Journal of Theoretical and Applied Information Technology
10th May 2015. Vol.75. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# STEGANOGRAPHY USING PIXEL VALUE DIFFERENCING SPIRAL

[1]AFAN GALIH SALMAN, [1]ROJALI, [1]VIVI,
[1]Dept. of Computer Science, Bina Nusantara University, Jalan KH.Syahdan No. 9 Palmerah Jakarta 11480, Indonesia
E-mail: [1]asalman@binus.edu,[1]rojali@binus.edu,

**ABSTRACT**

The Further progessive technology make information exchange can be easily accessed by the unauthorized person. Threrefore the method of steganography is made for hiding information in some medium in such a way that the medium seemingly is not contained a piece of information when it seen by human eyes. One of the steganography methods is Pixel Value Differencing (PVD). PVD is inserting message byte into the difference in bytes of the applied medium. This steganography use the modified PVD with some modification. The modification will be carried out on the pixel pick up pattern using spiral pattern to form pixel pair. It will make the message extraction become more difficult. Based on Peak Signal to Noise Ratio(PSNR) and Mean Square Error (MSE) calculation, The results of this study and survey show that using method of Spiral PVD, the quality of the produced image is relatively good.The image before and after message insertion process has relatively same quality. It is clearly evident in the image of "Ungu Cahaya" based on survey as well as MSE and PSNR calculation is proved that it has good quality after message insertion.

**Keywords:** *Steganography Methods, Pixel Value Differencing (PVD), Pixel Pick Up Pattern*

## 1. INTRODUCTION

The recent technology becomes more advanced, facilitating technology user to exchange information. The more ease user to do information change, the more attention should be paid to enhance security and manage person who entitle to access the information, so that it not just anyone can get the information.

In order the information is securely sent by one person and received by the addressee (the message cannot be seen by unauthorized person), and cannot be accessed by anyone, then people start to think how to make information securely sent. One of the solutions which later found is steganography. The steganography method is capable of inserting information into some medium (These medium might in form of text, image, audio or video). But the inserted medium seemingly is not contained a piece of hidden information, so that it is slight possible the medium will arouse suspicion. Steganography comes from the Greek"stego" which means closed and "Graphia" which means writing. Steganographyis the art and science of hiding the fact on going communication[1].

One of the triggers in steganography technic development is steganalis attack which is succesful cracking message that hidden by using the widely known steganography method. It encourage a desire to find an alternative of the message hiding method that has never been thought before.

One of the methods shows how to encrypt and hide data in a xy graph and the other method shows a new way of encrypting and hiding data through Unicode symbols [2].

Another research developed an application which can check the Email content of corporate mails by S-DES algorithm along with the neural networks back propagation approach. A new filtering algorithm is also developed which can used to extract only the JPG images from the corporate emails. Experimental research shows that this algorithm is more accurate and reliable than the conventional methods[3].

Recently the steganography has been advancing and has many methods, one of the methods is Pixel Value Differencing (PVD). This PVD methods apply the value deference in one pixel with that of other pixel, later the result of value deference of two pixels will be used to insert message into the other mediun which aim to be hidden. Having the message been inserted into the message storage

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

medium, the pixel value will be change. Its value change in accordnce with the PVD calculation formula.

However the PVD generally has a weakness on its method, namely its pixel pair has orderly pattern and its method has already been known by many people. These weakness bring out possibility that the message insertion on the other medium can be decrypted by unauthorized person. There are many researchers attempt to modify PVD in order to get maximal result.

## 2. RELATED WORKS

In 2003 Wu Da-chun and Tsai Wen-Hsiang made the new efficient steganography methodthat is embedding the secret message in grey value of the image cover [4].

Awad Kh. Al-Asmari and Owayed A. Al-Ghamdi also carried out a modification on PVD method in 2006. They performed modification by dividing image into several subblocks which has semi hexagonal form[5].

In 2007 four persons from two universities in Taiwan, namely Wang Chung Ming, Wu Nan I, Tsai Chwei Shyong, and Hwang Min Shiang, performed research on steganography method by combining PVD method with modolus function [6].

In 2009 the research also carried out by Rojali. In this PVD modification, its algorithm was also modified, that is if the difference of the adjacent pixel is more than 7 then the message insertion is done with the usual PVD algorithm, but if the difference is less than or 7 the messge is inserted using the Pixel Value Diferrencing Modified (PVDM) Algorithm [7].

Research on PVD method also was performed by J. K. Mandal and Debashis Das in 2012. Modification was carried out to solve the problem of pixel value on the stego image which its value beyond the range of 0 – 255[8].

The proposed solution in this paper is modifying PVD by change the way of pick up the pixel pair pattern. The way of pixel pick up pattern to be combined is picking up one pixel in the first row in image, then one pixel in the last column then proceeded to pick up one latest row at the end then one of the first pixel colomn.

This way is repeated until all pixel has been picked up. There is one thing that need to remember that is once the pixel being picked up it will never picked up again to be combined with other pixel to form the next pixel pair.

The supremacy of this method is modifying the way of pixel pick up so that it is not general anymore, by this way the unauthorized people will more difficult to extract the inserted message within the message storage medium.

Scope :

- The tabel that is used for counting the number of the stored message bit is not changed.
- The inserted message is in the form of *file* .txt and there is only one message inserted into the reception medium with the provision that the message size shall be smaller than reception medium.
- The medium that is used as a reception for the inserted message is picture with the *file type* .bmp, jpg, and png.
- The language program used in this application is c#.

## 3. THE ARCHITECTURE SYSTEM

The pattern of pixel pick up has been widely known by many people who used to apply PVD method. Therefore, if we want to insert a message into some image by using the ordinary PVD, the possibility that the message can be successfully extracted by unauthorized person will be higher. To understand easier, the following figure illustrated the way of pixel is picked up (the blue number indicates sequence of pixel picking up, whereas the blue one indicates the coordinate on the image pixel) see Fig.1.

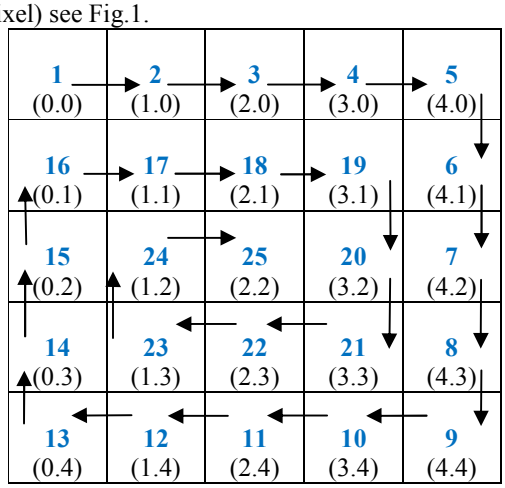


*Fig.1. The Sequence Of Image Pixel Pick Up In The Spiral Pattern*

By using this method, the inserted message will be more secure because this method is new that not known by many peoples. In this way, it will become more difficult to unauthorized person to extract message from the image.

Journal of Theoretical and Applied Information Technology
10th May 2015. Vol.75. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

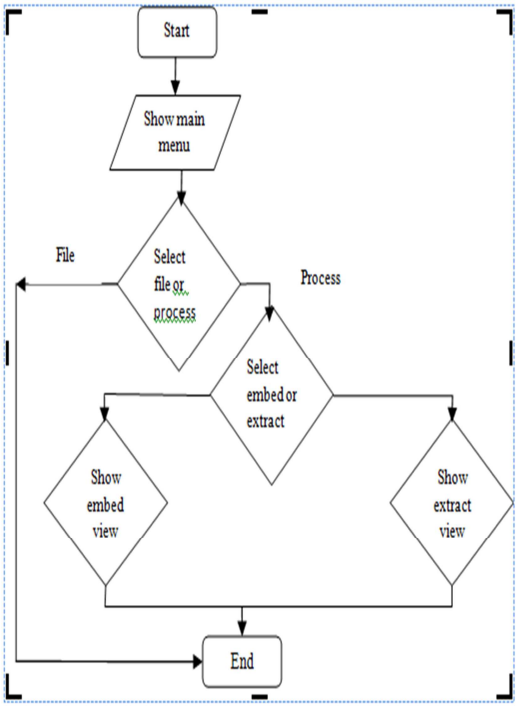


*Fig.2. The Flow Chart Of System*

Fig.2. shows the Flow Chart of System with some process such as :

**Show main view**
When the application operated the main view will be displayed with the menu options 'file' or 'process' .
**Select file or process**
To show the next menu, user has to select what menu that they would like to see.
**Select embed or extract**
If the 'process' menu selected, the next menu option will appear, namely display menu of 'embed' or 'extract'.
**Show embed view**
The display of 'embed' menu will be shown if user selects 'embed' menu.
**Show extract view**
Similarly, if the user select menu of 'extract', the display of 'extract' menu will be shown.

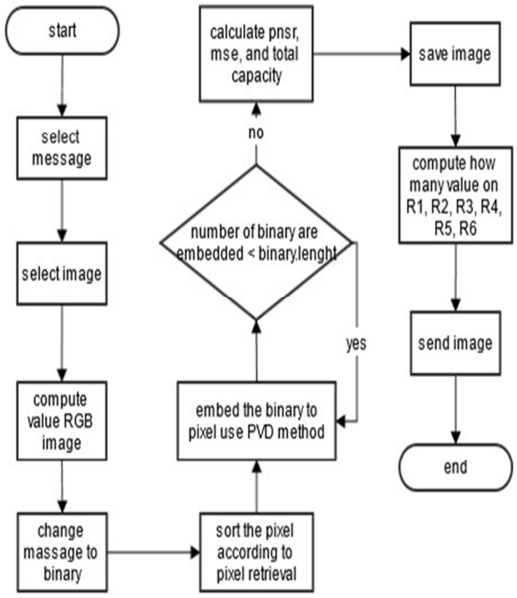


*Fig.3. Flow Chart Of Embed Menu*

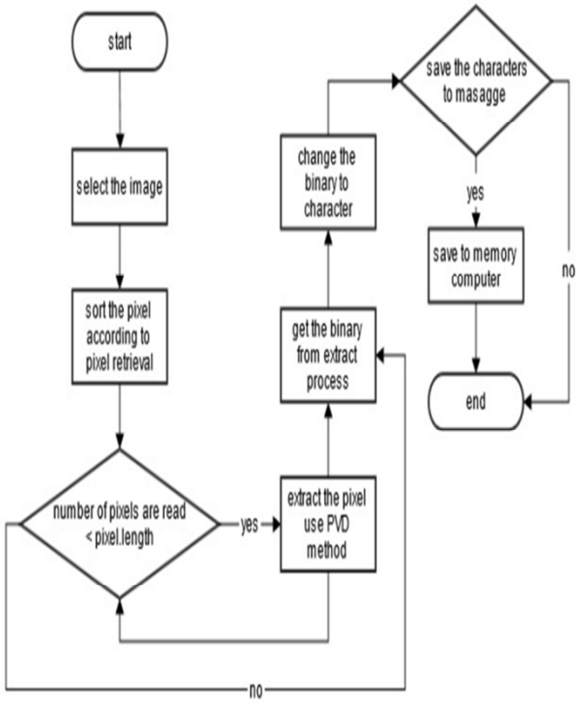


*Fig.4. Flow Chart Of Extract Menu*

Fig.3. and Fig.4.shows step by step of embed menu and extract menu.

Journal of Theoretical and Applied Information Technology
10th May 2015. Vol.75. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

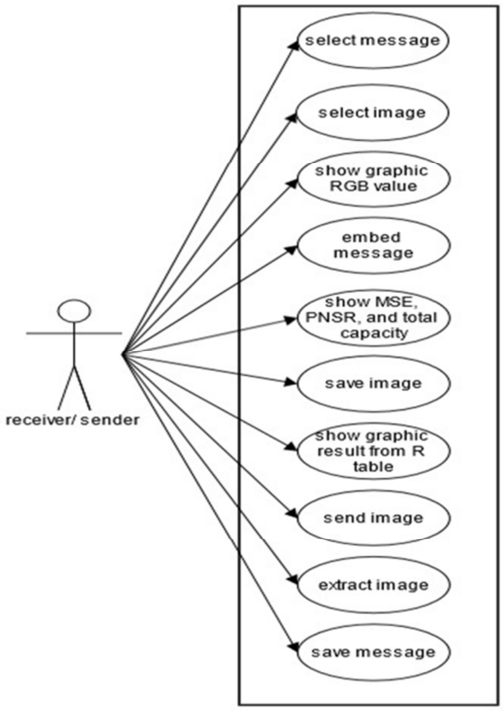


*Fig.5. Use Case Diagram*

Fig.5. show Use Case Diagram is the whole description of program [9].

The features contained in this application capable of selecting message that intended to be inserted and image which will be the inserted medium. After the message and the image have been selected, the application able to do embedding process. This application also is able to show graphic of characteristic of the applied image medium.

Having embedding, the application will show Peak Signal to Noise Ratio (PNSR) value[10]and Mean Square Error (MSE [11])to find error or how many differences in the original image and the image that contained the inserted message. This application also features the capacity of message that can be stored in the image medium. Saving the image result which contained the inserted image can be done by this application. In addition to that this application is also capable of showing calculation graphic concerning how many difference in two pixels which is counterpart on the table of R range. In order to share message which successfully have been inserted, the user can send the message by email.

The other feature on this application is able to extract the image contained inserted message. Extracting is carried out by selecting the image which is contained information that intended to be read. Having done extracting, user can save the message. As a result of embedding and extracting features which present in this application, user is able to share information safely.

## 4. EXPERIMENTS AND RESULT

On this designing spiral PVD application program the trial test is performed by using eight images with dimension 512 x 512 in image type of jpg, png, and bmp. The eight images were selected in order to get eight characteristics of image representing the RGB combinations on the image. On this test the file.txt with the same size of 44,3 kb is also used for each of eight tested images. The time which is taken to insert and extract the message will be presented in the format of minutes: second, millisecond (mm:dd:md). The Evaluation of the Image Capacity Result, MSE, PSNR, The Embedding time and Extract time can be seen on the Table.1.

*Table .1. Evaluation*

| Image Name | Image Capacity (Bit) | MSE | PSNR | Embbed Time mm:dd:md | Extract Time mm:dd:md |
|---|---|---|---|---|---|
| Putih Retak | 1190160 | 3.638 | 42.52 | 02:15.00 | 02:34.90 |
| Kuning Air | 1203984 | 0.678 | 48.81 | 02:10.17 | 04:26.60 |
| Ungu Cahaya | 1200851 | 0.469 | 51.41 | 03:30.18 | 04:24.22 |
| Aqua Awam | 1183380 | 1.001 | 48.12 | 02:27.45 | 04:20.84 |
| Bunga Merah | 1233330 | 1.067 | 47.84 | 02:08.93 | 04:29.92 |
| Hijau Daun | 1188278 | 1.890 | 45.34 | 03:09.51 | 04:29.74 |
| Biru Banyu | 1234165 | 0.710 | 49.61 | 02:16.38 | 04:34.62 |
| Hitam Fractal | 1191248 | 0.606 | 50.30 | 03:21.71 | 04:09.93 |

Table.1. show that almost all images have MSE which is small enough, except the image of “Putih Retak” has the largest MSE, namely 3.638. The smaller MSE the better because the PSNR image will be bigger, meaning the quality of image will be better as displayed on fig.6.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

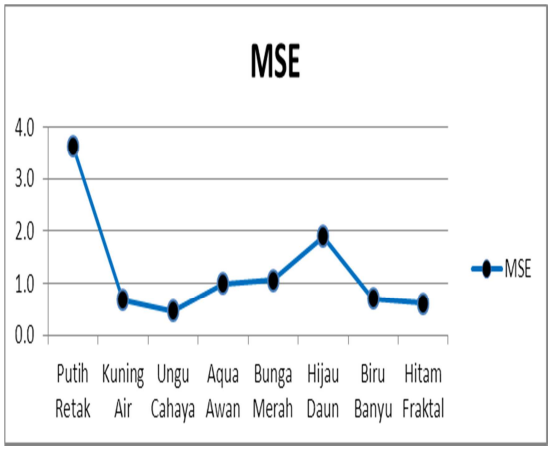


*Fig.6. MSE*

Fig.6. shows image of "Ungu Cahaya" has the Smallest MSE. However the above graphic indicates that the inserted image is relatively good.

From table 1 tindicates that the image of "Ungu Cahaya" has the longest time to be inserted by a message. Whereas "Bunga Merah" has the fastest time to be inserted by a message. However compare to capacity graphic, the size of the tested image capacity do not impact on the speed rate of message insertion into image.

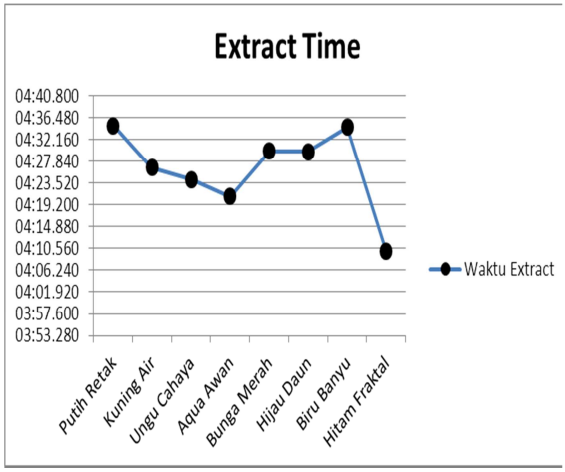


*Fig.7. Extract Time*

Fig.7. show the required time to read the messagewhich inserted into image. The trial test on the above eight images resulting in the fact thatextracting secret message takes time beyond four minutes.

## 5. CONCLUSION

The application program successfully implementing PVD method which modifying message inserting process on the pixel with spiral pattern.

The image before and after message insertion process has relatively same quality. It is clearly evident in the image of "Ungu Cahaya" based on survey as well as MSE and PSNR calculation is proved that it has good quality after message insertion.

The results of this study and survey show that using method of Spiral PVD, the quality of the produced image is relatively good.

The limitations of the research are the inserted message is in the form of file .txt and only one message that inserted into the storage medium, under the provisions that the message size must be smaller than the applied storage medium. The medium that is used as storage of the inserted message is an image with the file type of .bmp, .jpg, and.png. and the applied program language is c#.

Further Research are :

- Performing implementation Spiral PVD method on mobile devices.
- Developmend of Spiral PVD modification method without pattern.

## REFRENCES:

[1] Krenn, J.R:.Steganography and steganalysis. http://www.krenn.nl/univ/cry/steg/article.pdf (2004).

[2] Raphael, A.J. and V. Sundaram.: New approaches to ancient crypto-steganography methods.Am.j.Applied.Sci.,9:40-46.DOI: 10.3844/ajassp.2012.40.46.(2012).

[3] Anitha, P.T., M. Rajaram and S.N. Sivanandham.: A hybrid approach for detecting stego content in corporate mail using neural network based simplified-data encryption standard algorithm. Am. J. Applied Sci., 9: 766-771.**DOI:** 10.3844/ajassp.2012.766.771 (2012).

[4] Wu, D.-C., & Tsai, W.-H.: A Steganographic Method for Images by Pixel-Value Differencing. Pattern Recognition Letters 24 (2003), 1-14.

[5] Al-Asmari, A. K., & Al-Ghamdi, O. A., 2006. High Capacity Data Hiding Using Semi-Hexagonal Pixels Value Difference (2006), 1-4.

[6] Wang, C.-M., a, N.-I. W., Tsai, C.-S., & Hwang,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

M.-S., 2007. A High Quality Steganographic Method with Pixel-Value Differencing and Modulus Function. Systems and Software,(2007) 1-9.

[7] Rojali.: Perbaikan dan Evaluasi Kinerja Algoritma Pixel Value Differencing (PVD). Institut Pertanian Bogor (2009).

[8] Mandal, J. K., & Das, D.: Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain. International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4,(2012) 1-11.

[9] Pressman, R. S.: Software Engineering : A Practitioner's Approach. San Fransisco: Mc Graw Hill (2010).

[10] Male, G.M,Wirawan & Setijadi.: Analisa Kualitas Citra Pada Steganography untuk Aplikasi e-Government. Prosiding Seminar Nasional Manajemen Teknologi XV, (2012) 1-9.

[11] Cole Eric.: Hiding in Plain SightSteganography And The Art Of Covert Communication. Wiley Publishing.Wiley Publishing Inc.Indiana USA (2003).