A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys

Yogendra Kumar Jain ykjain_p@yahoo.co.in
Head of the Department
Computer Science & Engineering Department
Samrat Ashok Technological Institute
Vidisha (M.P) 464001 India

R. R. Ahirwal ram2004_ahirwal2004@rediffmail.com
Computer Science & Engineering Department
Samrat Ashok Technological Institute,
Vidisha (M.P) 464001 India

Abstract

To enhance the embedding capacity of image steganography and provide an imperceptible stego-image for human vision, a novel adaptive number of least significant bits substitution method with private stego-key based on gray-level ranges are proposed in this paper. The new technique embeds binary bit stream in 24-bits color image (Blue channel) or in 8-bits gray-scale image. The method also verifies that whether the attacker has tried to modify the secret hidden (or stego-image also) information in the stego-image. The technique embeds the hidden information in the spatial domain of the cover image and uses simple (Ex-OR operation based) digital signature using 140-bit key to verify the integrity from the stego-image. Besides, the embedded confidential information can be extracted from stego-images without the assistance of original images. The proposed method can embed 4.20 bits in each pixel of gray-scale image and 4.15 bits in each pixel of color image. The presented method gives better results than the existing methods.

Key-words: Steganography, stego-key, data hiding, digital image, PSNR (Peak-Signal-to-Noise-Ratio).

1. INTRODUCTION

The emergent possibilities of modern communication need the exceptional way of security, especially on computer network. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity are essential to protect against unauthorized access. This has resulted in an explosive growth of the field of information hiding. Moreover, the information hiding technique could be used extensively on applications of military, commercials, anti-criminal, and so on [1]. To protect secret message from being stolen during transmission, there are two ways to solve this problem in general. One way is encryption, which refers to the process of encoding secret information in such a way that only the right person with a right key can decode and recover the original information successfully. Another way is steganography, steganography literally means covered writing. Its goal is to hide the fact that communication is taking place. In the field of steganography some terminology has been developed. The term cover is used to describe the original, innocent message, data, audio, still video, and so on. If the cover media is a digital image hidden with secret data, this image is called stego-image. Steganography hides the secret message with the host data set and its presence is imperceptible [2]. PCs facilitated sending and exchanging photographs, greeting cards, birthday cards, etc. in a manner that thousand of these are exchanged on the internet on the daily basis. It is not only economical, but users can choose cards from a vast Varity of them freely available and takes no time taken to send to them.

Additionally audio and video files are also exchanged freely. This exchange of cards and files has further given strength to steganography.

Watermarking, another way of data hiding aims at different purposes from steganography. Copyright protection and authentication is on primary target of image watermarking and it is required that embedded information can be prevented, resisted, or altered up to some degrees of distortion while the watermarked image is attacked or damaged. Because of this requirement, robustness becomes the main benchmark emphasized by the image watermarking techniques. Unlike watermarking, capacity, security and invisibility are the benchmarks needed for data hiding techniques of steganography.

2. TYPES AND MEDIA

Steganography may be classified as pure, symmetric, and asymmetric. While pure steganography does not need any exchange of information, symmetric and asymmetric need to exchange of keys prior to sending the messages [3]. Symmetric steganography is employed in our proposed method in which stego-key is exchanged. Steganography is highly dependent on type of medium being used to hide the information. Medium being commonly used include, text, images, audio-files, and network protocols used in network communication [4].

Image steganography is generally more preferred media because of its harmlessness and attraction. Image steganography may classify according to working domain: (a) Spatial domain and, (b) Frequency domain. Spatial domain steganography work on the pixel value directly and modify the pixel gray-value [5]. In Frequency domain based methods [6], images are first transformed into the frequency domain and then message are embedded in the transform coefficients.

A digital image is an array of numbers that represent light intensities of various points [7]. The light intensities or pixels are combines to form the images raster data. The images can be grayscale (8-bits) or color (24-bits). Although larger size image file facilitate larger amount of data to be hidden but transferring require more bandwidths and therefore increases the cost. Two types of file compression generally used to overcome above said problem are lossy compression and lossless compression. JPEG (Joint photographic group) is an example of lossy compression. Its advantage is that it saves more space but in doing so loses its originality. On the other hand GIF, PNG and BMP are examples of lossless compression which is in general recommended media types. Since both of these retain their originality [8]. Our algorithm is simple and flexible using LSBs technique. We have selected the formats that commonly use lossless compression that is BMP, PNG, TIF and GIF. We can make use of any of these formats or convert BMP into any of the above said format.

3. REVIEW OF RELATED WORK

The usage of a stego-key is important, because the security of a protection system should not be based on the secrecy of the algorithms itself, instead of the choice of a secret key [9] as shown in Fig. 1. The steganographer's job is to make the secretly hidden information difficult to detect given the complete knowledge of the algorithm used to embed the information except the secret embedding key. This so called kerckhoff's principle is the golden rule of cryptography and is often accepted for steganography as well [10]. Some steganographic methods [11] [12] uses a stego-key to embed message for achieving rudimentary security. Mehboob et. al. proposed technique uses predictive position agreed between two parties as stego-key [3]. Same position used only once to enhance security. But drawback of the algorithm is small amount of data to be embedded.

The most common and simplest steganographic method [13] [14] is the least significant bit insertion method. It embeds message in the least significant bit. For increasing the embedding capacity two or more bits in each pixel can be used to embed message. At the same time not only the risk of making the embedded statistically detectable increase but also the image fidelity degrades. So how to decide the number of bits of each pixel used to embed message becomes an important issue of image steganography.

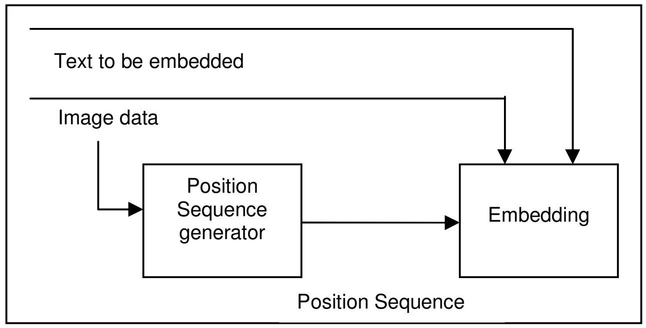

Fig. 1: Generalized Stego-key system

Cheeldod et al. [15] proposed an adaptive steganography that select the specific region of interest (ROI) in the cover image. Where safely embeds data. The choice of these regions based on human skin tone color detection. Adaptive steganography are not an easy target for attacks especially when the hidden message is small [16]. The tri-way pixel value differencing method proposed by ko-chin-chang can successfully provide embedding capacity and outstanding imperceptibility for the stego-images.

Suresh Babu et al. [17] Proposed steganographic model authentication of secret information in image steganography, that can be used to verify the integrity of the secret message from the stego-image. In this method payload is transformed from spatial domain to discrete wavelet transform. The DWT coefficients are then permuted with the verification code and then embedded in the special domain of the cover image. The verification code is generated using to special coefficient in the DWT domain. Thus the method can verify each row has been modified or forget by attacker.

Moon and Kavitkar [18] proposed a fixed 4LSB method to embedding an acceptable amount of data; 4LSB embedding data can easily be implemented and do not visually degrade the image to the point of being noticeable. But drawback of the scheme is that the encoded message can be easily recovered and even altered by 3rd party. So techniques must be developed to solve above said problems. Lie et al. [19] proposed an adaptive method based on using variable amount of bits substitution instead of fixed length for adjusting the hiding capacity.

Adnan Gutub, et al. proposed a steganography technique for RGB color images [20]. They proposed an image-based steganography technique called triple-A algorithm. The algorithm adds more randomization by using two different seeds generated from a user-chosen key in order to select the component (s) used to hide the secret bits as well as the number of the bits used inside the RGB image component. This randomization adds more security especially if an active encryption technique is used such as AES. While Enayatifar et al. proposed a method, in which two chaotic signals for specifying the location of the different parts of the message in the picture [21]. An 80-bit key was used to reach the preliminary measures of the two chaotic signals and this caused a kind of scattering format for the data embedding place in the image, as they are randomly selected. But one can easily find the place and order of the data embedding by knowing the chaotic function and the key values (two 5 bit keys). It is noticeable that a minor change in the key values (primary values of the keys) will bring about a drastic change in the produced values of the chaotic functions.

4. PROPOSED METHODOLOGY

The proposed scheme works on the spatial domain of the cover image and employed an adaptive number of least significant bits substitution in pixels. Variable K-bits insertion into least significant part of the pixel gray value is dependent on the private stego-key K_1. Private stego-key consists of five gray-level ranges that are selected randomly in the range 0-255. The selected key shows the five ranges of gray levels and each range substitute different fixed number of bits into least significant part of the 8-bit gray value of the pixels (in gray image and in color image blue channel). After making a decision of bits insertion into different ranges, Pixel p(x, y) gray value "g" that fall within the range Ai-Bi is changed by embedding k-message bits of secret information into new gray value “g’ ”. This new gray value “g’ ”of the pixel may go beyond the range Ai-Bi that makes problem to extract the correct information at the receiver. Specific gray value adjustment method is used that make the new gray value “g’ ” fall within the range Ai-Bi. Confidentiality is provided by the private stego-key k_1 and to provide integrity of the embedded secret information, 140-bit another key K_2 is used. Digital signature of the secret information with the key K_2 were obtained and appended with the information. The whole message plus signature is embedded into the cover image that provides some bit overheads but used to verify the integrity. At the receiver key K_1 is used to extract the message and key K_2 is used to verify the integrity of the message.

4.1 Private stego-key generation

Private stego-key K_1 play an important role in proposed scheme to provide security and deciding the adaptive K bits insertion into selected pixel. For a gray scale image (or RGB color image blue channel) 8-bit used to represent intensity of pixel, so there are only 256 different gray values any pixel may hold. Different pixels in image may hold different gray values. We may divide the pixels of images into different groups based on gray ranges. Based on this assumption let five ranges of gray levels are < A_1-B_1, A_2-B_2, A_3-B_3, A_4-B_4, A_5-B_5 > each range starting and ending value are in 8-bits, total 80-bits are used to make a key K_1. If the difference of each range is denoted by Di=Bi-Ai (for i=1, 2, 3, 4, 5; Ai denote starting value and Bi denote ending value of the range), it should not be less than 32 gray values and any range should not be overlap with other ranges. For Example selected key K_1: 2-36, 38-73, 74-102, 105-170, and 178-245. Difference $D_2=B_2-A_2$ will be $D_2 = 73-38=35\geq32$, and any range is not overlapping. Hence key is usable.

4.2 Method to decide Bits insertion in each range

Let the five gray ranges decided by the stego-key are <A_1-B_1, A_2-B_2, A_3-B_3, A_4-B_4, A_5-B_5 > and number of pixel count from cover image in each range are < N_1, N_2, N_3, N_4, N_5 >. Range with maximum pixel count will hold maximum bits insertion let five bits, second maximum count will hold four bits insertion and so on. In this way we decide the fixed number of bits insertion into each range and adaptive number of bits insertion into different ranges based on pixel count of cover image in different ranges. In similar way we decide the bits extraction from each range. For Example assume key K_1 is 2-36, 38-73, 74-102, 105-170, 178-245 and let pixel count in each range from any image are 300,100,34,4000,700. Then range first insert three message bits in the pixel that comes within the range, range second insert two message bits in the pixel ,range third insert one bit in the pixel ,range four insert five bits in the pixel and range five insert four message bits in the pixel that comes in this range. In this manner we decide the bits insertion into each range.

4.3 LSB substitution

Least significant substitution is an attractive and simple method to embed secret information into the cover media and available several versions of it. We employ in propose scheme adaptive LSB substitution method in which adaptive K-bits of secret message are substituted into least significant part of pixel value. Fig.2 shows entire method for K-bits insertion.

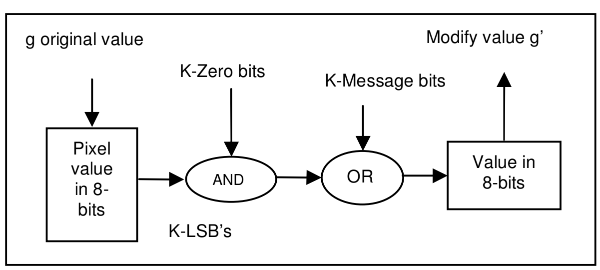

Fig 2: Method for K-bits insertion

To decide arbitrary k-bits insertion into pixel, first we find the range of pixel value and then find the number of bits insertion decided by method given in section IV (b) and insert K-message bits into least significant part of pixel using LSB. After embedding the message bits the changed gray value g’ of pixel may go beyond the range. To make value within the range, reason is that receiver side required to count pixels to extract message, pixel value adjusting method is applied to make changed value within range.

4.4 Pixel value adjusting method

After embedding the K-message bits into the pixel gray value g new gray vale g' may go outside the range. For example let our range based on key is 0-32. Let the gray value g of the pixel is 00100000 in binary forms (32 in Decimal), decided K-bits insertion is 3-bits are 111. The pixel new gray value g' will be 00100111 in binary forms after inserting three bits (39 in Decimal). Modified value is outside the range. To make within the range 0-32, K+1 bits of g' is changed from 0 to 1 or via- versa. And checked again to fall within range if not K+2 bit is changed and so on until gray value fall within range. For example, 00100111- 00101111- 00111111- 00011111. Figure 3 shows the whole process.

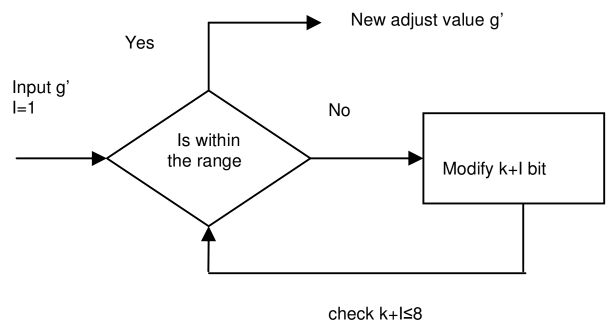

Fig. 3: Pixel value adjusting method

4.5 Digital signature

To verify the integrity of the stego-image and secret information, a simple Ex-OR method to find signature of secret message with random stego-key of 140 bits is used and appended with the message, some overheads occurs but integrity of the message is checked at the receiver. Block Diagram of whole process is given in Fig. 4 (a) and 4 (b). Algorithm for coding and decoding the secret information is given below.

Algorithms: Coding

Input: Cover-image, secret message, keys K_1, K_2.
Output: Stego-image.
Step1: Read key K_1 based on gray-Level ranges.
Step2: Read cover image (8-bit gray Image or 8-bit color image blue Channel)
Step3: Decide No. of bits insertion into each range describe in section IV (b).
Step4: Read the secret message and Convert it into bit stream form.
Step5: Read the key K_2.
Step6: Find the signature using K_2 and append with the message bits.
Step7: For each Pixel
    7.1: Find gray value g.
    7.2: Decide the K-bits insertion based on gray ranges.
    7.3: Find K-message bits and insert using method given in section IV(c).
    7.4: Decide and adjust new gray Value g' using method described in sec. IV (d)
    7.5: Go to step 7.
Step 8: end

Algorithm: Decoding

Input: Stego-image, keys K_1, K_2;
Output: Secret information;
Step1: Read key K_1 based on gray-level ranges.
Step2: Read the stego image.
Step3: Decide No. of bits extraction into each range. Describe in section IV (b).
Step4: For each pixel, extract the K-bits and save into file.
Step5: Read the key K_2 and find the signature of bit stream
Step6: Match the signature.
Step7: End

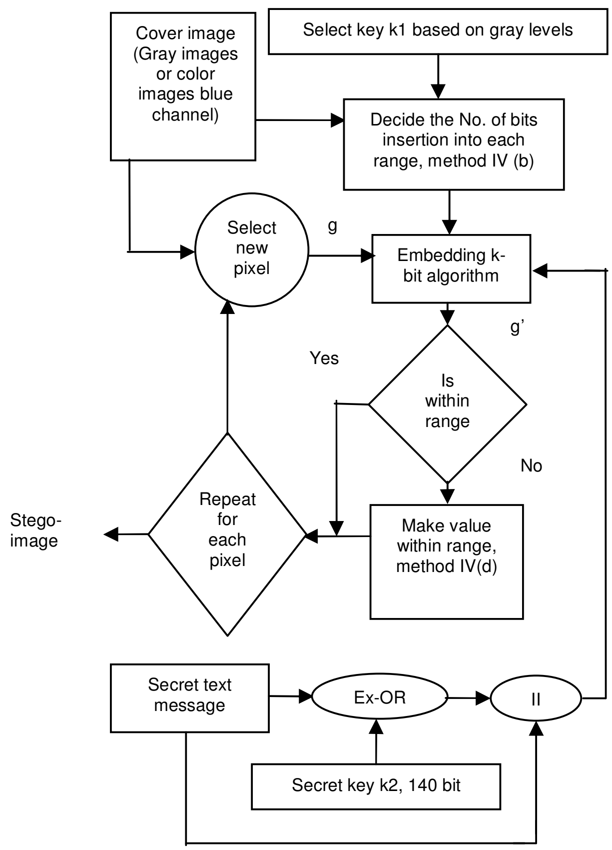

Fig. 4 (a): Message Embedding with signature

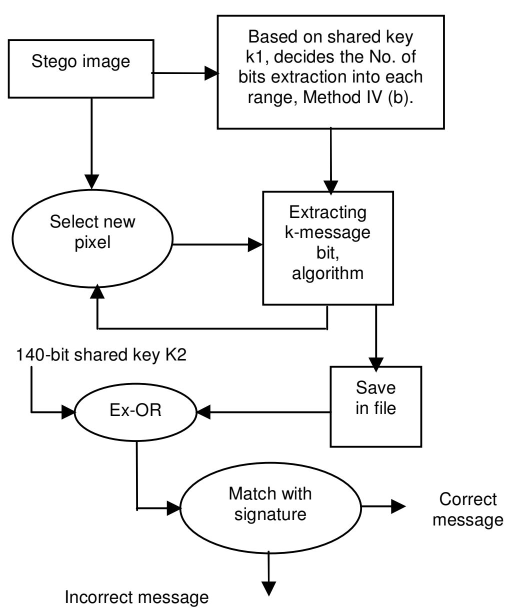

Fig. 4 (b): Message extraction and Integrity check

5. RESULTS AND DISCUSSIONS

To demonstrate the accomplished performance of our proposed approach in capacity and imperceptibility for hiding secret data in the cover-image, we have conducted different experiments using different images to compare the proposed approach with fixed 4 LSB method [18] and the method given in [19]. According to invisibility benchmark PSNR 30dB is acceptable. Results are considered for each image (gray image and color image) size 150x150 with 100% capacity using different stego-keys (five ranges in each key).

The well known Peak-Signal-to-Noise Ratio (PSNR) is used as performance measurement criteria, which is classified under the difference image distortion metrics, is applied on the Stego and the Original images. It is defined as [22]:

$$PSNR = 10 \log_{10}\left(\frac{{C_{max}}^2}{MSE}\right) \qquad \text{---------(1)}$$

Where, C_{max} holds the maximum value in the original images and MSE denotes Mean Square Error and given as:

$$MSE = \frac{1}{MN} \sum_{m=1} \sum_{n=1} \left(S_{xy} - C_{xy}\right)^2 \quad \text{(For Grayscale Images)} \qquad \text{-------(2)}$$

Where, x and y are the image coordinates, M and N are the dimensions of the image, S_{xy} is the generated Stego image and C_{xy} is the cover image

$$MSE = \left[\frac{MSE(R) + MSE(G) + MSE(B)}{3}\right] \quad \text{(For Color RGB Images)} \qquad \text{---------(3)}$$

As a performance measurement for embedding capacity, the average number of bits embedded into each pixel is calculated as:

$$Capacity = \left(\frac{\text{Total Number of bits embedded into image}}{\text{Total Number of Pixels in image}}\right) \quad \text{(bits/pixel)} \quad \text{------(4)}$$

The embedding capacity and PSNR results of proposed method for the different grayscale and color images are shown in Table-1, Table-2. Table-1 shows the results when the message is embedded into gray scale images and Table-2 shows the result when the message is embedded into the blue channel of the RGB color images using different key.

Different keys (Using five ranges)	Grayscale Images (8-bit)							
	Cameraman		Shadow		Baboon		Pout	
	CAP	PSNR	CAP	PSNR	CAP	PSNR	CAP	PSNR
0-33, 34-70, 71-105, 106-170, 171-255	4.11	34.4979	4.1373	32.7129	4.16	37.8410	4.5031	32.8608
2-35, 37-73, 74-105, 106-170, 171-255	4.1178	33.9581	4.1260	32.5237	4.1469	37.9279	4.5030	31.5815
2-35, 37-73, 74-115, 116-170, 171-250	3.9836	34.1044	3.9698	33.4759	4.15	37.6350	4.5850	31.4671
0-45, 47-85, 86-143, 144-190, 191-255	4.1211	32.2653	4.0009	34.0415	4.1248	38.6471	4.6652	31.4089
0-45, 47-85, 86-143, 144-188, 189-255	4.1077	32.6375	4.0076	34.0831	4.1305	38.5906	4.6650	31.4585
Average Values	4.0881	33.4926	4.0483	33.3674	4.1424	38.1283	4.5842	31.7553

Table 1: Results in terms of Embedding Capacity and Image Quality (In PSNR) using different keys for different grayscale images [(CAP- Embedding Capacity in bits/pixel), (PSNR-Peak-Signal-to-Noise-Ratio)].

Different keys	Color Images (24 bit)

(Using five ranges)	Lena		Onion		Football		Baboon	
	CAP	PSNR	CAP	PSNR	CAP	PSNR	CAP	PSNR
0-33, 34-70, 71-105, 106-170, 171-255	4.1568	36.9145	4.2208	37.0962	4.0685	45.9343	4.0685	45.9343
2-35, 37-73, 74-105, 106-170, 171-255	4.1284	36.8187	3.8610	37.4604	4.0361	45.9434	4.0361	45.9434
2-35, 37-73, 74-115, 116-170, 171-250	4.1968	36.8365	3.8574	37.4886	4.0157	45.9260	4.0157	45.9260
0-45, 47-85, 86-143, 144-190, 191-255	4.3933	37.4985	4.3999	37.2020	4.1693	44.7775	4.1693	44.7775
0-45, 47-85, 86-143, 144-188, 189-255	4.3902	37.5066	4.3992	37.1964	4.1695	44.5496	4.1695	44.5496
Average Values	4.3131	37.1149	4.1476	37.2887	4.0918	45.4261	4.0918	45.4261

Table 2: Results in terms of Embedding Capacity and Image Quality (In PSNR) using different key for different color images [(CAP-Embedding Capacity in bits/pixel), (PSNR-Peak-Signal-to-Noise-Ratio)].

Table-3 shows the comparison of results in terms of Embedding Capacity (in bits/pixel) and Image Quality (PSNR in dB) of Proposed Method with 4LSB method and Adaptive Method. The 4LSB Method [18] can embeds upto 4 bits/pixel for gray-scale and color images, while Adaptive Method [19] can embeds upto 4.025 bits/pixel for gray-scale and color images. On the average case, our proposed method can embed 4.20 bits in each pixel of gray-scale image and 4.15 bits in each pixel in blue channel of color image. Hence, the embedding capacity is better than the existing 4LSB Method and Adaptive Method. Also, the image quality attained in proposed method is better than the existing methods.

Images	Embedding methods					
	4LSB Method		Adaptive Method		Proposed Method	
	CAP	PSNR	Average CAP	PSNR	Average CAP	PSNR
Gray-Scale images	4	31.71	4.025	32.57	4.20	34.18
Color images using Blue Channel	4	--	4.025	--	4.15	40.99

Table 3: The Comparative Results in terms of Embedding Capacity and Image Quality (In PSNR) of Proposed Method with 4LSB method [18] and Adaptive Method [19] [(BC-Blue channel of color image), (CAP-Capacity in bits/pixel)].

The Comparison of existing methods with Proposed Method in terms of in term of embedding capacity, image quality for grayscale and color images are shown in figure 5. Therefore, it is clearly seen from the experimental results that the performance of proposed method is better than the existing methods. In addition to that, the advantage of proposed method is that employment of stego key in embedding process provides better security.

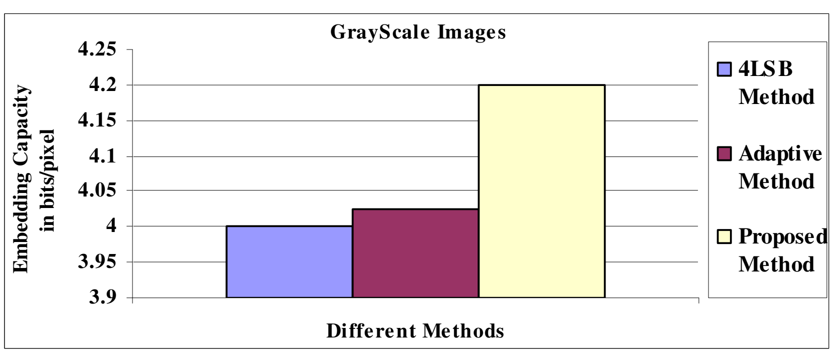

Fig. 5 (a): Comparison of different methods with Proposed Method in term of embedding capacity

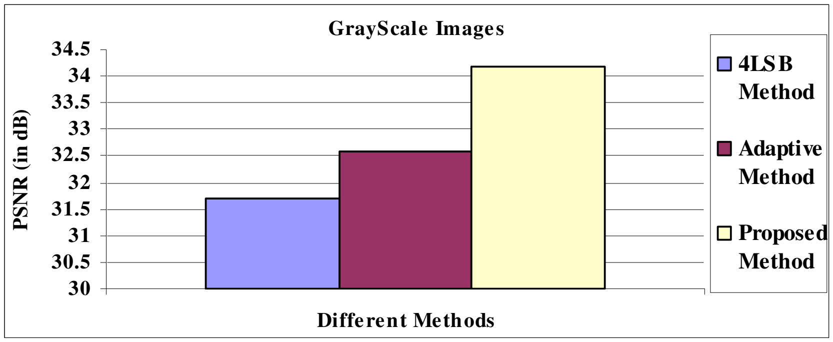

Fig. 5(b): Comparison of different methods with Proposed Method in term of image quality

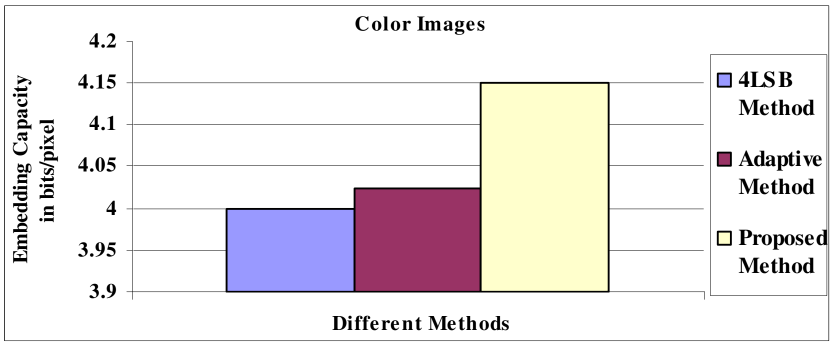

Fig. 5 (c): Comparison of different methods with Proposed Method in term of embedding capacity

6. CONCLUSION

We have introduced a novel image steganographic model with high-capacity embedding/extracting module that is based on the Variable-Size LSB substitution. In the embedding part based on stego-key selected from the gray value range 0-255. We used the pixel value adjusting method to minimize the embedding error and adaptive 1-5 bits to embed in the pixel to maximize average capacity per pixel. Using the proposed method, we embedded at least four message bits in each pixel while maintaining the imperceptibility. For the security requirement we have presented two different ways to deal with the issue. The major benefit of supporting these two ways is that the sender can use different stego-keys in different sessions to Increase difficultly of stegano analysis on these stego images. Using only the stego-keys, which is used to count the number of pixel in each range and second 140-bit key to verify the integrity of the message, the receiver can extract the embedded messages exactly. Experimental results verify that the proposed model is effective and efficient.

7. REFERENCES

[1] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, *"Information Hiding - A Survey"*, Proceeding of the IEEE, vol. 87, issue 7, pp. 1062-1078, July 1999.

[2] S. Dumitrescu, W. X. Wu and N. Memon, *"On steganalysis of random LSB embedding in continuous-tone images"*, Proceeding of International conference on image Processing, Rochester, NY, pp. 641-644, 2002.

[3] B. Mehboob and R. A. Faruqui, *"A steganography Implementation"*, IEEE – International symposium on biometrics & security technologies, ISBAST'08, Islamabad, April 2008.

[4] K. Ahsan and D. Kundur, *"Practical data hiding in TCP/IP"*, Proceeding of the workshop on multimedia security at ACM multimedia, 2002.

[5] A. Westfeld, *"F5- A steganographic algorithm: High capacity Despite Better Steganalysis"*, Proceeding of 4th Int. Information Hiding Workshop, Springer-Verlag, vol. 2137, 2001.

[6] I. Cox, J. Kilian, T. Leighton and T. Shamoon, *"Secure spread spectrum watermarking for multimedia"*, IEEE Transaction on Image processing, vol. 6, issue 12, pp. 1673-1687, 1997.

[7] Neil F. Johnson, and Sushil Jajodia, *"Exploring Steganography: Seeing the Unseen"*, IEEE computer society press vol. 31, issue 2, pp 26-34, Feb. 1998.

[8] D. E. Denning, E. Dorothy, *"Information Warfare and Security",* Boston, MA: ACM Press, pp. 310-313, 1999.

[9] Jian Zhao, E. Koch, *"Embedding Robust Lables into Images for Copyright Protection"*, Proceeding of the international Conference on Intellectual property Right for specialized information, Knowledge and New Technologies, Vienna, August 1995.

[10] Jiri Fridrich. "*A New Steganographic Method for Palette-Based Images",* Center for Intelligent Systems, SUNY Binghamton, Binghamton, NY 13902-6000, U.S Government, a grant number F30602-98-C-0009.

[11] F. A. P. Petitcolas, R. J. Anderson, *"On the Limit of Steganography"*, IEEE J. Sel. Areas Communication, vol. 16, issue 4, pp. 474-481, 1998.

[12] M. Kutter, E. Jordan and E. Bossin, *"Digital signature of Color images using amplitude modulation"*, Journal of Electronics imaging, vol. 7, issue 2, pp. 326-332, 1998.

[13] E.T. Lin, E.J. Delp, *"A review of data hiding in images "*, Proceedings of the conference on image processing image quality image capture systems, PICS'99, pp. 274-278, April 1999.

[14] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, *"Techniques for data Hiding"*, IBM, syst. J., vol. 35, issue 3&4, pp. 313-336, 1996.

[15] A. Cheddad, J. Condell, K. Curran and P. McKevitt, *"Enhancing Steganography in digital images"*, IEEE - 2008 Canadian conference on computer and Robot vision, pp. 326-332, 2008

[16] Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang, and Te-ming Tu, *"A novel image steganographic method using Tri-way pixel value Differencing"*, Journal of multimedia, vol. 3, issue 2, June 2008.

[17] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal, L. M. Pataki, *"Authentication of secret information in image steganography"*, IEEE Region 10 Conference, TENCON-2008, pp. 1-6, Nov. 2008.

[18] S. K. Moon and R.S. Kawitkar, *"Data Security using Data Hiding"*, IEEE International conference on computational intelligence and multimedia applications, vol. 4, pp. 247-251, Dec. 2007.

[19] W. N. Lie and L. C. Chang, *"Data Hiding in images with adaptive numbers of least significant bits based on human visual system"*, IEEE international conference on image processing, vol. 1, pp. 286-290, 1999.

[20] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh, *"Triple - A: Secure RGB Image Steganography Based on Randomization"*, IEEE/ACM international conference on computer systems and applications, pp. 400 - 403, 2009.

[21] R. Enayatifar, S. Faridnia, H. Sadeghi, *"Using the Chaotic Map in Image Steganography"*, IEEE international conference on signal processing systems, pp. 754 - 757, 2009.

[22] J. Zollner, H. Federrath, H. Klimant, et al., *"Modeling the Security of Steganographic Systems"*, in 2nd Workshop on Information Hiding, Portland, pp. 345-355, April 1998.