Enhanced Pixel Value Modification based on Modulus Function for RGB Image Steganography

Aurélien Laffont[1], Pascal Maniriho [2], Anaïs Ramsi [1], Guillaume Guerteau [1], Tohari Ahmad [2]
[1]Department of Informatics, Ecole Internationale des Sciences du Traitement de l'Information (EISTI), Cergy 95000, France
[2] Department of Informatics, Institut Teknologi Sepuluh Nopember (ITS), Surabaya 60111, Indonesia

Abstract— **Digital image steganography is one the best security measures to be adopted while exchanging multimedia data via the public network. Data can be exchanged in the form of text, audio, video or image. Therefore, securing communication is ideal since data must be delivered to the intended recipients without any alterations. That is, data have to be received exactly as they were sent. Recently, several methods that deal with increasing the embedding capacity and the quality of the stego image have been already implemented. Additionally, with reference to the literature study, in most of the existing methods developed based on pixel value modification, two pixels are required for concealing one digit of the secret data which is relatively low. Thus, to increase the embedding capacity and security which are desirable for any image steganographic algorithm, another method which conceals data by modifying pixel values is suggested in this paper. Different from the previous method which only hides data based on modulus three function, the suggested method can handle any modulus function, i.e., the limitations encountered in the previous method are completely removed. This allows one digit of the secret data to be concealed in each pixel. Moreover, the effect of varying modulus function is also analyzed. The experiment shows that the suggested enhanced-PVM does achieve good performance. Besides, good embedding capacity and PSNR are achieved while using modulus 2, 3 and 4. On the other hand, for modulus 5, 6 and more, the embedding capacity changes slightly.**

Keywords— Protecting data, information security, information hiding, pixel value modification, modulus function.

I. INTRODUCTION

Recently, the best way to exchange data between individuals or different communication parties is to use the internet. That is, having connected to this public network, it does require a few seconds to talk to anybody from anywhere in world. Nevertheless, this advantage is taken by unauthorized users (also called attackers) who are always intending to intercept data while being transferred to the intended destination. Therein, security is needed to protect data and ensure that they are received intact. Digital image steganography is among the well-known research areas in information security. Steganography is a technique of concealing secret data into a multimedia carrier such as image, video, etc. different from other types of communication, however, in steganography nobody is aware that sensitive data are being transmitted except the source and destination. This makes the communication invisible which prevents unintended access. Hence, this technology has attracted many researchers to develop sophisticated data hiding algorithms.

The common approach of steganography is the Least Significant Bit (LSB). Besides, steganographic methods implemented based on transformations, masking and filtering, or insertion techniques have been already provided [1]. Chan and Cheng [2] proposed LSB substitution with an optimal pixel adjustment for data embedding in a simple manner. An approach whereby data are mapped by changing the gray level was implemented by Potdar and Chang [3]. Pixel mapping approach was further suggested by Bhattacharyya et al. [4]. By employing a counter clockwise direction, adjacent pixels were selected based on the intensity values.

Medeni and Mamoun [5] presented a model that employs spatial domain approach, i.e., data were hidden in grayscale images after dividing the image into blocks of the same size. Note that, the secret data were concealed in each block by considering its edge. Cheddad et al. [6] wrote an article about digital image steganography where they provided the review and analysis on various existing steganographic techniques along with some specified standards taken from literature.

This paper presents an enhanced pixel value modification approach for RGB image that conceals secret data based on modulus function while achieving good embedding capacity and good PSNR. Moreover, the secret data are concealed into each plane of RGB image with less deformation. That is, the stego image generated after applying the suggested pixel value modification method is nearly the same as the original one which ensures the security of the hidden secret data.

Overall, the proposed Enhanced-PVM approach provides good results. The following points will be covered in the next part of this paper. Section 2 discusses the related work on image steganography while Section 3 presents the design and deep explanation on the proposed method. The experimental results and discussion are given in Section 4 thereafter Section 5 presents the conclusion.

978-1-5386-2827-0/17/$31.00 ©2017 IEEE

II. Related Works on Image Steganography

Some of the existing methods on image steganography are discussed in this section.

A. LSB-based Method

Various data hiding methods based on image steganography have been around for several decades. The LSB method is famous due to its simplicity [7]. In this method, the embedding is carried out by substituting each pixel's LSB. What exactly performed is that each LSB of the pixel value in the original image (also known cover image) is directly substituted for the secret data bit. Although with this approach good payload capacity is yielded, it is highly susceptible to various image processing operations such as compression, cropping etc. [8].

B. Pixel Value Differencing-PVD

Wang et al. proposed a method based on PVD [9]. This approach splits up the cover image into blocks which are non-overlapped each having two pixels. After generating all blocks, the difference between pixels is computed thereafter the secret data are hidden by first modifying each difference value. The large difference value results in a significant modification of the original image pixel after hiding data. This means that with small difference values the quality of the cover image can be preserved. To get back the hidden data the stego image is segmented into the same number of blocks as it exactly carried out during the embedding. By referring to this method, further new PVD-based methods were implemented. One of them is Wu and Tsai [10] method which utilizes three pixels value differencing. The embedding capacity and the PSNR values were greatly improved compared to the original PVD approach [9].

C. Difference Expansion-DE

A data hiding method based on difference expansion was presented in the research carried out by Tian [11]. This method explores the redundancy in digital images to obtain extremely high embedding capacity, and keep the noise low. Few years later, Lou et al. presented a multiple layer data hiding scheme for certain images [12] using reduced difference expansion technique to hide bit stream in the LSBs of the expanded difference. With this method, large size of data can be hidden into the image while maintaining the quality. Besides, the carrier image can be recovered after extracting the payload from the stego.

D. Quad Difference Expansion

Arham et al. [13] implemented a multiple layer data hiding scheme based on difference expansion of quad focusing on increasing capacity and visual quality of the stego image by reducing the difference. Researchers in [14] suggested another method that hides secret data using modulus function. The secret message was converted into a series of base three ($base\ 3$) numbers thereafter it was compared with values obtained after applying modulus three function to the difference computed between pixels in each quad. The new pixel value is similar to its original one since alteration is only made for values which are between -2 and $+2$. The experimental results show that the image is able to accommodate large size of secret message while still maintaining the quality.

E. Pixel Value Modification Method using Modulus Function

In 2013, Nagaraj et al. [15] introduced a pixel value modification method using modulus function. Their method divides colored cover image into three planes (or components) namely, Red, Green and Blue where every pixel contains 24 bits (8 bits for each color). Additionally, in this method, all three components have been used for data embedding after applying modulus three function to the pixel values in each color component. Their embedding process is explained by following steps:

Step 1: Separate the color image into three components color matrices and apply the next steps on each of them sequentially i.e. apply the next steps on the first pixel value of Red matrix, Green matrix and the first pixel of the Blue matrix. The same process continues for the second pixel value of each plane until all pixels are accessed.

Step 2: Let S be the secret digits in base 10. These digits are first converted into base 3 values after that the obtained digits are embedded into three planes.

Step 3: Pixel values are grouped into different sets [g_{ri}, $g_{gi}, and\ g_{bi}$] with these three parameters representing the set for Red, Green and Blue pixel values respectively.

Step 4: The suitable pixel to be selected for embedding should fall in the range of $0 \leq g_i \leq 250$.

Step 5: Perform the embedding by increasing or decreasing the original pixel value by 1 or -1 respectively. Note that the decision for embedding data is taken after comparing the modulus values and the digits to be concealed. That is, having the secret digits S and the values obtained by applying modulus three function on each pixel value which are denoted by f, three criteria are considered:

- Criterion 1: $If\ s = f$ the original pixel value is not modified.
- Criterion 2: $If\ s \neq f\ and\ f < s$, the original pixel value is increased by 1.
- Criterion 3: $If\ s \neq f\ and\ f > s$ the original pixel value is decreased by 1.

During the extraction, the stego image is divided into three planes Red, Green and Blue correspondingly after that the secret digits are obtained by applying modulus three function to each pixel value. Moreover, the extracted digits values have to be converted back to base 10 to get the original secret message.

III. The Proposed Enhanced-PVM

We suggest a data hiding method that extends the functionality of the existing ones. Specifically, the suggested method is designed to improve the one presented by Nagaraj et al. [15]. The extension lies to the modulus functions which controls the embedding process. As it was previously discussed, their method enables data to be hidden by only

applying the modulus three function to the pixel values. To remove this limitation, a new method where data hiding can be controlled by applying any modulus function is suggested. This extension makes sense since users are free to choose the modulus function to be applied on the pixel value based on the embedding capacity needed. Furthermore, this is because different embedding capacity and quality of the stego image can be achieved after applying different modulus functions. Therein, making the method flexible is ideal. Besides, the embedding and the extraction procedures are also enhanced so as to improve the embedding capacity and the quality as well. To demonstrate the dissimilarities between these methods, the main steps for concealing and extracting the secret data are presented as follows.

A. Steps for Performing the Embedding

Having the RGB image and the secret message to be embedded, the embedding process is performed throughout these steps. Besides, the entire process can be viewed from Fig. 1.

Step 1: The secret message to be hidden in the cover image is converted into ASCII number after that the obtained decimal digits are further converted to different base numbers such as base 2, base 3, base 4, etc. depending on the modulus function to be applied. For example, let S represents the secret message after being converted to base 5 $\rightarrow S = [23410 \ldots]$, where $S_1 = 2,\ S_2 = 3,\ S_3 = 4, \ldots, S_n = n$

Step 2: The first secret digits (S_1) will be hidden in the first Red color component value. we apply the modulus function with the same base as in [15] in order to allow the secret digits to be recovered as they were hidden. In this way, considering $S = [23410 \ldots]$ and the first pixel values (p_ values) $\rightarrow [p_1$=226, p_2 =229, $p_3 = 215]$, the modulus function is applied as follows.

Red color pixel value:

$$f_1 = 226 \, mod \, 5 = 1; \quad (1)$$

Green color pixel value:

$$f_2 = 229 \, mod \, 5 = 4; \quad (2)$$

Blue color pixel value:

$$f_3 = 215 \, mod \, 5 = 0; \quad (3)$$

Notice that in the (1), (2) and (3), the parameters f_1, f_2, f_3 are used to denote values obtained after applying the modulus function (in this case modulus five).

Step 3: In contrast to the previous method, compute the difference (d) between the i^{th} secret digit (S) and i^{th} f value as demonstrated in (4), (5), and (6).

Red Color:

$$d_1 = S_1 - f_1 = 2 - 1 = 1 \quad (4)$$

Green Color:

$$d_2 = S_2 - f_2 = 3 - 4 = -1 \quad (5)$$

Blue Color:

$$d_3 = S_3 - f_3 = 4 - 0 = 4 \quad (6)$$

Step 4: Embed the secret digits by adding the obtained difference values $(d_1, d_2, d_3, \ldots . d_n)$ to the original pixels. That is, all modifications are made by adding up the difference to the pixel's value using (7), (8) and (9).

Red Color:

$$226 + 1 = 227 \quad (7)$$

Green Color:

$$229 + (-1) = 228 \quad (8)$$

Blue Color:

$$215 + 4 = 219 \quad (9)$$

To obtain the value for the pixel in the stego image, the difference value is added to the original pixel value instead of f value. Besides, if the difference value is negative, the pixel's value is decreased instead of being increased. On the other hand, if the value obtained after subtracting the i^{th} f value from the i^{th} secret digit (S) is not less than the base number divided by 2 $(d < base\ number/2)$, the embedding is carried using (10). The example can be seen from the value obtained in (6) which is further adjusted using (13) in order to get the stego pixel value for the Blue color which is nearly close to the original one.

$$p' = Pixel\ value - (\text{base number} - \text{difference}) \quad (10)$$

This is intended to prevent the original pixel's value from being highly increased since it can result in decreasing the quality of the stego image. Therefore, the final values to be

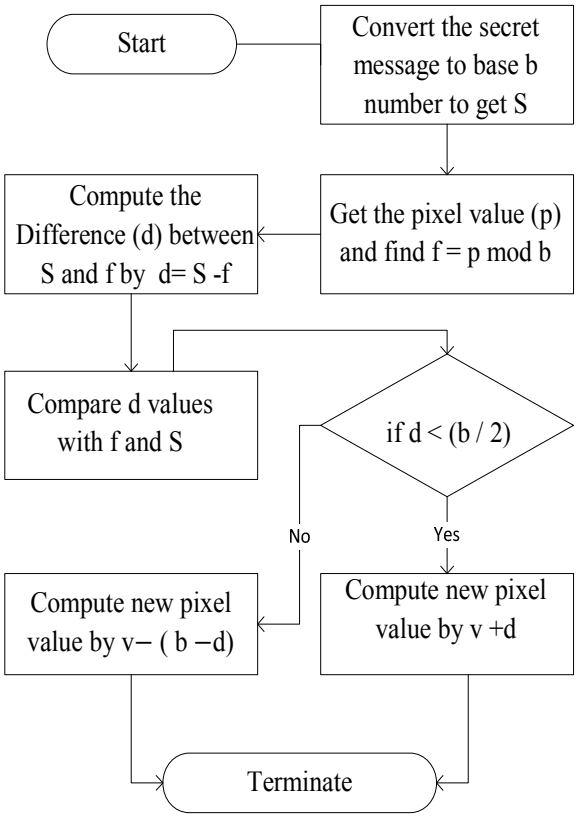

Fig. 1. Steps for embedding data

utilized while constructing the stego image are obtained by applying (11), (12) and (13).

Red Color:

$$p'_1 = 226 + 1 = 227 \quad (11)$$

Green Color:

$$p'_2 = 229 + (-1) = 228 \quad (12)$$

Blue Color:

$$p'_3 = 215 - (5 - 4) = 215 - 1 = 214 \quad (13)$$

Here, $p'_1, p'_2,$ and p'_3 represent the new pixels after hiding the data. Notice that step (11) and (12) are the same as (7) and (8) except (13) which is different from (9). After these operations, the stego image is constructed by combining all three channels' pixel values and the embedding process terminates.

B. Procedures for Extracting the Hidden data

The extraction procedure is almost similar to the previous one [15]. It is performed by separating the stego image into three components (planes). To get the hidden data, pixels are accessed from each plane after that the same modulus function (modulus function used during the embedding phase) is applied. Given three stego pixels p' for Red, Green and Blue channels, with values $p' = [p'_1 = 227, p'_2 = 228, p'_3 = 214]$, the secret digits are extracted as shown in equation (14), (15) and (16).

For the stego pixel values $\rightarrow$ $p' = [p'_1 = 227, p'_2 = 228, p'_3 = 214]$, the hidden digits are extracted as follows.

$$S_1 = 227 \; mod \; 5 = 2$$

$$S_2 = 228 \; mod \; 5 = 3$$

$$S_3 = 214 \; mod \; 5 = 4$$

The first digits of the secret message are $S \rightarrow [234]$. The same process is done until all hidden digits are extracted, thereafter they get converted to the original form in order to get the full message. In addition, Fig. 2 illustrates the necessary steps for extracting data.

IV. EXPERIMENTAL RESULTS

This section presents and discusses the results of the experiment. The suggested approach is tested using different images. Furthermore, different scenarios are carried out to evaluate the performance of this suggested approach with respect to the modulus function being applied. Before presenting the experimental results, we have to notice that as we use different modulus values, we have to convert the secret message which forms ASCII character. For example, 127 in base 2 is 1111111 and 1002 in base 5.

As we could see in base 2 the length is 7 while in base 5 it is 4. In base 2, we need 7 digits to be able to code any ASCII character, while in base 5, we only need 4 digits. Consequently, when we increase the modulo value, the size of the payload can also increase. To analyze this scenario, we fix the modulo value and vary the size of the secret data whose results can be found in Table I.

What interesting is that the PSNR value obtained after applying modulo 6 is nearly the same as the one for modulo 5 and this is because the proposed method does maintain both payload capacity and the quality of the stego image, i.e., the variation of the modulo value (modulus function) allows more secret digits to be hidden in the image while maintaining an acceptable PSNR value. In Fig. 3, the PSNR value slightly decreases when modulo gets higher. Obviously, From Table II and Fig. 4, the PSNR value decreases when payload gets higher. That is, as the modulus increases, the payload increases too while the quality decreases. However, a good PSNR value is still being achieved.

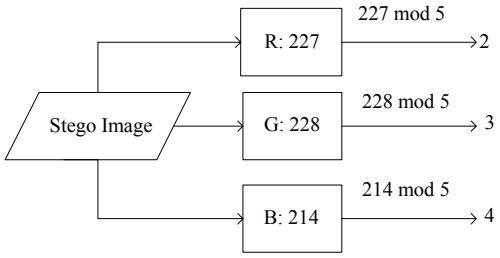

Fig. 2. Extracting the secret data

TABLE I. PSNR VALUES DEPENDING ON THE SIZE OF THE SECRET MESSAGE WITH MODULO 4

Cover image	PSNR (dB)				
	1kb	*5kb*	*10kb*	*25kb*	*50kb*
Lena	71.902	62.174	58.534	54.487	51.394
Baboon	71.86	62.142	58.5	54.457	51.385
Pepper	71.091	61.971	58.391	54.396	51.317
Average	71.618	62.096	58.475	54.447	51.365

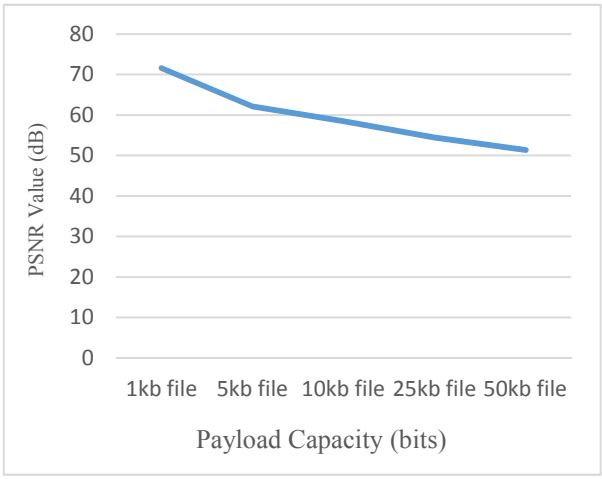

Fig. 3. PSNR Value Depending on the size of the seceret message

TABLE II. PSNR VALUES DEPENDING ON MODULUS FUNCTION WITH 1KB OF PAYLOAD

Cover image	PSNR (dB)				
	Mod 2	***Mod 3***	***Mod 4***	***Mod 5***	***Mod 6***
Lena	75.071	74.154	71.902	69.388	69.615
Baboon	75.106	73.976	71.86	69.601	69.484
Pepper	75.016	73.541	71.091	68.657	68.729
Average	75.064	73.89	71.618	69.215	69.276

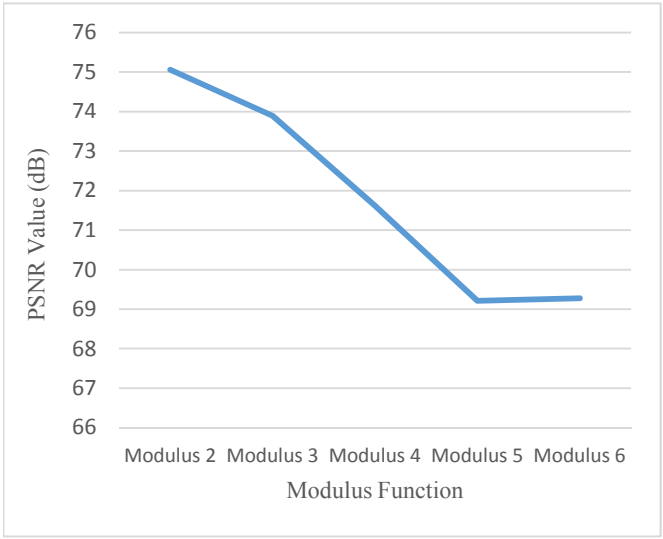

Fig. 4. PSNR value depending on modulus function

V. CONCLUSION

A new image steganographic approach developed based on modulus function is presented in this paper. This approach has removed the limitations encountered in the previous method where only base three modulus function was considered. In addition, the experimental results are analyzed to figure out the effect of varying modulus function with respect to the capacity. Furthermore, the secret data are concealed by modifying pixel values in each channel of RGB image using modulus function which controls the embedding. In the extraction phase, the hidden data are recovered by applying the same modulus function which was applied during the pixel value modification. This makes the extraction straightforward since no further steps are required. Besides, the secret data are recovered as they were concealed i.e. without any deformation. Generally, the simplicity of this method lies on both embedding and extraction stages.

REFERENCES

[1] R. J. Anderson and F. A. P. Petit colas, "On the limits of steganography". IEEE Journal on Selected Areas in Communications, pages 474–481, 1998.

[2] C.K. Chan, L.M. Cheng," Hiding data in images by simple LSB substitution", pattern recognition vol. 37, Issue 3, pp. 469-474, 2004.

[3] V. M. Potdar and E. Chang, "Grey Level Modification Steganography for Secret Communication," in International Conference on Industrial Informatics, 2004. INDIN '04. 2004 2nd IEEE, 2001, pp. 223–228.

[4] S. Bhattacharyya, A. Khan, A. Nandi, A. Dasmalakar, S. Roy, and G. Sanyal, "Pixel Mapping Method (PMM) Based Bit Plane Complexity Segmentation (BPCS) Steganography," in *2011 World Congress on Information and Communication Technologies*, 2011, pp. 36–41.

[5] O. Medeni and E. Mamoun, "A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution," in *2011 International Conference on* Multimedia Computing and Systems, 2010, pp. 1–4.

[6] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt "Digital image steganography: Survey and analysis of current methods Signal processing", March; 90(3): 727-752, 2010

[7] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB Steganography in Scale Images," *IEEE Multimed.*, pp. 22–28, 2001.

[8] V. Vijayalakshmi, G. Zayaraz, and V. Nagaraj, "A Modulo Based LSB Steganography Method," in *International Conference on Control, Automation, Communication and Energy Conservation, INCACEC.*, 2009, no. June, pp. 6–9.

[9] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," J. Syst. Softw., vol. 81, no. 1, pp. 150–158, 2008.

[10] D. Wu and W. Tsai, "A steganographic method for images by pixel-value differencing," vol. 24, pp. 1613–1626, 2003.

[11] J. Tian, Reversible data embedding using a difference expansion, IEEE Transactions on Circuits and Systems for Video Technology 13 (8) (Aug. 2003) 890–893.

[12] D.C. Lou, M.C. Hu, J.L. Liu, Multiple layer data hiding scheme for medical images Computer Standards & Interfaces, 31(2): 329-335, 2009

[13] A. Arham, H.A. Nugroho, T.B. Adji,Multiple layer data hiding scheme based on difference expansion of quad,Signal Processing 137 52–62, 2017

[14] Y. Kurniawan, L.A. Rahmania, T. Ahmad, W. Wibisono, R.M. Ijtihadie, " Hiding Secret Data by using Modulo Function in Quad Difference Expansion" IEEE 978-1-5090-4629-4/16, 2016

[15] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Color Image Steganography based on Pixel Value Modification Method Using Modulus Function," in 2013 International Conference on Electronic Engineering and Computer Science Color, 2013, vol. 4, pp. 17–24.

This page intentionally left blank