ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

An Improved Image Steganography Technique using Pixel Pair Matching driven by Spatial Frequency and Luminance Masking

Akhil P V[1], Jyotsna E[2], Divya John[3]

PG Student, Department of Computer Science, FISAT, Angamaly, India [1]

PG Student, Department of Computer Science, FISAT, Angamaly, India [2]

Assistant Professor, Department of Computer Science, FISAT, Angamaly, India [3]

Abstract: This paper proposes a new improved steganographic technique based on pixel pair matching which is driven by spatial frequency and luminance masking. The cover image is scanned using a spatial frequency and luminance mask and the result is used as the candidate region to perform data hiding using pixel pair matching. The basic idea of pixel pair matching (PPM) is to use the value of a pixel pair as a reference coordinate, and search a coordinate in the neighbourhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit. In contrast to the existing methods based on PPM, the masking driven approach has lower distortion for various payloads. Experimental results reveal that the proposed method provides better performance than the existing techniques and also is secure under some well-known steganalysis techniques.

Keywords: Image steganography, LSB encoding, Adaptive pixel pair matching, masking, payload, cover image, stego-image, security.

I. INTRODUCTION

In recent years, the security and the confidentiality of the sensitive data has become of prime and supreme importance due to the explosive growth of internet and the fast communication techniques. Therefore how to protect secret messages during transmission becomes an important issue and hiding data provides a good layer of protection on the secret message. One of the widely accepted data hiding technique is image steganography. Steganography is different from cryptography in maintaining the secrecy of hidden information in the medium that is used for transmitting the data. Image steganography uses a digital image as cover media and hence it is called cover image. The data is hidden in the cover image and the resulting image is called stego image. The data can be extracted out from the stego image and the existence of a hidden message in the cover image is invisible. The embedding of data in an image can cause distortion in the cover image and this distortion caused by data embedding is called embedding distortion. A good data-hiding method should be immune to statistical and visual detection while providing an adjustable payload [1], [2]. There are a number of techniques available which can perform image steganography in a digital image and this paper focuses on analysing the different techniques and proposing a method which can offer better results over the methods that are studied.

A. *Digital Steganography*

A digital steganographic encoder is shown on Figure 1. The message is the data that the sender wishes to keep confidential and can be text, images, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. This is also referred to as the message wrapper. The message embedding technique is strongly dependent on the structure of the cover. It is not required that the cover and the message have homogeneous structure.

The image with the secretly embedded message produced by the encoder is the stego-image. The stego-image should resemble the cover image under casual inspection and analysis. In addition, the encoder usually employs a stego-key(optional) which ensures that only recipients who know the corresponding decoding key will be able to extract the message from a stego-image [3]. This improves the security of the data that is being transmitted.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

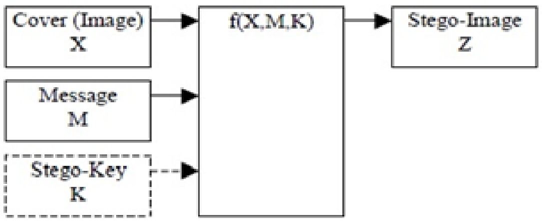


Fig. 2 . Steganographic Encoding

B. Human Visual System and Image Steganography

The property of human eye on how an image is perceived is exploited by the human visual system (HVS). Certain characteristics of an image and not easily visible to human eye and those characteristics can be used and combined with image steganography to avoid visual and statistical detection of the embedded data. The key factors [17] which influence them include:

- The eye is less sensitive to noise in the high resolution bands and in those bands having orientation of 45.
- The eye is less sensitive to noise in those areas of the image where brightness is high or low.
- The eye is less sensitive to noise in highly textured areas, but, among these, more sensitive near the edges.

These properties can prove handy when combined and exploited in image steganography. Many of the data embedding techniques developed so far has concentrated only on the data hiding aspect of image steganography and not on studying the image characteristics and hiding the data.

The rest of this paper is organized as follows. Section 2 explains the various methods developed for image steganography, a proposed system is presented in section 3 and section 4 includes the experimental analysis and results. Section 5 presents the conclusion and remarks.

II. SURVEY

There are various data hiding techniques developed in recent years.

J. Mielikainen developed a method [4] which is based on pixel pair matching and it uses a pair of pixels as the embedding unit. The LSB of first pixel carries one bit of information and a binary function of the two pixel values carry another bit of information. This method offers same payload (number of bits embedded in the cover image) as LSB matching with fewer changes to cover image. The MSE of LSB for 1 bpp is 0.5, while for LSBMR it is 0.375.

OPAP [5] is an enhancement of LSB substitution method and it is based on embedding error. It uses only one pixel as embedding unit. In this method, for a m-bit pixel, if message bits are embedded to the right-most r LSB's then other m-r bits are adjusted by a simple evaluation. These m-r bits are either replaced by the adjusted result or otherwise kept unmodified based on if the adjusted result offers smaller distortion.

An improvement of LSB matching revisited method is EMD [6] in which each (2n+1)-ary notational system is carried by n cover pixels and at most only one pixel is increased or decreased by 1. The secret message is converted into a sequence of digits in the notational system with an odd base. Then pseudo-randomly permute all cover pixels according to a secret key, and divide them into a series of pixel-groups, each containing n pixels. The method is very well able to provide better stego image quality under the same payload than traditional LSB.

Diamond Encoding [7] an extension of EMD method and it first partitions the cover image into non-overlapping blocks of two consecutive pixels and transforms the message to a series of K-ary digits. For each block a Diamond Characteristic Value (DCV) is calculated and one secret K-ary digit is concealed into DCV. The DCV is modified to secret digit and it is done by adjusting pixel values in a block. This method is capable of hiding more secret data while keeping the stego-image quality degradation imperceptible.

Method used in [8] is an enhancement of the EMD method and this method segments the cover image into pixel sections and each section is partitioned into the selective and descriptive groups. The EMD embedding procedure is then performed on each group by referencing a predefined selector and descriptor table. The method combines different pixel groups of the cover image to represent more embedding directions with less pixel changes than the EMD method. By selecting the appropriate combination of pixel groups, the embedding efficiency and the visual quality of the stego image is enhanced. It offers higher embedding efficiency than EMD method.

The method [9] partitions the cover image into non-overlapping blocks of two consecutive pixels. The difference value is calculated from the values of the two pixels in each block and all possible difference values are classified into a number of ranges. The selection of the range of intervals is based on the characteristics of human vision's sensitivity to gray scale values from smoothness to contrast. The difference value is then replaced by a new value to embed the value of a sub-stream of the secret message. The resultant image offers better quality results.

Edge Adaptive Image steganography [10] extends the LSB matching revisited steganography. The method first divides the cover pixels into blocks and rotates each block by a random degree based on the secret key. The rotation causes new edges to appear and among the edges a threshold value is used to get the most suitable areas where data is hidden. Now the blocks are rotated back to normal and thus the data gets embedded. The reverse of the method is employed to extract the data. The method offers better image quality and immunity to steganalysis than the LSBMR method.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

Reversible data embedding using interpolation and reference pixel distribution introduced in [11] is a reversible data hiding method based on image interpolation and detection of smooth and complex regions in the cover image. A binary image that represents the locations of reference pixels is constructed according to the local image activity. In complex regions, more reference pixels are chosen and fewer pixels are used for embedding and vice-versa for smooth regions. Pixels are interpolated according to the constructed binary image, and interpolation errors are then used to embed data through histogram shifting. It offers better prediction and a mechanism to add or remove reference pixels based on local image characteristics. The method achieves better PSNR for a range of embedding rates.

Pixel Pair Matching(PPM) [12] method uses the values of pixel pair as a reference coordinate, and search a coordinate in the neighbourhood set of this pixel pair according to a given message digit. The searched digit conceals the digit and it replaces the pixel pair. It makes use of a more compact neighbourhood set than used in Diamond encoding. The extraction process finds the replaced pixel pair to extract the message data. Exploiting Modification Direction (EMD) method has a maximum capacity of 1.161 bpp and Diamond Encoding (DE) extends the payload of EMD by embedding digits in a larger notational system. The proposed method offers lower distortion than DE by providing more compact neighbourhood sets and allowing embedded digits in any notational system. Compared with the optimal pixel adjustment process (OPAP) method, the proposed method always has lower distortion for various payloads.

The proposed method in [13] is a hiding scheme by replacing the LSB of a cover according to the difference values between a pixel and its four touching neighbours. Although this method can embed most secret data along sharper edges and can achieve more visually imperceptible stegos, the security performance is poor. Since the method just modifies the LSB of image pixels when hiding data, it can be easily detected by existing steganalytic algorithms, such as the RS analysis.

Optimized Bit Plane splicing algorithm [14] is implemented by M. Naseem et.al. where in the pixels are grouped based on their intensity and then the number of bits are to represent the hidden data are chosen. As the bits are grouped based on the intensity of the pixels, more number of darker intensity pixels can be used to represent the hidden data than just the LSB.

In [15] the authors implemented a Combined Linked-list and LSB technique that uses the concept linked list of randomly embedding the data in the image and linking them together. The attacker is unable to guess the next message as the data is not hidden sequentially. Also, without the password it is not possible to access the hidden data.

III. PROPOSED SYSTEM

The data embedding methods discussed so far does not take into consideration any of the image characteristics. A good data-hiding method should be capable of evading visual and statistical detection while providing an adjustable payload. This immunity can be achieved by exploiting the characteristics of the human visual system (HVS).If the image characteristics are considered and candidate areas in an image for data embedding are found out, the data can be embedded on those areas, and the result can offer more immunity towards statistical and visual evaluation methods of steganography. The proposed method uses two levels of masking namely, spatial frequency masking and luminance masking. These two masking considers the image characteristics and extracts out the suitable regions for data embedding. The combined result of two levels of masking is considered as the candidate area for data embedding. The resultant area applies the Pixel Pair Matching(PPM). The Pixel Pair Matching(PPM) method has only very little detection methods available and is considered to be a method which offers very good results. In this method where the values of pixel pair as a reference coordinate, and search a coordinate in the neighbourhood set of this pixel pair according to a given message digit. The searched digit conceals the digit and it replaces the pixel pair. Thus the data is embedded in the cover image and during extraction, the corresponding pixel pair is found to extract the data.

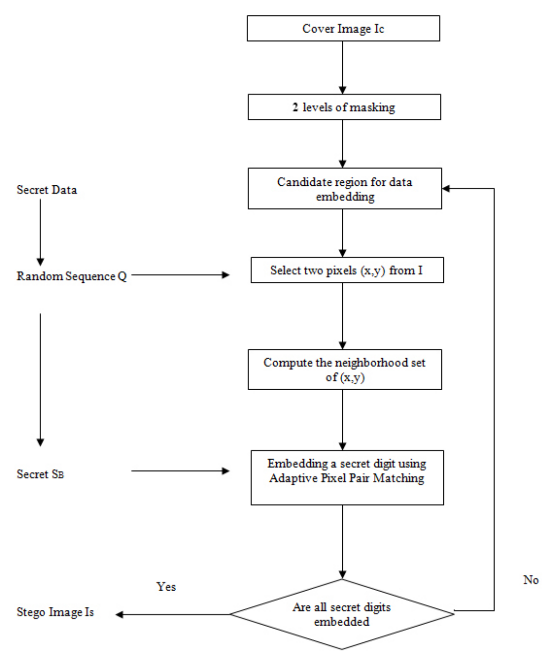


Fig 2: Proposed System

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

A. Candidate region extraction using Spatial Frequency Masking and Luminance Masking

The input image is scanned first and spatial frequency masking and luminance masking are performed. The results of both the operations are combined using OR-operation. The masking process is described below.

In the spatial frequency method, the cover image is read. The image has to be prepared before the spatial frequency mask is applied. The multiwavelet subband structure is obtained prior to masking. For the given image, single-level discrete 2-D wavelet transform is performed. In matlab, for the decomposition into multi-wavelet subbands dwt2 function is used and it is done for a particular wavelet and here '*haar*' wavelet is used. Discrete wavelet transform decompose signals into subbands with smaller bandwidths and slower sample rates. Here two-dimensional discrete wavelet transform (DWT) leads to a decomposition of approximation coefficients at level j in four components: the approximation at level $j + 1$, and the details in three orientations (horizontal, vertical, and diagonal).

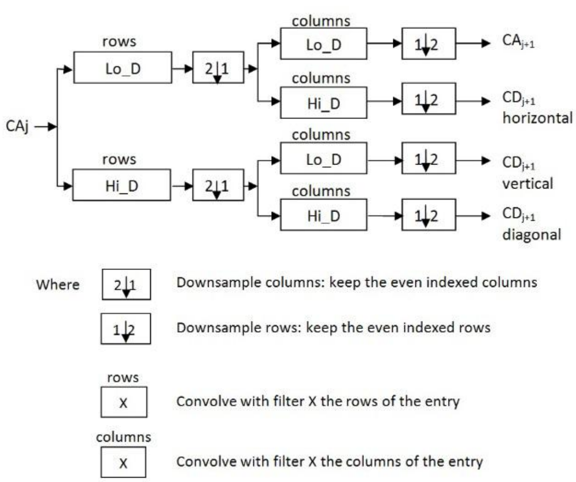


Fig. 3. Two Dimensional DWT

During the first 'dwt2' transformation the cover image resized using 'nearest' interpolation is given as input. It generated the wavelet transforms or subbands in four levels; approximation, horizontal, vertical and diagonal. The LL-subband is taken and 2-D wavelet transform is again performed on it. This process is repeated two more times and every time only the LL-subband of previous decomposition is considered. Finally we obtain sixteen subbands is identified by a pair of integers (λ,θ) , where λ is transform level and θ is orientation. The orientations are indexed as 1, 2, 3, 4 corresponding to Low-Low (LL), High-Low (HL), High-High (HH) and Low-High (LH) subbands respectively. In the process of obtaining the mask the following formula is used:

$$F(\lambda, \theta, i, j) = \left(\frac{v\lambda \max ,LL,i',j'}{vmean}\right)^{\alpha T} \qquad (1)$$

where λ_{max} is the highest level of the DWT decomposition and is set to 5 in this work, v_{mean} is the LL subband constant corresponding to the mean luminance of the display (128 for an unsigned 8-bit image). In the formula, $v\lambda_{max},i',j'$ is the value of the DWT coefficient, in the LL subband, that spatially corresponds to location (λ,θ,i',j') . In this case, i' and j' can be calculated as $i'=\lfloor i/2^{\lambda max-\lambda}\rfloor$ and $j'=\lfloor i/2^{\lambda max-\lambda}\rfloor$, where floor is the operation of rounding to the nearest smaller integer. The parameter that controls the degree to which masking occurs is αT and takes a value of 0.649.

For spatial frequency masking, single-level inverse discrete 2-D wavelet transform is applied next on the horizontal, vertical and diagonal details to obtain the approximation details. Matlab uses '*idwt2*' function to perform the inverse discrete wavelet transform operation. The reason why horizontal, vertical and diagonal details are chosen is because these three are considered to be the details of an image and has more influence on the spatial frequency details compared with approximation. The first approximation is reconstructed from the details of an image and the further approximation is obtained for two more levels from the approximations generated before it. Now to obtain the mask of our interest a threshold is used. This filters out the less significant areas of the result and gives area of interest as the result. This mask is deployed on to the image and the result returned is used to combine with luminance masking. The luminance masking also takes the original image as input and not the result of spatial frequency masking. It is the results of both these masking, that is combined.

The Luminance masking method also follows the same initial steps as of for spatial masking like reading the input image and then obtaining the multiwavelt subbands namely LL, HL, HH and LH. Then it also uses the same equation (1) to obtain the mask. But the method is different at reconstructing the wavelet transforms. This method also uses '*idw2*' function to perform the inverse wavelet transformation. For luminance masking it is on the approximation subband the reconstruction or inverse transform is concentrated. Here we tend to avoid the details comprising of horizontal, vertical and diagonal subbands. Hence the inverse wavelet transformation is first performed on fourth approximation subband which results in third approximation. This third approximation is used to generate the second approximation using same inverse wavelet transformation function. This process is repeated again on the second approximation to finally obtain the first approximation. It is from this first approximation the mask is calculated and that is done by performing an inverse wavelet

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

transformation on it. Now finally we use a threshold to obtain the area which dominates the luminance mask result and removes the areas which have least influence in the luminance property of the image.
Finally the results of both the masking operations are combined using OR-operation to get our candidate region for data embedding.

B. Data Embedding in Candidate region using Adaptive Pixel Pair Matching (APPM)

The result returned by the masking technique serves as an input to the data embedding process. Data embedding method is performed on the candidate region. The data embedding method is discussed below.
The adaptive pixel pair matching technique uses pixel pair (x,y) as the coordinate, and searches a coordinate (x′,y′) within a predefined neighbourhood set Φ(x,y) such that f(x′,y′) = sB , where f is the extraction function and sB is the message digit in a B-ary notational system to be concealed. Data embedding is done by replacing (x,y) with (x′,y′). Suppose a digit sB is to be concealed. The range of sB is between 0 and B-1, and a coordinate (x′,y′) ϵ Φ(x,y) has to be found such that f(x′,y′) = sB. Therefore, the range of f(x,y) must be integers between 0 and B-1, and each integer must occur at least once. In addition, to reduce the distortion, the number of coordinates in should be as small as possible. The method also satisfies the following three requirements:
1) There are exactly B coordinates in Φ(x,y).
2) The values of extraction function in these coordinates are mutually exclusive.
3) The design of Φ(x,y) and f(x,y) is capable of embedding digits in any notational system so that the best can be selected to achieve lower embedding distortion.
The definitions of Φ(x,y) and f(x,y) significantly affect the stego image quality. The designs of Φ(x,y) and f(x,y) have to fulfil the requirements: all values of f(x,y) in Φ(x,y) have to be mutually exclusive, and the summation of the squared distances between all coordinates in Φ(x,y) and f(x,y) has to be the smallest. This is because, during embedding, (x,y) is replaced by one of the coordinates in Φ(x,y). Suppose there are B coordinates in Φ(x,y), i.e., digits in a B-ary notational system are to be concealed, and the probability of replacing (x,y) by one of the coordinates in Φ(x,y) is equivalent. Data is embedded by using PPM based on these f(x,y) and Φ(x,y).
The extraction function f(x,y) is decribed as follows :

$$f(x,y) = (x + c_B * y) \bmod B \qquad (2)$$

The base B which is followed in implementing the APPM method is 16 and the cB value used is 6. Thus we have the neighbourhood set defined by Φ16(x,y).

Embedding Procedure
Suppose the cover image is of size M × M, S is the message bits to be concealed and the size of S is |S|. First we calculate the minimum B such that all the message bits can be embedded. Message digits are sequentially concealed into pairs of pixels. The detailed procedure is listed as follows.
Input: Cover image I of size M × M, secret bit stream S, and key K.
Output: Stego image I′, c_B , $\Phi_{B(x,y)}$ and K_r.
1. Find the minimum B satisfying ⌊M ×M/2⌋ ≥ $|S_B|$, and convert S into a list of digits with B -ary notational system S_B.
2. The value of c_B and $\Phi_{B(x,y)}$ are computed.
3. In the region defined by $\Phi_{B(0,0)}$, record the coordinate $(x_i′,y_i′)$ such that $f(x_i′,y_i′) = i$, $0 \le i \le B - 1$.
4. Construct a nonrepeat random embedding sequence Q using a key K_r.
5. To embed a message digit s_B, two pixels (x,y) in the cover image are selected according to the embedding sequence , and calculate the modulus distance between s_B and f(x,y), then replace (x,y) with $(x + x_d, y + y_d)$.
6. Repeat Step 5 until all the message digits are embedded.

Extraction Procedure
To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The embedded message digits are the values of extraction function of the scanned pixel pairs.
Input: Stego image I′, c_B , $\Phi_{B(x,y)}$ and K_r..
Output: Secret bit stream S.
1. Construct the embedding sequence Q using the key K_r.
2. Select two pixels (x′,y′) according to the embedding sequence Q.
3. Calculate f(x′,y′), the result is the embedded digit.
4. Repeat Steps 2 and 3 until all the message digits are extracted.
5. Finally, the message bits S can be obtained by converting the extracted message digits into a binary bit stream.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Image steganography technique tries to minimize the embedding distortion in the stego image and also to make it secure. Security in image steganography means the presence of data in a stego-image should not be detectible under steganalytic tests.

A. Quality Analysis

The stego image is tested for its quality. Image quality is a characteristic of an image that measures the perceived image degradation. For our quality analysis Mean Square Error (MSE) formula used is:

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

$$\text{MSE} = \frac{1}{M*M}\sum_{i=0}^{M}\sum_{j=0}^{M}(pi,j\ -\ p'i,j)2 \qquad (3)$$

where M x M denotes the image size, pi,j and p′i,j denote the pixel values of the original image and the stego image, respectively. MSE represents the mean square error between the cover image and stego image. A smaller MSE indicates that the stego image has better image quality.

Six images Lena, Boat, Elaine, House, Lake and Baboon each sized 512 × 512 are taken as test images to compare the MSE obtained by APPM and APPM-SF-L. The notations used in representing the methods are APPM for adaptive pixel pair matching, SF for Spatial Frequency and L for Luminance and the combination of more than one method is represented by this symbol "-" . The payloads were set to 500 000, 750 000 and 1 000 000 bits respectively.

TABLE I
MSE COMPARISION(Payload = 500 000 bits, 1.907 bpp)

Image	APPM	APPM-SF-L	MSE Improvement
Lena	0.942	0.719	0.223
Boat	0.940	0.716	0.224
Elaine	0.938	0.712	0.226
House	0.932	0.720	0.212
Lake	0.941	0.716	0.225
Baboon	0.937	0.714	0.223
Average	0.938	0.716	0.222

TABLE II
MSE COMPARISION (Payload = 750 000 bits, 2.861 bpp)

Image	APPM	APPM-SF-L	MSE Improvement
Lena	3.219	2.910	0.309
Boat	3.222	2.907	0.315
Elaine	3.217	2.913	0.304
House	3.224	2.917	0.307
Lake	3.227	2.911	0.316
Baboon	3.220	2.915	0.305
Average	3.221	2.912	0.309

TABLE III
MSE COMPARISION (Payload = 1 000 000 bits, 3.815 bpp)

Image	APPM	APPM-SF-L	MSE Improvement
Lena	16.183	15.053	1.13
Boat	16.190	15.050	1.14
Elaine	16.194	15.055	1.139
House	16.188	15.057	1.131
Lake	16.189	15.048	1.141
Baboon	16.192	15.051	1.141
Average	16.189	15.053	1.136

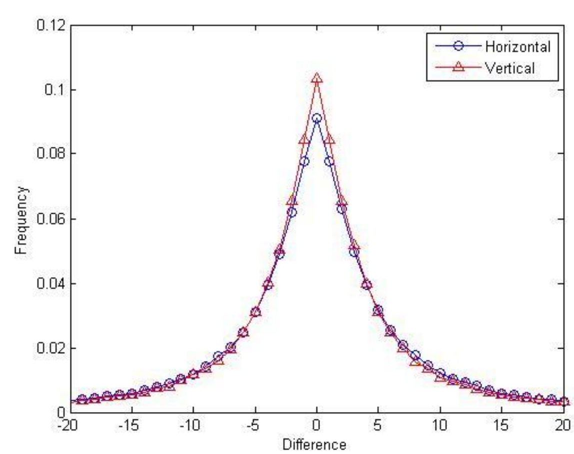
Tables I-III reveal that the performance of the proposed method APPM-SF-L method is the best under various payloads than the existing APPM. For example, with the payload 1 000 000 bits, the averaged MSE of APPM is 16.189, whereas the averaged MSE of APPM-SF-L is 15.053. That is, it shows a significant improvement by 1.136.

B. Security Analysis

The efficiency of a steganographic technique is determined by the ability of the method to stay immune towards steganalysis. It is apparent that MSE is not a good measure of security against the detection of steganalysis. In this section, we analyze the security of APPM under a statistical steganalysis scheme, the HVDH (Horizontal Vertical Difference Histogram) scheme proposed by Zhao et al. [16] which is based on the statistical analysis of histogram differences. The HVDH scheme is used to detect the presence of hiding message according to the distance between vertical and horizontal histograms. Zhao et al. observed that for many pairwise embedding methods, the difference between the horizontal difference histograms H_h and vertical difference histograms H_v are significantly altered. . Zhao et al. use the distance between H_h and H_v as a statistical detector to detect the abnormality of histogram. The distance is defined as:

$$D = \sqrt[2]{\sum_{i=-2T}^{2T}(Hh(i) - Hv(i))} \qquad (4)$$

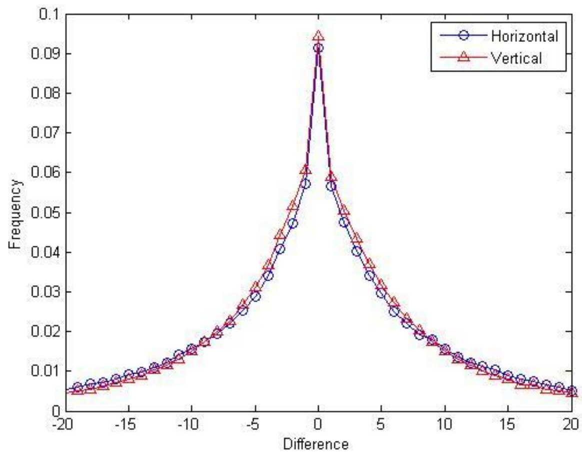
where T is a predefined threshold. A larger D indicates that H_h and H_v have larger differences and thus, the image is likely to have messages embedded. We compare the different methods at high payload because the abnormality of histograms often occurs when the payload is high. In the experiment, randomly selected 25 images were used. All the test images were fully embedded and T = 20 was used in the experiments. These images were given as input to all the different techniques discussed above at high payload conditions. The stego-images produced by the methods were used for evaluation using HVDH method. The stego-images were given as input to the HVDH method which returns the distance D showing the presence of data in the image. Among the results obtained for a method, the results were averaged and the averaged the horizontal and vertical difference histograms of the stego images are shown below.



(a)

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013



(b)

Fig 3. Comparison of the averaged vertical and horizontal difference. (a) HVDH of APPM (D = 0.0169) (b) HVDH of APPM-SP-L (D = 0.012)

Among the different methods the adaptive pixel pair matching driven by spatial frequency masking and luminance masking shows the lowest distance value and hence we can infer it is more secure than adaptive pixel pair matching method.

V. CONCLUSION

This paper has focused on making the process of image steganography more adaptive and intelligent. This is achieved by studying the image characteristics before embedding the data using masking techniques and then using a data embedding technique which is known to offer very good results. The conclusions were formed after a thorough analysis of various masking techniques and their combinational effect on working with pixel pair matching techniques. The analytic study performed in this paper evaluated two methods as mentioned in the above section. The experimental results reveals that a stego image of high quality and steganalytic immunity can be produced when spatial frequency masking is combined with luminance masking to find the candidate region and performing adaptive pixel pair matching in those regions. This new method is a definite improvement over the already existing adaptive pixel pair matching technique. The method shows the lowest MSE when compared with the other technique studied above. It also offers fairly good immunity to steganalysis perfomed by HVDH method. So the adaptive feature improves image steganographic quality and security.

REFERENCES

[1] T. Filler, J. Judas, and J. Fridrich, "*Minimizing embedding impact in steganography using trellis-coded quantization*," in Proc. SPIE, Media Forensics and Security, 2010, vol. 7541, DOI: 10.1117/12.838002.
[2] S. Lyu and H. Farid, "*Steganalysis using higher-order image statistics*,"IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 111–119, Mar.2006.
[3] E Lin and E Delp, "*A Review of Data Hiding in Digital Images*" CERIAS Tech Report 2001-139
[4] J. Mielikainen, "*LSB matching revisited*," IEEE Signal Process. Lett., vol. 13, no. 5, pp. 285–287, May 2006.
[5]] C. K. Chan and L. M. Cheng, "*Hiding data in images by simple LSB substitution*," Pattern Recognition., vol. 37, no. 3, pp. 469–474, 2004.
[6] X. Zhang and S. Wang, "*Efficient steganographic embedding by exploiting modification direction*," IEEE Commun. Lett., vol. 10, no. 11, pp. 781–783, Nov. 2006
[7] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "*A novel image data hiding scheme with diamond encoding*," EURASIP J. Inf. Security, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.
[8] J. Wang, Y. Sun, H. Xu, K. Chen, H. J. Kim, and S. H. Joo, "*An improved section-wise exploiting modification direction method*," Signal Process., vol. 90, no. 11, pp. 2954–2964, 2010.
[9] Da-Chun Wu, Wen-Hsiang Tsai, "*A steganographic method for images by pixel-value differencing*", ELSEVIER Pattern Recognition Letters 24 (2003) 1613–1626
[10] Weiqi Luo, Fangjun Huang, "*Edge Adaptive Image Steganography Based on LSB Matching Revisited*" , IEEE ransactions on infoemation forensics and security, Vol. 5, No. 2, June 2010
[11] W. Hong and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism," J. Vis. Commun. Image Represent., vol. 22, no. 2, pp. 131–140, 2011.
[12] Wien Hong ,Tung-Shou Chen, "*A Novel Data Embedding Method Using Adaptive Pixel Pair Matching*", IEEE transactions on information forensics and security, Vol. 7, No. 1, February 2012.
[13] K. Hempstalk, "*Hiding behind corners: Using edges in images for better steganography*," in Proc. Computing Women's Congress, Hamilton, New Zealand, 2006.
[14] M. Naseem, Ibrahim M. Hussain, M. Kamran Khan, Aisha Ajmal, "*An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding*", International Journal of Computer Applications, Vol. 29, No. 12, 2011. Foundation of Computer Science, New York, USA, pp. 36-43.
[15] M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati, "*Embedding stego-text in cover images using linked list concepts and LSB technique*", Journal of American Science, Vol. 7, No. 6, 2011, pp. 97-100.
[16] H. Zhao, H. Wang, and M. K. Khan," *Statistical analysis of several reversible data hiding algorithms*", in Proc. Multimedia Tools and Applications, 2009.
[17] M. Barni, F. Bartolini, V. Cappelini, A. Lipi, and A. Piva, "*Improved wavelet-based watermarking through pixel-wise masking*", IEEE Trans. Image Process., vol.10, no. 5, pp. 783791, May 2001.