International Journal of Advanced Science and Technology
Vol.104 (2017), pp.43-52
http://dx.doi.org/10.14257/ijast.2017.104.05

Comparative Analysis of Canny Edge based Image Steganography with RSA Encryption

Sanjay Yadav[1] and A. K. Thripati[2]

Department of computer science & Engineering [1, 2]
Institute of Technology &Management, Gwalior [1, 2]
sy23557@gmail.com[1], rajendrasingh.ind@rediffmail.com[2]

Abstract

In this survey, we give a brief overview on image steganography, which is based on Edge detection with RSA and Least Significant Bit (LSB) methods. There are two main problems, viz. Steganography and Cryptography. In the Cryptography process, it changes the arrangement of the text itself, whereas in Steganography covers the text behindhand some other digitally illustrative media, thus communicating it unintentionally. But with the enlarge in networks practice and advancements in expertise, it has developed progressively more difficult to defend the facts. The proposed method takes different types of color (RGB) image as a carrier to hide text data. The encrypting text with the support of a key which makes the location of unique content difficult still if some impostor succeeds in obtaining the hidden data. The canny detection method is used to hide encrypted message and the hash function is used to embed text message or data in the image. The proposed method is going to be implemented using MATLAB and its strength will be matched through computing the mean square error and the peak signal noise ratio. Probably the proposed method may have better security against Steganalysis attacks.

Keywords*: RSA; PSNR; MSE; Canny Method; Image Steganography*

1. Introduction

Image Steganography is the art of hiding concealed mails in a way that none the receiver knows message behind, this is used in contrast with cryptography wherever the way of life of the message itself is not hidden but the content is hidden. The same process is done with steganography likewise cryptography where the message is hidden within others, so no one aware of any kind of message. For use of steganography method apply to cover files like any archives of video, image or sound files are mostly used. Similarly, hiding information can be anything: text, image, video, sound, etc. [1]

Steganography algorithms work in two domains as spatial domain (altering the desired characteristics on the file itself) and the transform domain (performing a series of changes to the cover image before hiding information. To select the best areas the Discrete Cosine Transform (DCT), Wavelet Transform, etc. are used). The algorithm work in the spatial domain is simpler and faster, whereas transform domain are more robust and resistant to attacks. In spatial domain the best known stenographic method is Least Significant Bit (LSB) [1], which exchange the LSB of pixels selected to hide the information. This method has several implementation versions that improve the algorithm in certain aspects [1].

ISSN: 2005-4238 IJAST

Table 1. Comparison between Steganography and Cryptography

Steganography	Cryptography
Unknown Message passing	Known Message passing
It prevents the discovery of existence of communication	Encryption prevents an unauthorized party from discovering the contents of a communication
Little Technology is known	Common technology is used
Steganography doesn't modify or alter the secret message structure	Cryptography modify or alter the structure of the secret message

2. Kinds of Steganography

In steganography the information can hide in different ways as:

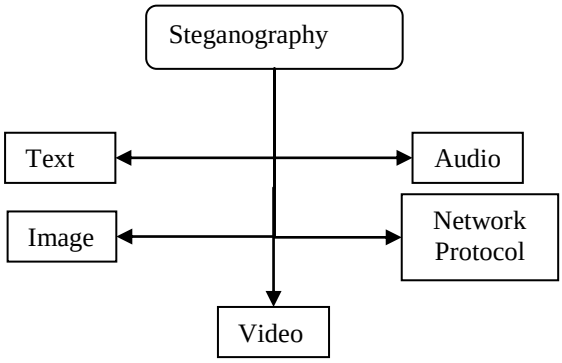

Figure 1. Digital Methods to Achieve Steganography [5]

2.1. Text Steganography

This method is used to hide a top-secret memo in each n^{th} letter of each word of a text message. Text steganography using digital records is not second hand very often because the text files have a very lesser amount of dismissing data.

2.2. Image Steganography

In this method, images are used as the general cover substances for steganography. In digital image a message is embedded through an embedding algorithm, using a secret key. The resultant stego image is sent to the receiver. On the other side, it is processed via the extraction algorithm by the same key. At the transmission of stego image unauthenticated person only seen image transmission and can't find the covered message

2.3. Audio Steganography

In this method hide information that is imperceptible to the human ear. An audible, sound can be noiseless in the occurrence of another louder noticeable sound. This property permits to select the channel in which to hide info. [3]

2.4. Protocol Steganography

In this method insert statistic within network protocols such as TCP/IP. We hide statistics in the header of a TCP/IP packet in certain fields that can be whichever optional or else are never used.

3. Properties of Steganography

Steganography refers to conceal data in an overt carrier file in such a manner, so that a third party intruder is difficult to recover or detect the hidden data. The efficiency of steganography algorithm is determined by three properties: [6, 7].

3.1. Hiding Capacity

It refers to the hiding number of bytes covered inside the carrier file without any damage or distortion. In case of image steganography, hiding data is most important as much as possible inside carrier image without an increase in brightness or making blurry and without changing size and pixelating. This is a key factor in making hidden data imperceptible and carrier image innocent and unsuspicious.

3.2. Imperceptibility

It refers to the ability of the steganography algorithm to hide data in an undetectable way so that no one can see any visible artifacts or distortions in the carrier file. Therefore avoids the worries about any secret communication is taking place.

3.3. Irrecoverability

It refers to how much an intercepted carrier file can be easily decoded and reverse-engineered so as to extract the data hidden inside it. An irrecoverable steganography algorithm makes it hard for eavesdroppers and unauthorized third parties to recover the hidden data from the carrier file despite knowing that steganography has been employed.

4. Methodology

4.1. Spatial Domain Methods

In this method the secret data are embedded directly in the intensity of pixels. It means image some pixel values are changed directly during hiding data. Spatial domain techniques are classified into following categories:

4.1.1. LSB:

This method is generally used for hiding data. In this embedding is done by changing the least significant bits of image pixels with the bits of secret data. The generated image after embedding looks same as the original image because the change in the LSB of image pixel does not bring too much difference in the image.

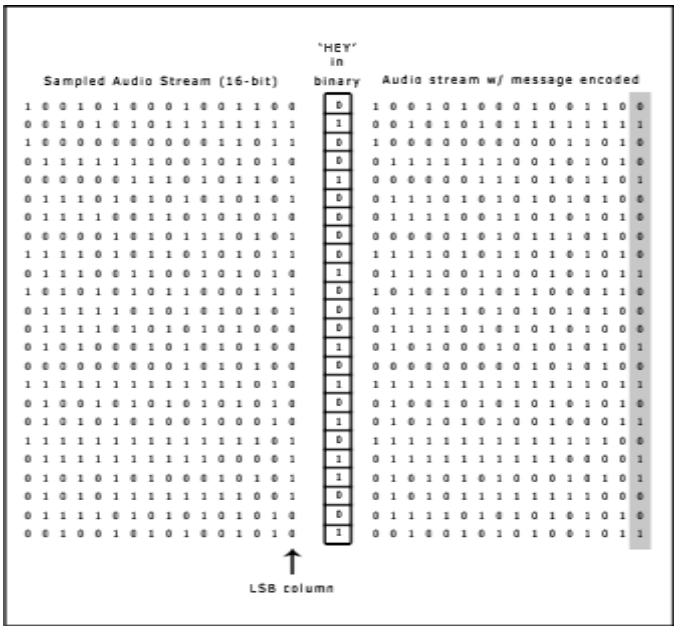

Figure 2. LSB Coding Example

4.1.2. BPCP:

In this segment, the images are used by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data.

4.1.3. PVD:

In this method, for embedding the data, select two sequential pixels. The payload is calculated by checking the difference between sequential pixels and it defines whether such pixels belong to smooth the area or edge area.

4.2. Spread Spectrum Method

In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it is becoming difficult to detect the presence of data. Even if parts of the data are eliminated from several bands, there would be still enough information is present in other bands to recover the data. Thus, completely removing data is difficult without entirely destroying the cover. It is a very robust technique mostly used in military communication.

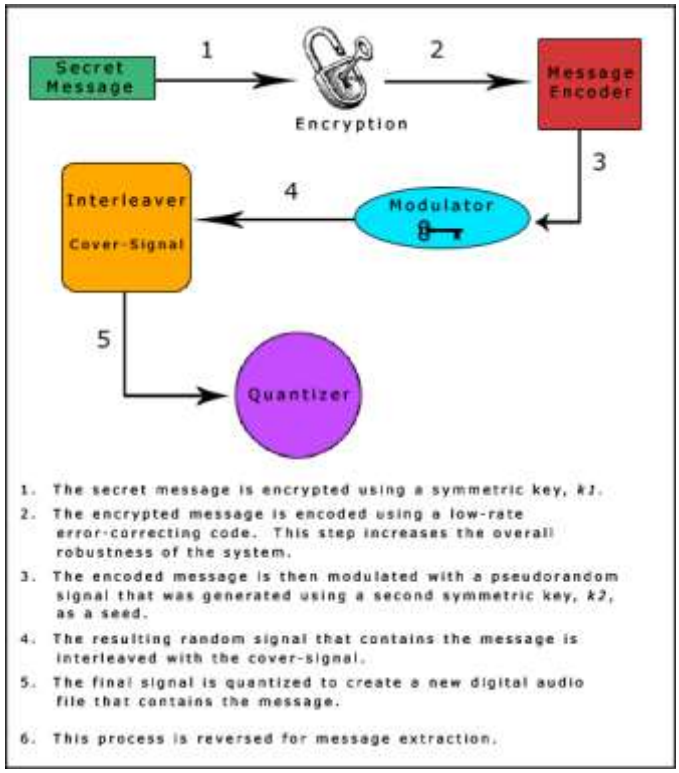

Figure 3. Spread Spectrum (SS)

4.3. Statistical Method

In this method, the message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one, otherwise no modification is required.

4.4. Transform Domain Method

In this method; the secret message is embedded in the transform or frequency domain of the cover. It is a more complex method for hiding messages inside an image. Several different transformations and algorithms are used to hide message in an image. Transform domain techniques are broadly classified such as

- Discrete Fourier transforms technique (DFT)
- Discrete cosine transforms technique (DCT)
- Discrete Wavelet transforms technique (DWT)
- Embedding in coefficient bits communication.

4.5. Distortion Method

In this method, the secret message is stored by altering in signal. A number of modifications are applied over the cover by the encoder. At the other end, decoder find the difference between original cover and the distorted cover to identify the order of the modifications and subsequently recover the secret message.

4.6. Masking and Filtering Method

In this method hide information by marking an image. Steganography only hides the information, whereas watermarks become a portion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level. The

watermarking method applied over an image without worry of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and grayscale images. [4]

5. RSA Algorithm

The RSA algorithm works in pair, i.e; use of two keys (d and e), for decryption and encryption, respectively. A plaintext message P is encrypted by cipher text C

C =Pe mod n

The plaintext is recovering from

P = Cd mod n

Now a colored image is taken as carrier and its edge is used to hide the secret message. Every pixel in a color image composed of three colors (channels) i.e. Red, Green and Blue each of 8 bits. In the proposed technique, all the three components have been used for data embedding. An edge is used to take the advantage of being undetected because editing in edge areas cannot be easily detected by the human visual system. The edge area may contain a large number of secret bits as compared to smooth areas. Edge detection is the process of identifying the sharp changes in intensity of adjacent pixels. The point where discontinuity occurs in an image is identified as edge. For edge detection canny edge detector is used which is based on finite difference approximation of the partial derivatives. First image smoothing is performed using Gaussian filter, then gradient magnitude and orientation is computed with the help of partial derivatives. The location on the edge where data has to be embedded is calculated by the hash function. This hash function deals with the LSB bit position within the pixel and the position of each hidden image pixel and also with the number of bits of the LSB.

6. Canny Edge Detection

It is the process of identifying points in a computer image at which the brightness of image changes abruptly, for instance, pixels deviating from low intensities to high intensities or vice versa, exhibiting some discontinuities [13]. The main objective of edge detection is to identify and capture important events and changes in the properties of the image.

7. Applications of Steganography

- E-Commerce
- Database Systems.
- Digital watermarking.
- Confidential Communication and Secret Data Storing
- Access Control System for Digital Content Distribution
- Protection of Data Alteration

8. Comparative Analysis

Table 2. Comparative between Techniques

Domain	Technique	Advantages	Disadvantages
Spatial	Adaptive LSB	Integrity of secret hidden information with High Capacity	Hide extra bits of signature with hidden message
Spatial	Texture, Brightness and Edge based Adaptive LSB	High Hidden Capacity with Considering of Good Visual Quality	Experimental Dataset is limited
Spatial	PVD (on edges) with Adaptive LSB (smooth)	High Hidden Capacity with Considering of Good Visual Quality	Computational Complex
Spatial	Hybrid (canny + fuzzy) edge detection with LSB	High PSNR with high hidden capacity	Limited Dataset with ideal images and Extensive edge based images may fail
Transform	DCT Coefficient based	High PSNR	Noticeable artifact of hidden data
Transform	DWT Coefficient permuted and embedding in Spatial domain	Integrity of hidden data in stego-image	Computationally complex
Transform	Secret bits plus Bit-depth embedded into coded-block	Useful for binary image	Not for Color image support

9. Related Work

In this section, we are presenting some of the research work of the prominent authors in this field and will be giving various ways in which secure image Steganography is done using edge detection.

In author proposed an approach that provides high embedding capacity and better quality stego image by combing LSB technique with edge detection. Two edge detection techniques: fuzzy edge detection and canny edge detection are performed on image successively. The combination of both edge detectors gives a large number of edge pixels with less computational overhead. After detecting the edge pixel image is divided into block of n pixel and first pixel contains status information of all pixels in that block. And

finally embedding is performed based on edge pixel and smooth pixel using the LSB substitution method. The proposed method has property to resist Steganography from statistical Steganalysis. [7]

In "author presented improved PVD method with modulus function. Instead of modifying the pixel value the reminder of two consecutive pixels is calculated and secret data are embedded by modifying these reminder values. The proposed PSNR is higher due to improved edge distortion. [8]

In describing the image steganography, which is based on canny method. Besides employing the hash based approach as a fundamental stage, it takes advantage of edge detection technique. The proposed scheme achieves high embedding capacity and enhances the quality of the encoded image. The proposed scheme first detects the edges in the image by well-known canny method and then the hash sort is used to embed the text data into the edges of the color image. The hash function provides a secure and fast approach for image steganography. [10]

In this paper, image steganography using LSBMR with Sobel edge detection presented and analyzes the LSB matching revisited (LSBMR) algorithm and the edge adaptive image steganography based on LSBMR. They conducted several experiments on algorithms with a set of 200images. The improvement can be seen by using some image processing technique called Sobel edge detection to find the edges of the images that can hold the secret information. The result showed that proposed technique improves the quality of the steganography images where sharper edges are used for low capacity rate. [11]

In this paper presented an improved LSB based Steganography technique for better information security of hiding secret statistics in descriptions. There is a huge range of steganography methods having some complex issues than others and all of them have corresponding strong and weak topics. It confirms that the eavesdroppers will not have any mistrust that memo bits are hidden in the image and normal steganography detection procedures can't evaluate the length of the secret message appropriately. In this paper, it presented improved Steganalysis methods, based on the most consistent detectors of thinly-spread LSB steganography currently known, concentrating on the case when grayscale Bitmaps are cast-off as cover images. [12]

10. Conclusion

In this survey presented existing work on image steganography. The data is hidden in the edge by finding location using hash function, thus providing a higher PSNR value. It makes the technique more robust and secure. Moreover, the image size does not change after hiding the text in it. Expected results show that the proposed scheme is successful in not only achieving a high embedding payload, but also in obtaining a stego image of satisfactory quality. In the future work, we will use the combination of LSBRSA and canny method.

References

[1] J. J. Roque, J. M. Minguet, J. C. Maxwell, "SLSB: Improving the Steganographic Algorithm LSB", Universidad Nacional de Educación a Distancia (Spain), pp 1-12.
[2] T. Sharp, "An implementation of key-based digital signal steganography", Proc. 4th International Workshop on Information Hiding. Springer LNCS, vol. 2137, **(2001)**, pp.13-26.
[3] P. C. Mandal, "Modern Steganographic technique: A survey", International Journal of Computer Science & Engineering Technology (IJCSET), vol. 3, no. 9, **(2012)**, pp. 444-448.
[4] J. Kour, D. Verma, "Steganography Techniques –A Review Paper", International Journal of Emerging Research in Management &Technology, vol. 3, no. 5, pp. 132-135.
[5] M. Hussain and M. Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology, vol. 54, **(2013)**, pp. 113-124.

[6] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, "Authentication of secret information in image steganography", IEEE Region 10 Conference, TENCON-2008, **(2008)**, pp. 1-6.
[7] W.-J. Chen, C.-C. Chang, T. Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications vol. 37, **(2010)**, pp. 3292–3301.
[8] Jeong-Chun Joo, H.-Y. Lee, and H.-K. Lee1, "Improved SteganographicMethod Preserving Pixel-Value Differencing Histogram with Modulus Function", Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing, **(2010)**.
[9] S. P. Kaur, S. Singh, "A New Image Steganography Based on 2k Correction Method and Canny Edge Detection".
[10] K. Singla1, and S. Kaur, "Hash Based Approach For Secure Image Steganography Using Canny Edge Detection Method", vol. 3, no. 1, **(2012)**, pp. 155-157.
[11] Z. Fouroozesh, J. Al ja'am, "Image Steganography based on LSBMR using Sobel Edge Detection", pp. 141-145.
[12] M. Devi, N. Sharma, "Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images", Proceedings of 2014 RAECS UIET Panjab University Chandigarh, **(2014)**, pp. 06 – 08.
[13] Y. Bassil, "Image Steganography based on a Parameterized Canny Edge Detection Algorithm", International Journal of Computer Applications, vol. 60, no.4, **(2012)**, pp. 36-40.
[14] C. D. Scott and R. E. Smalley, "Diagnostic Ultrasound: Principles and Instruments", Journal of Nanosci. Nanotechnology, vol. 3, no. 2, **(2003)**, pp. 75-80.

