An Active Steganographic Scheme Using SSB

Sarathkumar. R, Kalpana. V
School of Computing, Sastra University
India
sksarathcse@gmail.com
kalpana@cse.sastra.edu

ABSTRACT: *Steganography is the art of hiding the reality that communication is carried out, by concealing data in other data. The Steganographic techniques increse the security by exploring the possibility of data analytics to hide data efficiently and securely. The proposed active steganographic method examines each pixel in an image and categories the pixel into primary and secondary pixels and based on that it creates a mask image that helps to increase the payload and embedding rate with secure encoding function. Then inpainting technique is employed over the mask image to increase data hiding. Hiding data in individual colour segments through selected significant bit (SSB) provides secure data storage and efficient data retrieval and the use of Huffman compression techniques will increase the embedding ratio. During the recovery mechanism the cover image and the secluded data can be retrieved from the stego image without any loss of data and distortion to the cover image. Thus, the proposed scheme renders secure communication along with a greater embedding ratio and improved visual tone.*

Keywords: Selected Significant Bit (SSB), Embedding Ratio, Payload, Visual Tone, Compression, Inpainting

Received: 17 July 2017, Revised 28 August 2017, Accepted 6 September 2017

1. Introduction

The source and manipulation of cyberspace plays a vital role in present digital world to maintain the anonymity of data and communication through steganography is extensively used. Steganography acquires more importance as most of our day today communication relay on cyberspace. Steganography is a technique to suppress the data into another innocuous file, so that no one can discover the suppressed data and unaware whether the communication is taken place or not. The digital media is used to embed the suppressed data. Steganography have wide benefits over cryptography and watermarking techniques as these techniques are based on complex embedding scheme that requires high computational recourses and ineffective in preventing the data loss, whereas steganography provides not only security but also privacy and anonymity. The application of the steganography ranges in various field such us military to convey the secret information, intelligence agencies to embed the personal details in to the image, in the medical field patience information's are suppressed into the image and also utilized in securing mobile banking.

2. Literature Survey

In the reversible data embedding digital images are embedded with payload algorithm using Difference Expansion (DE) method, Generalized Least Significant Bit (G-LSB) and RS method. Finally the comparative study of DE method shows best result of embedding. The lossless data embedding technique to recover the original host signal without losses. This is achieved by compressing portion of the signal using F-LSB embedding algorithm and also they use binary to L- ary conversion for the water marked images. By testing on various images founded that G-LSB is more advantageous over the Conventional LSB [2]. A new technique in reversible steganographic method for vector quantization process of image compression is done by declusterisation which minimizes the error in side matching and discovered the original image [3].The study result obtained is satisfactory with standard quality of the image and also the Iwata et al., scheme proven in suppressing data [4]. Histogram of a cover image is modified to hide the secret data and thus it leads to reversible data encoding methods. Images are tested under various algorithms and histogram is used for the tonal distribution. Final comparison stated that lower bound of the PSNR shows good result and it will embed about 5 to 80 kb for marked image and 48 db above for original image. [5]. A multilevel histogram is utilized to enhance the hiding capacity but there is a problem on visual quality [6]. Watermarking technique requires additional information to recover secret data from the stego image and requires additional computation resources during the recovery process [7].

3. Proposed System

In our conspiracy the pixels are classified into primary and secondary pixels because hiding data into the cover image directly will leads to loss of some data, to avoid certain loss of data pixels are sorted based on the dynamic thresholding. Primary pixels are the vital elements in an image that mainly contribute to core nature of an image and these pixels are more sensitive if any changes happen to these pixels this leads to distortion. Secondary pixels are the one that contribute minor elements in an image so these pixels can be used to conceal secret data which won't affect the characteristics of an image and make the modifications unpredictable. Then, by utilizing primary pixels exemplar basis inpainting technique is imposed to produce the prophecy image that has identical nature of a cover image. In order to have a secured and higher embedding rate selected significant pixel technique is employed. The flow diagram of embedding technique is shown in Fig. 1. The restoration mechanisms are more or less the reversal procedure of embedding method.

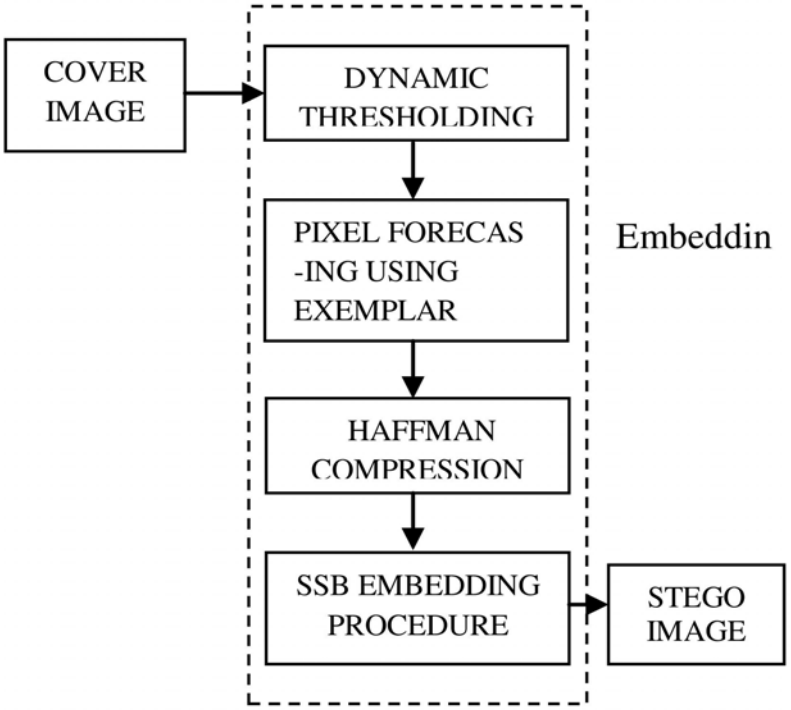

Figure 1. Flow diagram of embedding technique

3.1 Pixel Selection using Dynamic Thresholding

Dynamic Thresholding is applied to segment an image based on its pixel values. It takes digital images as input and converts it into a gray scale image and explores each pixel in an image and calculates threshold values for each pixel and it also performs local thresholding. The threshold value will vary for each images and it is not a static value that actually helps in efficient pixel selection process. The value are chosen by examining pixels and find a local mean value in each segment and finally creates a binary image that is similar to the nature of cover image. After converting a digital image to a grayscale image.

Let the image $P(x_1, y_1) \in [0.255]$ be the pixel value at location (x_1, y_1). In dynamic thresholding method the main intention is to calculate the threshold value $T(x_1, y_1)$ for individual pixel which satisfies

$$Q(x_1, y_1) = \begin{cases} 0 & \text{if } P(x_1, y_1) \leq T(x_1, y_1) \\ 255 & \text{otherwise} \end{cases}$$

The local thresholding value is computed based on the neighbouring pixel intensity values.

Local mean = $m(x_1, y_1)$

Then the average of maximum of local mean and minimum of local mean is calculated and finally the threshold value is computed and implemented on the original image. The result of dynamic thresholding is shown in Figure 2.

$$T = \frac{max + min}{2}$$

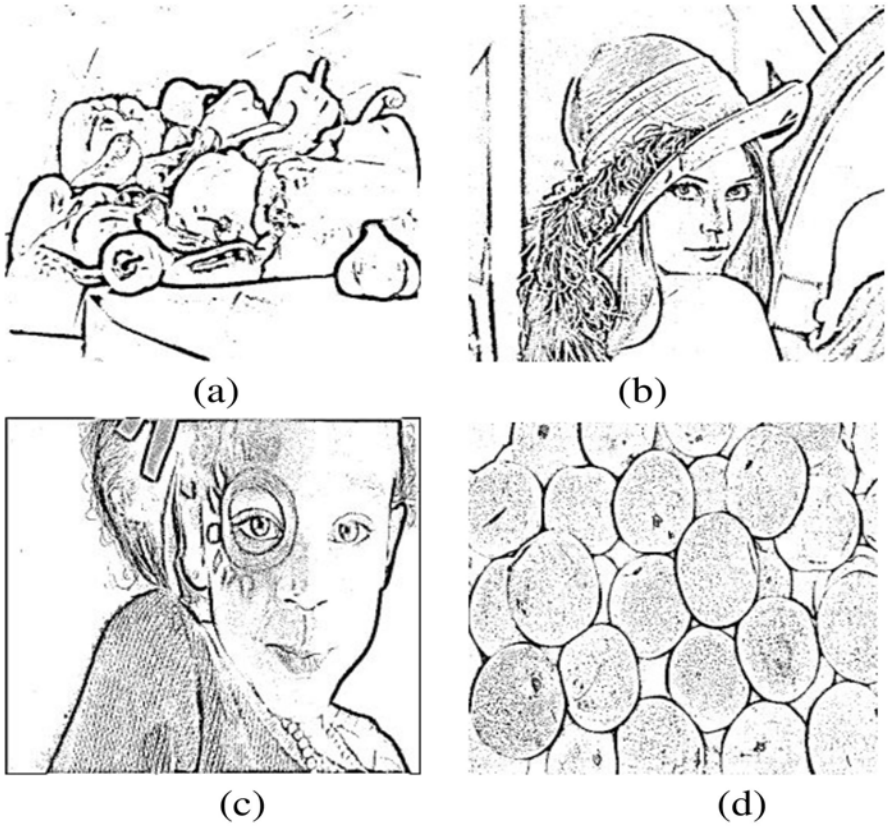

Figure 2. Binary location of primary pixels using dynamic thresholding with different cover image Peppers (a), Lena (b), Girl (c) and pears (d)

3.2 Pixel Forecasting using Exemplar

Inpainting is a technique that helps in restoring the missing region of a picture and it is also referred as image interpolation. It is widely used in film industry and photography to overcome the distortion in image. There are different methods of inpainting that focuses on different characteristics of an image like structure and texture of a picture. We use Exemplar based inpainting which is effective in covering the mask image into a cover image that is similar to the nature of the original image as shown in Figure. 3 by reconstructing the missing area in the mask image. We had symbolizes the terms accordingly *S* - the fundamental image, λ - the objective region, i.e. the region to be inpainted, ξ - the trace region. Commonly, $\xi = S - \lambda$ and $\eta\ \lambda$ to symbolize the periphery of the target region. We symbolize the patch by χ.

Step 1: Initiate the objective area

The objective area is initiated using any color, no lacking of generality. A supplementary image dispensation tool is required to do this process. Let us assume the shading color be red (i.e. *R* =255, *G* =0, *B* =0).

Step 2: Determine the periphery of the objective area.

Step 3: Choose an area to be patched with inpainting.

The size of the patch would be greater than the obvious image texture element. The patch is indicated with the notation **"χ"**.

Step 4: Best chosen patch with the original patch to be found.

The error metric technique is used for matching the patches which is chosen. To determine the finest matching, an equation called Mean Square Error is used such that;

$$\mathbf{MSE} = \sum \frac{\left(\mathbf{P}_{x_1,y_1} - \mathbf{Q}_{x_1,y_1}\right)^2}{\mathbf{n}}$$

Where,
Px_1, y_1 - the element of the patch χ, Qx_1, y_1 - the elements of the patch for MSE, n - the total number of elements in the patch.

Step 5: The image data to be renovated and data are renovated as per found in the former steps. The result always based on the chosen patch for inpainting. Using Criminisi's algorithm an equation is formed below, the main concern function for chosen the finest patch from the objective area in multiplicative form is:

$$\mathbf{B(p) = A(p)\ x\ R(p)}$$

Where,
A (*p*) - the assertion term for the patch and *R* (*p*) - the record term for the patch.

The assertion and record term of patch is explained below:

$$\mathbf{C(p)} = \frac{\sum \mathbf{q} \in \chi \cap \xi\, \mathbf{A(q)}}{|\chi|}$$

$$\mathbf{A(p)} = \frac{\sum \nabla \mathbf{I}_{p_1} . \mathbf{U}_p}{\zeta}$$

Where, $|\chi|$ - the area of the patch, *Z* - the standardization factor (i.e. 255), U_p - a unit vector orthogonal to the front $\eta\ \lambda$ at the point *o* and ΔI_{p1} - represents the perpendicular isophote at point *o*.

Step 6: Using the gradient of the trace region U_p is estimated.

The trace area correspond a points with all ones of matrix which area not in the objective region and for the point in λ. With the help of the pitch of the image isophote is estimated. The equation is framed in such a way that the count of weights to numerous module of precedence term with the intension that stability among assertion and record term would be sustained. The revised precedence equation can be corresponding as:

$$B(p)=\alpha \times M_a(p)+ \beta \times R(p), 0\leq\alpha, \beta\leq1$$

Where,
α - the module weights for the confidence, β - the module weights for the data terms and $M_a(p)$ - the methodical assertion term.

$$M_a(p)=(1-\gamma) \times A(p)+ \gamma, 0 \leq \gamma \leq 1$$

Where,
γ – Standardizing factor for scheming the smoothness of the curve.

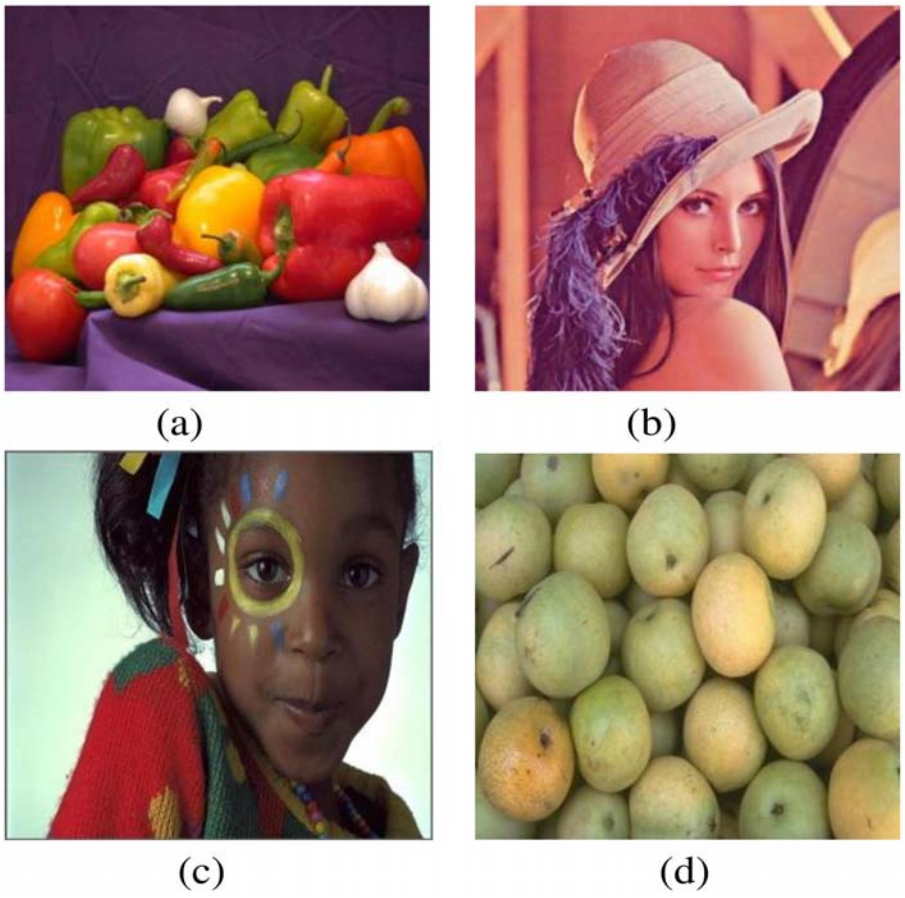

Figure 3. Forecasted image based on exemplar inpainting that depicts as original image without any distortion Peppers (a), Lena (b), Girl (c) and pears (d)

3.3 Huffman Compression

Huffman encoding is an optimum lossless compression algorithm that is based on repeatedly occurring of a symbol which is used to squeeze the data. To increate the embedding ratio the image is compressed .First, the image that is to be hidden is covert to text file and then the Huffman generate a sequence of source decline by gathering the least possibility of symbols (i.e. pixels that are not-repeated) convert to single symbol which will be substitute for the further process. The demonstration of this concept is below:

Original Source		Source Reduction	
Symbol	Probability	1	2
υ1	0.5	0.5	0.5
υ2	0.1875	0.3125	0.5
υ3	0.1875	0.1875	
υ3	0.125		

The next process is the least source to be coded, initiating with minimum source and operating with the basic source. The binary code is used to represent the length i.e., 0 and 1. The demonstration is below:

Original Source			Source Reduction			
Symbol	Probability	Code	1		2	
υ1	0.5	1	0.5	1	0.5	1
υ2	0.1875	00	0.3125	01	0.5	0
υ3	0.1875	011	0.1875	00		
υ3	0.125	010				

The coding process in the Hoffman is n immediate distinctively decode able since each block is fixed and each word is string.

4. Embedding Process using SSB

In the embedding technique the pixels are selected using selected significant bit process as each pixel are classified based on Primary pixels and secondary pixels. Secondary pixels are used to embed the secret data using secured functions which helps in increasing the security in the embedding procedure.

Step 1: Forecasting image that we got from exemplar inpainting using dynamic thresholding image Q is taken as I_e and the contrast image is easily computed as

$$C = I - I_e$$

Step 2: Then the histogram of contrast image C is computed and taken as HCe. Next, the top two peak levels are taken as P1 and P2 and their relations are as follows

Case I: if P1-P2 > 0

Case II: if P1-P2 < 0

Step 3: Based on the HCe value the cases are chosen, if the HCe value satisfies the Case I then from P1it start lookup for the next null value and denoted as Q1. Similarly from P2 it lookup for next null value and denoted as Q2. If the values are not fond then search in a vice versa.

Step 4: After getting the all the values P1, P2, Q1 and Q2. Identify the pixel $C(x_1, y_1)$ that matches with $C(x_1, y_1) = 1$ in the contrast image. If HCe corresponds to Case I then $C(x_1, y_1)$ is altered to $C'(x_1, y_1)$.

The secret data is hidden to the image and it is represented as *K*.

$$C'(x_1, y_1) = \begin{cases} C(x_1, y_1) + 1, \\ \text{if } C(x_1, y_1) = P1 \text{ and } K = 1 \text{ or if } P1 < C(x_1, y_1) < Q1 \\ C(x_1, y_1) - 1, \\ \text{if } C(x_1, y_1) = P2 \text{ and } K = 1 \text{ or if } Q2 < C(x_1, y_1) < P2 \\ C(x_1, y_1), \\ \text{if } C(x_1, y_1) = P1 \text{ or } P2 \text{ and } K = 0 \text{ or otherwise} \end{cases}$$

If HCe correspond to Case II it performs as

$$C'(x_1, y_1) = \begin{cases} C(x_1, y_1) + 1, \\ \text{if } C(x_1, y_1) = P2 \text{ and } K = 1 \text{ or if } P2 < C(x_1, y_1) < Q2 \\ C(x_1, y_1) - 1, \\ \text{if } C(x_1, y_1) = P1 \text{ and } K = 1 \text{ or if } Q1 < C(x_1, y_1) < P1 \\ C(x_1, y_1), \\ \text{if } C(x_1, y_1) = P1 \text{ or } P2 \text{ and } K = 0 \text{ or otherwise} \end{cases}$$

Step 5: Stego image S_e is formed by adding the altered C' to the image I_e.

$$S_e = I_e + C'$$

5. Extraction and Recovery Mechanism

Step 1: In the extraction process the forecasting image I_e is retrieved from stego image S_e by using same procedure during the embedding scheme.

Step 2: Based on the P1 and P2 values corresponding Case that are used in the embedding technique is identified and used in the recovery operation.

Step 3: Then the secondary pixels are identified form them stego image S_e and based on the embedding technique the Cases are selected and the secret data is extracted from *K* which contains secret data. If it belongs to Case I then it forms as follows

$$C_x'(x_1, y_1) = \begin{cases} C'(x_1, y_1) + 1, \text{and } K = 1, \text{if } C'(x_1, y_1) = P2 - 1 \\ C'(x_1, y_1) - 1, \text{and } K = 1, \text{if } C'(x_1, y_1) = P1 + 1 \\ C'(x_1, y_1), \text{and } K = 0, \text{if } C'(x_1, y_1) = P1 \text{ or } P2 \\ C'(x_1, y_1) + 1, \text{if } Q2 \le C'(x_1, y_1) < P2 \\ C'(x_1, y_1) - 1, \text{if } P1 < C'(x_1, y_1) \le Q1 \\ C'(x_1, y_1), \text{otherwise} \end{cases}$$

Step 4: If the embedding technique belongs to Case II then it perform as

$$C_x'(x_1, y_1) = \begin{cases} C'(x_1, y_1) + 1, \text{and } K = 1, \text{if } C'(x_1, y_1) = P1 - 1 \\ C'(x_1, y_1) - 1, \text{and } K = 1, \text{if } C'(x_1, y_1) = P2 + 1 \\ C'(x_1, y_1), \text{and } K = 0, \text{if } C'(x_1, y_1) = P1 \text{ or } P2 \\ C'(x_1, y_1) + 1, \text{if } Q1 \le C'(x_1, y_1) < P1 \\ C'(x_1, y_1) - 1, \text{if } P2 < C'(x_1, y_1) \le Q2 \\ C'(x_1, y_1), \text{otherwise} \end{cases}$$

Step 5: The secret data is retrieved by adding C_x' to forecasting image I_e.

$$R = I_e + C_x'$$

6. Experimental Results

Experiments where carried on set of JPEG images with different resolutions to prove the potential of proposed technique. The proposed strategy increases the security of the steganographic technique and also boosts the embedding rate and avoids distortion in the visual quality. The PSNR is computed for all the cover images and Table 1 shows its result.

Methods	PSNR(dB)
Nearest neighbour interpolation	35.78
Bilinear interpolation	36.76
CDD inpainting	37.06
Exemplar Inpainting	39.01

Table 1. PSNR VALUE for Lena

Table 1 shows the PSNR value in which Exemplar Inpainting has higher PSNR value when compared to all other existing methods, so the exemplar inpainting avoids much distortion in the restoration process and Fig.4. Shows the performance of each method based on their PSNR value.

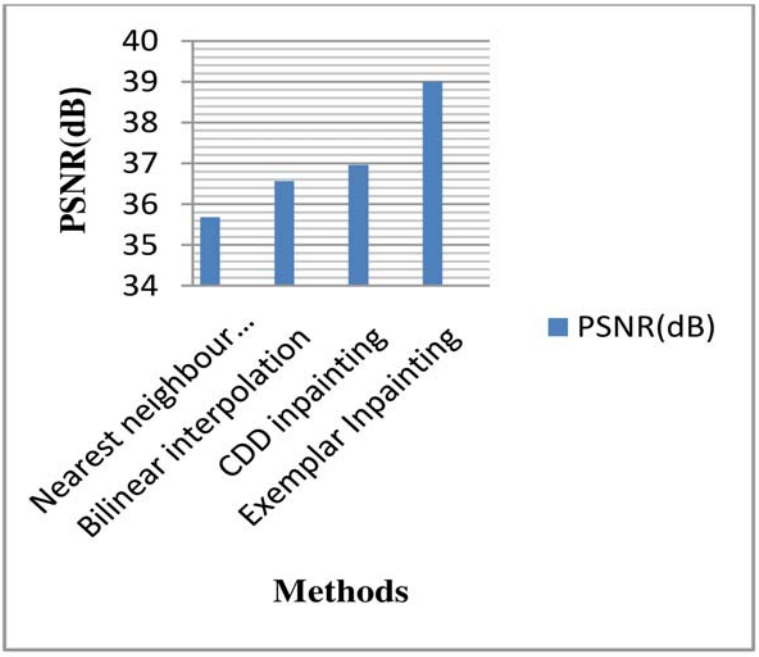

Figure 4. Performance of a proposed technique over existing methods

Then the different set of cover images Peppers (a), Lena (b), Girl (c) and pears (d) are taken with different resolutions and proposed embedding technique is implemented over it to identify the effectiveness of proposed system. The proposed mechanism maintains the visual quality and avoids distortions Fig.5. Shows its performance based on the PSNR.

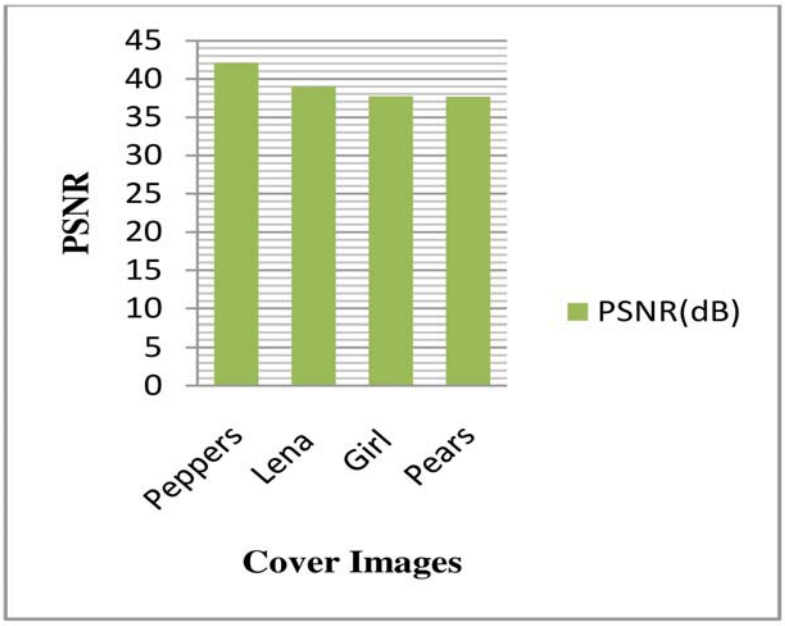

Figure 5. Performance of proposed method using different cover images

Exemplar based inpainting technique assist in increasing the embedding rate so that more amount of data can be concealed in an image in a secured way without affecting the visual quality the of the image. Fig.6. shows the Lena (b) images embedding level of the proposed mechanism over the existing practice in the Fig it clearly depicts the gain in the embedding level over the existing practice.

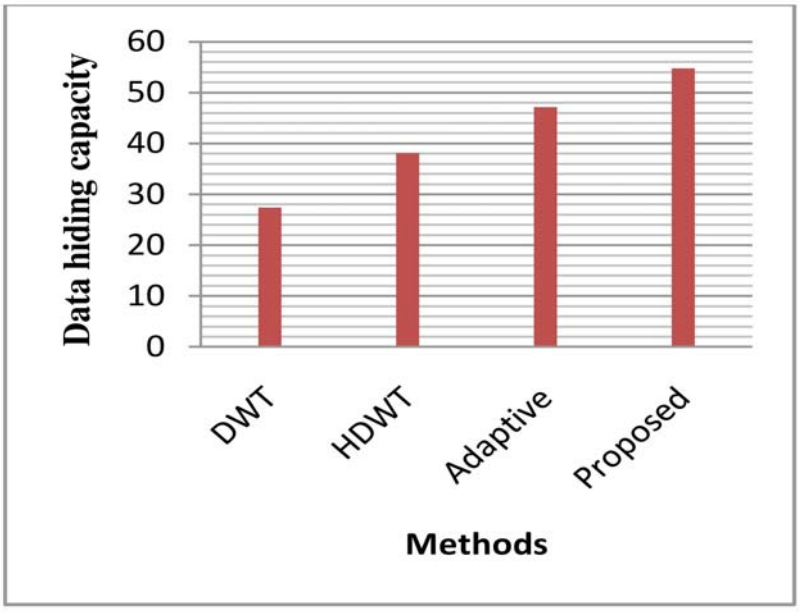

Figure 6. Comparison of proposed over existing scheme

7. Conclusion

An active steganographic scheme using SSB achieve greater embedding level and attains better visual quality compared

with existing procedure. It uses a novel method of embedding through selected significant bit based on the classification of primary and secondary pixel which increases the security of steganographic technique. The effective recovery mechanism extracts the concealed data and cover image without any inaccuracy and distortion to the image.

References

[1] Fridrich, J., Goljan, M., Du, R. (2002). Lossless data embedding—new paradigm in digital watermarking, *EURASIP J. Appl. Signal Processing*, (2) 185–196.

[2] Tian, J. (2002). Wavelet-based reversible watermarking for authentication, *In:* Security and Watermarking of Multimedia Contents IV—Proc. SPIE, E. J. Delp III and P. W. Wong, Eds., (4675) 679–690.

[3] Qin, C., Chang, C. C., Huang, Y. H., Liao, L. T. (2013). An Inpainting-Assisted Reversible Steganographic Scheme Using a Histogram Shifting Mechanism," *IEEE Transactions On Circuits And Systems For Video Technology*, 23 (7).

[4] Macq., B. (2000). Lossless multiresolution transform for image authenticating watermarking, *In:* Proc. EUSIPCO. 533–536.

[5] Tian, J. (2002). Reversible watermarking by difference expansion, *In:* Proc. Workshop on Multimedia and Security, J. Dittmann, J. Fridrich, and P. Wohlmacher, Eds. 19–22.

[6] Chang, C. C., Chen., T. S., Chung, L. Z. (2002). A steganographic method based upon JPEG and quantization table modification, *Information Sciences* 141 (1) 123–138.

[7] Chang, C. C., Lin, C. Y., Wang, Y. Z. (2006). New image steganographic methods using run-length approach, *Information Sciences* 176 (22) 3393–3408.

[8] Chang, Chin-Chen., Lin, Chih-Yang., Wang, Yu-Zheng. (2006). New image steganographic methods using run-length approach, *Information Sciences* 176. 3393–3408.

[9] Chang, Chin-Chen., Lin, Chih-Yang. (2006). Reversible steganographic method using SMVQ approach based on declustering, *Information Sciences*, Available online (October).

[10] Iwata, M., Miyake, K., Shiozaki, A. (2004). Digital steganography utilizing features of JPEG images, *IEICE Transactions on Fundamentals* E87-A (4) 929–936.

[11] Lee, Y. K., Chen, L. H. (2000). High capacity image steganographic model, *In:* Proceedings of the IEE International Conference on Vision, *Image and Signal Processing*, 147 (3) 288–294.

[12] Zeng, W. (1998). Digital watermarking and data hiding: technologies and applications, *In*: Proc. Int. Conf. Inf. Syst., Anal. Synth., (3) 223–229.

[13] Shih, F. Y., (2008). Digital watermarking and steganography: fundamentals and techniques, CRC Press., FL.

[14] Wang, S., Yang, B., Niu, X. (2010). Secure steganography method based on genetic algorithm, *Journal of Information Hiding and Multimedia Signal Processing*, (1) 1. 28-35.

[15] Rossi, L., Garzia, F., Cusani, R. (2009). Peak-shaped-based steganographic technique for JPEG images, *EURASIP Journal on Information Security*.

[16] Provos, N., Honeyman, P. (2003). Hide and seek: an introduction to steganography, *IEEE Security and Privacy Magazine* 1 (3) 32–44.

[17] Cheddad, A., Condell, J., Curran, K., Kevitt, P. M. (2010). Digital image steganography: survey and analysis of current methods, *Signal Processing* 90 (3) 727– 752.

[18] Zhang, X., Wang, S. (2006). Efficient steganographic embedding by exploiting modification direction, *IEEE Communications Letters* 10 (11) 781–783.

[19] Wang, H., Wang, S. (2004). Cyber warfare—steganography vs. steganalysis, *Communications of the ACM* 47 (10) 76–82.

[20] Chang, C., Len, C. Y. (2007). Reversible steganographic method using SMVQ approach based on declustering, *Informat. Sci*., (177) 8. 1796–1805.

[21] Alattar, A. M. (2004). Reversible watermark using the difference expansion of a generalized integer transform, *IEEE Trans. Image Process*., (13) 8. 1147–1156.