Data Hiding on Digital Images by Diamond Encoding driven through JPW Masking

Akhil P V[1] Dr. Shelbi Joseph[2] Seetha Parameswaran[3]
[1,2,3]Assistant Professor
[1,2,3]Division of IT, SOE, CUSAT

Abstract— This paper proposes a new improved steganographic technique based on pixel value adjustment which is driven by Just Perceptual Weighting (JPW) masking[14]. The cover image is scanned using a spatial frequency and luminance mask (called as JPW masking) and the result is used as the candidate region to perform data hiding using diamond encoding method[15]. The process of embedding partitions the candidate region into non-overlapping blocks of two consecutive pixels and transforms the secret messages to a series of k-ary digits. For each block, the diamond encoding technique is applied to calculate the diamond characteristic value, and one secret k-ary digit is concealed into the diamond characteristic value. The diamond characteristic value is modified to secret digit and it can be obtained by adjusting pixel values in a block. This scheme is designed in such a way that the distortion of each block after diamond encoding is never out of the embedding parameter k, and the block capacity is equal to $\log_2(2k^2 + 2k + 1)$. In contrast to the existing methods based on LSB, the masking driven approach has lower distortion for various payloads. It is expected that the proposed method provides better performance than the existing techniques and also to be more secure to steganalysis techniques.

Key words: Image steganography, Diamond encoding, Pixel Value Adjustment, 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. 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]. The embedding capacity and invisibility are the major concerns in a data hiding scheme analysis. The capacity of a data hiding scheme refers to the quantity of the secret data that can be embedded into the cover image, and the term invisibility indicates how imperceptible the fact is to illegal users when the cover image has been manipulated and turned to be a stego-image. There are a number of techniques available which can perform image steganography in a digital image and this paper focuses on analyzing 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]

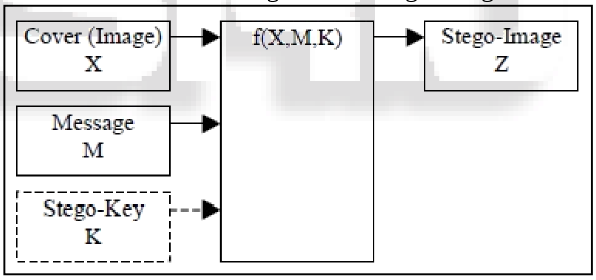

Fig. 1: Steganographic Encoding

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 [20] 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 studies the various methods developed for image steganography, a proposed system is presented in section 3 and section 4 includes 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.

Optimized Bit Plane splicing algorithm [7] 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.

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.

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 neighborhood 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 neighborhood 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. 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 neighbors. 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.

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 Diamond Encoding method which partitions the candidate region into non-overlapping blocks of two consecutive pixels and transforms the secret messages to a series of k-ary digits. For each block, the diamond encoding technique is applied to calculate the diamond characteristic value, and one secret k-ary digit is concealed into the diamond characteristic value. The diamond characteristic value is modified to secret digit and it can be obtained by adjusting pixel values in a block. This scheme is designed in such a way that the distortion of each block after diamond encoding is never out of the embedding parameter k, and the block capacity is equal to $\log_2(2k^2 + 2k + 1)$.

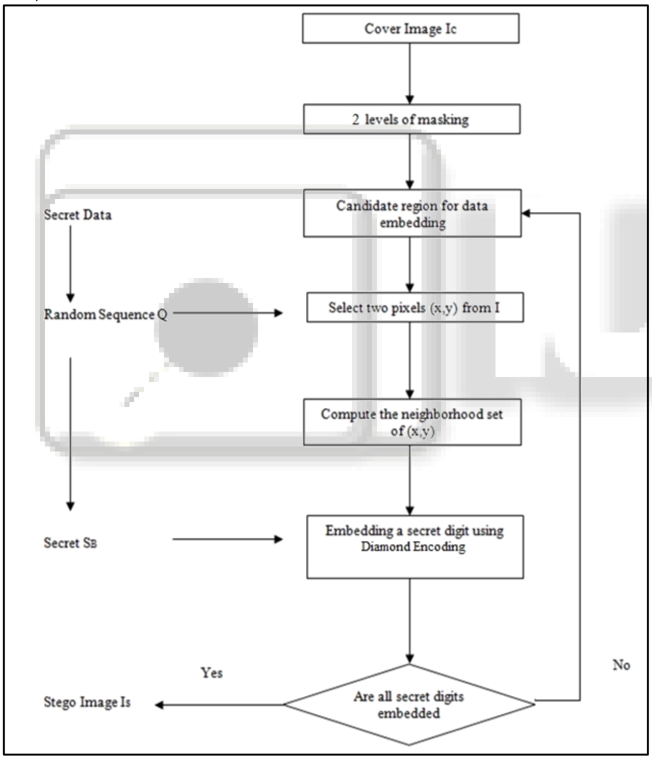

Fig. 2: Proposed System

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 here, 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).

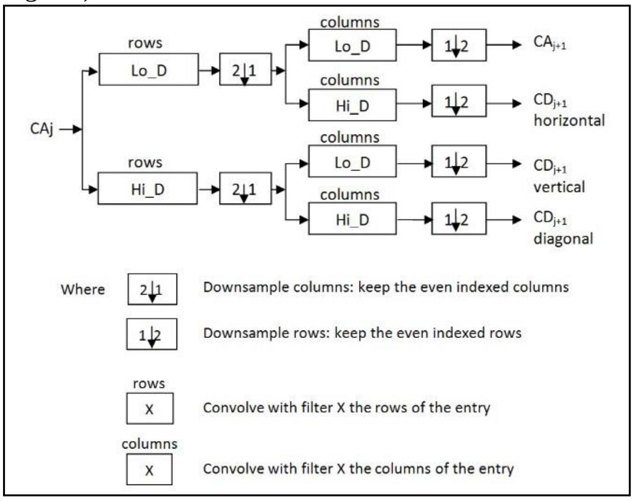

Fig. 3: Two Dimensional DWT

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 decoposition 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 :

$$\mathrm{F}(\lambda, \theta, i, j) = \left(\frac{v_{\lambda_{\max}, LL, i', j'}}{v_{\text{mean}}} \right)^{a_T} \quad (1)$$

where λmax is the highest level of the DWT decomposition and is set to 5 in this work, $vmean$ 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' and j', 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 be 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 for embedding data.

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 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 cobined using OR-operation to get our candidate region for data embedding.

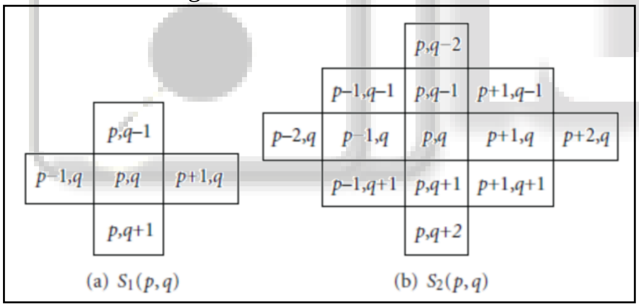

Fig. 2: (a) Diamond encoding patterns with k = 1 and (b) diamond encoding patterns with k = 2.

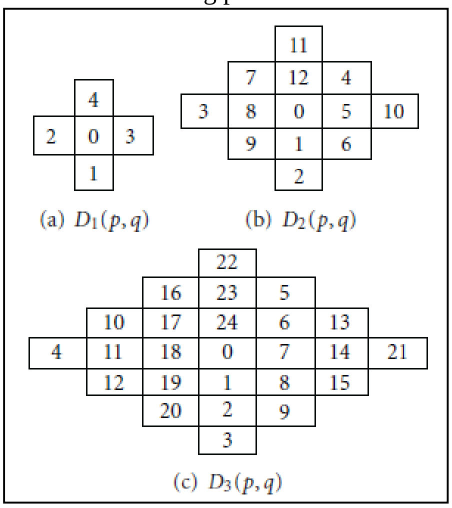

Fig. 3: Diamond encoding patterns D_k with k = 1, k = 2, and k = 3.

B. Data Embedding in Candidate region using Diamond Encoding (DM)

In this section, we shall introduce the general operation of the diamond encoding technique. The EMD scheme embeds (2n + 1)-ary digit into n cover pixels, but the diamond encoding scheme can conceal $(2k^2 + 2k + 1)$-ary digit into a cover pixel pair where k is the embedding parameter. The detail of this scheme is described as follows.

Assume that a, b, p, and q are pixel values, and k is a positive integer. The neighborhood set $S_k(p, q)$ represents the set that contains all the vectors (a, b) with the distance to vector (p, q) smaller than k, and $S_k(p, q)$ is defined as the following form:

$$S_k(p,q) = \{(a,b) \mid |p-a| + |q-b| \le k\}. \qquad (2)$$

Let the absolute value $|S_k|$ denote the number of elements of the set S_k, and each member in Sk is called neighboring vector of (p, q). We calculate the value of $|S_k|$ to obtain the embedding base and embedded base with a parameter k. The examples of S_k are illustrated in Figure 2, and we can obtain $|S_1| = 5$, $|S_2| = 13$, $|S_3| = 25$, and so on. Moreover, we compute the $|S_k|$ value by the following equation, and the embedding base equals to the value of $|S_k|$,

$$\begin{aligned} |S_k| &= \left(\sum_{i=0}^{k}(2i+1)\right) + \left(\sum_{i=1}^{k}(2i-1)\right) \\ &= 1 + \left(\sum_{i=1}^{k}(2i+1)\right) + \left(\sum_{i=1}^{k}2i-1\right) \\ &= 1 + \left(\sum_{i=1}^{k}(2i+1)+(2i-1)\right) \\ &= 1 + \left(\sum_{i=1}^{k}4i\right) \\ &= 1 + \frac{k(k+1)}{2} \times 4 \\ &= 1 + 2k(k+1) \\ &= 2k^2 + 2k + 1. \end{aligned} \qquad (3)$$

The proposed diamond encoding method uses a diamond function f to compute the diamond characteristic value (DCV) in embedding and extraction procedures. The DCV of two pixel values p and q can be defined as follows:

$$f(p,q) = ((2k+1) \times p + q) \bmod l, \qquad (4)$$

where l is the absolute value of S_k. The DCV have two important properties: (1) the DCV of the vector (p, q) is the member of S_k belongs to $\{0, 1, 2, \ldots, l-1\}$ and (2) any two DCVs of vectors in $S_k(p, q)$ are distinct. Assume that E_k represents the embedded digit and E_k belongs to $\{0, 1, 2, \ldots, l-1\}$. For secret data embedding, we replace the DCV of the vector (p, q) with the embedded secret digit. Therefore, the modulus distance between f (p, q) and S_k is $d_k = f(p, q)-E_k \bmod l$. For each k, we can design a distance pattern D_k to search which neighboring pixel owns the modulus distance d_k, and different D_k are shown in Figure 3. Then, the vector (p, q) is replaced with the neighboring vector (p', q') by d_k. The vector (p', q') is the member of $S_k(p, q)$ and the DCV of (p', q') equals to the embedded secret digit E_k. The vector (p', q') can extract the correct secret digit by (5):

$$f(p', q') = ((2k+1) \times (p' + q')) \bmod l. \qquad (5)$$

C. *Embedding Procedure*

In our method, the embedding parameter k is determined firstly, and the diamond encoding with parameter k can conceal secret data into the cover image.

Step 1. To begin with, according to the secret data size, a parameter k is selected, and we transform secret data into diamond encoding digits. Assume that the secret data size is s, and then the embedding parameter k is determined by finding the minimal positive integer that satisfies the following inequality:

$$\left\lfloor \left(\frac{m \times n}{2}\right) \log_2(2k^2 + 2k + 1) \right\rfloor \geq s. \qquad (6)$$

Set the embedding base l = $2k^2$ + 2k + 1. Then, the secret message is regarded as a sequence of digits in *l*-ary notational system.

Step 2. In the data embedding procedure, the original image is segmented into a number of non-overlapping two pixel blocks. Then, we can select each block from top-down and left-right in turn for data embedding process. The block vector (x, y) is defined as x = I(2t) and y = I(2t +1) where I is the cover image sized m × n, and t is the block index. The embedded secret data bit stream is transformed into *l*-ary digit sequence. Moreover, the embedded secret digit s_t is obtained from the *t*th index of the sequence of *l*ary digits.

Step 3. Compute the DCV of two pixel values x and y by (4)

$$f(x, y) = ((2k+1) \times x + y) \bmod l. \qquad (7)$$

Step 4. The new stego-image pixel pair can be calculated by replacing f (x, y) with s_t. The used equation is shown as follows:

$$d_t = (s_t - f(x, y)) \bmod l. \qquad (8)$$

The symbol dt shows the modulus distance between the st and f (x, y). By applying the distance d_t, the stego-pixel values x' and y' can be found in D_k such that the DCV is replaced with s_t. However, in this step, the overflow or underflow problems might be occurred; that is, the stegopixel value x' or y' might go beyond 255 or below 0. If it happens, the next step, namely Step 5, has to be processed; otherwise, Step 5 has to be skipped, and the data embedding procedure is finished.

Step 5. When one stego-pixel value has the overflow or underflow problem, the critical vector (x', y') has to be adjusted to the appropriate value. The adjustment rules are defined as follows:

$$\begin{array}{|l|}\hline (1)\ \text{if } x' > 255,\ x' = x' - l; \\ (2)\ \text{if } x' < 0,\ x' = x' + l; \\ (3)\ \text{if } y' > 255,\ x' = x' - l; \\ (4)\ \text{if } y' < 0,\ y' = y' + l. \\ \hline \end{array}$$

From the above rules, it can be observed that the overflow/underflow problem is solved and the DCV also has the same value. After all, we take the next pixel pair from the cover image and repeat Steps 2–5. Repeat until all the secret data have been concealed. Then we collect all stego-pixel values to form the stego-image I'. The embedding parameter k has to transmit to the receiver in order to extract data.

D. *Extraction Procedure*

Here are the steps to extract the secret data from the stego-image I' and the detailed secret data extraction is described as follows.

Step 1. To begin with, in the data extraction procedure, the original image is segmented into a number of nonoverlapping two-pixel blocks. Then, we can select each block from top-down and left-right in turn for data extraction process.

The block vector (x', y') is defined as x' = I'(2t) and y' = I'(2t + 1). The block construction of the proposed scheme is illustrated by Figure 2.

Step 2. According to the parameter k, set the embedding base l = 2k2 +2k +1. For each stego-pixel pair p' and q', the DCV of (x', y') is obtained from (5):

$$f(x', y') = ((2k+1) \times x' + y') \bmod l. \qquad (9)$$

Therefore, the secret digit st is obtained by the DCV of (x', y').

Step 3. Take the next pixel pair from the stego-image and repeat Steps 1 and 2. The same thing goes on and on until all secret digits have been extracted for each block with index t.

Step 4. Finally, the secret data can be obtained by transforming the secret symbols to binary bits with base 2.

Here is an example to describe how the proposed algorithm actually works. Assume that the embedding parameter k = 2 and l = 13. Suppose we have pixel pairs x = 20 and y = 31 and we use (4) to calculate DCV by computing f (20, 31) = (20 × 5 + 31)mod13 = 1. Now let us take s_t = 11(13) as the embedded secret digit, and we can obtain the modulus distance d_t = 11−1mod 13 = 10 by computing (8). Then, we search D_2(20, 31) which is shown in Figure 2 and obtain the neighboring vector (22, 31) locating in set S2(20, 31) and dk = 10. Therefore, the values of pixel pair (20, 31) are replaced with (22, 31). In the secret data extraction phase, the stego-pixel pairs x' = 22 and y' = 31 can be used to compute the DCV by f (22, 31) = 22 × 5 + 28mod13 = 11. Finally, the secret digit s_t is obtained.

IV. Conclusion

This paper has focused on making the process of image steganography more adaptive and intelligent. This is achieved by studying the image characteristics first before embedding the data using masking techniques and then embedding data using diamond encoding technique which is known to offer very good results. The diamond encoding method has been used to alleviate distortions after hiding a secret digit into two cover pixels. It not only keeps high stego-image quality but also conceals large amount of data into cover images for secret communication. The performance of the proposed scheme proves to be better than the simple LSB method and other existing schemes in terms of payload and stego-image quality

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] 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.
[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] Lihong Cui, Wenguo Li "Adaptive Multiwavelet-Based Watermarking Through JPW Masking" in IEEE Transactions on Image Processing, Volume: 20 Issue: 4 2010.
[15] Ruey-Ming Chao, Hsien-Chu Wu, "A Novel Image Data Hiding Scheme with Diamond Encoding" in EURASIP Journal on Information Security, 2009.