A New Method Avoids the Falling-Off Boundaries by Using Try-Way Pixel Value Difference and Modulus Function in Image Steganography

Dr.K.B.Jayarraman[#1],G.Dhakshana Moorthi[#2], A.Revathy[#3]
[1] Professor,Head of Department of Computer Science and Engineering, Manakula Vinayagar Institute Of Technology,
Pondicherry University, Pondicherry.
[2]Department of Computer Science and Engineering, Manakula Vinayagar Institute Of Technology,
Pondicherry University, Pondicherry.
[3]Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering college,
Pondicherry University, Pondicherry.
[1]annaijayaraman@yahoo.com ,[2]dhakshanamoorthi@outlook.com, [3]revy2890@gmail.com,

ABSTRACT - In the present scenario, to protect secret message from being stolen during transmission, there are two ways to solve this problem in general. One way is encryption, which refers to the process of encoding secret information in such a way that only the right person with a right key can decode and recover the original information successfully. Another way is Steganographic and this is a technique which hides secret information into a cover media or carrier so that it becomes unnoticed and less attractive. To enlarge the capacity of the hidden secret information and to provide an imperceptible stego-image for human vision, a novel Steganographic approach using tri-way pixel-value differencing (TPVD) is proposed in this work. In addition, to reduce the quality distortion of stego-image brought from setting larger embedding capacity, an optimal approach of selecting the reference point and adaptive rules are presented. Experimental shows the Theoretical estimation and experimental results demonstrate that the proposed scheme can provide superior embedding capacity and give secrecy protection from dual statistical stego-analysis.

Keywords*:* Steganographic, Data hiding and modulus function, Pixel–value differencing, Try-way pixel value difference.

1. INTRODUCTION

Steganography is a way of secret communication carried out by using some digital multimedia to convey the critical messages, and therefore the major demand here is for both a high embedding capacity and good imperceptibility [1].The word Steganographic means “covered writing” and comes from the Greek words steganos, which means covered or secret and graphy, which means writing or drawing. Steganographic is the “cousin” of cryptography and is the art of covert communications. Today, Steganographic is usually referred to as hiding data in digital media (Cole). For example, a text document can be hidden in an image, sound or another text file. This paper concentrates specifically on data hiding in images. First, it presents some terminology and background information about images and some of their formats. Next, different methods for Steganographic will be discussed which are publicly available and widely used today.

For the past decade, many Steganographic techniques for still images have been presented. A simple and well-known approach is directly hiding secret data into the least-significant bit (LSB) of each pixel in an image. Then based on the LSB technique, a genetic algorithm of optimal LSB substitution is now also available to improve the stego-image quality of the simple LSB method [2]. However, since some pixels cannot tolerate changes of substitution during the embedding process, then those pixels appear apparently different from their original values. This effect occurs seriously in the smooth area that those changes are noticeable for human eyes. Thus, improving the stego-image quality and adaptive adjusting hiding capacity are two major aims to expand related researches about LSB. Therefore, Wu and Tsai [3] proposed a pixel value difference (PVD) provides both high embedding capacity and outstanding imperceptibility for the stego-image. Ko-Chin Chang [4] proposed a try-way pixel value difference provides better high embedding capacity and outstanding imperceptibility for the stego-image compare to PVD. In this paper organized as fallows. Section review of try-way pixel value difference. In Section III, the proposed construction scheme is presented. Experimental results are illustrated and discussed in Section IV, prior to Conclusions in Section V.

2. REVIEW OF TRY-WAY PIXEL VALUE DIFFERENCE (TPVD)

In the TPVD method, two horizontal and consecutive pixels can only represent a vertical edge, but the edge can have different directions. This motivates us to improve the TPVD method by considering three directions. In general, the edges in an image are roughly classified into vertical, horizontal, and two kinds of diagonal directions. Motivated from the TPVD method, using two-pixel pairs on one directional edge can work efficiently for information hiding. This should accomplish more efficiency while considering four directions from four two-pixel pairs. This can be implemented by dividing the image into 2 × 2 blocks with 4 pixels and one example block is shown in Fig. 1.

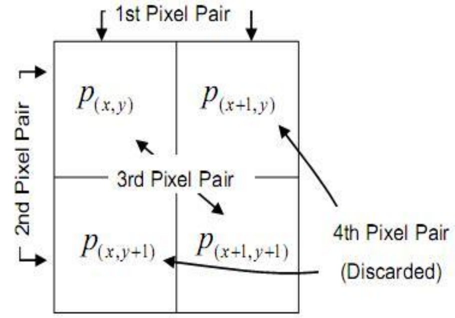

Fig.1.Four pixel pairs of TPVD

However, since the changing of pixel values for the fourth pixel pair affects the first and the second pairs, the fourth pair is useless and has to be discarded. Therefore, we propose that three pairs are used to embed the secret data. As show in fig 1.Each block contain4 pixels. They are P(x,y),P(x,y+1),P(x+1,y),P(x+1,y+1),Where x,y are the pixel location in given image. ($P_{(x+1,y+1)}$ and $P_{(x+1,y)}$) is the useless pair and discarded in our experiment. We propose that three pairs are used to embed the secret data, those pairs are P_1=($P_{(x,y)}$,$P_{(x,y+1)}$),P_2=($P_{(x,y)}$, $P_{(x+1,y+1)}$) and P_3=($P_{(x,y+1),}$ $P_{(x+1,y+1)}$) respectively. For the original TPVD method [2], the secret data is assumed to be a long-bit stream and the cover image is a gray-level image.

The embedding algorithm is described as follows:

1. Calculate the difference value d_i between two consecutive pixels p_i and p_{i+1} for each block in the cover image. The value is given by d_i=p_{i+1}-p_i .
2. Using $|d_i|$ to locate a suitable R_k in the designed range table that is to compute j=min(u_k-$|d_i|$).Then R_j is the located range.
3. Compute the amount of secret data bits t that can be embedded in each pair of two consecutive pixels by R_j. The value t can be estimated from the width W_j of R_j, this can be defined by t=floor ($\log_2^{Wj}$).
4. Read t bits from the binary secret data and transform the bit sequence into a decimal value b . For instance, if bit sequence =110, then the converted value b=6 .
5. Calculate the new difference value $d_i^{'}$ given by $d_i^{'}$=l_j+b , if d_i>=0 or $d_i^{'}$=-(l_j+b),if d_i<0 to replace original difference.
6. To apply the modulus function to the new difference values. Modulus function procedure explained in III.a. Repeat Step 1-6 until all secret data are embedded into the cover image, then the stego-image is obtained.

3. THE PROPOSED METHOD

Instead of the difference value, the proposed scheme modifies the remainder of two consecutive pixels $P_{(i,x)}$ and $P_{(i,y)}$ for better stego-image quality. The proposed modulus function is presented in the subsection below.

a. Modulus Function:

Given a sub-block F_i composed of two continuous pixels $P_{(i,x)}$ and $P_{(i,y)}$ from the cover image, obtain the new difference value as explained in II. Then Compute the remainder values $P_{rem(i,x)}$, Prem(i,y) and Frem(i) of P(i,x), P(i,y) and sub-block Fi
respectively by using the following equations:

Prem(i,x)= P(i,x)mod t'
Prem(i,y)= P(i,y)mod t'
Frem(i)=(P(i,x)+ P(i,y)) mod t'

Where t' is the decimal value of t. Embed t_i bits of secret data into F_i by altering $P_{(i,x)}$and $P_{(i,y)}$ such that $F_{rem(i)}$ =t'. The optimal approach to altering the $P_{(i,x)}$ and $P_{(i,y)}$ to achieve the minimum distortion is as follows:

Case 1: $F_{rem(i)} > t_i'$ and $m \leqslant (2^{t_i})/2$ and $P_{(i,x)} \geqslant P_{(i,y)}$
$$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} - \lceil m/2 \rceil, P_{(i,y)} - \lfloor m/2 \rfloor);$$
Case 2: $F_{rem(i)} > t_i'$ and $m \leqslant (2^{t_i})/2$ and $P_{(i,x)} < P_{(i,y)}$
$$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} - \lfloor m/2 \rfloor, P_{(i,y)} - \lceil m/2 \rceil);$$
Case 3: $F_{rem(i)} > t_i'$ and $m > (2^{t_i})/2$ and $P_{(i,x)} \geqslant P_{(i,y)}$
$$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} + \lfloor m_1/2 \rfloor, P_{(i,y)} + \lceil m_1/2 \rceil);$$
Case 4: $F_{rem(i)} > t_i'$ and $m > (2^{t_i})/2$ and $P_{(i,x)} < P_{(i,y)}$
$$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} + \lceil m_1/2 \rceil, P_{(i,y)} + \lfloor m_1/2 \rfloor);$$
Case 5: $F_{rem(i)} \leqslant t_i'$ and $m \leqslant (2^{t_i})/2$ and $P_{(i,x)} \geqslant P_{(i,y)}$
$$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} + \lfloor m/2 \rfloor, P_{(i,y)} + \lceil m/2 \rceil);$$

Case 6: $F_{rem(i)} \leqslant t'_i$ and $m \leqslant (2^{t_i})/2$ and $P_{(i,x)} < P_{(i,y)}$
$$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} + \lceil m/2 \rceil, P_{(i,y)} + \lfloor m/2 \rfloor);$$
Case 7: $F_{rem(i)} \leqslant t'_i$ and $m > (2^{t_i})/2$ and $P_{(i,x)} \geqslant P_{(i,y)}$
$$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} - \lceil m_1/2 \rceil, P_{(i,y)} - \lfloor m_1/2 \rfloor);$$
Case 8: $F_{rem(i)} \leqslant t'_i$ and $m > (2^{t_i})/2$ and $P_{(i,x)} < P_{(i,y)}$
$$(P'_{(i,x)}, P'_{(i,y)}) = (P_{(i,x)} - \lfloor m_1/2 \rfloor, P_{(i,y)} - \lceil m_1/2 \rceil).$$

Where m=| $F_{rem(i)}$ -t'|,m_1=2t_i-| $F_{rem(i)}$ -t'| and $P'_{(i,x)}$, $P'_{(i,y)}$ are new pixel values after the embedding of t_i bits of the secret data into sub-block F_i. After Step 8, if $P'_{(i,x)}$ and $P'_{(i,y)}$ overflows the boundary value 0 or 255, then execute below for revising $P'_{(i,x)}$ and $P'_{(i,y)}$. If not, the purpose of concealing secret data will be completed after the replacement of ($P_{(i,x)}$,$P_{(i,y)}$)by ($P'_{(i,x)}$ $P'_{(i,y)}$) in the cover image.

Consider the three situations below where the falling-off-boundary problem happens and revise $P'_{(i,x)}$ and $P'_{(i,y)}$ as follows:

Case 1: If $P_{(i,x)} \approx 0$, $P_{(i,y)} \approx 0$ and $P'_{(i,x)} < 0$ or $P'_{(i,y)} < 0$, then re-adjust $P'_{(i,x)}$ and $P'_{(i,y)}$ to be $P''_{(i,x)}$ and $P'_{(i,y)}$ by
$$(P''_{(i,x)}, P''_{(i,y)}) = (P'_{(i,x)} + (2^{t_i})/2, P'_{(i,y)} + (2^{t_i})/2).$$

Case 2: If $P_{(i,x)} \approx 255$, $P_{(i,y)} \approx 255$ and $P'_{(i,x)} > 255$ or $P'_{(i,y)} > 255$, then re-adjust $P'_{(i,x)}$ and $P'_{(i,y)}$ to be $P''_{(i,x)}$ and $P''_{(i,y)}$ by
$$(P''_{(i,x)}, P''_{(i,y)}) = (P'_{(i,x)} - (2^{t_i})/2, P'_{(i,y)} - (2^{t_i})/2).$$

Case 3: If $P_{(i,x)}$ and $P_{(i,y)}$ form a great contrast (i.e. $d_i > 128$), then re-adjusted $P'_{(i,x)}$ and $P'_{(i,y)}$ by
$$(P''_{(i,x)}, P''_{(i,y)}) = \begin{cases} (0, P'_{(i,y)} + P'_{(i,x)}), \\ \quad \text{if } P'_{(i,x)} < 0 \text{ and } P'_{(i,y)} \geqslant 0; \\ (P'_{(i,x)} + P'_{(i,y)}, 0), \\ \quad \text{if } P'_{(i,x)} \geqslant 0 \text{ and } P'_{(i,y)} < 0; \\ (255, P'_{(i,y)} + (P'_{(i,x)} - 255)), \\ \quad \text{if } P'_{(i,x)} > 255 \text{ and } P'_{(i,y)} \geqslant 0; \\ (P'_{(i,x)} + (P'_{(i,y)} - 255), 255), \\ \quad \text{if } P'_{(i,x)} \geqslant 0 \text{ and } P'_{(i,y)} > 255. \end{cases}$$

b. The Extraction Algorithm:

To retrieve the embedded secret data from the stego-image, the extraction algorithm is described in the following steps.

i. Partition the stego-image into 2×2 pixel blocks, and the partition order is the same as that in the embedding stage.

ii. Calculate the difference values $d^{\wedge}_{i(x,y)}$separately for each block in the stego-image given by $d^{\wedge}_{i}$=p_{i+1}-p_i.

iii. $d^{\wedge}_{i(x,y)}$ is used to locate the suitable $R_{k,I}$ as introduced in Step 2 of the embedding phase. At the same time, the amount of embedding bits t_i where t=floor ($\log_2{}^{Wj}$) is obtained. If t_i satisfies the branch conditions, two independent pixel pairs are selected; otherwise, three pixel pairs are used for further processing.

iv. After $R_{k,I}$ is located,l_{iis} the $d^{\wedge}_{i(x,y)}$ and $b^{\wedge}_{i}$ is obtained. Finally, is $b^{\wedge}_{I}$ converted from a decimal value into a binary sequence with t_i bits where t=floor ($\log_2{}^{Wj}$).

4. EXPERIMENTAL RESULTS

In our experiments, 12 cover images with 512 × 512 image resolutions were used to evaluate the performance of the proposed scheme. They include Lena, Baboon, camera Man as shown in fig 2. PSNR value is utilized to evaluate the invisibility of the stego-images. Some examples of the cover image and its stego-image are shown in Fig. 2. Table I lists the experimental results after the secret data is embedded using proposed method. The hiding capacity (in bytes) and PSNR values achieved by the proposed scheme three images are shown. We used a series of pseudo random numbers as the secret data to be embedded into the cover images. The peak signal-to-noise ratio (PSNR) was utilized to evaluate the stego-image quality. The PSNR is defined as follows:

$$\text{PSNR} = 10\log_{10}\frac{255^2}{\text{MSE}}\ \text{dB}$$

and

$$\text{MSE} = \left(\frac{1}{M \times N}\right)\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(\alpha_{i,j} - \beta_{i,j})^2.$$

Here, $\alpha_{i,j}$ is the pixel of the cover image where the coordinate is (i, j), and $\beta_{i,j}$ is the pixel of the stego-image where the coordinate is (i, j). M and N represent the size of the image. A larger PSNR value indicates the fact that the discrepancy between the cover image and the stego-image is more invisible to the human eye.

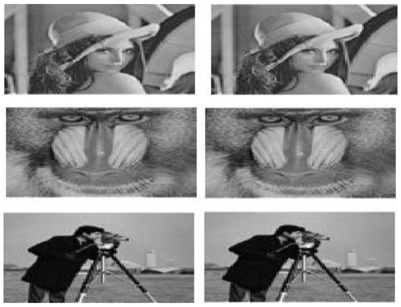

Fig.2. Cover image and stego-image of lena baboon and cameraman respectively.

Image name	BITcapacity	PSNR(dB)
lena	513484	75.43
Baboon	517007	70.6431

cameraman	502097	73.0953

Table I. Lists the experimental results after the secret data is embedded using proposed method

5. ADVANTAGES

Steganography has some pretty standard advantages and disadvantages. The advantages are that the hidden text doesn't stand out. It can be passed in innocuous content like an image. By making some slight changes to color values, for example, you can transmit a few bits here and there that are practically undetectable. The downside usually includes things like size and protection. You usually have to send much more padding around your secret text so that your secret text doesn't stand out.If you're only sending something simple like GPS coordinates or an email address, that's fine. But if you have a long document (e.g., a book) that you want to hide with Steganography, it's pretty hard. And then there's the protection factor: typically secrets that are protected by Steganography are not protected by anything else. If no one sees it, it's safe. If they see it, it’s game over.

6. CONCLUSION

In this paper, we propose a novel scheme to greatly reduce the visibility of the hiding effect presented. The proposed scheme utilizes the remainder of the two consecutive pixels to record the information of the secret data which gains more flexibility, capable of deriving the optimal remainder of the two pixels at the least distortion. The proposed method can also solve the falling-off-boundary problem by re-adjusting the remainder of the two pixels. Experimental results show the proposed scheme has a much better performance.

REFERENCES

[1] Der-Chyuan Lou , Nan-I Wu , Chung-Ming Wang , Zong-Han Lin , Chwei-Shyong Tsai, “A novel adaptive steganography based on local complexity and human vision sensitivity” The Journal of Systems and Software 83 (2010) 1236–1248

[2]Chan, C.-K., Cheng, L.-M., 2004. Hiding data in images by simple LSB substitution. Pattern Recognition 37, 469–474.

[3]D.-C. Wu, and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognition Letters,Vol. 24, pp. 1613–1626, 2003.

[4] Ko-Chin Chang, Chien-Ping Changa, Ping S. Huangb, and TeMing Tua “A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing” 2008 academy publisher.

[5] Wu, H.C., Wu, N.I., Tsai, C.S., Hwang, M.S., 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings – Vision Image and Signal Processing152(october)611-615.