International Journal of Engineering Innovation & Research
Volume 4, Issue 6, ISSN: 2277 – 5668

Image Fringe Steganography

Sonal Nigam
M.Tech. Final Year Student
KIT, Kanpur, 208001, U.P. (India)
Email: sonalkit@gmail.com

Praveen Kr. Tripathi
Assistant Professor
KIT, Kanpur, 208001, U.P. (India)
Email: prt@kit.ac.in

Dr. Vibhash Yadav
Associate Professor
KIOT, Kanpur, 208001, U.P. (India)
Email: vibhashds10@gmail.com

Abstract **– Steganography is method used for hiding information in secure manner. Advantage of Steganography over cryptography is that intended secret message does not attract attention to itself as an object of scrutiny. In this paper we proposed a new image steganographic technique that embeds secret image only in the fringe regions of the cover image while keeping the smoother regions intact. This technique of data hiding gives more security[1]. This is due to human visual system (HVS) that can tolerate some degree of changes in the fringes whereas it is sensitive to slight changes in smooth areas. Fringe of the cover image are calculated via Canny Edge Detection algorithm. Embedding is applied only in randomly selected fringe pixels rather than all fringes [2]. For embedding purpose, an indicator channel is selected from RGB channel. Secret data bits are embedded to variable no of LSB of other two channels. Indicator is selected as maximum intensity color channel to provide the information about data bits whether they are inserted into that pixel or not.**

Keywords **– Steganography, Least Significant Bit, Canny Edge Detection.**

I. INTRODUCTION

In current era of information technology, information security is very important concern. Cryptography was developed to encrypt and decrypt data to provide security. It is sometimes necessary to keep the existence of the message secret apart from keeping the contents secret. Steganography is one of powerful technique which can be applied to images, video file or an audio file to embed secret data without being suspicious. It is an art of invisible communication by concealing information inside other information .It contain 3 element -Cover Image (hides secret image pixel)the secret message/image and stego image(which is the cover object with message embedded inside it).After hiding a secret message into cover image, a stego image is obtained which is sent to receiver. Steganography on fringe region gives slight variation of color which can not detected by human visual system.

There are many steganographic methods like least-significant-bit (LSB) algorithm. it is one of the main techniques in spatial domain image Steganography. The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image. To increase security, Moazzam Hossain, Sadia Al Haque, Farhana Sharmin [7] proposed a method using neighborhood pixel information. The results showed poor visual quality and PSNR. An image is a combination of fringe and smooth areas and it is evident that fringe areas being high in contrast, color, density and frequency can tolerate more changes in their pixel values than smooth areas, so a large number of secret data can be hidden while retaining the original characteristics of image. In 2003, Wu and Tsai made use of this characteristics to propose "pixel-value differencing" steganographic method [10]. It used the difference value between two neighbor pixels to determine how many secret bits should be embedded.

Capacity of embed bits in fringe pixel is greater than capacity of smooth area pixel. That's why fringe pixels were embedded with more secret bits than that located in smooth areas. Now we have to partition the difference value in range [0, 255] before and after the embedding in such a way that it belong to same level. But this method is less tolerant to steganalysis. Li Li, Bin Luo, Qiang Xiaojun Fang [9] proposed a method based on fringe detection using Sobel operator but it was unable to find accurate fringes of image. A new approach based on parameterized canny edge detection [4] embedding came into existence in 2012. Parameterized canny edge detector uses three parameters i.e. higher threshold value, Gaussian filter and lower threshold value. The value of all these three parameters are user defined that enable the stego image more robust.

In this approach three LSBs of all three channels of fringe pixels are replaced with the secret data bits. That affects the extraction process as using the same threshold on the stego image for detecting fringes might not give the same fringe pixels. So in extraction process, it is mandatory to use cover media for security aspects. In this paper we introduced an approach that is image fringe that uses variable embedding to hide secret data which overcomes the previous disadvantages. This proposed approach of variable embedding improves the data hiding with a good visual clarity and PSNR. The next section of this research paper describes the proposed work, covering and the uncovering algorithm and results along with conclusion[6].

II. PROPOSED WORK

This Paper focuses on image Steganography method based on fringe detection with variable length embedding in the RGB color channels of the cover image. Fringes of an image are detected by Canny Edge Detection Algorithm. First of all, a RGB image is taken and then edges are extracted by using Canny Edge Detection method. It has three user defined parameter : a low threshold value ,a high threshold value and the size of the Gaussian filter(kernel). If threshold value is high then it detects less no of fringes in image. In all existing

Copyright © 2015 IJEIR, All right reserved

technique, all fetched fringes are used in embedding process but in our technique we increased its security by randomizing the selection of this pixel. To obtain this, we applied the Canny Edge Detection Algorithm in twice with two different threshold values on cover image and then their difference is considered as final fringes which are used for embedding process. Now we have to find the relationship between the content of image and secret message that is to be embedded. When message size increases, more fringe regions cab be adaptively released by adjusting the threshold.

In next Step of research, achieved 24-bit image is divided into three 8-bit color channels i.e. RED, GREEN, And BLUE.. Maximum intensity channel is considered as indicator channel and rest two channels LSB is used for data embedding that's why these channel named as data channel [1]. The channel which has maximum intensity in forming fringe pixel is selected as indicator channel because modification in lower color value has less impact on overall color of pixel as compared to modification in higher values. Indicator channel will be used for informing whether or not data is embedded in other two data channel. In data embedding process, variable numbers of bits are embedded into LSB of the data channel for achieving higher security and robustness. Due to data embedding, minor modification is reflected [3]. This modification is imperceptible to human visual system but this is able to produce different fringes on the same threshold values. The reason behind this, canny edge detection affects the neighboring pixel also. So if attacker knows the threshold values and apply the reverse process to stego image still won't able to find the secret embedded message.

A. Canny Edge Detector

Fringe detection is used to find out such point in an image where we can perform some abrupt modification in its intensity value i.e pixels values fluctuating from high intensity value to low intensity value and vice versa showing some discontinuities in its pixel. These modifications are because of several following event described below: Discontinuities in surface orientation, modification in material properties, discontinuities in depth and modification scene illumination [8, 9].Now a days there are many edge detection algorithm are using Steganography. The Canny Edge Detection Algorithm is one of most effective algorithm used for edge detection. Now days there are so many fringe detection algorithm are in use but canny edge is one of the most effective and widely known algorithm. It was developed by John Canny in 1986 [4].Main purpose of this algorithm to full fill these criteria:

1. Error rate should be low by good detecting of only existent fringes.
2. Achieve good localization : distance between fringe pixel and real fringe pixel should be minimum.
3. Minimum Response: Only one detector(Sobel detector) should response per fringe.

The Canny Edge Detection Algorithm has five stages:

i. Gaussian filter: Fringes are easily effected by noise so noise should be removed to prevent false detection. To smooth the image Gaussian filter is used. Example For Gaussian Kernel Sixe=5 is shown below :

$$K=\frac{1}{159}\begin{bmatrix}2 & 4 & 5 & 4 & 2\\ 4 & 9 & 12 & 9 & 4\\ 5 & 12 & 15 & 12 & 5\\ 4 & 9 & 12 & 9 & 4\\ 2 & 4 & 5 & 4 & 2\end{bmatrix}$$

ii. Searching the Intensity gradients: Fringe Strength is calculated by taking the intensity gradient with large magnitude. It use Sobel operator .It is fringe detector operator which is applied in x and y direction:

$$G_x=\begin{bmatrix}-1 & 0 & +1\\ -2 & 0 & +2\\ -1 & 0 & +1\end{bmatrix}$$

$$G_y=\begin{bmatrix}-1 & -2 & -1\\ 0 & 0 & 0\\ +1 & +2 & +1\end{bmatrix}$$

Gradient direction and strength is calculated by following formula :

$$G=\sqrt{G_x^2 \quad + G_y^2} \tag{1}$$

$$\theta = \arctan\left(\frac{G_y}{G_x}\right) \tag{2}$$

iii. Non-maximum suppression: It is fringe thinning technique. In this it marks local maxima as fringes and discard those pixel values which does not belong to part of edges.

iv. Double Threshold: After non-maximum suppression, there are still some fringes at this point caused by noise and color variation. To resolve this noise problem it is essential to filter out the fringe pixel with weak gradient value and preserve the fringe with the high gradient value. So it gives accurate edge pixel [11].

v. Hysteresis: In this section, it selected the fringe pixel by comparing the pixel gradient to higher threshold value and lower threshold value. If pixel gradient is higher than higher threshold value is considered as fringe and if pixel gradient less than lower threshold value then it is rejected form edge list and pixel gradient is between two threshold value then it will accept only if it is connected to a pixel that is above the upper threshold. Example of canny edge algorithm is given below with lower threshold as 85 and higher threshold as 235. The original image and the resultant fringe detected as shown:

(a) (b)

Fig.1. (a) original color image (b) fringes produced by Canny algorithm.

Copyright © 2015 IJEIR, All right reserved

B. Variable Embedding

In Variable embedding is method in which secret message is converted into bit stream then we have to find out optimal number of bits that can be embedded in each pixel. As per phenomenon variation of fringes is not easily detectable by human visual eyes. So optimal number of bits which is achieved by variable embedding is used for embedding in fringe pixel. Thus stego image quality is not distorted and more number of data bit can be embedded with an allowable PSNR. For data hiding we used only 3 least significant bits of pixel. Number of LSB will be varied according to the number of of 1's in the 4 MSBs of the data channel of pixel [5]. This approach works as secret key so attacker could not fetch secret data without knowing it. So it makes more security, only authorized person can fetch the hidden data bits.

C. Algorithm

In our proposed algorithm, we described whole processing in two basic step :In first step we hide secret message into cover image(data hiding process/covering process) and generate carrier image.

In second step at receiver end we fetch the secret message from carrier image. First step for data hiding has described below in several sub steps:

1. First we read color 24 bit image I which has n number of pixels then it spited into three channels: Red, Green, Blue. Length of Each Channel is 8 bit.
2. Using Lower and higher threshold value, Canny Edge detection algorithm is applied on I and its resultant fringes is stored in E1 then again we apply canny edge algorithm with different higher and lower threshold value and its resultant fringes stored in E2.Now we calculated difference of |E2-E1| and obtained some random fringe pixel. This technique increases the security even if attacker know the data hiding process based on fringe adaptive still could not be able to find the exact pixel where data bits are embedded. Because of this difference some important fringe would deleted from cover image but those fringes should be present in E1 and E2.Those essential fringes will achieved by adding fringe pixel calculate at maximum threshold. If message size increases then we can adjust threshold value to achieve maximum fringes in which data embedding perform[8].
3. Further secret message processing performed. Secret message always stores in binary format. So it converted into it and denoted by B = {b0, b1, b2,…, bt-1} where b is a single bit in B and t is the total number of bits in B.
4. In next sub step we have to find the indicator channel from three channel. For this purpose we have to calculate intensity value of each cannel which is achieved by summing up the intensity value at selected pixel of the cover image. The channel which has maximum intensity become indicator channel which used to indicate data bits embedded in other channel or not in same pixel values. Two LSB of indicator channel will have similar value (00/11) for pixel subjected to data hiding process and different values for remain pixel. So two LSBs of indicator channel will be either 00 or 11 and 01 or 10 for the rest of them in I. For indicator channel, we have to perform least alteration because this channel has maximum color share in forming pixel so only first LSB is changed according to the 2nd LSB value.
5. The other two channel is treated as data channel because they are used for hiding of data bits. In our proposed method we does not embed data on fixed number of LSB. We perform variable data bit embedding based upon the number of 1s in 4 MSBs. In embedding process, we use bitwise AND and OR operator on data bits and LSB of channel. The Count of data bits in the three LSB of pixels is calculated by table shown below:

Table I: Number of data bits to be embedded

Number of 1s in MSBs of data	Number of bits to be embedded in the LSBs of data
0	2
1	3
2	2
3	3
4	1

6. In this step we repeat step 5 until all bits in B are exhausted. The final image is called carrier image which is similar to I. For example if we are using a pixel C for embedding purpose and RGB values for this pixel is 10110110 11101101 01100001 respectively.

Suppose Red is indicator channel then we have to modify its intensity value to indicated its data channel has embedded data bits so we check last two bits of R, we found it different now we have to convert lower LSB according to second LSB to make it same(00/11 format).So finally we got R 10110111.Other two channel are data channel where data bits decided by number of 1s present in 4 MSB for Green channel number of 1s is 3 in MSB so according to table number of data bits would be three .For Blue number of 1s is two so data bits will be two. Now we have to calculate data bits for pixel so we fetched data bits series and substituted to form carrier image.

The Next step of algorithm is performed on receiver side where receiver have to extracted secret message from carrier image. To achieve this goal ,we have to divide into carrier image into RGB channel . Receiver knows the indicator channel by which receiver determined carrying pixel which has secret message. Pixel locations of resulting fringes are used to indicate the carrier in the carrier image. After scanning of data channel reverse processing is performed to fetch hidden message .Now receiver have to concatenated the obtained bits to form original data format. Variable embedding criteria serves as Stego key. If receiver does not know this then extraction is not possible.

III. EXPERIMENTS AND RESULTS

By given example, we are going to show our proposed methodology in this section. We have chosen OpenCV 3.0 using C++ platform for implementing our algorithm. OpenCV (Open Source Computer Vision) is a open library of programming functions mainly focused at real

Copyright © 2015 IJEIR, All right reserved

time computer vision. Processing speed of OpenCV is faster than MATLB that's why we are using it in our algorithm. It is freely available as well. We have tested our algorithm for secret images. By this algorithm , size of final image along with secret message remains same because we are making changes only in LSBs of fringes. Minimum Payload depend upon given parameter:

1 .It is important factor to choose cover image according to size of the secret image because fringe region varies according to cover image.

2. In same way Canny threshold values also effects the number of fringes produced. So Minimum Payload is not unique vary according to Cover image.

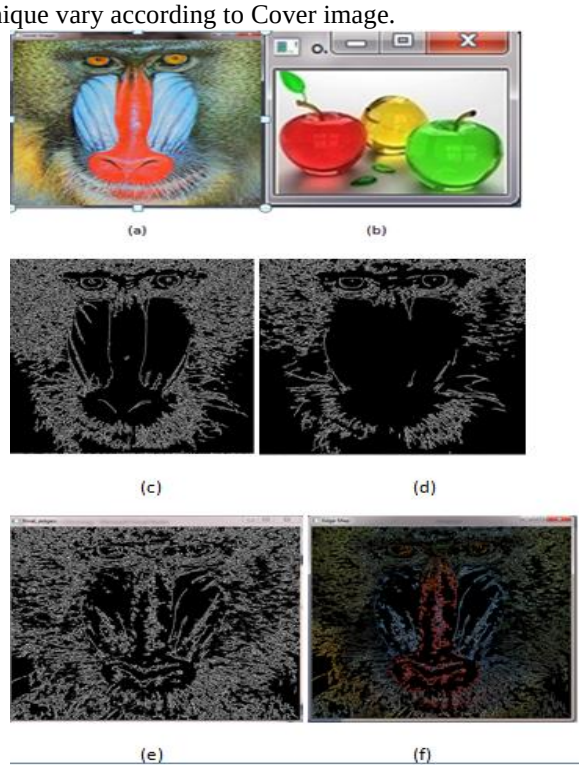

Fig.2. (a) Original color image (b) Original Secret image (c) Fringe(E1) produced by Canny algorithm with LT_1 as 50 (d) Fringe (E_2) produced by Canny algorithm with LT_2 as120. (e) Fringe(E3) produced by Canny algorithm with LT_2 as170. (f) $|E_1 - E_2 + E_3|$ gives the final fringe pixels to be used for covering process.

In our first experiment, we have used Baboon image of size 512×512.First set of fringes is calculated by, LT_1 (lower threshold) = 50, HT_1 (higher threshold) = 150. On calculating another set of fringes, LT_2 (lower threshold) = 120, HT_2 (higher threshold) = 360. The results for the same are shown alongside. The total number of carrier pixels for the above example is 56691.Now we are going to calculate Maximum payload for this example

Maximum payload = 56691* 2 * 3

=340146 bits=42518 bytes (approx. 42KB)

For selected threshold values, maximum capacity for hiding data is 42KB. The secret image is of size 6KB with dimension 128×96.Now we have to convert our secret image into gray scale image then we have to embed data bits in similar ways as described in our algorithm. Finally we got stego image:

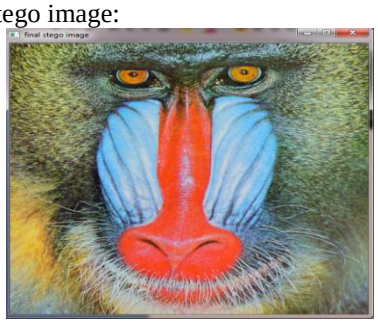

Fig.3. The stego image obtained for Baboon image

As we can see, the resultant stego image (512 × 512) looks similar to the original cover image and modification in its pixel does not reflect to human eyes. For its quality measurement now we have to calculate Peak Signal to Noise Ratio (PSNR). It used to measure the invisibility of hidden message. If PSNR value is high then quality of final image is good and it will be more similar to original image. It is calculated by this formula :

$$PSNR = 10\, log_{10}\left(\frac{R^2}{MSE}\right) \quad (3)$$

in previous equation, R stands for the maximum fluctuation in the original image data type. Example: R is 1 for double-precision floating point data type and R is 255 for 8-bit unsigned integer data type of image etc and Mean Square Error (MSE) is used to calculate cumulative squared error between original image and carrier image and if MSE value is low then it shows low error rate. It is calculated by:

$$MSE = \frac{\sum_{M,N}[I_{1(m\ \ ,n)} - I_{2(m\ \ ,n)}]^2}{M*N} \quad (4)$$

where M and N are the number of rows and columns in the input images.

For this example PSNR value is 52.456 dB that means quality degradations could hardly be perceived by human eye. Also after retrieval at receiver end , the message extracted was exactly the same as the secret message hidden.

Image	Hiding Capacity (in bytes)	Bytes hidden	PSNR
Baboon.jpg	42518	6095	52.456

According the algorithm at the receiver end hidden image is shown like this:

Fig.6. The recovered image obtained for stego image

The proposed method is showing better result other than various Steganography Technique.

Copyright © 2015 IJEIR, All right reserved

IV. Conclusion and Future Work

The Main purpose of this paper to give highly secured Image Fringe Steganography Technique for hiding the secret image into other image. Via Canny Edge Detection, we detect all fringes of cover image at different threshold value but final fringes selected by random preprocessing method. Further, Maximum intensity channel selected as indicator channel from RGB channel and others are treated as data channel. We embed secret data bits in variable number of LSBs of data channel based on the number of 1s present in the MSBs. In our method we hide the secret data on certain fringes pixel values rather than all pixel of cover image. So it produced least modification in cover image which is imperceptible to human visual eyes and shows improved PSNR value. By proposed technique only authenticated who has stego key can fetch the correct secret message from cover image. Without stego key, fetching of secret message is not possible because this algorithm generates different output for same input image and secret image so it becomes necessary to know stego key. If any attacker tries to fetch hidden data by applying canny edge detection for same threshold value then it would be misguide them without generating correct fringes for reverse process. This technique makes Steganography more robust and secured as compared to other technique so that two parties can easily communicate their secret data without compromising original image quality.

As future work, techniques like Run length encoding can be used which will not only enhance the embedding capacity but also secure the data as information will be hidden in encoded form.

Acknowledgement

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with success.

I would like to thank, first and foremost, my parents, who taught me how to learn, always encouraged me to pursue my interests and never failed to support me in any endeavor.

I wish to express my deepest gratitude to Mrs. Shubha Jain(HOD,CSE), [Kanpur Institute of Technology, Kanpur] for providing me a with a platform to conduct research, and for supporting and guiding me throughout my studies.

I am grateful to my supervisor Mr. Praveen Tripathi Assistant Professor, KIT Kanpur & Dr. Vibhash Yadav, Associate Professor, KIOT, Kanpur for their guidance, inspiration and constructive suggestions that helped me in the preparation and execution of this research work.

References

[1] Akhtar.N, "An Improved Inverted LSB Image Steganography", IEEE International Conference On Issues And Challenges In Intelligent Computing Technologies, p. 749-755, 2014.

[2] Deepali Singla, Mamta Juneja,, "An Analysis of Edge Based Image Steganography Techniques in Spatial Domain", Proceedings of 2014.

[3] Mamta Juneja and Parvinder S. Sandhu, "A New Approach for Information Security using an Improved Steganography Technique" , J Inf Process Syst, Vol. 9, No. 4, 2013.

[4] Geng Xing, Chen ken , Hu Xiaoguang "An improved Canny edge detection algorithm for color image" IEEE TRANSATION, 2012 978-1-4673-0311-8/12/$31.00 ©2012 IEEE..

[5] Youssef Bassil, "Image Steganography Based on a Parameterized Canny Edge Detection Algorithm," International Journal of Computer Applications (0975 – 8887), vol. 60, no. 4, 2012.

[6] M. Bachrach, and FY. Shih, "Image Steganography and Steganalysis", wiley interdisciplinary reviews: computational statistics, vol. 3, pp. 251-9, 2011.

[7] Moazzam Hossain, Sadia Al Haque, Farhana Sharmin. "Variable Rate Steganography in Gray Scale Digital images Using Neighborhood pixel information", The International Arab Journal of information technology, vol. 7, No. 1, January 2010.

[8] Arvind Kumar and KM. Pooja, "steganography- a data hiding technique", international journal of computer applications (0975 – 8887) volume 9– no.7, November 2010

[9] Li Li, Bin Luo, and Qiang Li Xiaojun Fang., "A color Images steganography method by multiple embedding strategy based on Sobel operator," International conference on multimedia information networking and security, IEEE 2009, 978-0-7695-3843-3/09.

[10] D. C. Wu, & W. H. Tsai,"A steganographic method for images by pixel-value differencing". Pattern Recognition Letters, vol.24, no. 9-10, pp. 1613–1626, 2003.

[11] C. C. Thien and J. C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function,"Pattern Recognit., vol. 36, no. 3, pp. 2875–2881, 2003.

Author's Profile

Sonal Nigam
pursuing her M. Tech (final year). in Computer Science and Engineering from Kanpur Institute of Technology, Kanpur, 208001,U.P. (India).
Email: sonalkit@gmail.com

Praveen Kr. Tripathi
is presently working as Assistant Professor in Department of Computer Science and Engineering in Kanpur Institute of technology, Kanpur. He is having more than 7 years teaching experience with expertise in Artificial Intelligence, Neural Networks, Cryptography and Programming in C.
Email: prt@kit.ac.in

Prof Dr. Vibhash Yadav
is presently working as Director, Krishna Institute of Technology, Kanpur. He is having more than 10 years of teaching experience with expertise in Software Engineering, Object Oriented Systems, Artificial Intelligence & Computer Networks.
Email: vibhashds10@gmail.com

Copyright © 2015 IJEIR, All right reserved