A Survey on Image Steganography Techniques

*Bhumika Neole¹, Pallavi Parlewar², Prerana Jain³, Akshita Samant⁴, Vedant Khire⁵, Radhika Sainani⁶

¹*Assistant Professor, Shri Ramdeobaba College of Engineering and Management, Nagpur, India

²Associate Professor, Shri Ramdeobaba College of Engineering and Management, Nagpur, India

^{3,4,5,6}Department of Electronics and Communication Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, India

ABSTRACT

Steganography refers to the exchange of hidden data. It deals with the study of invisible communication between the sender and the receiver. In today's modern world transferring secured data over a network is the main concern, hence for secured communication steganography is used. The data that is to be sent is concealed behind a text, image, or an audio file. The attacker or the eavesdropper, who observes the object with embedded data, will not notice it and thus would not try to decrypt the hidden data. Steganography is useful in many areas like efficient confidential communication, protection from data modification, and media database systems. It preserves the confidentiality of the information, which ensures that during communication there will be no alteration in the content of the information. Steganography can be classified into image steganography, audio/video steganography, or text steganography. This paper gives an overview of image steganography and its various techniques to hide the data behind the image. The techniques are discussed and analysed based on their ability to hide the information securely.

KEY WORDS: HIDDEN DATA, SECURED COMMUNICATION, IMAGE STEGANOGRAPHY, DISCRETE COSINE TRANSFORM (DCT), DISCRETE WAVELET TRANSFORM (DWT).

INTRODUCTION

Steganography is an important tool required to hide data. It differs from cryptography. In cryptography we use a certain code language to hide the data, which does not assure full security. But in steganography we encrypt the data using a key, and only users with the key can see the hidden material. There are various types of steganography like image steganography, text steganography, audio steganography etc. As their names suggest, we can hide data using texts images and audios.

In image steganography a cover image is used to hide the original image and the overall result image is said to be a stego image. There are various steganography techniques. They are majorly divided into spatial and frequency domain. The techniques mentioned in this paper are LSB, Masking and filtering, Spread Spectrum, pixel value difference, Statistical method, Distortion techniques, DCT and DWT.

LSB method involves modification of LSB layer of cover image, since the magnitude of change is very small it is not visible to human eye and the stego image looks similar to cover image though it has data embedded on it. In masking and filtering, significant pixels on the cover image are chosen where the secret message will be embedded, instead of hiding the data behind the cover image i.e. the information is not stored at the 'noise' level but stored inside visible areas of the image. Statistical methods change the properties of the image and it uses 1 bit message modification. Distortion techniques blur the image and insert hidden data.

ARTICLE INFORMATION

*Corresponding Author: neoleba@rknc.edu

Received 17th Oct 2020 Accepted after revision 29th Dec 2020

Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA

Thomson Reuters ISI Web of Science Clarivate Analytics USA and Crossref Indexed Journal

NAAS Journal Score 2020 (4.31)

A Society of Science and Nature Publication, Bhopal India 2020. All rights reserved.

Online Contents Available at: <http://www.bbrc.in/>

Doi: <http://dx.doi.org/10.21786/bbrc/13.14/85>

Spread Spectrum is achieved by combining three different techniques: spread spectrum, error encoding and image processing. The main principle of Spread Spectrum is the integration of Hidden data into noise, which is then applied to the digital image. In pixel value difference, the cover image is split into non-overlapping blocks of two connecting pixels and the difference is altered in each section. Discrete cosine transform or DCT is a method used to transfer the image into frequency domain. The process of image hiding in frequency domain has shown better result when comparison is made with spatial domain for performing the same function. In Image Steganography, DCT is a widely used method. Discrete wavelet transform or DWT transforms the image in frequency domain. As mentioned earlier, data hiding works best in frequency domain. Unlike DCT, DWT is divided into 4 frequency bands instead of 3 as low-low, low-high, high-low and finally high-high frequency bands.

MATERIAL AND METHODS

a. Least Significant Bit (LSB): LSB or Least Significant Bit method is the simplest approach used in Image Steganography. It involves alteration of least significant bits of cover image, the changes in the LSB bit of a random pixel is not recognizable by the human visual system as the amplitude change is very small.

This approach involves following steps:

Encryption-

1. Selecting the cover image and the secret text message which is to be sent.
2. Converting the secret text message into binary code.
3. Find Least Significant Bit of each pixel of cover image.
4. Substitute LSB bit of image with individual bit of secret text.
5. A final stego image which looks similar to cover image is formed.

Decryption-

1. Get the stego image.
2. Evaluate the LSB bit of each pixel of stego image.
3. Recover the bits and decode the 8 bit character.
4. The secret message is decrypted.

For example:

Since each pixel has three components Red(R), Green (G) and Blue (B), the above image (Figure 1) illustrates how LSB bit of each component can be substituted with the bit of the secret text that is to be sent. The final stego image obtained looks similar to the cover image. The LSB method has a few advantages such as no human perceptible distortions can be observed in the stego image, large amount of data can be encrypted in the cover image. This approach lacks in some of the aspects like it can be easily detected by the stego attacks i.e. data is less secure and it is also less robust in nature.

b. Masking and Filtering: This method functions close to that of watermarking technique. Though masking modifies the cover image but it is not visible to human eye. Due to this the technique is more robust in nature than LSB technique in case of a lossy compression algorithm. The pixels are chosen by specific mathematical expression hence the security of this steganography method is strengthened.

It involves the following steps:

Embedding the secret information-

1. Choose the significant pixels of cover image using a mathematical key.
2. The grey pixel values are converted
3. Transform the secret information into bits.
4. If first bit in the secret text is zero, then the first pixel value will not be changed.
5. If first bit is one, then the first pixel is made odd by adding one to the pixel value.
6. Continue this step till all the secret bits are embedded.
7. The new pixels are then put back to form the stego image.
8. Decoding the secret information-
9. Look for the specific pixels in the stego image by using the same mathematical key.
10. If the value of the pixel is odd, then the embedded bit is one.
11. If the value of the pixel is even, then the embedded bit is zero.
12. Find the entire embedded bits
13. Convert the bits into character to find the secret text.

c. Spread spectrum: The main principle of Spread Spectrum is the integration of Hidden data into noise, which is then applied to the digital image. This noise is similar to the noise in image acquisition method. When this noise is kept at low levels it is not seen by the human eye, neither is detected by the computer unless the computer have real image. For Spread Spectrum to be a blind steganography, to recover an approximation of the embedded signal applied to the cover, a sort of the original image must be obtained from the stego image. Image restoration method is used to manage it. Ultimately, since the noise is of low power and the method of restoration is not perfect. Embedded signal estimation is low which results in a high rate of embedded signal bit error (BER), which is not ideal. A low-rate error-correcting code is integrated to compensate it.

In this way an accurate blind image steganography is achieved with the help of combination of communication and image processing technique. This approach offers a technique for hiding a digital signal inside a cover image by not increasing the image dimension or dynamic span. The requirement that both sender and recipient have the same keys offers a degree of protection. In addition, relative to the cover picture, the embedded signal power is negligible, giving a low chance of noticing and leaving an observer unknowing that the hidden data exists. Disadvantages of Spread Spectrum are that its robustness is limited, increased complexity, large Bandwidth and if the pseudo random generator is not synchronised properly, the desired output is not obtained.

d. Pixel value differencing (PVD): In this process the cover image is split into non-overlapping blocks of two connecting pixels and the difference is altered in each section. The bigger difference in the original pixel value allows for a bigger improvement. The number of hidden bits that can be hidden depends on the edge or smooth region of the pixel. The difference between the neighbouring pixels is greater in the edge area, while it is smaller in the smooth area. Therefore, more data in the edge region is embedded in pixels than in the smooth area. Since this device integrates data by directly changing the difference value between two adjacent pixels instead of changes in pixel values, it offers better outcome in terms of hiding and stego image quality compared to LSB data hiding process replacement. value difference lacks in security of the data, decoding process of the method is often incorrect, reduces precision at curves and corners, sensitive to noise and time consuming.

e. Statistical methods: Statistical steganography, changes the statistical parameters of the image to hide the data. It uses 1 bit modification. The cover image is split into blocks and 1 message bit is embedded in each block. It is modified only if the size of the message is 1 otherwise there is no change in cover while restoring the original message. A test is required to differentiate between modified and unmodified blocks which make it difficult to apply. Statistical methods are hard to apply as there is need of proper testing and also a function to implement the whole procedure.

f. Distortion techniques: In distortion techniques, the image is distorted in order to send the secret message. The message is extracted by calculating the difference between original and distorted image. For example, to indicate a 0 no change is made, for 1 a random value is added. This method is not reliable as it requires the knowledge of original image and if unauthorized users have the access to the original data, they can decode the image easily using the same procedure. Distortion techniques are hardly used as it does not ensure proper security of the hidden data.

g. Discrete cosine transform method: DCT divides the image in three frequency bands like low, med and high frequency bands. DCT has some disadvantages like very low bit rate and distortion in image coefficients

at higher frequency. Therefore, DCT is combined with another technique to improve its performance. An image is divided into 8x8 pixel blocks and 2D-DCT or 1D-DCT (applied twice, row and column) is performed on each of these blocks which decomposes the image into 64 harmonic cosine coefficients. Amongst 64 coefficients, only 1 is a DC coefficient and the rest are AC coefficients. These coefficients are altered to hide the information. There are many methods which uses DCT to hide information. For example, when a text message needs to be embedded in an image, the LSB bit of DC coefficient of the cover image is altered to hide the message.

One author used the secret image is Huffman encoded and then is embedded into the LSB DC coefficient of the cover image. There was a proposed method where the DC coefficient above threshold were only altered and this threshold was assigned by the respective author. Another author used Arnold's transform scrambles the secret image. More the number of iterations, more scrambled the image but after some iterations, the image starts getting restored. Here, the author scrambled the image with 10 iterations. Now, 2D DCT transform is performed on the cover image and then quantization of coefficient is altered using the scrambled image. The operations are performed in medium range frequency. To get the secret image, inverse DCT is performed on both stego and cover image. Then Arnold's transform 10 iterations are performed resulting into the original image.

h. Discrete wavelet transform method: DWT has similar process like DCT for image steganography. DWT has higher payload capacity but low PSNR value indicating that the quality of image is reduced. One author suggested a method where Haar-DWT was combined with Singular Value Decomposition (SVD). SVD is used for image compression, noise reduction and image watermarking. Here, DWT transform is applied for all the frequency bands of the cover image and text message is converted into binary and then into binary image or secret image. Then, SVD outlines the cover image as well as the secret image to improve the quality of the stego image. Quality of image provided by DCT surpasses other methods. The method of using DCT with Arnold's Transform offers PSNR value greater than 40 and MSE value near to 1 which surpasses other methods. But, Arnold's Transform is a complex method and its anti-transform takes a lot of time. Also DCT has low payload capacity. Whereas, DWT has a larger payload capacity but lower quality of the image. Hence the method of DWT with SVD is a very efficient and provides optimised solution to all the observing factors. It has PSNR value above 40 and MSE value near 1 with a larger payload capacity.

CONCLUSION

This paper gives an overview of steganography and types of image steganography. The various techniques like LSB, masking and filtering, spread spectrum, pixel value differencing, statistical, distortion, DCT and DWT have been reviewed and analysed on the basis of how securely data can be hidden behind an image. The efficiency of the

method can be best determined by the security of the data and the quality delivered after decoding the stego image. The comparison parameters observed under quality of the image are its robustness, payload capacity, distortion after decoding, etc. We found that LSB method does not provide essential security to the data being transferred and its less robust in nature. Masking and filtering was insufficient in payload capacity and restricted to grey scale images. Disadvantages of Spread Spectrum are that its robustness is limited, increased complexity, large Bandwidth and if the pseudo random generator is not synchronised properly, the desired output is not obtained.

PVD lacks in security of the data, decoding process of the method is often incorrect, reduces precision at curves and corners, sensitive to noise and time consuming. Statistical methods are hard to apply as there is need of proper testing and also a function to implement the whole procedure. Distortion techniques are hardly used as it doesn't ensure proper security of the hidden data. Quality of image provided by DCT surpasses other methods. The method of using DCT with Arnold's Transform offers PSNR value greater than 40 and MSE value near to 1 which surpasses other methods. But, Arnold's Transform is a complex method and its anti-transform takes a lot of time. Also DCT has low payload capacity. Whereas, DWT has a larger payload capacity but lower quality of the image. Hence the method of DWT with SVD is a very efficient and provides optimised solution to all the observing factors. It has PSNR value above 40 and MSE value near 1 with a larger payload capacity. Therefore, we propose the method comprising combination of DWT and SVD the efficient method amongst other mentioned method.

REFERENCES

- Adam Nevriyanto, "Image Steganography combining Discrete Wavelet Transform and Singular Value Decomposition", 2018 IEEE conference ICECOS.
- Anjali Tiwari, "A Review on Different Image Steganography Techniques", IJEIT, Volume 3, Issue 7, January 2014, pp 121-124.
- Anupriya Arya and SaritaSoni," A Literature Review on Various Recent Steganography Techniques".
- Ashadeep Kaur, Rakesh Kumar, Kamaljeet Kainth,"Review Paper on Image Steganography",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 6, Issue 6, June 2016.
- Barnali Gupta Banik, "Implementation of Image Steganography Algorithm using Scrambled Image and Quantization Coefficient Modification in DCT", 2015 IEEE conference ICRCICN.
- J. Anita Christaline , D. Vaishali, "image steganographic techniques with improved embedding capacity and robustness", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, MIT, Anna University, Chennai. June 3-5, 2011.
- J. K. Mandal and Debashis Das," Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain", International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.
- K. Thangadurai and G.SudhaDevi,"An analysis of LSB Based Image Steganography Techniques",2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 - 05, 2014, Coimbatore, INDIA.
- Lisa M. Marvel, Charles G. Boncelet, Jr., and Charles T. Retter," Methodology of Spread-Spectrum Image Steganography", ARL-TR-1698 June 1998.
- Mansi S. Subhedara , Vijay H. Mankarb," Current status and key issues in image steganography".
- Masoud Nosrati ,Ronak Karimi, Mehdi Hariri," An introduction to steganography methods", World Applied Programming, Vol (1), No (3), August 2011. 191-195,ISSN: 2222-2510.
- Mehdi Hussain, Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, May, 2013, pp 113-124.