the recipient through the unsecured channel.

D. Extraction process

This section consists of embedded image file as the input with secret key and secret text message as the output. First, discrete wavelet transform is applied to the stego image. It separates the image into 4 sub bands. The LL-band is selected for extraction process. To extract the data, the secret key is important. If the key entered by the recipient matches with the sender's key, then only the extraction process will be started. Otherwise, the program will be terminated. Thus the key plays a vital role in the message extraction. After matching the key, the data is extracted from the LSB of each pixel in the LL-band. The bits of the LSB are retrieved and placed in the array. Then content of the array converts into decimal value that is actually ASCII value of the secret message. The data is retrieved without any loss of information and the image is reconstructed by using inverse discrete wavelet transform. The original image is obtained which is similar to the cover image.

3. Experimental results



(a) Cover image (b) DWT image

(c) Stego image (d) IDWT image

Fig. 3. Experimental results

enter 4 bit Key

****

Fig. 4. Secret Key

This proposed method ensures high hiding rates and also maintaining the security in high levels. The experimental work is done by using MATLAB and the messages are successfully embedded into the cover images. The complexity of the image is not disturbed. The difference between the stego image and cover image can hardly be distinguished after using the LSB insertion technique. The size of stego image is same as the size of original image and most importantly the messages are also extracted successfully.

Experiment results are based on the following steps:

1. The input image with size of 512*512 is taken as grayscale image. The color image can also be converted into grayscale image for this process.
2. The discrete wavelet transform is applied to separate the image to subbands, which is used to help the embedding process.
3. Secret data is created by us in the notepad file and save the document. This data is used for hiding into the input image.
4. Secret key is given as integer values with four bits, which is same for both embedding and extracting processes.

5. The embedded image contains secret data bits at the least significant bit of each pixel in the low sub band of DWT image using LSB technique.
6. After applying the extraction process with secret key, the image is reconstructed using inverse discrete wavelet transform.
7. The secret data can be extracted from the image, and then it is displayed in the Editor window of the MATLAB.

4. Conclusion

The data hiding technique using LWT and LSB replacement or secret data communication is implemented. The LSB method is used here to increase the hiding capacity and minimize the distortion. Optimal pixel adjustment process is also followed by embedding process to reduce embedding error. Here the application is also secured by RSA algorithm to transmit the data effectively. Further it can be implemented by using encryption technique which provides more security with this system.

References

[1] Lionel Fillatre, “Adaptive steganalysis of LSB replacement in Grayscale natural images” IEEE transactions on signal processing, vol. 60, no. 2, February 2012.

[2] R. Böhme, “Advanced Statistical Steganalysis”. New York: Springer, 2010.

[3] J. Fridrich, “Steganography in Digital Media-Principles, Algorithms and Applications”. New York: Cambridge Univ. Press, 2009.

[4] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, “Digital Watermarking and Steganography”. San Francisco, CA: Morgan Kaufmann, 2007.

[5] A. Ker, “Steganalysis of LSB matching in grayscale images,” Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. .2005.

[6] H. Sencar, M. Ram kumar, and A. Akansu, “Data Hiding Fundamentals and Applications: Content Security in Digital Multimedia”. Elsevier: Academic, 2004.

[7] O. Dabeer, K. Sullivan, U. Madhow, S. Chandra sekaran, and B. S. Manjunath, “Detection of hiding in the least significant bit,” IEEE Trans. Signal Process., vol. 52, no. 10, pp. 3046–3058, 2004.

[8] P. Lu, X. Luo, Q. Tang, and L. Shan, “An improved sample pairs method for detection of LSB embedding,” in Proc. Int. Workshop on Inf. Hiding, 2004, vol. 3200, pp.116–127.