A New Steganography Technique Based on Layers of Image and Sensitivity Vectors Acquiring HVS

Jagvinder Kaur [#1]

[#] *M.Tech Scholar, Electronics and Communication Engineering,*
Amritsar College of Engineering and Technology,
Amritsar, 143001, India

Abstract— *Steganography is the art and science of hiding the existence of information. To provide an imperceptible stego-image quality and to improve the capacity of the hidden secret data, a steganography technique based on layers of image and sensitivity vectors is proposed in this paper. In this technique, firstly the whole host image is divided into 8x8 blocks and each block is further sub-divided into the 8x8 sub block which is formed by the binary representation of pixel values of the image. The SVBA algorithm then analyzes the mean value of gray block by block, and sets a sensitivity vector for each block with considering HVS features. It adjusts the embedding of secret message for steganography schema dynamically according to the block sensitivity vectors. The simulation experiment results on Matlab7.10 show this algorithm has a balanced performance on efficiency, capacity, imperceptibility and robustness.*

Keywords— *Steganography, Peak Signal-to-Noise Rate (PSNR), Mean Square Error (MSE), Manhattan distance (Mdist); HVS features; Block sensitivity vector.*

I. INTRODUCTION

Steganography, known as an art of hiding information, is a means of embedding data within another data while protecting its secrecy. The secret data is embedded inside the cover data by a hiding method and is sent to a receiver. The receiver applies the reverse process on the cover data and reveals the secret data. The main goal is to protect the existence of hidden data from being realized by the third parties.

Unlike cryptography, which simply conceals the content or meaning of a message, steganography conceals the very existence of a message. The steganography is such a helpful process that if it is used and implemented properly, the hidden message will not be noticed from unwanted links, who might be trying to attack over it. The others can neither identify the meaning of the embedded object, nor can recognize its existence. It ensures complete security of the data. Only the recipient who must know the technique used, can recover the message and then decrypt it.

Thus, the method aims to cause minimum amount of distortion on the cover object. Images are the most popular cover objects used for steganography. Steganography based on still digital image has been one of the most important research issues due to its wide application in digital copyright protection, digital media content surveillance, content authentication, and covert communication.

II. STEGANOGRAPHY EMBEDDING

The basic embedding procedure is illustrated in Fig.1

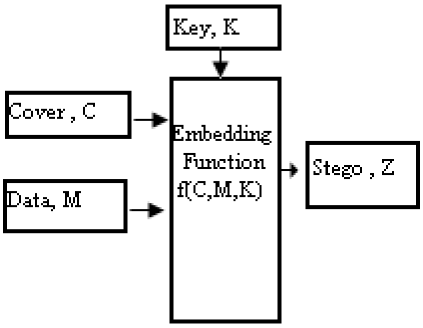


Fig.1. A General Steganography Model for embedding of Secret Message.

The secret message is embedded inside the cover object by a hiding algorithm and is sent to a receiver. The embedding function, i.e. steganography algorithm, tries to preserve the perceptive properties of the original image. A suitable image, called the cover/carrier, is chosen. The secret message is then embedded into the cover using the steganographic algorithm, in a way that does not change the original image in a human perceptible way. The receiver then applies the reverse process on the cover data and reveals the secret data. The result is new image, the stego-image that is not visibly different from the original [14] [15]. From an observer's view, the existence of a secret message is (visibly) hidden. The motive of using image is of no importance, it serves only as a carrier for hidden message. Since, images are quite popular cover or carrier objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist.

In *Image Domain* methods secret messages are embedded using the intensity of the pixels values directly and are relatively simple compared to the other methods and are sometimes characterised as the "simple systems" [13]. However, they are generally more sensitive to small changes on the image such as filtering, resizing and squeezing [1]. While image domain methods use the least significant bits in binary value of image pixel, transformation domain methods transform image data to frequency domain and perform hiding process in that domain. The transformation domain methods, on the other hand, are more robust to changes, but their data hiding capacity is lower than the image domain methods.

In this study, a new image domain method, based on layers of image and block sensitivity vectors acquiring HVS features is proposed which hide the secret data within image blocks. SVBA first divides cover image into 8*8 blocks. After representing pixel values in binary system it fully utilizes the below mentioned HVS features and the statistical features of each block to get a block sensitivity vector, and adjust the embedding method according to the sensitivity vector. Performance measure of the proposed method is done against steganalysis. For this reason, randomly selected secret bit streams are embedded different cover images. There are two important error metrics used to compare host image and stego-image; Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR), which are used to measure the degradation on the cover images. The Normalized Cross-Correlation shows the robustness of the algorithm against stego-attacks.

The given paper is explained as follows. The section III, discusses important features of HVS. The section IV discusses the proposed steganography technique based on layers of image and block sensitivity vectors acquiring HVS features respectively. In the experiments, PSNR, MSE and Normalized Cross-Correlation parameters are calculated on different images and with various iterations. These are explained in section V. Finally, the section VI discusses the conclusion of the paper and the future studies on the topic.

III. IMPORTANT FEATURES OF HVS

HVS (Human Visual System) is an optical information processing system that can perceive process, analyze, and understand optical signals from outside. Important features include the following three aspects:

1) *Brightness Mask Feature*: In the background of fixed luminance, human eyes' perception effect depends on the contrast of average background brightness and the brightness of target area. HVS has a nonlinear change characteristic to different brightness level; the sensitivity is the highest towards middle level brightness, and declines nonlinearly in both directions to lower or higher level. Comparatively speaking, the sensitivity declines faster in the darker direction than in brighter direction [2].

2) Texture Mask Feature: In the background of fixed luminance, HVS is most sensitive to the grayscale change in smooth regions, as the frequency increases, the resolution of human eyes will decline sharply and become quite dull to the change of grayscale in regions with complex texture.

3) *Edge Mask Feature*: The edge information of image is very important for vision, especially the position information because HVS is more likely to detect position error than the grayscale error in edge regions [3].Besides there are features like direction sensitivity, etc.

IV. PROPOSED STEGANOGRAPHY METHOD

In this method, the capacity of the secret message to hide and image quality is our main concern. Here, SVBA algorithm then analyzes the mean for grayscale cover image block by block, and sets a sensitivity vector for each block with considering HVS features. The Fig. 2 shows the block diagram the embedding process.

The steps for the embedding method are illustrated below:

1) Divide the cover image into 8*8(pixel) blocks.

2) Calculate the gray mean value 'I' of each block. Suppose the grayscale value of pixel (x, y) in block B $_k$ is *i(x,y)*, and the probability of grayscale value I is P*i*, m=255, n=8*8, I can be calculated by the following formula;

$$I = \sum_{i=0}^{255} i.Pi \qquad (1)$$

3) According to HVS mask features, gray sensitivity model of human eye, the noticeable differences (ND) for the each block of the image can be calculated by the below given formula in (2);

$$ND = \begin{cases} 1 - \dfrac{1 * I}{256}, & (I \leq 128) \\ \dfrac{1 * I}{256}, & (128 \leq I \leq 255) \end{cases} \qquad (2)$$

However the real situation is that grayscale sensitivity of human eyes declines nonlinearly from middle level grayscale to higher and lower grayscale, and HVS is more sensitive in brighter areas than darker areas.

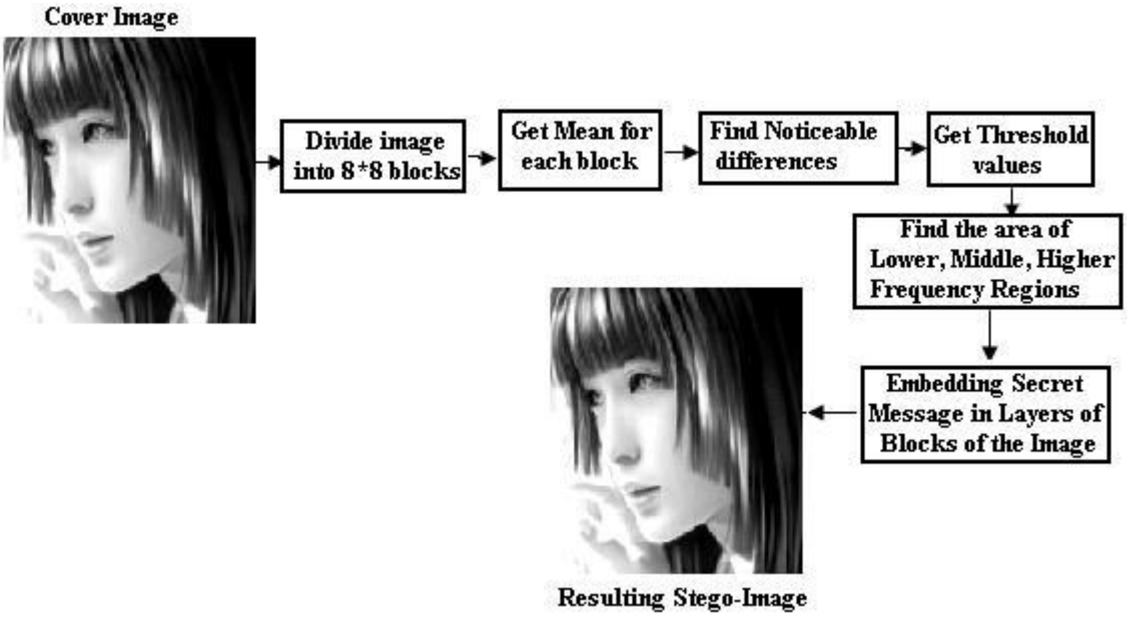

Cover Image
Divide image into 8*8 blocks
Get Mean for each block
Find Noticeable differences
Get Threshold values
Find the area of Lower, Middle, Higher Frequency Regions
Embedding Secret Message in Layers of Blocks of the Image
Resulting Stego-Image

Fig.2. The Embedding Process of Proposed Method

4) Now, set three thresholds levels T_1 =50, T_2 =80, T_3=180 and simplify the ND derivation by formula (3) for block B_k.

$$NDt = \begin{cases} 3 & when\ (I \leq T1) \\ 2 & when(T1 < I \leq T2, T3 < I \leq 255) \\ 1 & when\ (T2 < I \leq T3) \end{cases} \tag{3}$$

When NDt=3, this block is classified as a region of lower frequency grayscale sensitivity, and set grayscale sensitivity component *Sk* =1; When NDt=2, this block is classified as a region of middle frequency grayscale sensitivity, and set grayscale sensitivity component *Sk* =2; When NDt =1, this block is classified as a region of higher frequency grayscale sensitivity, and set grayscale sensitivity component S*k* =3.

5) Now, represent the values of all pixels in the cover image in their binary form. The blocks of the cover image are separated into further sub blocks [4] [8].

6) Now, the algorithm's search process will run through all the blocks of the cover image. That is, the algorithm will find the values of NDt.
If NDt=1, the secret message will be embedded in the higher frequency gray scale region.If NDt=2, the secret message will be embedded in the middle frequency gray scale region. If NDt=3, the secret message will be embedded in the lower frequency gray scale region. The Fig. 3 shows all the frequency region of the cover image.

7) Comparatively in Huang's method [10], secret data is embedded in some of the low frequency coefficients, which will cause obvious blocking effect and visual quality distortion. Experiment results show that this method has good performance in both invisibility and robustness against normal attacks. The position of frequency coefficients chosen is shown in the Fig.3.

8) Now the steganalysis part which is must for any steganography technique. The steganalysis is the extraction of the hidden data from the stego-image. The first step in steganalysis is to determine the existence of secret message in host image by measuring the degradation in the stego-image [16]. Therefore, the performance measure of the proposed method is done against steganalysis. This provides minimum amount of degradation on the cover image.
The original cover image is always needed to extract the embedded hidden secret data. Firstly the cover image is divided into 8*8 blocks and analyzed to get the SV of each block. According to the sensitivity vector, one can easily determine the embedding schema and choose the corresponding extraction method to get the hidden data. The steganalysis process is the reverse of the proposed method. All the hidden information embedded in the original cover image can be easily extracted using the reverse process followed in the Fig.2.
The performance of steganography methods is mainly measured by the degree of robustness to the steganalysis techniques. The first step in steganalysis is to determine the existence of secret message in host image by measuring the degradation in the stego-image. Two of the error

metrics used to compare the host image and stego-image are Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

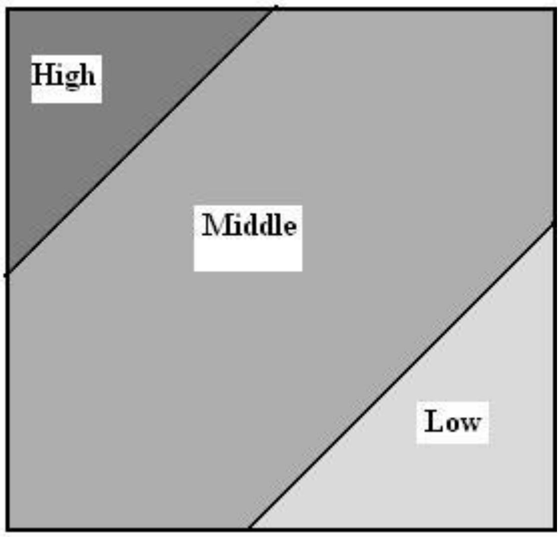


Fig.3. The Low, Middle and High Frequency region of the cover image

V. EXPERIMENTAL RESULTS

The PSNR represents a measure of the peak error, whereas, MSE represents the cumulative squared error between the resultant image and the original image. The lower the value of MSE, the lower is the error [6]. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images [11]. This ratio is often used as a quality measurement between the original and a resultant image. The higher is the PSNR, the better the quality of the reconstructed image [12].

$$MSE = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} (s(i,j) - c(i,j))^2 \qquad (4)$$

$$PSNR = 10 * Log_{10} \frac{R^2}{MSE} \qquad (5)$$

Where *c(i,j)* and *s(i,j)* is the gray value of pixel at *(i,j)* in cover image and stego-image respectively. *R* is the maximum fluctuation in the input image data type or we can say that it gives the maximum intensity value of image. For example, in the presented proposed method, the value of R is 255 [6].

The Normalized Cross-Correlation calculates the cross-correlation in the spatial or the frequency domain, depending on size of images. Then it calculates the local sums by pre-computing running sums. Use local sums to normalize the cross-correlation to get correlation coefficients. The resulting matrix or image matrix contains the correlation coefficients, which can range in value from -1.0 to 1.0.

$$NC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} s(i,j) * c(i,j)}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} s(i,j)^2 * \sum_{i=1}^{M} c(i,j)^2}} \qquad (6)$$

Among all the formats of digital image, 256 level grayscale BMP image is considered to be the best carrier of secret information [7].In this paper, 256 level grayscale BMP images named Tina, Circ, Candles, Lenna, Lady, and Tulip as cover images are taken to carry out the experiments. The Table 1 shows the average values of PSNR, MSE and Processing time of algorithm, computed over different image with over 20 iterations.

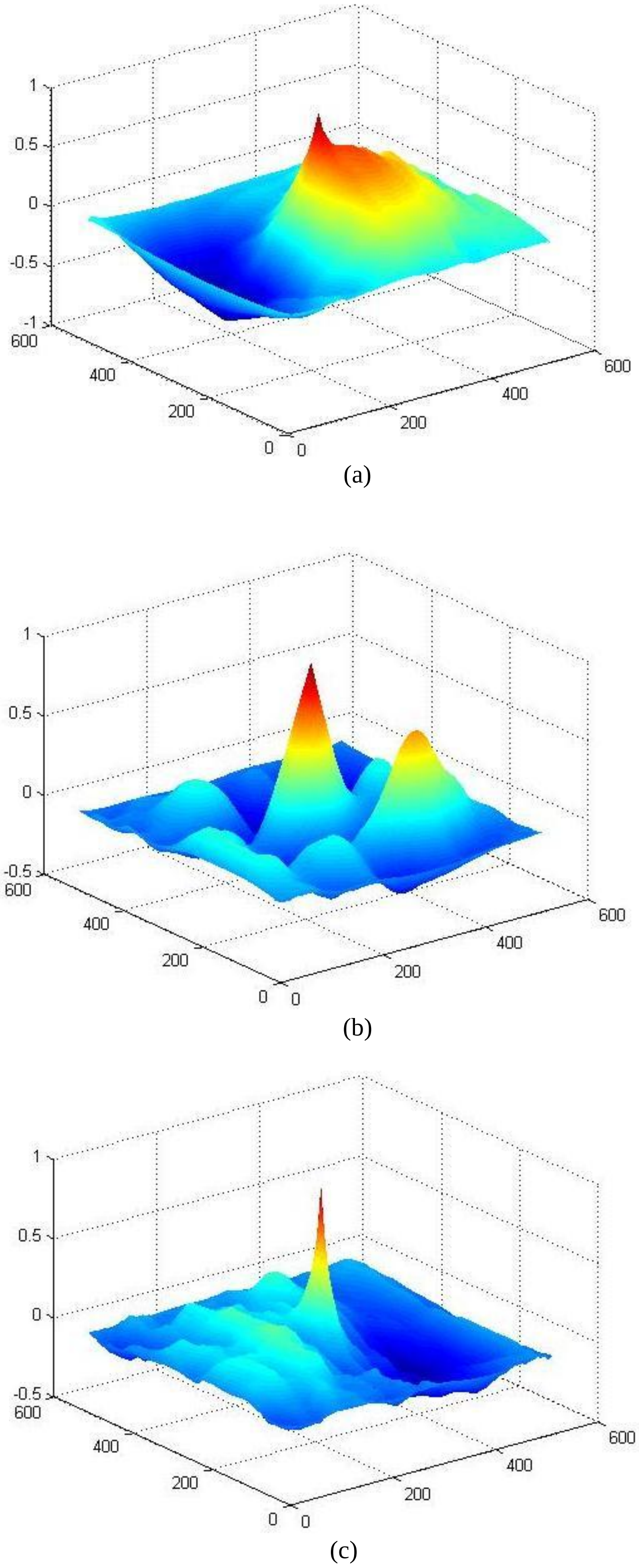
Table 1. The Resultant Values of PSNR, MSE, and Processing Time of Algorithm

Different Cover Images	**Average PSNR**	**Average MSE**	**Average Processing Time(Seconds)**
Tina	60.1551	0.0627	20.762645
Circ	60.2232	0.0618	22.221279
Candles	60.1975	0.0621	22.326428
Lenna	60.0859	0.0638	22.592515
Lady	60.2093	0.0620	21.010528
Tulip	60.2642	0.0612	20.785734

The performance of proposed method is calculated using various grey level images with length 256x256. In the experiments, randomly selected messages are embedded into all the images. The images are divided into 8 by 8 blocks and 8 bit secret data is embedded into each block.

Considering the size of the images and the pixel values represented by 8 bits, the length of messages embedded into each image will be as high as 8192 bits. The embedding secret data does not cause an obvious distortion in the image quality, the stego-image is highly alike to cover image. The performance wise the proposed approach is much better than Huang’s algorithm [10] and Yi-zhen Chen’s algorithm [5].

The Normalized Cross-Correlation results in the form of Matlab 7.10 figures are shown in Fig. 4(a-c). Due to the space problem, we have only shown three normalized cross-correlation for the cover images Tina, Candles and Lenna. If the cover image is of low texture complexity and low grayscale value, performance against JPEG compression will be better; otherwise the algorithm will be comparatively vulnerable towards compression attacks. Generally speaking, the robustness performance differs to some extent depending on the characteristics of the cover image. The results say that this method decreases the degradation in the quality of the host image.



(a)

(b)

(c)

Fig. 4. The Normalized Cross-Correlation results for cover images Tina, Candles and Lenna

Although we have tried our best keep the hiding capacity better than the previous methods, but still, the hiding capacity is not as important as image quality and the robustness to the stego attacks.

VI. CONCLUSIONS

The proposed method makes less degradation to the host cover image. The image quality remains much conserved and robustness to the stego-attacks is also better in our proposed steganography technique based on layers of image and block sensitivity vectors acquiring HVS Features. This was the main concern of this research. The method presented has very good performance in imperceptibility. The capacity is effectively enhanced compared with Huang's algorithm. The cover image by 8*8 blocks, when the cover image is of low or high grayscale and of low texture complexity, it will be robust against attacks like compression.

However, this technique is not so matured in because although the algorithm has good performance in imperceptibility and capacity due to its dynamically selected embedding schema, it does not reach an ideal performance in robustness. In addition, it does not allow hiding different number of sequences into the blocks according to the optimal correspondence. Therefore, the quality of stego-image can increase. It will be planned to do research on variable size secret data hiding methods. And these will be further studied in future research work.

ACKNOWLEDGMENT

I would like to acknowledge Er. Sanjeev Kumar, Assistant Professor/ Electronics and Communication Engineering /Amritsar College of Engineering and Technology, Amritsar, India, for his immense contribution towards this work. His encouragements made me believe in me. Working on this research has been a brain stimulating experience. I would extend special thanks to my parents and my husband for their love and support.

REFERENCES

[1] Juan Jose Roque, Jesus Maria Minguet, "SLSB: Improving the Steganographic Algorithm LSB".

[2] Simmons. The prisoners' problem and the subliminal channel proceedings of cryptology' 83. Plenum Press, 1984, pp.51–67.

[3] B.M.Macq, Jean Jacques Quisquater. Cryptology for digital TV broadcasting. Proceedings of the IEEE. June 1995, 83(6), pp.944–957

[4] Omer Kurtuldu, Nafiz Arica, "A New Steganography Method Using Image Layers", IEEE, 2008

[5] Yi-zhen Chen, Zhi Han, Shu-ping Li, Chun-hui Lu and Xiao-Hui Yao, "An Adaptive Steganography Algorithm Based On Block Sensitivity Vectors Using HVS Features", CISP, IEEE, 2010

[6] http://www.mathworks.com

[7] J.Fridrich, M.Goljan, R.Du. Detecting lsb steganography in color and gray-scale images. IEEE Multimedia, 8(4), pp.22–28, 2001

[8] M.A.Khan, V.Potdar, E.Chang, "An Architecture Platform for Grey Level Modification Steganography", Industrial Electronics Society, 2004. IECON'04. 30th Annual Conf. of IEEE, Vol. 1, pp. 463- 471

[9] T. Morkel , J.H.P. Eloff , M.S. Olivier , "An Overview Of Image Steganography"http://mo.co.za/open/stegoverview.pdf.pp.2.5

[10] Jiwu Huang, YunQ Shi, Ruohe Yao. Adaptive Image Watermarking Based on Block Classification [J]. Journal of I mage and Graph ics.1999,4(8), pp. 640–643.

[11] Rafael C. Gonzalez, Richard E. Woods and Steven L. Eddins, "Digital Image Processing Using Matlab" Prentics Hall, 2003

[12] Anil K Jain, "Fundamentals of Digital Image Processing", University of California-Davis, Prentice Hall,1988

[13] Eric Cole ,"Hiding in Plain Sight: Steganography and the Art of Covert Communication"

[14] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998

[15] Lee, Y.K. & Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000

[16] N.F. Johnson, S. Jajodia, "Steganalysis: The Investigation of Hiding Information", *IEEE*, 1998.