Steganographic on Pixel Value Differencing in Iris Biometric

Nur Khaleeda Mansor1, Syed Muhammad Hazry Asraf1a and Syed Zulkarnain Syed Idrus1b

1Faculty of Information and Communication Technology, Universiti Teknikal Melaka Malaysia
2School of Human Development and Techno-communication, Universiti Malaysia Perlis

a hazrysyed@gmail.com; b syzul@unimap.edu.my

Abstract. Biometric technology was widely used in more than a decade ago and become convenient since human uses their own physical traits and behaviour rather than using keys and IDs to enter the systems. As the arising of biometric use, the issues of security in biometric data and the system points exist. The security and integrity of biometric data presents a major challenge as many benefits of biometric may quite easily become impediment. Every point of vulnerability in the biometrics system consist of specific defend techniques to prevent the misidentification of the real person. In biometric security system, techniques such as watermarking and steganography have been used in attempt to improve security of biometric data. Steganography has become one of the technique used in defending data and system in biometric security The techniques of steganography is divided into two embedding methods which are the least significant bit (LBS) and pixel value differencing (PVD). LBS is most popular techniques for data hiding field and data embedding since it embeds the fixed-length secret bits in the same fixed-length of pixel. While, PVD works better by providing a high quality stego image, besides the high capacity of concealed information. PVD provides high capacity and produces a stego image with good pixels value. PVD technique is also resistant to statistical attacks. It embeds the secret data in the difference as well as in the sum of the two contiguous pixels. In steganography technique, standard measurement to test the performance of stego image quality due to the hiding of message by using the Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE). The aim is to achieve higher value of PSNR that indicates a better reconstruction. The expected findings show a better results of stego image quality based on PSNR and MSE. As a conclusion, the study of the project brings a good impact of higher security towards steganography field in biometrics applications.

1. Introduction

Watermarking and steganography techniques are widely used in biometric security systems as an effort to protect the secret data. Steganography techniques are divided into two embedding methods, which are the least significant bit (LBS) and pixel value differencing (PVD) [1][2]. PVD works even better by providing high-quality stego images as well as high capacity hidden information.
The development system of steganography in biometric as security for the personal data can be enhanced by using this integration [3]. For this project, the use of spatial domain algorithms that implement the PVD scheme as a new model will instantly embed the iris-implicit image data into the cover pixel image [4].

Biometric technology has been used extensively over a decade ago and it is very convenient because humans use their own physical characteristics and behaviors rather than using keys and IDs to enter the system [5]. With the increased of biometric usage, security issues in biometric data and system points also exist. Biometric security and integrity data provide a major challenge as many biometric benefits may be a barrier. Every point of the vulnerability in the biometric system consists of certain defense techniques to avoid the misidentification of the real person.

Steganography which means ‘writing in hiding’ that purposely to hide data in a cover media by embedding message within other that seemingly harmless message. The word Steganography combines within the Ancient Greek word *steganos* which means “covered, concealed or protected” while the *graphein* meaning is “writing”. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. In image steganography, it is broadly classified into spatial domain and transforms domain steganography.

In this spatial domain image, there are 3 type of image used in digital image processing. They are binary image, gray scale image and color image. Only two possible values for each pixels in binary image. It is typically used for black and white though any two colors can be used. While gray scale is the image that have single sample value of each pixels that only carries intensity information. Also known as black-and-white, are composed exclusively of shades of gray (0-255), varying from black (0) at the weakest intensity to white (255) at the strongest. The color image includes color information for each pixels. To determines its appearing color, each pixels have particular value. The 3 primary decomposition color are red, green and blue which quantified by a number between 0 and 255. (M. Kumari, P. Somesh & K. Dewangan, 2014).

The word “biometric’ came from Greek which divided into two roots: “bio” means life and “metrics” – to measure. Biometric used for automatically recognizing or verifying the identity of a human being by a unique, measurable, biological characteristic or traits. (Ayoub & Nori, 2013). The process of biometrics is to making sure that who is the person claims to be. Characteristics of Biometric Technology:

1. Universality: something that each person has.
2. Uniqueness: something that separates this very person from others. This means that not all characters can be suitable for biometrics.
3. Permanence: biometric measurement should be constant over time for each person.
4. Measurability (collectability): it should be easy to measure, should not demand too much time and cost.
5. Performance: speed, accuracy and robustness.
6. Acceptability: how well people accept biometrics

According to (M. Douglas, K. Bailey, M. Leeney et al.) biometrics used physical qualities such as face recognition, hand geometry, fingerprint, iris sequences and personal attributes. For iris biometric, it operates by scanning and analyzing that are present in the colored tissues around the eye pupil. The human iris is a thin circular anatomical structure in the eye. It is function to control the diameter and size of the pupils and also controls the amount of light that progresses to the retina. (Ayoub & Nori, 2013).
2. Methods

To begin research, the first step that needs to be done is to identify the problems encountered. An appropriate technique which is PVD is selected to be applying to the problem and to enhance the technique by implement into an area of concern.

The design will involve 2 process which is embedding and extracting process. It will require cover image and message to form a stego image. We will use the iris image as the message in order to secure the biometric data.

The process of gathering and measuring information from various articles will be held during the data analysis phase. We will analyze the quality value of the stego image based on the PSNR and MSE value due to the hiding of message by using several steganography pixel value differencing techniques [6].

We figure out from the several PVD techniques which method and tools is the best to implement with iris biometric. Using the data collected from the previous phase, we will justify the best PVD technique to produce good visual quality of the iris stego-image. Thus, high protection of steganography system in iris biometric created.

The simulation system being tested to get the good quality of output image. Value of PSNR and MSE are calculated. The higher the PSNR value give the better image quality. The preferable value of PSNR is 30 dB and above.

2.1. Approach Architecture

In digital imaging, PVD scheme uses the difference value between consecutive pixels that used to determine how many secret bits can be embedded. It is one of the most important algorithms used for hiding data that changes continuously since 2003 [7]. For this project, steganography techniques of PVD scheme used the image based steganography system included the biometric to provide security.

![Proposed approach iris biometric using PVD steganography](image)

**Figure 1: Proposed approach iris biometric using PVD steganography**

2.2. Metric Measurement

In steganography technique, standard measurement to test the performance of stego image quality due to the hiding of message by using the Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE). The aim is to achieve higher value of PSNR that indicates a better reconstruction.

2.2.1. Peak Signal-to-Noise Ratio (PSNR)

PSNR is used to determine the ratio of the cover image quality before and after inserting the message by using Equation 1:

\[
PSNR = 10 \log_{10} \left( \frac{2^n - 1}{\sqrt{MSE}} \right) = 10 \log_{10} \left( \frac{255^2}{\sqrt{MSE}} \right)
\]  

(1)
2.2.2. Mean Squared Error (MSE)

It is the most common estimation method used to check the fidelity of image. MSE is employ by PSNR to evaluate image quality by using the Equation 2. The lower the MSE value, the better the result is.

\[ MSE = \frac{1}{MN} \sum_{i=0}^{N} \sum_{j=0}^{N} (x(i,j) - y(i,j))^2 \]  

(2)

3. Analysis

In order to propose the simulation method, analysis from the previous research is carried out to find the best PVD techniques. First, the summary on the steganography research is done followed with the summary PVD method and comparison between capacity and PSNR value of several PVD techniques.

![Figure 2: Comparison of Capacity in PVD Techniques](image1)

![Figure 3: Comparison of PSNR in PVD Techniques](image2)
Figure 2 summarises between the value of PSNR and Capacity of the Lena, Baboon and Pepper image based on PVD methods is tabulated and plotted in graphs. In this section, the correlation between the capacity and PSNR is studied. Figure 3 shows the higher PSNR value produced high security because it indicates minimum difference between the original and stego values which no one can easily suspect the hidden information. However, it is obvious if the capacity size is smaller, obtained PSNR greater. We found that previous work seemed does not achieved the main goals of the correlation. Hence, we combined the methods with the higher capacity and higher PSNR to produce high quality image based on the analysis.

From the comparison of LSB and PVD [8], Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are used to comparing the squared error between the original image and the reconstructed image [9]. There is an inverse relationship between PSNR and MSE. Thus, a higher PSNR value indicates the higher quality of the image (better). More number of messages bit is stored in PVD method compared to LSB. The image quality after embedding shows that LSB is better than PVD. Nonetheless, a larger number of data bits are stored in PVD method without compromising quality while a larger number of data can be stored in LSB method but degrades the image quality. So, they already conclude that PVD method giving better result than LSB method as more data bits is hide, good image quality and not easily detectable thus communication more secure. For the proposed method, we will use the iris image as the message image in order to protect the iris data from the database template from seen by the intruder. We compare the PVD technique such as Modulus PVD [11], PVD+LSB and others based on the quality value of PSNR and MSE.

From the analysis on previous research regarding PVD steganography technique, the best techniques are defined and the design for the simulation is made. The PVD techniques that showed a bigger value of PSNR are combined to produce high quality image based on the analysis. The combination simulation method also included the common steganography techniques.

4. Design

The design of the proposed method explained below based on their process to produce the output. The process involved two steganography techniques. We evaluated the steganography technique in MATLAB by using the following algorithm with respect to image steganography. The iris image embedded with cover image.

4.1. Pixel value differencing process

Initially, the cover image is partitioned into non-overlapping blocks. The two consecutive pixels of the block are calculated to find the difference [12]. The difference value \( d \) is quantized into several regions of range table. From the range table, a new difference is calculated to form a new pixel pair in the cover image. The PVD process involves the following steps:

- Step 1: Read cover image
- Step 2: Calculate difference value designed using range table
- Step 3: Calculate new generated difference value
- Step 4: Display PVD cover image

4.2. Significant bits process

Two bits of the cover image were replaced with the bits of secret message. The bits of secret message embed the first message bits in the least and most significant bit of the cover byte. The bit shift process involves the following steps:
Step 1: Read iris image
Step 2: Set the bit to be imbed
Step 3: Shift over (8-imbed) bits into cover image
Step 4: Display message image

4.3. Overall process of Pixel value differencing and bit shift
The overall process involves the following steps:

Step 1: Input cover image
Step 2: Calculate difference value designed using range table
Step 3: Calculate new generated difference value
Step 4: Input iris image
Step 5: Set the bit to be imbed
Step 6: Shift over (8-imbed) bits into cover image
Step 7: Add the secret image into cover image
Step 8: Display stego image

5. Simulation
The operating system used is Windows platform for the environment setup. The simulation system is developed using open source coding and is run using MATLAB. The purpose is to determine the quality of images. Personal workstation with standard performance is used as long as it can run the MATLAB and produce output results.

The development of Pixel Value Differencing (PVD) and Most Significant Bit (MSB) was run in the MATLAB using the open source coding. The process of obtaining the output stego image is explained in the following subsections.

5.1. Process of applying PVD in cover image
The pixel pair of cover image is replaced by using the PVD techniques to form a PVD stego image shown in Figure 4.
5.2. Process of applying bit shift in message image

Then, second process involving bit shifting that used for iris image. Three bits from the iris image is selected to imbed with the cover image and formed a message image as shown in Figure 5.

![Figure 5: Bit shift of message image](image)

5.3. Process combining PVD and Message image

The final process is adding the cover image with the secret image involved MSB technique. PVD cover image then combined with the message image to form stego image as shown in Figure 6.

![Figure 6: Process of combining image](image)

5.4. Process combining PVD and Message image

After the process of applying the two techniques is done, the final output of stego image is display as shown in Figure 7.
5.5. Method overall process

The process of this simulation involved the process of PVD technique and MSB technique. Both cover and message image undergoes the techniques of steganography using the proposed method of steganography to form a stego image. First, cover image is applied with PVD techniques which the difference of pair pixel is calculated and replaced. After that, the bit shifting is applied in message image which bits to be imbedded with cover image using MSB shift to the right. The PVD cover image is then combined with the message image to form an output image called stego image. The stego image is compared with the cover image to calculate the quality value of MSE and PSNR after the embedding process. The overall flow of the project implementation is shown in Figure 8.

Figure 7: Output after applying two techniques

Figure 8: Overall flow of the project implementation
6. Testing

The purpose of testing is to find out the effectiveness of the steganography techniques for iris image protection. It also to test the stego-image visual quality produced using the implemented PVD techniques of steganography. The simulation testing has been proven by reading the peak signal noise ratio (PSNR) and mean square error (MSE) value between cover image and stego-image. The higher PSNR value with the lower MSE value indicates a better quality result of the image. The analysis of this project is result is compared using the grayscale image and colour image.

6.1. Testing plan

There are two types of testing has been conducted. The first test is by using grayscale image as the cover image while the second part using colour image. The purpose of this two testing are to evaluate the quality of the stego image after embed using the simulation of the steganography technique in order to secure the iris image. The system tested using the same image dimension of 512x512 pixels with grayscale image and colour image (baboon.bmp, lena.bmp) as cover. The iris image with the same dimension size is used as the message image for each cover image respectively.

6.1.1. Testing using Grayscale image

Run the ‘pividi.m’ code in the MATLAB platform. Image grayscale of ‘lena.bmp’ is selected as input cover image, while the message image of iris is ‘a.jpg’. The output will display the cover with stego image and the PSNR and MSE value are calculated and display, as illustrated in Figure 9 and 10.

![Figure 9: Grayscale cover image displayed](#)

![Figure 10: Grayscale stego image displayed](#)

Using the grayscale image as cover image produced 1.51 value of MSE and 46.38 dB of PSNR value. The lower the value of MSE and the higher the value of PSNR indicate a good quality of stego image, as shown in Figure 11.

![Figure 11: Input image and quality for Grayscale](#)
6.1.2. Testing using Colour image

In the MATLAB platform, ‘pividiRGB.m’ is run to get the output of stego image by using colour cover image, ‘lenna.bmp’. The message iris image used is the same which is ‘a.jpg’. The result will display the image output and quality measure, as illustrated in Figure 12 and 13.

![Colour cover image displayed](image1)
![Colour stego image displayed](image2)

Figure 12: Colour cover image displayed  Figure 13: Colour stego image displayed

The result obtains by using the colour cover image displayed three value of MSE and PSNR value. It represents the component of colour image which is Red, Green and Blue (RGB) [13]. These three value quality measure increase the accuracy of the performance of the stego image compare to grayscale due. The value of MSE is lower and the PSNR value is higher of the colour image than the grayscale. The input image and quality for colour is shown in Figure 14.

![Input image and quality for colour](image3)

Figure 14: Input image and quality for colour

7. Conclusion and Perspectives

This project can be has completely done and the project also can be considered successful since it met the objectives that has been discuss before starting the projects. We have develop the techniques that suitable for iris biometric protection that produce a high quality image by using the differencing of two pixel pair and also shifting of the bits of steganography technique [14]. The contribution of this project is to create a high protection of steganography system in iris biometric by combining PVD techniques. This project produced a high quality of stego image as the best quality is in the range of
40-50 dB of PSNR value. The size of the image also remains same after embedding that will prevent attacker to detect the hidden data. Since this project testing including the use of grayscale and colour image cover, the colour image produced 3 value of the quality measure that will increase the accuracy due to the RGB matrices compare with grayscale.

For future works, this project can be improve by combining steganography with encryption for data security as data security is most encouraged after all and highly open to potential risks. The cryptography and steganography are closely related to each other which can provide a high security protection toward the data security.

References

[1] Ranade, S. K. (2017). A Secure Steganographic Method Using Modified LSB (Least Significant Bit) Substitution, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 6, Issue 8, August 2017, ISSN: 2278 – 1323. http://ijarcet.org/wp-content/uploads/IJARCET-VOL-6-ISSUE-8-1268-1273.pdf

[2] Tseng, H. W., & Leng, H. S. (2013). A steganographic method based on pixel-value differencing and the perfect square number. Journal of Applied Mathematics .Volume 2013, Article 189706, 8 pages. http://dx.doi.org/10.1155/2013/189706

[3] Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2017). An overview of steganography techniques applied to the protection of biometric data. Multimed Tools Appl (2018) 77: 17333. https://doi.org/10.1007/s11042-017-5308-3.

[4] This reference has two entries but the second one is not numbered (it uses the ‘Reference (no number)’ style. Chikane, Y. R., & Rawat, M. K. (2013). Hiding Text In To Image by Pixel Value Differentiation Using Private Key, International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 3, Issue 1, February 2013

[5] Idrus, S. Z. S., Cherrier, E., Rosenberger, C., & Schwartzmann, J. J. (2013). A review on authentication methods.

[6] Prasad S, Pal AK. 2017 An RGB colour image steganography scheme using overlapping block-based pixel-value differencing. Soc. open sci. 4: 161066. http://dx.doi.org/10.1098/rsos.161066

[7] Dhruw, T., & Tiwari, N. (2016). Different Method Used in Pixel Value Differencing Algorithm, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. IV (May-Jun. 2016), PP 102-109 www.iosrjournals.org

[8] Coe, S., Coe, S., & Coe, S. (2015). Comparison of LSB and PVD Steganography Methods, (Ncesc), 15–17. Indonesian Journal of Electrical Engineering and Computer Science Vol. 2, No. 3, June 2016, pp. 712 ~ 719 DOI: 10.11591/ijeecs.v2.i3.pp712-719

[9] Rojali, R., Siahaan, I. S. R., & Soewito, B. (2017). Steganography algorithm multi pixel value differencing (MPVD) to increase message capacity and data security. AIP Conference Proceedings, 1867.

[10] Sahu, A. K., & Swain, G. (2016). A review on LSB substitution and PVD based image steganography techniques. Indonesian Journal of Electrical Engineering and Computer Science, 2(3), 712–719.

[11] MODULUS FUNCTION AND PIXEL VALUE DIFFERENCING COUPLED WITH MODIFIED PIXEL INDICATOR BASED SECRET. (2016). International Journal of Advances in Science Engineering and Technology, ISSN: 2321-9009, Vol-4, Iss-2, Spl. Issue-3 Jun.-2016

[12] Kumari, M., Somesh, P., & Dewangan, K. (2014). High Security System Provided by Steganographic Technique Using Palm and Iris Scan, International Journal of Engineering and Computer science. 3(11), 9270–9272.
[13] Pradhan, Anita & Krovi, Raja Sekhar & Swain, Gandharba. (2017). Digital image steganography using LSB substitution, PVD, and EMD. Mathematical Problems in Engineering, 1–15.

[14] Pixel Value Differencing a Steganographic method: A Survey, 2013, 1–6. International Journal of Computer Applications (0975 – 8887) International Conference on Recent Trends in engineering & Technology - 2013(ICRTET'2013)