IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 2 (May. - Jun. 2013), PP 36-40
www.iosrjournals.org

Efficient Technique for Image Stenography Based on coordinates of pixels

S.Thenmozhli[1], Dr.M.Chandra sekaran[2]
[1]*(Research Scholar, Anna / Anna University, Chennai)*
[2]*(HOD ECE , GCE / Anna University Name,Salem)*

Abstract : *A novel data hiding scheme in digital images with the diamond encoding by pixel value adjustment is proposed. The proposed method is the extension of the diamond encoding embedding scheme. First, choosing the cropped region from given cover image select 4 pixel pairs from cropped region, 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. Here embedding parameter k, and the block capacity is equal to log2(2k2 + 2k + 1). The diamond encoding provides an easy way to produce a more perceptible result than those yielded by simple least-significant-bit substitution methods. The embedded secret data can be extracted without disturbing the original cover image. Experimental results have demonstrated that the proposed method is capable of hiding more secret data while keeping the stego-image quality degradation imperceptible.*

Keywords *– stegnography,pixel pair matching,lsb*

I. INTRODUCTION

STEGANOGRAPHY is the art of hiding secret information in the form of cover which can be image complex audio, video or any sophisticated biometrics formats Clearly, the goal of cryptography is to protect the content of messages , steganography is to hide the existence of messages. An advantage of steganography is that it can be employed to secretly transmit messages without the fact of the transmission being discovered. Generically, the steganography process is classified into two phases in majority of the prior research work e.g. message embedding and extraction. In the embedding operation, a secret message is transformed into a bit stream of bits; this is embedded into the least significant bits (LSBs) of the image pixels. The embedding overwrites the pixel LSB with the message bit if the pixel LSB and message bit do not match. Otherwise, no changes are necessary. For the extraction operation, message bits are retrieved from pixel LSBs and combined to form the secret message.

There are two main selection algorithms that can be employed to embed secret message bits: sequential and random. For sequential selection, the locations of pixels used for embedding are selected sequentially one after another. For instance, pixels are selected from left to right and top to bottom until all message bits are embedded. With random selection, the locations of the pixels used for embedding are permuted and distributed over the whole image. The distribution of the message bits is controlled by a pseudorandom number generator whose seed is a secret shared by the sender and the receiver. This seed is also called the stego-key. The latter selection method provides better security than the former because random selection scatters the image distortion over the whole image, which makes it less perceptible.

II. PROPOSED METHOD

2.1 k ary notational matrix :

The proposed method is the extension of the exploiting embedding scheme is the main idea of embedding scheme is that each $(2n + 1)$- k ary notational secret digit is carried by n cover pixels, and only one pixel value increases or decreases by 1 at most. For each block of n cover pixels, there are $2n$ possible states of only one pixel value plus 1 or minus 1.

The $2n$ states of alteration plus the case in which no pixel is modified form $(2n + 1)$ different cases. Therefore, the $(2n + 1)$- k ary notational secret digit is embedded into the cover pixels by changing the state. Before the data embedding procedure, the preprocess can convert the secret data into sequences of digits with $(2n + 1)$-k ary notational representation.

For the simplest case of $n = 2$, the secret data stream $S_{(2)}$ can be expressed as $S_{(5)}$ where $S_{(d)}$ denotes the d-ary notational system representation of secret data stream S. Thus, the 5-ary digits can conceal into blocks of two cover pixels by modifying at most one pixel value. Denote the gray values of a block of two cover pixels as p_1 and p_2, and the extraction function f is deepened as a weighted sum modulo 5:

Suppose that the transformed 5-ary secret digit s desired to be embedded into the cover pixels p_1 and p_2. According to the secret digit, the embedding process can be classified into 5 conditions.

Condition 1. If $(s - f(p_1, p_2)) \bmod 5 = 0$:

No modification is needed because the extraction function f can decrypt the correct secret data.

Condition 2. If $(s - f(p_1, p_2)) \bmod 5 = 1$: Increase the pixel value p_1 by 1.

Condition 3. If $(s - f(p_1, p_2)) \bmod 5 = 2$: Increase the pixel value p_2 by 1.

	$p,q-1$	
$p-1,q$	p,q	$p+1,q$
	$p,q+1$	

(a) $S_1(p,q)$

		$p,q-2$		
	$p-1,q-1$	$p,q-1$	$p+1,q-1$	
$p-2,q$	$p-1,q$	p,q	$p+1,q$	$p+2,q$
	$p-1,q+1$	$p,q+1$	$p+1,q+1$	
		$p,q+2$		

(b) $S_2(p,q)$

Diamond encoding patterns with $k = 1$ and (b) diamond encoding patterns with $k = 2$.

Condition 4. If $(s - f(p_1, p_2)) \bmod 5 = 3$ Decrease the pixel value p_2 by 1.

Condition 5. If $(s - f(p_1, p_2)) \bmod 5 = 4$: Decrease the pixel value p_1 by 1.

Compute the two pixel values x and y by

f(x,y) = ((2k + 1) * x + y) mod l ---------- 1

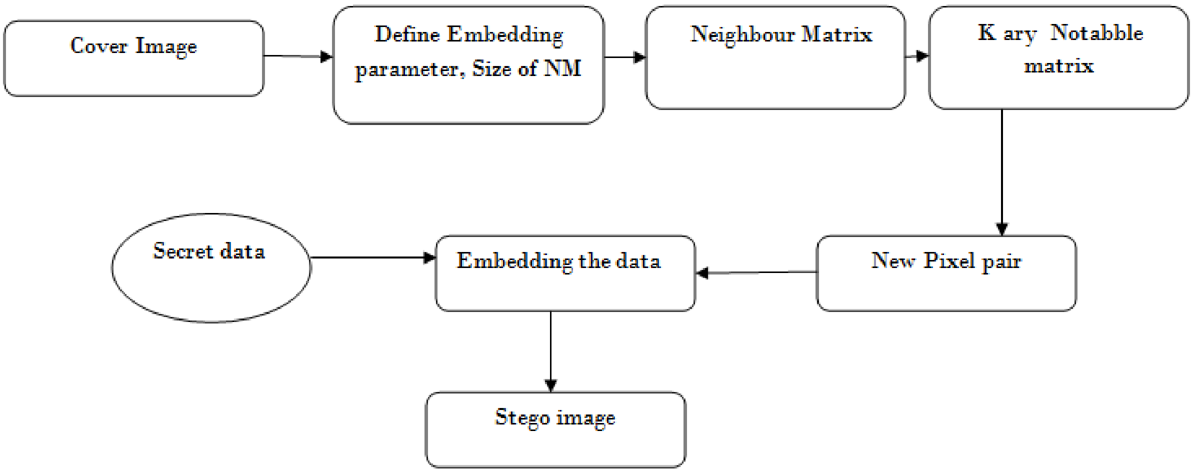
The new stego-image pixel pair can be calculated by replacing $f(x, y)$ with s_t. The used equation is shown as follows:

dt = st − f (x,y) mod l. ----------- 2

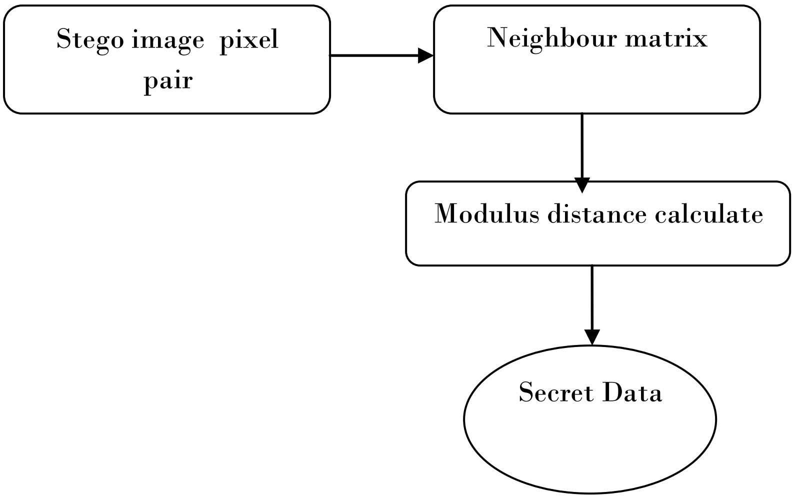
st - embedded secretdigit s_t is obtained from the t th index of the sequence of $l$ary mdigits.

2.2 Block Diagram :

2.2.1 Embedding Call back



2.2.2 Extracting Callback



III. INDENTATIONS AND EQUATIONS

In this section, we shall introduce the general operation of the diamond encoding technique. The proposed 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:

$S_k (p,q) = \{ (a,b) (p - q) + (q - b) <= k \};$ -------- 3

$s_k =$number of elements of the set S_k, and each member in S_k is called neighboring vector of (p, q). the following equations are used to be found s_k

$Sk = \sum_{i=0}^{k}(2i+1) + \sum_{i=0}^{k}(2i-1)$ ----------- 4

$= \sum_{i=0}^{k}(4i)$

$= 1 + ((k(k+1))) / 2 * 4 ;$

$= 1 + 2k(k+1);$

$= 2k^2 + 2k + 1;$

For extraction we are using the following formula:

$F (p',q') =\_(2k + 1) \times p' + q' \bmod l$ ------- 5

Here (p’ , q’) = coordinates of extracted pixel pairs

$l = 2k_2 + 2k + 1.$ ------------- 6

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 $f(20, 31) = (20 \times 5 + 31)\text{mod}13 = 1$. Now let us take $st = 11(13)$ as the embedded secret digit, and we can obtain the modulus distance $dt = 11-1\text{mod } 13 = 10$ by computing Then, we search $D2(20, 31)$ 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 $f(22, 31) = 22 \times 5 + 28\text{mod}13 = 11$. Finally, the secret digit st is obtained.

IV. FIGURES AND TABLES

4 .1 Resulting Images

In this paper five cover images Lena, Zelda, of 128×128 pixels as shown in the figure 4. 1a, 1b, 2 a,2b are considered. Then to evaluate the performance of the proposed method, several experiments have been carried by considering for secret text . The results of above algorithm have been shown below

Fig (1 a) input image

Fig (2 a) input image

Fig (1 b) stego image

Fig (2 b) stego image

In our experiments, the quality of the stego-image is measured by the peak signal-to-noise ratio (PSNR). The PSNR is the most popular metris to measure the distortion between the cover image and stego-image. It is defined as follows:

PSNR = 10 log 10 (255 *255 / MSE)
MSE = (1/ M X N) (I/p img – O/p img)^2

4.4 Table Comparison :

Smaller *k* means low capacity and less distortion whereas larger *k* means high capacity and increased distortion. As expected, Table 1 shows that the growth of payload did depend on the value *k*. The third column of Table 1 indicates that the numbers of pixels payload is nothing but no of bits to be embedded in an cover image Results of the proposed scheme with different parameter k

Table 1

K value	Sk	Payload	Psnr
1	1.16	52	
2	13	1.85	49
3	25	2.32	47
4	41	2.68	42

V. CONCLUSION

In this paper, we have presented a novel data hiding scheme based on the pixel pair matching technique. 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 considering large amount of data into cover images for secret communication. The performance of the proposed method proves to be better than the simple and modify LSB method and other existing schemes in terms of payload and stego-image quality.

Acknowledgements

This research project would not have been possible without the support of many people. The author wishes to express her gratitude to her supervisor, Prof. Dr . Chandra sekaran HOD / ECE Government Collgege of engg Salem who was abundantly helpful and offered invaluable assistance, support and guidance

REFERENCES

[1] S.-H. Wang and Y.-P. Lin, "Wavelet tree quantization for copyright protection watermarking," IEEE Transactions on Image Processing, vol. 13, no. 2, pp. 154–165, 2004.

[2] D.-C. Lou and J.-L. Liu, "Steganographic method for secure communications," Computers and Security, vol. 21, no. 5, pp. 449–460, 2002.

[3] P. L. Lin, C.-K. Hsieh, and P.-W. Huang, "A hierarchical digital watermarking method for image tamper detection and recovery," Pattern Recognition, vol. 38, no. 12, pp. 2519–2529, 2005.

[4] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownershipverification," IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1593–1601, 2001.

[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] Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," IEEE Transactions onCommunications, vol. 50, no. 8, pp. 1227–1231, 2002.

[7] A.Westfeld, "F5—a steganographic algorithm," in Proceedings of the 4th International Workshop on Information Hiding(IH '01), vol. 2137 of Lecture Notes in Computer Science, pp. 289–302, Pittsburgh, Pa, USA, April 2001.