Two Components based LSB and Adaptive LSB Steganography based on Hybrid Feature Detection for Color Images with improved PSNR and Capacity

Mamta. Juneja, and Parvinder S. Sandhu

***Abstract*—** This paper proposes a new approach for information hiding in RGB color images based on 3 new techniques 1) A new hybrid feature (line /edge /boundary /shape) detection technique combining Canny and Hough transform for bifurcating an image into edge and smooth areas 2) Two Component based Least significant bit (LSB) Substitution Technique for hiding encrypted messages in edges of images 3) An Adaptive LSB substitution technique for hiding messages to smooth areas. Firstly, the input cover image (Bitmap Image) is divided into edge and smooth areas using a new hybrid feature detection technique based on Canny Edge detection filter and Hough transform. Message bits are then embedded in the least significant bytes across edge pixels using new Two Component based LSB Substitution Technique. For the rest of the pixels across smoother areas, it utilizes an adaptive LSB .The proposed research is direct implementation of the principle that edge areas being high in contrast, color, density and frequency can tolerate more changes in their pixel values than smooth areas, so can be embedded with a large number of secret data while achieving high quality of the stego-image. Proposed technique is better than other existing techniques in comparison with PSNR, capacity and immunity to noise as shown experimentally.

***Keywords*—** Adaptive LSB, Bitmap images, Canny, Hough transform, Steganography, Two components LSB insertion.

I. Introduction

STEGANOGRAPHY is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured i.e. Cryptography scrambles messages so they cannot be understood. The purpose is to pass on the information without any regard or knowledge of others safely to the destination [1].

Mamta.Juneja is Assistant Professor in University Institute of Engineering and technology, Panjab Univesity, Chandigarh, e-mail:er_mamta@ yahoo.com.

Dr. Parvinder Singh Sandhu is working as Professor with Rayat and Bahara Institute of Engineering and Bio-Technology, Sahauran, Punjab, India.

Generally, a steganography message will appear to be simple picture, an article, a shopping list, or some other message. The advantage of steganography over cryptography alone is that messages produced by it do not attract attention to themselves, to messengers, or to recipients. An unhidden coded message, no matter how unbreakable it is, will arouse suspicion and may in itself be incriminating, as in some countries encryption is illegal. Both sciences can be combined to produce better protection of the message. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques. Therefore, the principle defined once by Kerckhoffs [2] for cryptography, also stands for steganography. *Steganography* can be broadly classified in Traditional (Wax tablets, Secret inks, Microdots, Cipher text etc.) and Modern Methods. Modern methods are further classified in text(Line-shift encoding, Word-shift encoding, Feature specific encoding),Audio/Video(Low Bit Encoding, Phase Coding, Spread Spectrum) and Image LSB Insertion, Masking and Filtering, Algorithms and Transformations, Redundant Pattern encoding, Encrypt and Scatter).

Image Steganography requires two files. The first is the innocent-looking image that will hold the hidden information, called the cover image. The second file is the message i.e. the information to be hidden. A message may be plain-text, cipher-text, other images, or anything that can be embedded in a bit stream. When combined, the cover image and the embedded message make a stego-image. A stego-key (a type of password) may also be used to hide then later decode the message. Image steganography is generally more preferred media because of its harmlessness and attraction. Image steganography is classified into two domains Spatial and Frequency domain according to working domain [5].In Spatial domain, steganography works on the pixel values directly and modify their values. In Frequency domain, images are first transformed into the frequency domain and then message are embedded in the transform coefficients.

The least significant bit insertion method [1] is probably the most popular image steganography technique. It is a common, simple approach to embed information in a graphical image file. When applying it to each byte of a 24-bit image, three bits can be encoded into each pixel as each pixel is represented by three bytes .Any changes in the pixel bits will be indiscernible to the human eye. For example, the letter A can be hidden in

three pixels. Assume the original three pixels are represented by the three 24-bit words below: (00100111 11101001 11001000) (00100111 11001000 11101001)(11001000 00100111 11101001) .The binary value for the letter A is (10000011). Inserting the binary value of A into the three pixels, starting from the top left byte, would result in: (00100111 11101000 11001000) (00100110 11001000 11101000) (11001001 00100111 11101001) .The emphasized bits are the only bits that actually changed. The main advantage of LSB insertion is that data can be hidden in the least and second least and so on as depicted from Figure 1.We can even hide information in more bits i.e. 2,3 etc without any significant visual difference till some particular level depending on type of image or location of insertion. After that level, differences can be noticed as number of bits to be substituted increases.

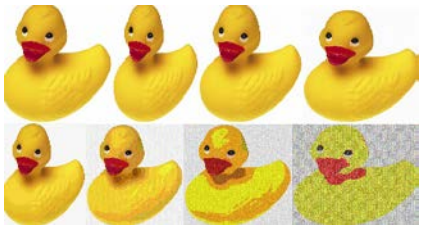


Fig. 1 LSB (original image,1,2,3,4,5,6,7 bit substitution)

The focus of this paper is image steganography based on LSB insertion. The cover media used in this approach is 24 bit RGB Bitmap (BMP) images[4].These are most popular as cover media because of being simple in structure, highly standardized, extremely widespread in use and contain minimal extra information.

II. LITERATURE SURVEY

Neil F. Johnson and Sushil Jajodia [7] discuss three popular methods for message concealment in digital images. These methods are LSB insertion, masking and filtering and algorithmic transformations. Kevin Curran and Karen Bailey [6] analyze seven different image based steganography methods. These methods are Stego1bit, Stego2bits, Stego3bits, Stego4bits,StegoColorCycle, StegoPRNG, and StegoFridrich. Further, Neil F. Johnson et al.[7], Chun-Shien Lu [8], Bender [9] presents with further advanced techniques LSB SUBTITUTION, LSB MATCHING and PVD. Wang et all[10] introduced moderate significant bit replacement which took huge computational time so further he improved this with genetic algorithm[11] and Chang et all introduced dynamic programming[12], modulus function[13] and Greedy algorithm[14] to reduce this time by seven times. Thien et all[15] increased it capacity and Chan et all[16] further introduced LSB substitution with OPAP to reduce Weighted mean square error to less than half of Simple LSB.LSB matching was given and worked on by Ker [17], Mielikan [18] and Li [19].All techniques[10-19] worked on fixed number of LSBs but all pixels cannot tolerate same number of changes so adaptive LSB was explored by lie[20], Lee[21], Liu[22], Chang[23],park[24,kekre[25].These techniques considered all images areas to be same while hiding data but in actual edge areas can tolerate more changes than smooth areas so PVD(pixel value differencing) was introduced by Wu and Tsai[26-27] and was further explored by Jung[29], Hwang[30] and Yang[28,31].Then concept of edge detection filters was introduced for extracting edge areas and smooth areas as PVD was quite time consuming and complex process. Alwan et al [32] proposed a novel approach of image embedding using Sobel mask filter, LSB and gray level connectivity using a fuzzy approach and the ASCII code. Hempstalk [33] introduced two new techniques FilterFirst and BattleSteg against more traditional image steganography techniques, BlindHide and HideSeek. results show that FilterFirst beat all the steganalysis techniques until embedding rates became greater than 7% and performed better than all other steganography algorithms tested. Also, Features of the cover, such as edges, are better way of hiding information.

Chang et al [34] proposed a large payload data embedding method for color images. The proposed method modifies the blue value of the color pixel in order to imply the secret data because the blue value is an insensitive color to human eyes. Furthermore, the number of secret bits that can be embedded into a cover pixel is dynamic and can be applied to both RGB and YUV color systems. Bhattacharya et al [35] proposed steganography in Network Security for data transmission. The method is based on the number of occurrence of 0s and 1s in data that has to hide and number of occurrence of 0s and 1s in the last bit of each pixel of binary image file. The proposed algorithm assures the security and the data hiding effect is quite invisible. Fang et al [36] proposed a color image steganography approach based on Sobel edge detection operator in which because of the strong relevance in gradient among R, G, and B planes, the corresponding LSB (Least Significant Bit) of pixel values to hide the secret data in other planes is modified. Finally, combine the stego-planes and restore the color image. Multi-times embedding can be adapted to obtain high data capacity. Experimental results show that there is no noticeable degradation after even three times use of hiding process and the average PSNR is about 45db with the data capacity of 6.3bpp.Hamid et al [37] proposed two approaches from LSB algorithm from which 3-3-2 approach reach up to 33.3%, 4-4-4 approach which increase the amount up to 50 % but poor in terms of imperceptivity and resistance to attacks. The proposed approach provides better Steganography in terms of Impreceptibilty, Capacity and Resistance to attacks. The rest of this paper is organized as follows. The Design of proposed system is presented in Section 3. Implementation and Analysis are shown in Section 4 and 5.Conclusion is drawn in Section 6.

III. DESIGN OF PROPOSED SYSTEM

The various techniques utilized in this proposed system are as follows:

3.1 A new hybrid feature detection technique: A new technique for extracting edge and smooth areas from an image is proposed which integrates Canny edge detector (Edge detection) and Hough transform technique (Edge Linking).

3.1.1 Edge Detection [39-41, 47]: Edges are defined as locations where there is a significant variation in the gray level or color of pixel in some direction and edge detection is locating areas with strong intensity contrasts.

Canny Edge Detector: It is most rigorously defined and widely used optimal edge detector due to its
Good detection, Good localization and Single response to edges. Based on these criteria, algorithm for canny runs in following steps:

Step 1:-The first step is to filter out any noise in the original image before trying to locate and detect any edges. And because the Gaussian filter can be computed using a simple mask, it is used exclusively in the Canny algorithm. Once a suitable mask has been calculated, the Gaussian smoothing can be performed using standard convolution methods. A convolution mask is usually much smaller than the actual image. As a result, the mask is slid over the image, manipulating a square of pixels at a time. The larger the width of the Gaussian mask, the lower is the detector's sensitivity to noise. The localization error in the detected edges also increases slightly as the Gaussian width is increased.

Step 2:- After smoothing the image and eliminating the noise, the next step is to find the edge strength by taking the gradient of the image. The Sobel operator performs a 2-D spatial gradient measurement on an image. Then, the approximate absolute gradient magnitude (edge strength) at each point can be found. The Sobel operator [6] uses a pair of 3x3 convolution masks, one estimating the gradient in the x-direction (columns) and the other estimating the gradient in the y-direction (rows). They are shown below:

$$K_{GX} = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \quad K_{GY} = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

The magnitude, or edge strength, of the gradient is then approximated using the formula:

$$|G| = \sqrt{Gx^2 + Gy^2} \approx |Gx| + |Gy|$$

Step 3:- The direction of the edge is computed using the gradient in the x and y directions. However, an error will be generated when sumX is equal to zero. So in the code there has to be a restriction set whenever this takes place. Whenever the gradient in the x direction is equal to zero, the edge direction has to be equal to 90 degrees or 0. degrees, depending on what the value of the gradient in the y-direction is equal to. If GY has a value of zero, the edge direction will equal 0 degrees. Otherwise the edge direction will equal 90 degrees. The formula for finding the edge direction is:

$$\theta = \tan^{-1}\left(\frac{Gy}{Gx}\right)$$

Step 4:- Once the edge direction is known, the next step is to relate the edge direction to a direction that can be traced in an image. So if the pixels of a 5x5 image are aligned as follows:

x x x x x
x x x x x
x x a x x
x x x x x
x x x x x

Then, it can be seen by looking at pixel "a", there are only four possible directions when describing the surrounding pixels - 0 degrees (in the horizontal direction), 45 degrees (along the positive diagonal), 90 degrees (in the vertical direction), or 135 degrees (along the negative diagonal). So now the edge orientation has to be resolved into one of these four directions depending on which direction it is closest to (e.g. if the orientation angle is found to be 3 degrees, make it zero degrees). Think of this as taking a semicircle and dividing it into 5 regions (Figure 2).

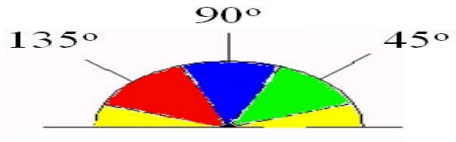


Fig. 2 Edge direction determination

Therefore, any edge direction falling within the yellow range (0 to 22.5 & 157.5 to 180 degrees) is set to 0 degrees. Any edge direction falling in the green range (22.5 to 67.5 degrees) is set to 45 degrees. Any edge direction falling in the blue range (67.5 to 112.5 degrees) is set to 90 degrees. And finally, any edge direction falling within the red range (112.5 to 157.5 degrees) is set to 135 degrees.

Step 5:- After the edge directions are known, non-maximum suppression now has to be applied. Non-maximum suppression is used to trace along the edge in the edge direction and suppress any pixel value (sets it equal to 0) that is not considered to be an edge. This will give a thin line in the output image.

Step 6:- Finally, hysteresis [13] is used as a means of eliminating streaking. Streaking is the breaking up of an edge contour caused by the operator output fluctuating above and below the threshold. If a single threshold, T1 is applied to an image, and an edge has an average strength equal to T1, then due to noise, there will be instances where the edge dips below the threshold. Equally it will also extend above the threshold making an edge look like a dashed line. To avoid this, hysteresis uses 2 thresholds, a high and a low. Any pixel in the image that has a value greater than T1 is presumed to be an edge pixel, and is marked as such immediately. Then, any pixels that are connected to this edge pixel and that have a value greater than T2 are also selected as edge pixels. If you think of following an edge, you need a gradient of T2 to start but you don't stop till you hit a gradient below T1.

3.1.2 Edge Linking: Edge Linking is implemented using global method named Hough Transform.
Hough Transform [42-44, 47]: It is performed after Edge Detection to improve its results as it is tolerant of gaps in the edges, relatively unaffected by noise, unaffected by occlusion in the image. It is technique to isolate the curves of a given shape / shapes in a given image, object recognition, Robust to partial deformation in shape and can detect multiple occurrences of a shape in the same pass. Classical Hough Transform can locate regular curves like straight lines, circles, parabolas, ellipses, etc.Generalized Hough Transform can be used where a simple analytic description of feature is not possible. The step wise description of this technique is all follows:

Find all of the desired points in the range.
For each feature point
For each possibility i in the accumulators that passes through the feature point

Increment that position in accumulator
Find local maxima in the accumulator

If desired map each maxima in the accumulator back to image space.

Advantages of proposed technique are 1) Using probability for finding error rate, 2) Localization and response, 3) Improving signal to noise ratio, 4) Better detection especially in noise conditions 5) Resistance of the former to noise in the image 6) Tolerance towards holes in the boundary line. The proposed feature extractor would firstly apply canny on input bitmap image whose output would be further refined by applying hough transform to overcome the flaws of canny.

3.2 Adaptive LSB substitution for Smooth areas: In this approach variable number of LSBs would be utilized for embedding secret message bits according to the mentioned algorithm:

For all components (RED, GREEN, BLUE) of each and every pixel of color image across smooth areas
Every pixel value in this image is analyzed and the following checking process is employed for all the three bytes respectively

If the value of the pixel say vi, is in the range 240 ≤ vi ≤255, then we embed 4 bits of secret data into the 4 LSBs of the pixel. This can be done by observing the first 4 Most Significant Bits (MSB's). If they are all 1's then the remaining 4 LSB's can be used for embedding data.

If the value of vi (First 3 MSB's are all 1's), is in the range 224 ≤ vi ≤239 then we embed 3 bits of secret data into the 3 LSB's of the pixel.

If the value of vi (First 2 MSB's are all 1's), is in the range192 ≤ vi ≤223 then we embed 2 bits of secret data into the 2 LSB's of the pixel.

And in all other cases for the values in the range 0 ≤vi ≤192 we embed 1 bit of secret data in to 1 LSB of the pixel.
Similar procedure is adapted for extracting the hidden text from the image.

3.3. A New Two Component based LSB Substitution Technique for Edge Areas:

An Image is represented as arrays of values which represent the intensities of the three colors R (Red), G (Green) and B (Blue), where a value for each of three colors describes a pixel. Thus, each and every pixel is represented by three components(R-Most Significant Byte, G, and B-Least significant Byte). Here, a new LSB based image steganography method is introduced which focuses on Two components(Complete Blue and Partial Green) out of total three components of a pixel of RGB image during embedding of hidden in cover image. The selection of these components is based on significance of each component in visual perception of color image .Human visual system predicts the blue component contributes least to visual perception and then green component and so on. Perceptibility of Blue component is minimum, average for green component and is maximum for red component in RGB image i.e. Red plays the most significant and Blue plays a least significant role in color formulation. So, we can integrate maximum changes in Blue component and average changes in green component and least change in red component without making much difference in color image.

Accordingly we targeted all bits of Blue component and partial bits of green components and none of bits of red component in this proposed technique. In this method, the 8-bits of first component (blue component) of pixels of image would be replaced with secret text message bits followed by embedding of secret message to 4 least significant bit of green component. For example, suppose one can hide a message in three pixels of an image (24-bit colors). Suppose the original pixel is (00100111 11101001 11001000) thus scheme could hide the data "**010000011111**", by altering the complete blue channel (8 bits) and partial green channel (4bits) of pixel with resultant value as (00100111 1110 **1111** **01000001**).

IV. IMPLEMENTATION OF PROPOSED SYSTEM

The proposed system comprises of two components as shown in Figure 3.
1. Embedding Module
2. Extracting Module.

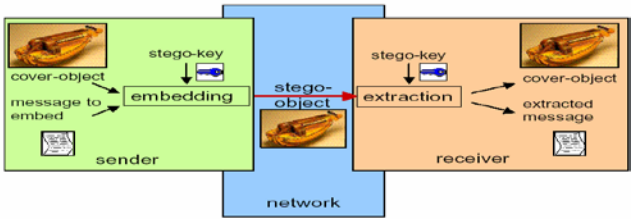


Fig. 3 Proposed System

4.1 Embedding Module

Embedding is the process of hiding the embedded message generating the stego image. Hiding information may require a Stego key which is additional secret information, such as password, required for embedding the information .For example, when a secret message is hidden within a cover image, the resulting product is stego image (stego object).
The main algorithm for the Embedded stage can be listed as follow:-

1. Input the secret text (message) that to be hide in the cover image.
2. Select the cover image (BITMAP file) from list of stored Image files and the text files.
3. Extraction of Input cover image to Edge and smooth areas using new edge detection filter (Section 3.1) is carried.
4. Calculate the size of the secret text
5. Secret text data is first encrypted using the simplified data encryption standard (S-DES)[45]
6. Substitute the encrypted secret characters from step 5 to cover image obtained from step 3 randomly using PRNG as:

For edge areas, embed secret text data using New Two Component based LSB Substitution Technique (Section 3.3) described in Procedure 4.1.1.
For smooth areas, embed secret text data using Adaptive LSB method section 3.2 described in Procedure 4.1.2.

4.1.1 Procedure for Embedding for Edge areas:

Extract all the pixels in the given image and store it in the array called Pixel-Array.

Extract all the characters in the given text file and store it in the array called Character- Array.

Extract all the characters from the stego key in key array.

Choose first pixel and pick characters from Key-Array and place it in 8 bits of first component of pixel. If there are more characters in Key- Array, then place rest in the 4 bits of its second component and then to next pixel and so on till there are characters in key-array.

Place some terminating symbol to indicate end of the key. '0' has been used as a terminating symbol in this algorithm.

Place characters of Character- Array in each 8 bits of first component (blue) and 4 bits of second component (green) of next pixels by replacing it and so on till all the characters has been embedded. Again place some terminating symbol to indicate end of data.

Obtained Stego image will hide all the characters that we input.

4.1.2 Procedure for Embedding for smooth areas:

For All RED-GREEN-BLUE components of all pixels

a. Calculate no. of bits available for embedding as given in section 3.2

b. Place the remaining characters from character into available bits of pixel array.

Repeat steps (a) and (b) till we reach end of character array.

4.2 Extracting Module

Extracting is the process of getting the embedded message out of the stego object again.

The main algorithm for the Embedded stage can be listed as follow:-

1. Extraction of Input cover image to Edge and smooth areas using new edge detection filter as in section 3.2.

2. Extraction of secret text message from stego image is carried from random pixels of cover image using PRNG.

For edge areas: Extract data from 8 bits of BLUE component and 4 least significant bits of GREEN component using Procedure 4.2.1

For smooth areas: Extract data from adaptive no. of bits using Procedure 4.2.2.

3. Apply *S-DES Decryption method [45]to extract the text data.

4.2.1Procedure for Extraction for Edge areas

Extract all the pixels in the given image and store it in the array called Pixel-Array.

Now, start scanning pixels from Pixel-Array and keep extracting key characters from first and second (partial) components of all pixels to Key-Array till we get the terminating symbol.

If this extracted key matches with the key entered by the receiver, then again start scanning next pixels and extract secret message characters from first (blue) and second (partial green) component of next pixels and place it in Character Array till we get terminating symbol.

4.2.2Procedure for Extraction for Smooth areas For All RED-GREEN-BLUE components of all pixels:

a. Calculate no. of bits available for embedding as given in section 3.2

b. Now, start scanning pixels from Pixel-Array and keep extracting characters from the no. of bits determined by step a in character array till we get terminating symbol.

V.RESULT ANALYSIS

Broadly Steganography techniques are evaluated in two aspects [45, 46]:

1. Imperceptibility / Stego-image quality:

It is the scale to measure the quality of stego image after hiding the details inside. It provides the imperceptibility and invisibility measurement and is highest if the differences in cover and stego image are not visible. As we all know, the higher the stego-image quality, the more invisible the hidden message. Therefore, the stego-image quality is a very important criterion to use when we evaluate the performance of a steganograpnic technique. We can judge whether the stego-image quality is acceptable to the human eye by using Peak Signal-to-Noise Ratio (PSNR).

PSNR

Imperceptibility takes advantage of human psycho visual redundancy, which is very difficult to quantify. PSNR can also be used as metrics to measure the degree of imperceptibility:

$$PSNR = 10LOG_{10}\frac{255^2}{MSE}\,dB$$

$$MSE = \left(\frac{1}{MXN}\right)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(P(x,y)-P'(x,y))^2$$

Where M and N are the number of rows and number of columns respectively of the cover image, P(x,y) is the pixel value from the cover image , P'(x,y) is the pixel value from the stego-image. Signal to noise ratio quantifies the imperceptibility, by regarding the message as the signal and the message as the noise.

2. Payload/Hiding Capacity:

The payload indicates the maximum number of bits that can be hidden with an acceptable resultant stego-image quality. Because the scheme would be of no value if the stego-image turned out seriously distorted despite the fact that it can hold a large amount of secret data, the hiding capacity does have its limit, especially when it comes to the binary image. We can say that a scheme does have its contribution to this field of research if it proves to either increase the payload while maintaining an acceptable stego-image quality or improve the stego-image quality while keeping the hiding capacity at the same level, or better if it can get both promoted.

Comparison Analysis:

The results of proposed technique on original image (Figure1) can be seen in figure 4 as

(a) (b)

Fig. 4: (a) Original image (b) Stego-image after applying proposed technique

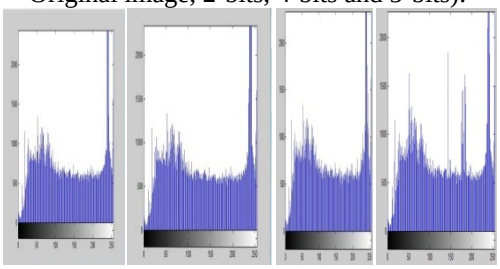
The Comparison of existing techniques and proposed results (on the basis of PSNR and Capacity) is shown in table 1 and analysis of red,green,blue components before and after embedding is shown in Figure 5.

TABLE I
CAPACITY AND PSNR VALUE COMPARISON OF EXISTING TECHNIQUES WITH PROPOSED TECHNIQUE.

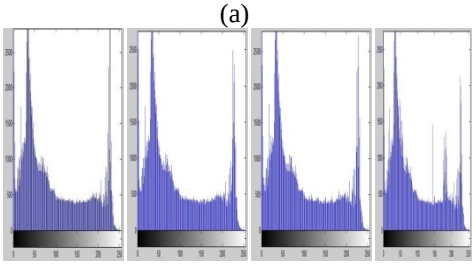
Cover Images	Simple LSB (3BIT)		OLSB(3 BIT)		PVD		Side Match		PVD,LSB	
	C	PSNR	C	PSNR	C	PSNR	C	PSNR	C	PSNR
Lena	98304	37.92	98304	40.73	51219	41.1	48626	41.2	95861	36.24
Baboon	98304	37.92	98304	40.73	57146	37	57146	34.1	89743	35.47
Pepper	98304	37.92	98304	40.73	50907	40.8	50907	40.6	96304	35.61

Cover Images	PVD & Modulus		Kekre		Adaptive LSB & PVD		HIGH CAPACITY PVD & LSB		Proposed	
	C	PSNR	C	PSNR	C	PSNR	C	PSNR	C	PSNR
Lena	51219	44.1	35827	59.05	101599	37.93	146573	36.23	393216	47
Baboon	57146	40.3	34235	59.36	109330	34.84	141834	37.92	363000	46
Pepper	50907	43.3	60317	56.24	100528	38.78	145863	36.37	370000	45

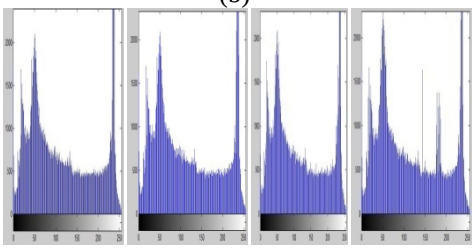
Testing and Results (Red Channel)
Original image, 2-bits, 4-bits and 5-bits):



Testing and Results (Blue Channel)
Original image, 2-bits, 4-bits and 8-bits)
(a)



Testing and Results (Green Channel)
Original image, 2-bits, 4-bits and8-bits)
(b)



Testing and Results (Green Channel)
Original image, 2-bits, 4-bits and 8-bits)
(c)

Fig. 5: Analysis of Red, Green, Blue components of Stego-image

VI. CONCLUSION

A new technique for information hiding based on LSB Steganography and Feature detection is proposed. It presents an improved steganography method for embedding secret message bit in least significant bytes (blue component and partial green component) of nonadjacent and random pixel locations in edges of images and adaptive LSBs of red, green and blue components of randomly selected pixels across smooth areas. No original cover image is required for the extraction of the secret message. A new feature detection filter which integrates CANNY edge detector and Hough transform for line/edge/shape detection is also proposed which performs better to predict edge areas in noisy image. The research was aimed towards the evaluation and development of a new and enhanced data hiding technique based on LSB. The primary objective of this research is to propose a solution that is robust, effective and to make it very hard for human eye to predict and detect the existence of any secret data inside the host image. This has been achieved by using those bits for data storage that are on edges and using blue and partial green component of color image to which human eye is least perceptive. The proposed solution has not only achieved what was required but has also increased the data hiding capacity of the host image by utilizing all the pixels as shown by experimental results.

REFERENCES

[1] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography, Seeing the Unseen," IEEE Computer Magazine, pp. 26-34, February 1998.
[2] Kerckhoffs, "La Cryptographie Militaire (Military Cryptography)," J. Sciences Militaires (J. Military Science, in French), Feb. 1883.
[3] Bret Dunbar, "A Detailed Look at Steganography techniques and their use in an Open Systems Environment ", January 18,2002 SANS Institute
[4] Beau Grantham, "Bitmap Steganography:An Introduction" COT 4810:Topics in Computer Science 2007-04-13
[5] T. Morkel, Jan H. P. Eloff, Martin S. Olivier," An overview of image steganography" ISSA 2005: 1-11
[6] Kevin Curran, Karen Bailey, "An Evaluation of Image Based Steganography Methods,"International Journal of Digital Evidence, Vol. 2 Issue 2, pp. 1-40, Fall 2003.
[7] Niel F. Johnson, Zoran Duric, Sushil Jajodia, "Information Hiding, and Watermarking - Attacks & Countermeasures," Kluwer Academic 2000.
[8] Chun-Shien Lu, "Multimedia Security - Steganography and Digital Watermarking Techniques for protection of IP," Idea Group 2000.
[9] BENDER, D.GRUHL,N.MORIMOTO, A.LU, "Techniques for data hiding", IBM Systems Journal, 1996, vol. 35,no. 3-4, p. 313-336.
[10] RAN-ZAN WANG, CHI-FANG LIN, JA-CHEN LIN," Hiding data in images by optimal moderately significant bit replacement.",IET Electronics Letters, 2000, vol. 36, no. 25, p. 2069-2070.
[11] RAN-ZAN WANG, CHI-FANG LIN, JA-CHEN LIN ,"Image hiding by optimal LSB substitution and genetic algorithm.",Pattern Recognition, 2001, vol. 34, p. 671-683.
[12] CHIN-CHEN CHANG, JU-YUAN HSIAO, CHI-SHIANG CHAN ,"Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy". Pattern Recognition, 2003, vol. 36, p.1538-1595
[13] CHIN-CHEN CHANG, CHI-SHIANG CHAN, YI-HSUAN FAN," Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels", Pattern Recognition, 2006, vol. 39, no. 6, p. 1155-1167.
[14] CHIN-CHEN CHANG, MIN-HUI LIN, YU-CHEN HU," A fast and secure image hiding scheme based on LSB substitution.", International Journal of Pattern Recognition and Artificial Intelligence, 2002, vol. 16, no. 4, p. 399-416.

[15] C.C.THIEN, J.C.LIN, “A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function”, Pattern Recognition, 2003, vol. 36, p. 2875-2881
[16] CHI-KWONG CHAN, L. M. CHENG,” Hiding data in images by simple LSB substitution”, Pattern Recognition, 2004, vol. 37, p.469-474.
[17] A.D.KER., “Improved detection of LSB steganography in grayscale images”, In Proc. 6th International Workshop. Toronto (Canada),May 23-25, 2004, Springer LNCS, vol. 3200, p. 97–115.
[18] JARNO MIELIKAINEN,” LSB matching revisited”, IEEE Signal lProcessing Letters, 2006, vol. 13, no. 5, p. 285-287.
[19] XIAOLONG LI, BIN YANG, DAOFANG CHENG, TIEYONG ZENG ,”A generalization of LSB matching”, IEEE Signal Processing Letters, 2009, vol. 16, no. 2, p. 69-72.
[20] WEN-NUNG LIE, LI-CHUN CHANG,“ Data hiding in images with adaptive numbers of least significant bits based on the human visual system”, In Proc. IEEE Int. Conf. Image Processing. Kobe (Japan), October 24-28, 1999, p. 286-290.
[21] Y. K. LEE, L. H. CHEN,” High capacity image steganographic model”, IEE Proc., Vis. Image Signal Process, 2000, vol. 147, no. 3, p. 288-294.
[22] SHAO-HUI LIU, TIAN-HANG CHEN, HONG-XUN YAO, WENGAO,” A variable depth LSB data hiding technique in images”, In Proc. 2004 International Conference on Machine Learning and Cybernetics. Shanghai (China), Aug. 26-29, 2004, vol. 7, p. 3990-3994.
[23] [23]CHIN-CHEN CHANG, , H.W .TSENG. ,”A steganographic method for digital images using side match. Pattern Recognition Letters, 2004, vol. 25, p.1431-1437.
[24] Y. R.PARK, H.H.KANG, S.U.SHIN, K.R.KWON,”A steganographic scheme in digital images using information of neighboring pixels. In Proc. International Conference on Natural Computation. Berlin (Germany), 2005, Springer-Verlag LNCS, vol. 3612, p. 962–968.
[25] KEKRE, H. B., ARCHANA ATHAWALE, PALLAVI N. HALARNKAR Increased capacity of information hiding in LSB’s method for text and image. International Journal of Electrical, Computer, and Systems Engineering, 2008, vol. 2, no. 4, p. 246-249.
[26] D.C .WU., W.H.TSAI,”A steganographic method for images by pixel-value differencing”, Pattern Recognit. Lett., 2003, vol. 24, no.9-10, p. 1613–1626.
[27] H.C.WU,N.I. WU,C.S.TSAI, M.S.HWANG” Image steganographic scheme based on pixel-value differencing and LSB replacement methods”, IEEE Proceedings-Vision, Image and Signal Processing, 2005, vol. 152, no. 5, p. 611-615.
[28] C. H. Yang, C. Y. Weng, “A Steganographic Method for.Digital Images by Multi-pixel Differencing”, International. Computer Symposium, (2006) 831-836.
[29] KI-HYUN JUNG, KYEOUNG-JU HA, KEE-YOUNG YOO ,”Image data hiding method based on multi-pixel differencing and LSB substitution methods”,In Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08). Daejeon (Korea), Aug. 28-30, 2008, p. 355-358.
[30] CHUNG-MING WANG, NAN-I WU, CHWEI-SHYONG TSAI,MIN-SHIANG HWANG,” A high quality steganographic method with pixel-value differencing and modulus function”, Journal of Systems and Software, 2008, vol. 81, no. 1, p. 150-158.
[31] CHENG-HSING YANG, CHI-YAO WENG, SHIUH-JENG WANG, HUNG-MIN SUN,” Adaptive data hiding in edge areas of images with spatial LSB domain systems”, IEEE Transactions on Information Forensics and Security, 2008, vol. 3, no. 3, p. 488-497.
[32] R. Alwan, F. Kadhim, and A. Al-Taani. (2005),” Data embedding based on better use of bits in image pixels”, International Journal Of Signal Processing. [Online].
[33] Kathryn Hempstalk ,”Hiding Behind Corners:Using Edges in Images for Better Steganography” Image Processing and Computer Vision,2006
[34] Yung-Chen Chou, Chin-Chen Chang, Kuan-Ming Li ,” A Large Payload Data Embedding Technique for Color Images”, Fundamenta Informaticae, Volume 88, Number 1-2 pp47-61,2008
[35] Debnath Bhattacharyya1, Arpita Roy, Pranab Roy, and Tai-hoon Kim3,” Receiver Compatible Data Hiding in Color Image” International Journal of Advanced Science and Technology,Volume 6, May, 2009.
[36] Li Li,Bin Luo,Qiang Li,Xiaojun Fang,”A Color Images Steganography Method by Multiple Embedding Strategy Based on Sobel Operator” In Proc of International Conference on Multimedia Information Networking and Security(huber,China),November 18-20,2009
[37] Hamid, A. M., M. L. M. Kiah, et al. (2009). “Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis.” International Journal of Engineering and Technology (IJET): 0975-4042
[38] DES Encryption Standard, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 46, National Technical Information Service, Springer Field, VA, April 1977.
[39] J. F. Canny. “A computational approach to edge detection”. IEEE Trans. Pattern Anal. Machine Intell., vol. PAMI-8, no. 6, pp. 679-697,1986.
[40] Mike Heath,y Sudeep Sarkar,y Thomas Sanocki,z and Kevin Bowyery,” Comparison of Edge Detectors:A Methodology and Initial Study”, COMPUTER VISION AND IMAGE UNDERSTANDING Vol. 69, No. 1, January, pp. 38–54, 1998 ARTICLE NO. IV960587.
[41] Canny Edge Detection 09gr820 March 23, 2009
[42] P.V.C. Hough, Method and Means for Recognizing Complex Patterns, U.S. Patent 3069654 (1962).
[43] V. Leavers, Shape Detection in Computer Vision Using the Hough Transform, New York, Springer-Verlag, 1992.
[44] R. O. Duda, and P. E. Hart, "Use of the Hough Transformation to Detect Lines and Curves in Pictures," Comm. ACM, Vol. 15, pp. 11–15 (January,1972).
[45] R. Chandramouli and N. Memon, “Analysis of LSB based Image Steganography”, IEEE ICIP, pp. 1022-1022, Oct. 2001.
[46] S. Venkatraman, A. Abraham, M. Paprzycki, "Significance of Steganography on Data Security", International Conference on Information Technology: Coding and Computing (ITCC'04), Las Vegas, 5-7 April 2004.
[47] Rafael C.Gonzalez, Richard E.Woods,Digital Image Processing, Pearson Education , 2003.