International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 1, No. 2
April 2015

2nd National Conference on "Recent Advances in Science Engineering & Technologies" RASET 2015

Organized by

Department of EEE, Jay Shriram College of Technology, Tirupur, Tamil Nadu, India.

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Special Issue, Vol. 1, No. 2, April 2015
2nd National Conference on "Recent Advances in Science, Engineering&Technologies" RASET-2015

Research Paper

A NOVEL JOINT DATA HIDING USING ADAPTIVE PIXEL VALUE DIFFERENCE

K Navas Khan[1]*, K Karthick[1], M Udayakumar[1] and G Dheepak[1]

*Corresponding Author: ***K Navas Khan*** ✉ navaskhan1692"gmail.com

In recent years, various techniques are used for hiding data. By means of scannig of an image, compression is carried out in order to hide the secret data. This is done effectively using the Adaptive Difference Pixel(ADP) technique which the image using digital image processing with varying degree of goodness. The prime goal is to enhance the data hiding capacity without much deteriorating the quality of the picture under consideration. The underlying steganography algorithm used is Adjacent Pixel value Difference (APVD) technique available in literature. The selection of the range intervals is based on the characteristics of human visions sensitivity to gray value variations from smoothness to contrast. The Hamming binary distance (based on binary XOR operation) is used for computing distances. This hamming code was tested on a real natural image collection Results are very good both in terms of speed and accuracy allowing near real-time image retrieval in very large image collections. By this technique error diffusion is effectively reduced, eventually retain the pixel overflow. By this ADP technique Peak Signal to noise Ratio(PSNR) is improved .

Keywords: Adjacent Pixel Difference (APD), PSNR, Capacity, Data-hiding, Embedding rate

INTRODUCTION

Due to the rapid development of multimedia and internet, presently it has become easier for the hackers to edit, modify and duplicate the data. Now a day it necessitates finding appropriate protection because of the sensitivity of information. Steganography deals with the techniques used for protection of information. Itis the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message (Jarno Mielikainen, 2006). It is kind of security through obscurity.The steganography is used in applications, which includes confidential communication,secret data storing, for providing protection against data alteration. The secret information can be stored in cover files like text, image, audio and video. Most of the steganographic techniques hide secret data in images as it is relatively easy to implement (Jarno Mielikainen, 2006). The most important property of the cover source is the

[1] Department of Electronics and Communication, Narasu's Sarathy Institute of Technology, Salem.

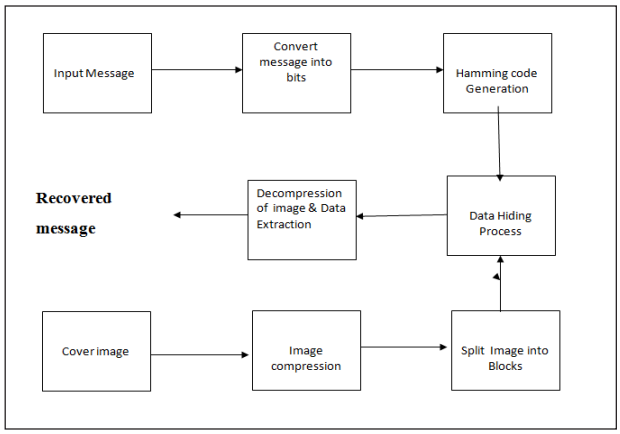
amount of data that can be stored in it without changing its properties. Many researches are working in this area and have proposed different techniques with varying capacities and with varying degree of success for hiding the data. Recently the neighbouring pixel difference techniques have gained interest among researches. It is a technique (Li Y C *et al*., 2010) in which difference of neighbouring pixel is taken of an image and the corresponding histogram is obtained. From the histogram peak points and zero points are calculated for embedding the data, as discussed ahead.However, there remain several issues which need to be resolved before an efficient steganography system is developed.

Inthis paper, we have investigated the issues of locating the appropriate location in a given image and have taken up the Adjacent Pixel difference (APD) technique (Li Y C *et al*., 2010) as the baseline algorithm. Three different benchmark images are taken and fixed message size is stored in all of them. The picture quality is measured by means of PSNR using MATLAB platform and compared. Certain terminologies pertaining to image analysis are discussed below: Histogram: The histogram represents the graphical representation of the tonal variation of digital images in image processing. It represents the number of pixels for each tonal value*.*

LITERATURE REVIEW

Yuan-Yu Tsai et.al in proposed a reversible data hiding algorithm for gray-scale images (Yu Tsai Y *et al*., 2012). The results revealed better in terms of embedding capacity and imperceptibility.Yu-Chiang Li et al. (Li Y C *et al*., 2010) presented data hiding using Adjacent Pixel Difference (APD) which used the histogram of the pixel difference for increasing the capacity of embedded data. The results were shown to have better embedding capacity and quality of image after hiding a data. proposed novel reversible data hiding algorithm, which could recover the original image from marked image after extracting a hidden message. This method used the zero or minimum points of the histogram of an image for embedding a data into the original image and the results were found to be better than that of other algorithms in terms of PSNR. In [6], ZaidoonKh. Al-Ani *et al*. provided a brief overview of the different types of steganography techniques and their classification. In Zhao *et al*. proposed a steganography method to embed the secret data into compressed images, video files so as to achieve a high embedding rate. N Senthil Kumara and R Rajesh presented image segmentation using an edge detection technique [7]. In [8] H. Motameni et al. proposed the method of hiding a text message in gray scale image. The results were noticed to be better in terms of security as that of existing method by converting an original image into binary image. T Morkel *et al.*, presented techniques used for image steganography and their uses. They tried to find the requirements of good steganography system and their uses according to the application. The results were concluded to be better in terms of efficiency of image segmentation as that of existing method. Hamid A Jalab *et al.*, presented a new information hiding system to make a steganography more secure. The results were found to be better in terms of security by using executive file as a cover file. In (Jarno Mielikainen, 2006) Abbas Cheddadet al. proposed different methods of existing steganography with some common standards by providing some embedding algorithm.

BLOCK DIAGRAM



Eg: Embedding data (1010)

a) Data Hiding(1010) in a 3X3 image

156	156	155
159	158	156
160	158	158

Host image

b) Arranging Pixel in raster scan order

155	156	155	156	158	159	160	158	158

c) Calculation of Adaptive Pixel Difference

155	-1	1	-1	-2	-1	-1	2	0

d) Shift and embed data secret data 1010

155	-2	1	-1	-3	-2	-1	2	0

e) Shifting and embeeding data

155	157	155	156	159	161	160	158	158

PRESENT WORK

In this work, we have analysed the APD algorithm by taking three benchmarking images. Basically our purpose is to detect the most appropriate location in an image, where the data can be embedded without much degradation of original image by calculating their PSNR.For this purpose we focused on different locations of the image and embedded a fixed size data by varying the block sizes. As the block size increases the number of edges tends to increase and its impact is analysed on the stego-image. The APD algorithm as described in section III was used, the images were taken in jpg format and their edges were calculated using MATLAB platform. Performancemetrics as used in the work are detailed below:

SECTION

The APDV deals with four section for hiding the data with the effectively embedding and compression rate as follows

1. Secret messageprocessing
2. Cover Image process
3. Data Hiding Process
4. Data Extraction

Secret Message Processing

The secret message process is carried out by steganography , it is an course of action which deal with hiding a message, image or file within another image. The secret image phenomenon is entitle as stego-image. In general stego-image is not discernible to Human visual System. The images like jpg,JPEG,RGB, adapt into the stego-image. This actual method is efficiently done by Adaptive pixel Difference value. Input Message is converted into ascii code and then ascii code is converted into bits.

Cover Image Process

In photography and computing, a grayscale or grey scale digital image is an image in which the value of each pixel is a single sample, that is, it

carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest.

Grayscale images are distinct from one-bit bi-tonal black-and-white images, which in the context of computer imaging are images with only the two colors, black, and white (also called *bilevel* or *binary images*). Grayscale images have many shades of gray in between

Image compression

Image compression is an application of data compression that encodes the original image with few bits. The objective of image compression is to reduce the redundancy of the image and to store or transmit data in an efficient form. This is efficiently conceded by vector Quantization. In this scheme image is certainly

Split into Residual blocks. Then evaluation of quality of compressed image is testified with the Formulae E>T.

Data hiding

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. The goal of Steganography is to mask the very presence of communication making the true message not discernible to the observer.

Data hiding in still images presents a variety of challenges that arise due to the way the human visual system (HVS) works and the typical modifications that images undergo. Additionally, still images provide a relatively small host signal in which to hide data.

Peak Signal to Noise Ratio (PSNR): This parameter computes the peak signal to noise ratio between two images. This ratio is used as a quality measure between original and embedded image. It is measured in decibels (dB). Higher the value of PSNR better is the quality of reconstructed image.

$PSNR$ = 10.log10($MAXI2/MSE$)

= 20log

MAXI M Here MAXI represents the maximum possible pixel value of an image. When the pixels are represented using 8 bits per sample, its value will be 255. The term MSE (Mean Square Error) represents the mean of the square of the differences in the pixel values between corresponding pixels of the two images and is given by:

MSE = 1mn

= $Ii,j – K(i,j)2$ (n–1)

Capacity: It is amount of data that can be safely hidden into the cover image without being detected. Higher the capacity, higher is the amount of data that can be embedded. Performance Analysis: The results as obtained on 3-benchmark images by varying block sizes are given below: a) Lena Image: The JPEG image of Lena is taken with bit size as 512x512. There are two different locations (Location 1 and Location 2) reflecting higher and lower edge densities selected in the image as shown in Fig4 and Fig 6. APD algorithm is applied on these locations and results obtained are shown in Table 1, Table 2, Figures 5 and 7. The size of the embedded data is taken as 1076 bits for all the test cases.

CONCLUSION

In this paper, we have proposed a steganographic method to embed secret data into still images by

using pixel-value diûerencing and least-signicant-bit replacement methods. It embeds more secret data into edged areas thansmooth areas in the cover image and has a better image quality by using PVD method alone. For the sake of increasing the capacity, we hid the secret datain the smooth areas by using LSB method and the edged areas are still usingthe PVD method. The experimental results demonstrate that the proposedmethod not only has an acceptable image quality but also can provide a large embedded secret data capacity.

REFERENCES

1. Li Y C, Yeh C M and Chang C C (2010), "Data hiding based on the similarity between neighbouring pixels with reversibility", *Elsevier Journal of Digital Signal Processing*, Vol. 20, pp.1116–1128.
2. Yu Tsai Y, Tsai D S and Liu C L (2012), "Reversible data hiding scheme based on neighbouring pixel differences", *Elsevier Journal of Digital Signal Processing*.
3. Zhao Z, Yu N, and Li X (2003), "A novel video watermarking scheme in compression domain based on fast motion estimation", in Proc. of IEEEIntl Conference on Communication Technology, pp. 1878-1882.
4. Ni Z, Shi Y Q, Ansari N and Su W (2006), "Reversible data hiding", *IEEE Trans. on Circuits and System for Video Technology,* Vol 16, pp. 354–362.
5. Morkel T, Eloff J H P and Olivier M S (2005), "An overview of image steganography", in Proc. of 5th Annual Information Security South Africa Conference (ISSA). Singh et al., *International Journal of Advanced Research in Computer Science and Software Engineering,* Vol. 3, No. 9, pp. 494-502 © 2013, IJARCSSE All Rights Reserved Page | 502.
6. Ani Z A I, Zaidan A A, Zaidan B B and Alanazi H O (2010), "Main Fundamentals for Steganography", *Journal of Computing*, Vol. 2 (ISSN: 2151-9617)
7. Chin-Chen Chang, Chi-Shiang Chan, Yi-Hsuan Fan (2006), "Image Hiding Scheme with Modulus Function and Dynamic Programming Strategy on Partitioned Pixels", *Pattern Recognition*, Vol. 39, No. 6, p. 1155-1167
8. Ker A (May 23-25, 2004), "Improved Detection of LSB Steganography in Grayscale Images", In Proc. 6th International Workshop, Toronto (Canada), Springer LNCS, Vol. 3200, p. 97–115.
9. Ker A (June, 2005), "Steganolysis of LSB Matching in Grey scale Images," IEEE Signal Process Letter, Vol. 12, No. 6, pp. 441– 444.
10. Jarno Mielikainen (2006), "LSB Matching Revisited", *IEEE Signal Processing Letters,* Vol. 13, No. 5, p. 285- 287.
11. Xiaolong Li, Bin Yang, Daofang Cheng, Tieyong Zeng (2009), "A Generalization of LSB Matching". *IEEE Signal Processing Letters*, Vol. 16, No. 2, pp. 69-72. 12. Stanley C A (2005), "Pairs of Values and the Chi-squared Attack", in CiteSteer., pp. 1-45.
13. Ker A (June, 2005), "Steganolysis of LSB Matching in Grey scale Images," *IEEE Signal Process Letter,* Vol. 12, No. 6, pp. 441– 444.
14. Halder T, karforma S (2013), "A LSB-Indexed

steganographic approach to secure E-governance data".paper presented at the SECOND INTERNATIONAL CONFERENCE ON COMPUTING AND SYSTEMS – 2013 (ICCS – 2013) SEPTEMBER 21 – 22, 2013, THE UNIVERSITY OF BURDWAN. Burdwan, West Bengal, India. ISBN(13): 978-9-35-134273-1 ISBN(10): 9-35-134273-5, p. 158.

15. Wu D C, Tsai W H (2003), "A steganographic method for images by pixel-value differencing", *Pattern Recognition Letters,* Vol. 24, pp. 9–10, 1613–1626.

16. Chang K C, Chang C P, Huang P S, and Tu T M (2008), "A Novel Image Steganographic Method Using Triway Pixel-Value Differencing," *Journal of Multimedia*, Vol. 3, No. 2, pp. 37-44.

17. Mandal J K, Debashis Das (2012), "Steganography Using Adaptive Pixel Value Differencing (APVD) for Gray Images through Exclusion of Underflow/Overflow ", *Computer Science & Information Series*, ISBN : 978-1- 921987- 03-8, pp. 93-102.

18. Wu H C, Wu N I, Tsai C S, Hwang M S (2005), "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", *IEE Proceedings-Vision Image and Signal Processing,* Vol. 152, No. 5, pp. 611–615.

19. Yang C H, Wang S J, Weng C Y (2007), "Analyses of pixel-value-differencing schemes with LSB replacement in steganography", In: *The Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 445–448.

20. Halder T, karforma S (2014), "A Novel E-Governance Data Hiding Approach Combining LSB-Steganography and Cryptography", *INDIAN SCIENCE CRUISER* (ISSN 0970-4256), Vol. 28, No. 4.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com