International Journal of Pure and Applied Mathematics
Volume 114 No. 12 2017, 267-276
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue
ijpam.eu

A Steganographic Method for Digital Images Using Harris Method

[1]S. Mangayarkarasi and [2]P. Sujatha

[1]Vels University, Chennai, India.

smangai.research@gmail.com

[2]Vels University, Chennai, India.

suja.research@gmail.com

Abstract

Now a day, every information is transmitted over the internet and mobile phones. But security is necessary for our information sharing. This is accomplished through data hiding. Steganography is an art of hiding secret information. It allows people to communicate and sharing of information secretly. The main scheme of Steganography is to hide secret data into any one of the mediums, i.e. Text, Image, Audio, and Video. In this paper, Harris corner detection method is used and using this method the corresponding interest points between a pair of images are identified.

Key Words: Information security, data hiding, steganography, corner metric, harris method.

1. Introduction

In modern times data hiding is associated with digital forms. The digital forms are cryptography, Steganography and watermarking. Cryptography is obscures the content of the message, but not the communication of the message. Watermarking is a pattern of bits inserted into a digital image, audio or video file, which identifies the files copyright information. The word Steganography combines the Greek word “steganos” and “Graphein”. Steganos means covered or concealed and Graphein means writing [5]. Steganography means “covered writing”, is hiding the communication of the message. In steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document, image, program or protocol. Media files are ideal for steganographic transmission because of their large size [2][4].

Steganography is a branch of information hiding. It allows the people to communicate secretly. As increasingly more material becomes available electronically like internet, mobile phones, etc. The influence of steganography on our lives will continue to grow. Much confidential information was leaked to a rival firm using steganographic tools that hide the information in music and picture files. Steganography can be used for various applications. Such as Military, Intelligence Agencies, Copyright control and Defense Organizations.

2. Image Steganography

In steganography the information may be hiding in different format. There are five different formats are followed. In this image Steganography is a branch of Steganography; digital images are the most popular carrier file format [1]. For hiding secret information in images there is a large number of techniques are available. The recent image steganography techniques can be classified into [7, 8]:

- Spatial Domain
- Transform Domain
- Spread Spectrum
- Compressed Domain
- Statistical Technique
- Distortion Technique

The two major techniques of image steganography are: Spatial domain and transform domain image steganography [1]. One of the most popular techniques of spatial domain image steganography is least significant bit (LSB) method. The spatial Domain techniques, also known as substitution techniques. In this the data (pixel values) has directly embedded image [15]. The common methods used in this domain are LSB, PVD, PMM, Texture based, Histogram based and Color palette based methods. In LSB technique information are hidden in the least significantbit, the rightmost bit is called the LSB because changing it has the least effect on the value of the number. The second method is transforms domain [3]. The various transform domain techniques are DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) and FFT (Fast Fourier Transform) are used to hide secret information in the form of transform coefficients of the cover images such as compression, filtering etc.

Major components used in image steganographyas:

A. Cover-Image: Cover image means original image, in which the secret information is going to be hidden. The cover image is sometimes called as “host”.

B. Stego-Image: The medium in which the information is hidden. The "stego" data is the combination of the cover image and the "embedded" information.

C. Payload: The information which is to be concealed. The information to be hidden in the cover data is known as the "embedded" data.

D. Secret key: It is a sequence of data generated by the sender during the embedding process and the same can be used by the receiver to recover the embedded message.

E. Embedding Algorithm: An algorithm used to hide the message.

F. Extracting Algorithm: An algorithm used to unhide the message.

3. Literature Review

In [9] Da-Chun et.al proposed embedding method is the quantization of differences of gray values of two-pixel blocks. In this method difference d is computed from every non-overlapping blocks of two consecutive pixel p_i and p_{i+1}, the two-pixel blocks run through all the rows of each image in a zigzag manner. The pseudo random scheme is used for extracting the embedded message.

Akhil et.al proposed Pixel pair matching [10], in this for embedding processing is performed by two levels of masking: spatial frequency masking and luminance masking. The two masking considers the exact region for data embedding. And Pixel pair method is used to extract the data. This method offers various MSE similarities Using different payload such as 1.907 bpp , 2.861 bpp, 3.815bpp.

In [11] Wien Hong proposed adaptive pixel pair matching. During Embedding process the coordinates (x,y) is replaced by one of the coordinates in ϕ(x,y).

Vipul et.al [12] proposed an image steganography method is comprised of two embedding techniques are data hiding technique and data retrieving technique. In data hiding a secret image and key is in the cover image; while the data retrieving technique is used to retrieve the key and the hidden secret massage from the stego image.

In [13] DebiprasadBandyopadhyay et.al proposed method logistic chaotic map method (C-LSB) is used to encrypt the secret message and then the secret message is embedded into the cover image using the base embedding technique. The logistic map is used to encrypt the secret data bits before embedding to enhance the security of the image steganography as the secret data bits are not embedded directly into the cover image.

In [14] Dipti.G.Dighe et.al proposed random insertion using data parity , R(x,y) is used as a controlling element & pair of data bits are embedded into G(x,y) & B(x,y). For any sequence of message bit pairs (m1, m2) (m3, m4). .. .. (m i-1,mi).

$$F(x,y)=R(x,y)+ G(x,y)+ B(x,y)$$
$$(R(x,y) + 2) \bmod(4) = 0$$

The difference between message bit pairs & two least significant bits of G(x,y) is calculated using

$$OE = G(b1,b0) -(mi-1,m\ i)$$

If OE is less than ±2, even parity data is embedded into G(x,y).

4. Proposed Method

In this paper, we proposed corner metric and corner point method is used as embedding algorithm and Harris algorithm is used as extracting intersect points between pair of images.

Corner Metric and Corner Point Method

Corner metric and corner point method traces the exterior boundaries of objects, as well as boundaries of holes inside these objects, in the binary image BW. Bwboundaries also fall down into the outermost objects (parents) and traces their children (objects completely enclosed by the parents). BW must be a binary image where nonzero pixels belong to an object and 0 pixels constitutes the background. The Output of corner metric and corner point method is represented in Fig 2, 3, 4 and 5.

Embedding Algorithm

Step 1: Select the original image

Step 2: Original image is converted into a binary image (grayscale image)

Step 3: Find the boundary region of image for analysis of image.

Step 4: Find corner features in agrayscale image.

Step 5: Secret data is appended to the grayscale image along with a secret key.

Step 6: output image is stego image.

Find Corresponding Interest Points between a Pair of Images Extracting Algorithm

The proposed method is local neighborhood and Harris algorithm. The corresponding interest points between a pair of images are identified using this method. The Output of Harris method is represented in Fig 6.

Step 1:Read stego images.

Step 2:Find the corners in the image.

Step 3: Extract the neighborhood features.

Step 4: Match the features.

Step 5: Retrieve the locations of corresponding points for each image.

Step 6: Visualize corresponding points

5. System Design

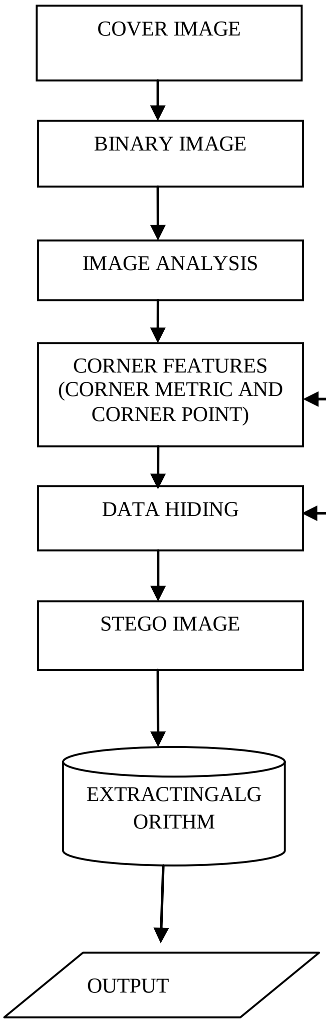


Figure 1: Proposed system

6. Experimental Results

The algorithm is tested in Matlab R2013a. Image Processing and Mapping toolbox can be used for testing. Image Processing Toolbox provides a comprehensive set of reference-standard algorithms, functions, and apps for image processing, analysis, visualization, and algorithm development. You can perform image analysis, image segmentation, image enhancement, noise reduction, geometric transformations, and image registration [6]. In Fig 2 represents the original image, then the image is converted into binary images represented in Fig 3. Then the boundary region of the image is identified, because within this region we can hide our information.

Figure 2: Original image Figure 3: Binary image

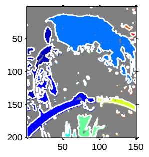


Figure 4: Boundary region

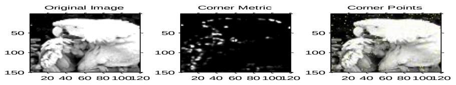


Figure 5: Corner features in grey scale image

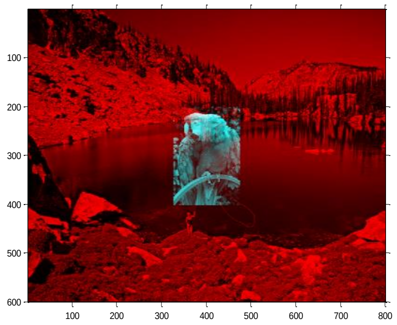


Figure 6: Interest points between a pair of images

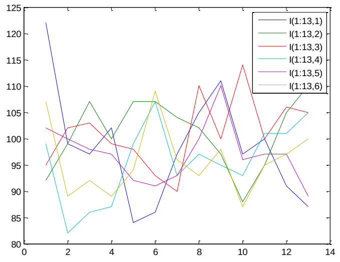


Chart 1: RGB Values of original Image I (Column 1 through 12)

7. Analysis

The performance of steganographic techniques can be measured by PSNR (Peak Signal to Noise Ratio) and MSE.

The Mean Square Error (MSE) is the cumulative squared error between the compressed and the original image [5].

$$\text{MSE } = \frac{1}{MN} \sum_{y=1}^{M} \sum_{\text{x}=1}^{\text{N}} [\,\text{I}(\text{x},\text{y}) - \text{I}'(\text{x},\text{y})]2$$

Where I (x,y) is the original image, I' (x,y) is the approximated version (the compressed image) and M, N are the dimensions of the images. A lower value of the MSE means lesser error.

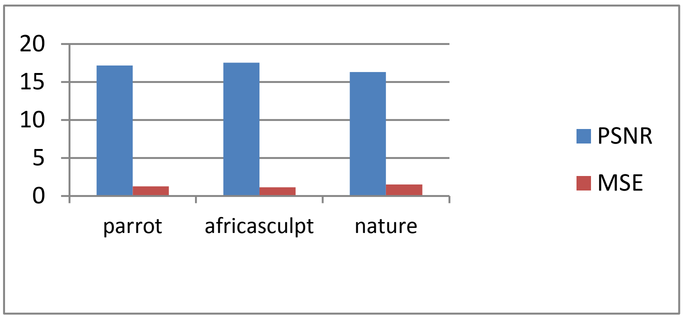
Peak Signal Noise Ratio (PSNR) is the measure of the peak error between two images in decibels. This ratio is often used as a quality measurement between the original and a compressed image. The PSNR value is higher; the quality of the compressed or reconstructed image is in better.

PSNR= 20 * log 10 (255 / Sqrt (MSE))

The higher value of the PSNR is good because the ratio of signal to noise is higher.

Table 1: Comparison between PSNR and MSE value for RGB Images

S.NO	IMAGE	PSNR	MSE
1	parrot	17.1627	1.2497
2	africasculpt	17.5287	1.1487
3	nature	16.3119	1.5202



8. Conclusion

This paper we have proposed Harris method and corner point method for image analysis. Using this method we can measure image boundaries and intersect points of stego images can be identified. It computes PSNR and MSE value of RGB images and Grey Scale images. The Higher PSNR value indicates the better quality of images.

References

[1] Khan I., Gupta S., Singh S., A New Data Hiding Approach in Images for Secret Data Communication with Steganography. International Journal of Computer Applications 135(13) (2016), 9-14.

[2] Sharma V., Kumar S., A new approach to hide text in images using steganography, International Journal of Advanced Research in Computer Science and Software Engineering 3(4) (2013).

[3] Banerjee I., Bhattacharyya S., Sanyal G., Hiding & analyzing data in image using extended PMM, Procedia Technology 10 (2013), 157-166.

[4] Cachin C., An information-theoretic model for steganography, International Workshop on Information Hiding Springer Berlin Heidelberg (1998), 306-318.

[5] Mangayarkarasi S., Sujatha P., Analysis of Digital Image Data Hiding Techniques, International Journal of Emerging Technologies in Engineering Research (IJETER) 4 (10) (2016).

[6] https://www.mathworks.com/products/image.html

[7] Jaber S.S., Fadhil H.A., Khalib A., Zahereel I., Kadhim R.A., Survey on Recent Digital Image Steganography Techniques, Journal of Theoretical & Applied Information Technology 66(3) (2014).

[8] Hamid N., Yahya A., Ahmad R.B., Najim D., Kanaan L., Steganography in image files: A survey, Australian Journal of Basic and Applied Sciences 7(1) (2013), 35-55.

[9] Wu D.C., Tsai W.H., A steganographic method for images by pixel-value differencing. Pattern Recognition Letters 24(9) (2003), 1613-1626.

[10] Akhil P.V., Jyotsna E., Divya J., An Improved Image Steganography Technique Using Pixel Pair Matching Driven by Spatial Frequency and Luminance Masking, International Journal of Advanced Research in Computer and Communication

Engineering 2(11) (2011).

[11] Hong W., Chen T.S., A novel data embedding method using adaptive pixel pair matching, IEEE transactions on information forensics and security 7(1) (2012), 176-184.

[12] Sharma V., Kumar S., A new approach to hide text in images using steganography, International Journal of Advanced Research in Computer Science and Software Engineering 3(4) (2013).

[13] Bandyopadhyay D., Dasgupta K., Mandal J.K., Dutta P., A novel secure image steganography method based on Chaos theory in spatial domain, International Journal of Security, Privacy and Trust Management (IJSPTM) 3(1) (2014), 11-22.

[14] Dighe D.G., Kapale N.D., Random Insertion Using Data Parity Steganography Technique, International Journal of Engineering Science and Innovative Technology 2(2) (2013), 364-368.

[15] Tiwari A., Yadav S.R., Mittal N., A review on different image steganography techniques, International Journal of Engineering and Innovative Technology (IJEIT) 3(7) (2014), 121-124.