International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Comparative Analysis of Image Hiding Approach in Encrypted Domain Based on Histogram Shifting Method

Irfanul Haque[1], Vipra Bohara[2], Laxmi Narayan Balai[3]

[1]P. G. Scholar, [2]Assistant Professor, [3]H.O.D,
Electronics & Comm, Yagyavalkya Institute of Technology, Jaipur, Rajasthan, India

ABSTRACT

In this paper we have used an efficient algorithm for hiding secret image also called payload in different types of cover image using histogram shifting method of reversible data hiding technique. Image utilized is jpeg, bmp and tiff images. We have analyzed this algorithm in MATLAB simulation tool. In this analysis we have calculated some parameters by varying payload in different types of cover image.

Keywords: *Steganography, Histogram, Fragile, Spatial, Reversible Data Hiding*

1. INTRODUCTION

Security of digital multimedia information, over networks has always been a difficult task for researchers and engineers. Nowadays, internet provides secure data communication for vital messages, secret data, images and documents. But with advanced hacking devices, any secured communication can be broken effortlessly. To eliminate this problem, two techniques have been developed; cryptography and steganography. In cryptography, the secret data hidden in the encrypted data can only be extracted using the private key. Despite the fact that the hacker gets access to an encrypted data, it is not possible to extract the secret content. But if the private key is broken or stolen, this technique will no longer secure the data. Secret data can also be hidden behind a cover image to such an extent that an observer is not aware of its existence. This kind of data hiding is called steganography.

Till now, many algorithms for information hiding have been presented but most of them unable to recover the cover image after secret data extraction. However, in some military and medical applications, it is wanted that the original cover image to be recovered without any loss after data extraction. The marking methods satisfying this requirement are known as reversible data hiding methods.

In the present time, fragile reversible data-hiding methods can be executed in three domains, that is, spatial domain, transformed domain and compressed domain. Semi-fragile data-hiding methods can be executed only in spatial and transform domain since high-level information about the architecture of the data stream generally is not available in compressed domain with embedded secret information. In case of spatial domain, the estimations of the pixels of the cover image are modified directly to embed the information. In case of transform domain, the cover image must be preprocessed by a transform, which are known as integer wavelet transform (IWT), discrete cosine transform (DCT), discrete wavelets transform (DWT) and discrete Fourier transform (DFT), to obtain the frequency coefficients. At that point, the frequency coefficients are altered slightly to embed secret information. Due to this alteration stego image is obtained. In compressed domain, the compression code is modified to embed the data.

Majority of the published literatures related to the reversible data-hiding methods address fragile methods because it is very tough to recover the cover image without any loss if the stego image passes through a lossy modification, such as JPEG compression. A nice fragile reversible data-hiding method should provide high embedding capacity and low distortion altogether. So, the main aim of fragile

methods is to provide a secure channel to protect secure communication among legitimate users.

2. STEGANOGRAPHY

Information Hiding methods have been gaining much attention today. The main goal for this encryption and decryption processes is that here the secret information is completely hidden and therefore does not gain attention. This process of hiding secret information is known as Steganography. Steganography or Stego as it is regularly referred to in the IT sector, literally signifies, "Secured writing" which is taken from the Greek language. Steganography is described by Markus Kahn as follows, "Steganography is the science and art of communicating in a manner which hides the presence of the communication. The objective of Steganography is to hide data inside other harmless data in a way that does not enable any attacker to even detect that there exists a second data". Steganography can be utilized in a huge amount of data formats [5] in today's digital world. The most fundamental data formats utilized are .doc, .bmp, .jpeg, .gif, .txt, .mp3 and .wav essentially because of their popularity on the Internet and the easy process of using the steganographic tools that depends on these data formats. These data formats are also popular due to their relative ease by which noisy or redundant information can be extracted from them and replaced with a hidden data.

3. HISTOGRAM SHIFTING

The basic histogram shifting scheme for reversible data hiding was first introduced by Zhicheng in 2006. In this proposed scheme, the image histogram is generated at first by considering all the pixel values of an image. To insert secret data, some pixel values are changed. At the receiver, for extracting the concealed data, the changed pixels are returned back to their actual condition. Thus the reversible data hiding scheme is obtained. During data embedding, at first from the image histogram the pair of zero and peak points are searched. The zero point refers to the pixel with least repeated value and the peak point refers to the pixel with most repeated value in the image histogram. Here, data is carried only by the peak pixel values. The peak pixel value is modified by 1 closer to the zero point for the corresponding secret data O. Where the data is 1 the peak pixel values remain unchanged. The pixels in between the pair of peak and zero points are also modified by 1 to a value closer to zero point but they do not carry any secret data. After processing all the pixels sequentially, the stego-image is produced. At last, the processed-image and the pair of peak and zero points are ready to transmit. At the receiver, the concealed data is regained and the actual image is regenerated. Lena image and its histogram are shown in Fig. 1 & Fig. 2 respectively.

Fig-1: Lena image

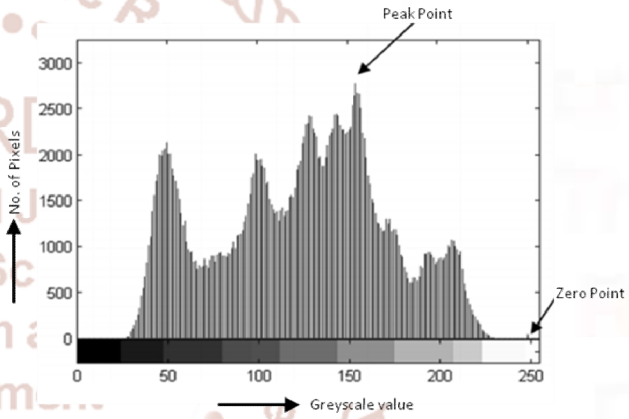

Fig-2: Histogram of Lena image

4. PROPOSED WORK

In our work we have comparatively analyzed an algorithm for finding various features of cover image by hiding different types of payload using histogram shifting method of reversible data hiding procedure. All the simulations are carried out in MATLAB simulation tool. Fig. 3 shows the algorithm to hide image in cover image and to obtain the stego image.

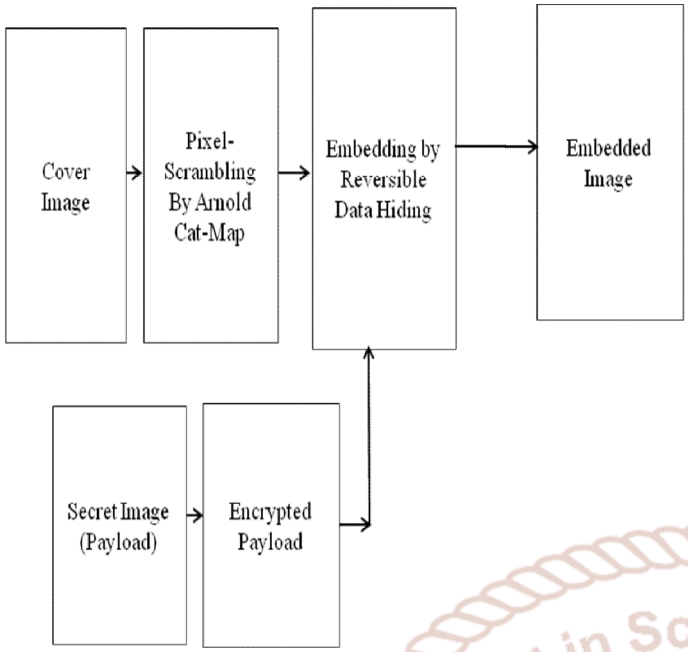

Fig-3: Proposed method to generate stego image

In this technique initially, the cover image in which secret image (payload) is hidden is selected. Then encrypted domain of a secret image is obtained with the help of Arnold cat map by using number of iteration and this parameter is treated as one part of secret key which is required at the time of retrieve the same original secret image at receiver side. After this, partial encrypted secret image is obtained. Now the histogram of cover image is calculated and find out the maximum repeated pixels in that image so that the total maximum repeated pixels are found out with their pixel locations.

The maximum repeated pixels provide the information of embedding capacity of data which is converted and obtained by the secret image. Then enter the secret image which is to embed, converted it into its pixel values and then converted into binary stream with the help of ASCII code.

Now, embedding of secret image in encrypted domain of image is done by proposed histogram method of reversible data hiding technique by selecting only maximum repeated pixel values, converted these pixels into their binary equivalent value and embed the ASCII converted binary stream of secret image as per proposed technique of histogram shift method of reversible data hiding. Then the pixels which are most responsible are converted back into their decimal equivalent and restore into their original position in encrypted domain and finally encrypted image is obtained.

5. EXPERIMENTAL RESULTS

In the proposed work we have considered different types of cover image of size 256 x 256 and different types of secret image (payload) of size 32 x 32. Histogram of cover image is calculated by MATLAB tool. Fig. 5,6 & 7 represents different types of cover image and Fig. 8, 9 & 10 represents different types of payload image.

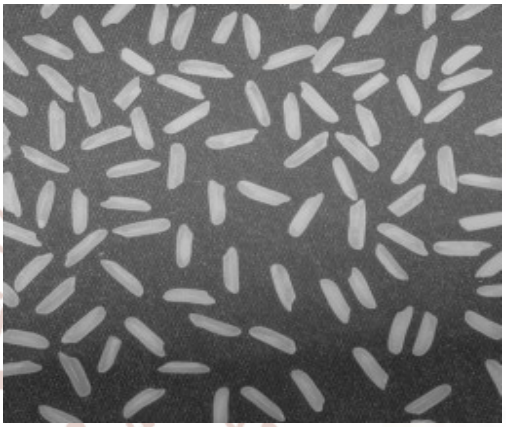

Fig5: Cover image as rice.png

Fig-6: Cover image as cameraman.tiff

Fig-7: Cover image as pirate.tiff

Fig-8: Payload as cameraman.tiff

Fig. 9 Payload as woman.tiff

Fig. 10 Payload as gorilla.tiff

In our work we have analyzed each cover image for hiding different types of payload and calculated some features for each case which are shown below.

Table 1: Results for rice.png

Payload	MSE	Normalized SNR	PSNR (dB)
cameraman.tiff	96.0492	0.9075	56.6117
woman.tiff	93.8172	0.9123	59.1832
gorilla.tiff	92.3176	0.9154	62.5925

Table 2: Results for cameraman.tiff

Payload	MSE	Normalized SNR	PSNR (dB)
cameraman.tiff	91.4864	0.8414	58.1678
woman.tiff	88.2796	0.8793	57.3444
gorilla.tiff	88.2145	0.8934	56.1567

Table 3: Results for pirate.tiff

Parameter	MSE	Normalized SNR	PSNR (dB)
cameraman.tiff	91.3567	0.8235	54.6544
woman.tiff	90.1954	0.8354	55.3234
gorilla.tiff	89.2586	0.8592	56.3564

6. CONCLUSIONS

In conclusion, it has been concluded that from histogram calculation of cover image we have found out the maximum repeated pixels values and minimum repeated pixel values. We have avoided the minimum repeated pixels value and considered only maximum repeated pixel values and embedded the secret image. We have analyzed each cover image for different payload and compared the results.

REFERENCES

1) Yu-Chiang Li, Chia-Ming Yeh, and Chin-Chen Chang, "Data hiding based on the similarity between neighbouring pixels with reversibility", International journal for Digital Signal Processing, 2009.

2) C. C. Chang, J. Y. Hsiao, and C. S. Chan, "Finding optimal LSB substitution in image hiding by dynamic programming strategy", Pattern Recognition, 2003.

3) Piyu Tsai, Yu-Chen Hu, and Hsiu-Lien Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting", International journal of Signal Processing, 2009.

4) S. Katzenbeissar and F. Petitcolas, "Information hiding techniques for steganography and digital watermarking," Artech House, 1999.

5) Zhao, Y., Pan, J.S., and Ni, R., "Reversible data hiding using the companding technique and improved DE method", Circuits Systems and Signal Processing, , 2007.

6) S. Jajodia, N. F. Johnson, and Z. Duric, "Information hiding: Steganography and Watermarking-attacks and Countermeasures," Springer, 2001.

7) Mehrabi, M.A, Faez, K, and Bayesteh, A.R, "Image steganalysis based on Statistical Moments of Wavelet Sub band Histograms in Different Frequencies and Support Vector Machine", 3 rd International Conference on Natural Computation, 2007.

8) Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang, "Reversible data hiding based on histogram modification of pixel differences", IEEE, 2009.