

Image Steganography Based on Hybrid Edge Detection and 2^k Correction Method

Amanpreet Kaur, Sumeet Kaur
er.amanpreet.kaur@gmail.com, purbasumeet@yahoo.com

Abstract- The transmission of most important & secret information has always been at risk of being tapped or stolen since ancient times. Information security has become a prime concern for everyone who use public channels to transmit their private data in this computer age also. Many techniques got developed over the time to communicate the secret messages without the risk of losing confidentiality. Steganography is one of popular techniques used to hide the confidential information in images without being detected by human eyes. We described the use of Steganography along with 2^k correction method & edge detection method in this paper. This technique proves to be better than earlier techniques because of its capability of carrying more payloads with better imperceptibility. This can be achieved by embedding more data in edge areas as compared to smooth areas of the image as human eye cannot detect the distortion at edges easily. The proposed algorithm yields better PSNR values vis a vis other methods used in steganography.

Index Terms— Steganography, Edge Detection, 2^k Correction, Pixel-value Differencing.

I. INTRODUCTION

As information exchange plays an important role in daily life. So the security of the information must be needed. Two approaches are available to achieve the security one is cryptography and another is steganography. Cryptography means “secret writing” whereas Steganography means “concealed writing” to establish communication between two parties whose existence is unknown to a possible attacker [7]. Steganography, derived from Greek word literally means “covered writing” [1]. There are two main guidelines in information hiding: protecting only against the detection of a secret message by a passive rival, and hiding data so that even an active rival cannot remove it. The classic situation, known as Simmons’ “Prisoners’ Problem”, Alice and Bob are in jail and try to discuss an escape plan, but all their communication can be observed by the warden. If their plan or the fact that they are discussing an escape plan were detected they would be transferred to a more secure prison. So they can only succeed if Alice can send messages to Bob so that the warden can’t even detect the presence of a secret [2].

Among the methods of steganography, the most common is the use of images for steganography. This is called image steganography [4]. This paper focuses on the problem: how two communicating parties send secret message over a public channel so that a third party cannot detect the presence of secret message. There are two types of techniques in Steganography one is Substitution method and another is Transfer Domain technique. The methods of Substitution

cause a noticeable change from the unmodified version of the image. Secret data is hidden in the frequency domain of the signal. Transform technique is applied throughout the image by dividing image into blocks.

In this paper we propose a modified algorithm which uses hybrid edge detector and 2^k correction method. We use an edge detection algorithm because in edges the embedding capacity is more as compared to smooth areas. In edges we can replace three bits and from smooth areas we can replace one bit at a time using LSB technique. A mathematical function 2^k correction is used to get better imperceptibility. Thus using the combination of hybrid edge detection algorithm & mathematical function i.e. 2^k correction, the capacity of hidden data and imperceptibility of image can be increased. The rest of the paper is organized as follows: Section I gives the information about the related work which is to be done under this field, Section II presents the proposed algorithm Section III shows the experimental results and in Section IV concludes the whole scheme.

Embedding Data: Embedding data, which is to be hidden, into an image requires two files. The first is the image that will hold the hidden information, called the cover image. The second file is the message. A message may be plain text, cipher text, other images, or anything that can be embedded in a bit stream. The cover image and the embedded message make a stegoimage. A stego-key may also be used to hide, and then later decode, the message [1]. The general form of Steganographic technique is shown in fig 1.

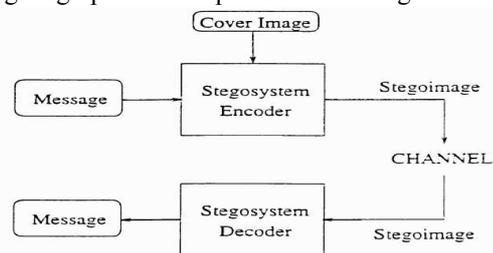


Fig .1. Steganographic Flow [6]

The four basic techniques used for Steganography are: [6]

LSB method: every least significant bit of some bytes inside an image is changed to a bit of the secret message.

Injection: Hiding data in sections of a file that are ignored by the processing application.

Substitution: causes a noticeable change from the unmodified version of the image.

Generation: Unlike injection and substitution, this does not require an existing cover file but generates a cover file for the purpose of hiding the message.

II. RELATED WORK

Least Significant bit insertion scheme: The least significant bit insertion method is probably the most well known image Stenography technique. It is a common, simple approach to embed information in a graphical image file [3]. The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. In this technique, the embedding capacity can be increased by using two or more least significant bits. LSB hides the message in such way that the humans do not recognize it, but the technique is so simple so it is possible for the opponent to retrieve the message. Therefore, if one can suspect of the secret message it is easy for invader to extract the message.

Canny Edge Detection: Edge detection is a tool used in image processing and computer visualization. It is the process which aims at identifying and locating sharp points in an image which are due to the change in pixel intensity. The most common algorithm used for edge detection is Canny Edge detection algorithm. Canny edge detection uses multistage algorithm to detect a wide range of edges in images. The popularity of the canny edge detector can be attributed to its optimality according to the three criteria of good detection, good localization, and single response to an edge [5]. The main characteristics of canny are: First is low error rate, the second criterion is that the edge points be well localized. In other words, the distance between the edge pixels as found by the detector and the actual edge is to be at a minimum. A third criterion is to have only one response to a single edge [5].

Fuzzy Edge Detection: Fuzzy techniques are used to develop new methods for edge detection due to the flexibility in dealing with the ambiguity and vagueness often present in digital images. Several fuzzy reasoning/inference and logic based edge detection techniques are there [5]. Fuzzy based rules are used in edge detection algorithms. In most of these methods, adjacent points of pixels are assumed in some classes and then fuzzy system inference is implemented using appropriate membership function [10]. In fuzzy edge detection algorithm membership grade values are computed and the degree of edginess is calculated then edge values are find out using some rules [5].

Hybrid edge detection: A hybrid edge detector is created using the combination of *canny edge detection* and *fuzzy edge detector*. We may use the edge detection algorithms to increase the capacity of hidden data. Smooth areas hide small amount of information as compared to edge areas. At the smooth area we can hide one bit of secret data but at the edge three bits of secret data in the pixel can be hidden. The combination of both edge detectors not only increases the number of edge pixels, but also clearly and precisely finds the object boundaries in the image.

2^k correction method [4], [8].

A mathematical method is used to achieve better imperceptibility. In some cases there are some differences

occurred in cover pixel and stego pixel due to this differences occurred in an image. To overcome these differences we use 2^k correction method.

Example:

Actual pixel value (APV) 195=11000011

Stego pixel value (SPV) 185=10111001

Error value $|195-185| = 10$

If Error value $\leq 2^k - 1$

No need to change

Else //if error value is $> 2^k - 1$

Then

New stego pixel value = Either $SPV - 2^k$ OR $SPV + 2^k$
Whichever is close to APV

In our case Error value = $10 > (2^3 - 1 = 7)$ so

New stego pixel value = Either $SPV - 2^3$ OR $SPV + 2^3$

Whichever is close to APV

= $(185 - 8 = 177)$ OR $(185 + 8 = 193)$

Whichever is close to 193

= 193 (11000001)

In this way the 2^k correction makes the intensity of the channel nearer to the actual pixel value without affecting the secret data.

III. PROPOSED METHOD

Algorithm for embedding the secret data.

ALGORITHM

INPUT: Image file and text image file

OUTPUT: Text embedded image

Procedure:

1. Select a cover image of $m \times n$ size
2. Convert the image into grey scale.
3. Select the secret data image of size $w \times h$.
4. Initialize the LSB 5-bit at all 0s per pixel in the cover-image temporarily.
5. Execute the Hybrid Edge Detection Algorithm.
6. The temporarily modified image is generated which shows the edges in the image.
7. Encrypt the secret data in cover image using appropriate algorithm.
8. Generate the image after hiding data
9. Execute the further steps of Canny edge-detection
10. With Sobel in X direction and Y direction using the image which is obtained after hiding data.
 - i. Pass the modified image through filter to remove noise.
 - ii. Apply Sobel in X direction to find gradient for column.
 - iii. Apply Sobel in Y Direction to find gradient for row.
 - iv. Implement Non maximum suppression.
 - v. Final image is received and compare it with Threshold values.
11. Apply Post Hybrid Edge detection Algorithm.
12. Apply 2^k correction method on final image.
13. Obtained image will hide all the characters that we input.

IV. RESULTS

The images of size 512×512 are used as the test images in our experiments. To measure image quality of the scheme PSNR and MSE is calculated. The MSE (Mean Square Error)

represents the cumulative squared error between the compressed and the original image. Equation for MSE:

$$MSE = \frac{1}{W \times H} \sum_{i=1}^W \sum_{j=1}^H (I_{ij} - I'_{ij})^2 \dots\dots [5]$$

Where W and H are the number of rows and columns in the input image respectively. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. Equation for PSNR:

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right) \dots\dots [6]$$

Where R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255, etc. The test is done on fig 2 Lena Image:



Fig. 2. Test Image Lena

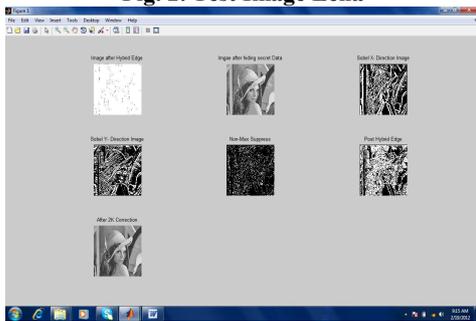


Fig. 3. Lena Image obtained after applying proposed algorithm.

Further, the test is done with Fig 4 Image Peppers:

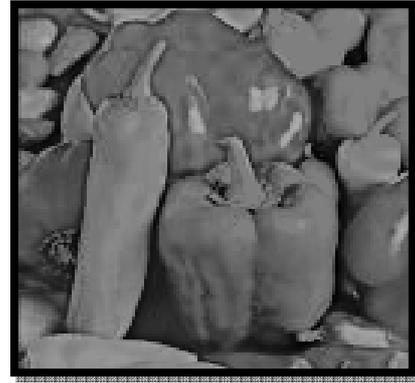


Fig. 4. Test Image Peppers

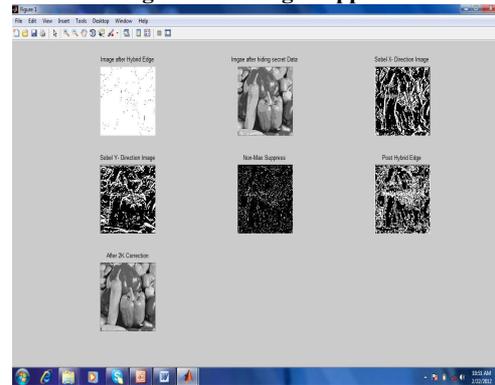


Fig. 5. Pepper Image obtained after applying proposed algorithm

After this the test is done with fig 6 Baboon image:

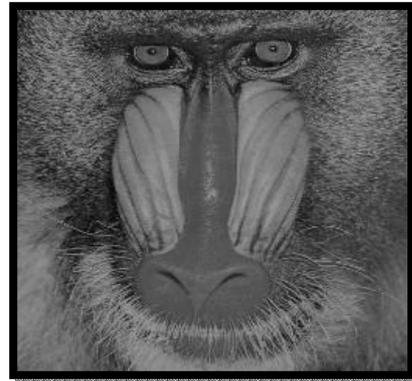


Fig.6. Test Image Baboon

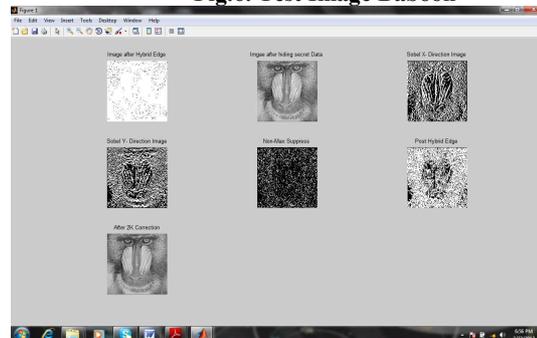


Fig. 7. Baboon Image obtained after applying proposed algorithm

Comparison of proposed technique with previous techniques for PSNR

The results of previous techniques are taken from Jae-Gil Yu's technique [4].

Table 1. Comparison of Different techniques

The PSNR value is high in proposed scheme as compared to

Cover image	LSB3 (PSNR)	PVD (PSNR)	Lie Chang's (PSNR)	Jae Gil Yu (PSNR)	Proposed Technique	
					PSNR	MSE
Lena	37.92	41.48	37.53	38.98	40.81	0.87
Peppers	37.9	41.58	37.02	38.27	40.51	0.85
Baboon	37.9	37.01	37.7	38.98	41.74	0.85

other techniques. Our technique is implemented with MATLAB. We have chosen this because of its advanced features to handle images.

V. CONCLUSION AND FUTURE WORK

Hybrid edge detection and 2k correction technique is presented in this paper. In our technique the quality of stego image is very impressive. The major factor is PSNR value because this parameter decides the imperceptibility & robustness parameter. If the imperceptibility will be high then there will be observably less visual attacks. So the main concern in this approach is imperceptibility so PSNR is intensely analyzed. The Embedding capacity of the image is increased by using the concept of Edge Detection.

We have achieved the good rate of PSNR in this proposed method. No doubt it is a good capacity as compared to LSB techniques but in future research we can increase the hiding capacity of image and also increase the rate of PSNR.

REFERENCES

[1] N.F. Johnson, S. Jajodia, and George Mason University "Exploring Steganography: Seeing the Unseen", IEEE computer, Vol. 31, No. 2, pages 26-34, February 1998.

[2] József LENTI, "Steganographic Methods", Periodic a polytechnic a Ser. El. Eng. VOL. 44, NO. 3-4, PP. 249-258 (2000).

[3] S .K. Moon, R.S. Kawitkar, "Data Security using Data Hiding", International Conference on Computational Intelligence and Multimedia Applications 2007.

[4] Jae-Gil Yu¹, Eun-Joon Yoon², Sang-Ho Shin¹ and Kee-Young Yoo, Dept. of Computer Engineering, Kyungpook National University Daegu, Korea," A New Image Steganography Based on 2k Correction and Edge-Detection", Fifth International Conference on Information Technology: New Generations 978-0-7695-3099-4/08 © April 2008 IEEE.

[5] Wen-Jan Chen a,* , Chin-Chen Chang b,c, T. Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector" Expert Systems with Applications 37 (2010) 3292-3301 , 2009 Elsevier Ltd..

[6] Weiqi Luo · Fangjun Huang · Jiwu Huang "A more secure steganography based on adaptive pixel-value differencing scheme" Springer Science Business Media, LLC 2009.

[7] Sujay Narayana and Gaurav Prasad, "Two Approaches for Secured Image Steganography using Cryptographic Techniques and type Conversions", Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010.

[8] Manish Mahajan and Akashdeep Sharma "Steganography in Colored Images Using Information Reflector with 2k Correction" 2010 International Journal of Computer Applications (0975 – 8887).

[9] Ei Nyein Chan Wai, May Aye Khine, "Syntactic Bank-based Linguistic Steganography Approach", 2011 International Conference on Information Communication and Management IPCSIT vol.16 (2011).

[10] Wafa bakhoda, Fardin Akhlaqian Tab, Om-Kolsoom Shahryari, "Fuzzy Edge Detection Based on Pixel's Gradient and Standard Deviation Values", Proceedings of the International Multiconference on ISBN 978-83-60810-22-4 Computer Science and Information Technology, pp. 7 – 10 ISSN 1896-7094.