ISSN 2347 - 3983
Volume 8. No. 9, September 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter154892020.pdf
https://doi.org/10.30534/ijeter/2020/154892020

Steganography Using Pixel Value Differencing and Diamond Encoding Based on Android

Ridho Erdika Pratama[1,2], Rojali[3], Afan Galih Salman[1]
[1]Computer Science Department, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia 11480
[2]Mathematics Department, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia 11480
[3]Mathematics Department, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia 11480, rojali@binus.ac.id

ABSTRACT

The PVD method in steganography used to embed secret message to image file by modifying pixel pair value. The addition of Diamond Encoding is to make difference of pixel pair dynamic so the difference in image's pixel can't be seen with naked eye. To make easier for user to choose and share image file, this application will be developed on Android smartphone.

Key words : Android, Diamond Encoding, difference in image's pixel, PVD method

1.INTRODUCTION

The development of technology is now more advanced; more and more people are exchanging information electronically in various ways too. According to a survey of internet users in Indonesia conducted in 2017 shows that the use of services to transfer data between other internet users such as chat and social media is almost close to 90%. With the increasing ease of internet users exchanging information, security in who has the right to access that information is getting more attention, so that not just anyone can get that information.

Various techniques are used to protect confidential information from unauthorized persons, one of which is steganography. The word steganography comes from the Greek word steganos, which means hidden or veiled and graphein, which means to write. In the technique of hiding messages digitally, steganography is a technique of hiding secret messages into a media so that the word becomes unknown. Media commonly used in the form of images or can be called a cover image. The cover image that has been inserted a secret message is called a stego-image.

Today, steganography has evolved and has many methods, one of which is Pixel Value Differencing (PVD) discovered by Wu and Tsai in 2003. The PVD method uses a difference in pixel values with other pixel values, where the difference between the two pixels results will later be used to insert messages on different media that you want to hide. After the word has been added to the message container, the pixel values will change. The cost will vary according to the PVD calculation formula. The development of the pixel value differencing method began in 2007 by Nan-I Wu by combining the modulus function. The PVD algorithm was also developed by Rojali in 2009, using only the difference between two pixels smaller or equal to seven. Marghny H. Mohamed also formed in 2012 by integrating the least significant bit method and the pixel value differencing method.

All developments from steganography techniques have the same goal, namely increasing Peak Signal to Noise Ratio (PSNR), increasing the quantity of data that can be hidden, or increasing the speed of the steganographic process. In 2012 Wien Hong, Tung-Shou Chen, and Chih-Wei Luo developed PVD by combining it with diamond encoding (DE) techniques to select pixel pairs that have a higher difference to produce stego images that produce higher PSNR values. High.

In this final project, an application will be developed on an Android-based smartphone because based on surveys carried out more than 83% of internet users in Indonesia are accessing the internet with smartphones and 75% of smartphone users in Indonesia use Android-based smartphones.

2. RESEARCH METHODOLOGY

Here is a framework for thinking of writing this thesis. This thinking framework is the development of the waterfall model flow in the process of making a process.

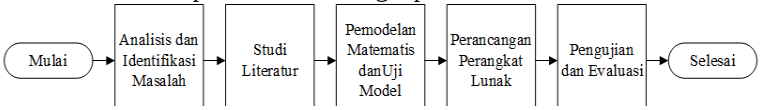

Figure 1: Thinking Framework

These steps are :

1. Problem Analysis and Identification
   In line with technological developments, the process of sending/exchanging data and information becomes effortless and fast. Various methods are used to secure the data transmitted, so it does not fall into the hands of unwanted parties. Steganography is one method that is

suitable to assist in the security of sending information or data.

Steganography is one of the encryption techniques where we insert data into other data. The advantage of steganography is the process of adding hidden information/data so that parties who are not senders and recipients do not know of the process of exchanging information/data, unlike the encryption process where data security is clearly visible so that unwanted parties can learn how to break into data securely encrypted.

2. Literature Study

From the problems above, the author wants to make an application that can increase the security of data transmission on Android-based smartphone users by using the steganography method — claims made in the form of insertion of text data into the cover image. The results, which are not visible to the visible difference between images that have been pasted and before the data are inserted. The results of the insertion of images and text are done by the Pixel Value Differencing and Diamond Encoding methods. And in this literature study, the application will be made in the Java programming language, which will be implemented on the Android application system.

3. Mathematical Modeling and Model Test

At this stage, mathematical modeling will be carried out in accordance with the method of modification of PVD and DE to do the encryption and decryption processes. Afterward, the model test is also done to ensure the encryption and decryption process runs well.

4. Software Design

In the design of this application will use a waterfall model divided into five stages, namely Communication, Planning, Modeling, Construction, and Deployment.

At the Communication stage, the writer identifies the required features by users who will use the steganography application on an Android-based image as well as with its aims and benefits. Next, determine the application will be able to carry out the encryption and decryption process by using the PVD & DE modification method.

The next stage is Planning. At this stage, planning is made from the application following the data collected in the communication process. And at this stage, java programming language planning will also be done, which will be used to build this application.

At the Modeling stage, the user interfaces design and perform display functions as well as the algorithm of developing this application.

The next stage is Construction, where at this stage applications will be developed following the plans that have been made in the previous step. The next step is to implement the Java programming language in the form of code.

After all the above stages have been passed, the final step is Deployment. Lastly, ensure that the application developed has been by the wishes and carried out trials to ensure all functions of the use run smoothly.

5. Testing and Evaluation

After designing the application, the testing and evaluation stages will be carried out. At this stage, the application will be tested whether it can do the encryption and decryption process with the PVD & DE method as well as evaluations such as evaluating the amount of data that can be entered and the speed of the encryption and decryption process.

6. Finish

At this stage, inevitably, the phases of developing mobile steganography applications using the Android-based PVD & DE method have been completed.Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary

3. RESULT AND DISCUSSION

3.1 Pixel Value Differencing and Diamond Encoding

The Edge Adaptive Pixel Value Differencing (EA-PVD) method proposed by [1]in 2008 tried to enter the value of different bits in the pixel pair blocks depending on the difference in the pixel in pixel pair (d_i). Of the range [0.255] which is the value $d_i$can be divided into two low-high (l-h) divisions, the value of which separates the division is called by T_0, so the l-h division can be written as [0, T_0] to division l and [$T_0 + 1$, 255] for division h. The values l and h represent the value of the bits to be embedded if the value d_i entered in the h division, the bits came will be higher than if the value d_i enter the division l

The Diamond Encoding (DE) method proposed by Chao et al. enter the value of bits into pixel pairs$(pi_1, pi_2)$by using an embed digit on the base $B$where $B = 2k^2 + 2k + 1$ with k is an embedding parameter that is an integer value greater than or equal to one. After the k value is determined, a neighborhood set Diamond Characteristic Value (DCV) value can be found$\Psi(pi_1, pi_2)$ by equation of $f(a, b) = mod((2k + 1)a + b, B)$. After entering the value bits (pi_1, pi_2) will be changed to (a, b) which has the same DCV value as (pi_1, pi_2).

In this thesis, the EA-PVD theory will determine the number of bits to be entered, and the DE theory will determine the new value of the pixel pair. The conclusions obtained by Hong et al. state that the PVD and DE theory (PVD-DE) produces a better PSNR value than using the DE theory and the PVD-DE provides better bits per pixel (bpp) values than EA-PVD.

3.2 Encryption Algorithm

The work of PVD-DE method:

1. Read pixel value from coverImage
2. Change the coverImage RGB pixel value to Grayscale
3. Read secretMessage inputted by the users

4. Change all the characters in secretMessage to hexadecimal. Each hexadecimal value is stored in a separate array.
5. Change all hexadecimal to decimal, for example, the character 'a' to array {54,49}
6. Retrieves the array data from the coverImage by the number of characters in the secretMessage * 8 +8
7. Insert a message starting from decimal value of(q)first, by using the first pixel pair ($p_{i,1}$,$p_{i,2}$)
8. Determine the Diamond Characteristic Value (DCV) of the decimal value at which k = 2 and B = 13 with the equation of: $S_{13} = mod(q, 13)$
9. Determine the neighboorhood setΨ($p_{i,1}$,$p_{i,2}$) with the equation of:
$$f(a,b) = mod((2k+1)a + b, B)$$
10. Find the value of $f(a,b)$ That has the same value as S_{13} , value $f(a,b)$ which turns to new pixel pair.
    a. Find the remaining value of q with the equation of $q' = (q - S_{13})/13$
11. Repeat steps 8-10 with the value of $q = q'$
12. Repeat steps 8-11 until all decimal values are used up.
13. Repeat steps 8-11 with the decimal value of(55,102)
14. Display images from the encryption process as steganoImage.

3.3 Decryption Algorithm

Retrieving secret messages from steganographic images that have been pasted with PVD-DE data is done by means of:

1. Reading the pixel value from steganoImage
2. Taking the value of pixel pair($p_{i,1}$,$p_{i,2}$)
3. Use the equation of: $f(\text{pi},1,\text{pi},2) = mod((2k+1)\text{pi},1 + \text{pi},2, B)$
   with k = 2 and B = 13, that holds the value of $f(\text{pi},1,\text{pi},2)$ to certain array
4. Repeat the step 3 until the decimal value meet (55,102)
5. By using the equation:
$$q = \sum_{i=1}^{n-1} \left(g_i \prod_{j=0}^{i-1} \times b_j \right) + g_0$$
   Where $\sum g_i$ (sigma g_i) is the sum of $f(\text{pi},1,\text{pi},2)$ and $\prod b_j$ (pi b_j) is the result of multiplication from value B then value q which is the decimal value of the hexadecimal secret Message that can be searched.
6. Repeat step 5 until the decimal value goes to(55,102), The applications do not calculate the value
7. Change the decimal value to hexadecimal, then from hexadecimal to secretImage

3.4 Example of the Encryption Process using the PVD-DE method

The following is a calculation of the process that will be performed if given a pixel as follows:

194	194	198	187	179	189	191	193
189	185	185	186	194	204	204	203

With secret messageas: a

1. Change the character 'a' into hexadecimal'61'
2. Change the character '6' and '1' from hexadecimal into decimal as follows:

Hexadecimal	6	1
Decimal	54	49

3. Each decimal character from the table above will be inserted into the picture starting from the upper left pixel pair, and because it uses the value k = 2, each decimal character will be added in 2-pixel pairs as follows:

Decimal character	54	49
Pixel Pair used	(194,194), (198,187)	(179,189), (191,193)

4. Add a decimal value (55,102) to indicate the end of the message.
5. Starting the process of inserting a message with the Diamond Encoding method beginning with the first decimal character, q = 54, because using k = 2, the data will be embedded in base B = 13 so that it can `be written:

$S_{13} = mod(54,13) = 2$…(1)

6. Determine the Diamond Characteristic Value (DCV) value of the pixel pair
   (a,b) = (194,194) with the equation of:
   $f(a,b) = mod((2k+1)a + b, B)$…(2)

   Until a pixel pair is found that has a value$f(a,b) = S_{13} = 2$ as can be seen in figure 2

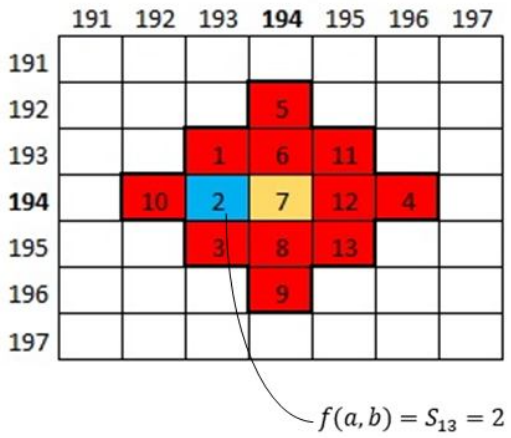

Figure 2: Process of Diamond Encoding

With the details of the PVD value calculation as follows:

$f(192,194) = 10$ $f(194,195) = 8$
$f(193,193) = 1$ $f(194,196) = 9$
$f(193,194) = 2$ $f(195,193) = 11$
$f(193,195) = 3$ $f(195,194) = 12$
$f(194,192) = 5$ $f(195,195) = 13$
$f(194,193) = 6$ $f(196,194) = 4$

$$f(194,194) = 7$$

So, it can be concluded pixel pair (194,194) changed to (193,194)

7. Calculates the remaining decimal values: $q' = (54 - 2)/13 = 4$
8. Repeat steps 4&5 so the value of q'inserted in pixel pair(198,187). The new value of q' will be 0, the decimal value of 54 is fully inserted.
9. Repeat steps 4 through 7 so that a decimal value of 49 can be inserted in the pixel pair (179,189) & (191,193)
10. Repeat steps 4 through 8 for decimal (55,102) using the next pixel pair
11. The pixel value after inserting the character 'a' will be like the following:

1	1	2	1	1	1	1	1
1	1	1	1	1	2	2	2

3.5 Example Decryption Process using the PVD-DE method

Next is the decryption process using data obtained from the encryption process above with the pixel values as follows:

193	194	200	187	180	189	191	192
190	184	185	184	193	203	205	204

With the details of the decryption process with the values, k = 2 and B = 13 as follows:

1. Take the first pixel pair (193,194), then use the equation of (2) thus, it is obtained:
$$f(193,194) = mod((2.2 + 1)193 + 194,13) = 2$$
2. Repeat for the first 4-pixel pairs:
$$f(200,187) = 4$$
$$f(180,189) = 10$$
$$f(191,192) = 3$$
3. By using the equation:
$$q = \sum_{i=1}^{n-1} \left(g_i \prod_{j=0}^{i-1} \times b_j \right) + g_0$$
We can calculate the decimal value of hexadecimal as follows:
$$q = (4,2)_{(13,13)} = (4 \times 13) + 2 = 54$$
$$q = (3,10)_{(13,13)} = (3 \times 13) + 10 = 49$$
4. Values 54 and 49 are decimal values of '6' & '1'. The number '61' is the hexadecimal of the character 'a.'
5. Repeat steps 1-4 for the next 4-pixel pairs, it will produce a decimal value (55.102) that value indicates that the message has ended and does not need to be changed to hexadecimal.

3.6 Analysis

In conducting experiments, carried out trials on eight images that are used as a cover image of the image :

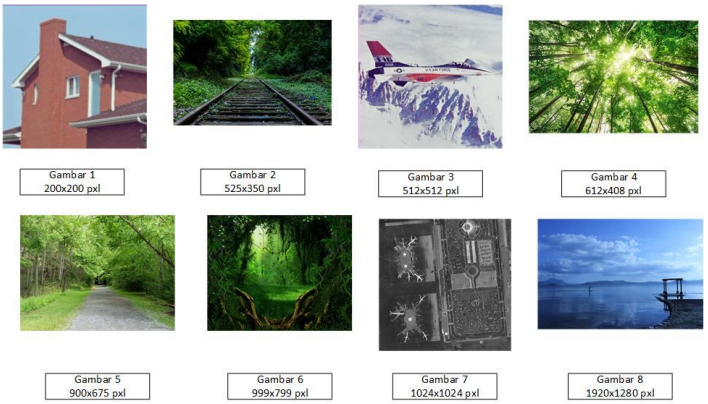

Figure 3: Cover Image and image size

The eight images will be inserted with a secret message with the number 652 characters as follows:

"The Moon is an astronomical body that orbits planet Earth and is Earth's only permanent natural satellite. It is the fifth-largest natural satellite in the Solar System and the largest among planetary satellites relative to the size of the planet that it orbits (its primary). The Moon is after Jupiter's satellite Io the second-densest satellite in the Solar System among those whose densities are known.

The Moon is thought to have formed about 4.51 billion years ago, not long after Earth. The most widely accepted explanation is that the Moon formed from the debris left over after a giant impact between Earth and a Mars-sized body called Theia."

3.7 Evaluation Comparison of Storage Capacity with PSNR Value

The evaluation is intended to determine whether there is an influence between storage capacity and PSNR values. First, the storage capacity of all images used for assessment will be calculated, after the storage capacity is obtained then the PSNR calculation evaluation will be carried out to find out with the same secret message whether the size of the capacity affects the PSNR value.

PSNR Calculation Formula

$$PSNR = 10.\log\left(\frac{MAX^2}{MSE}\right) MSE$$
$$= \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - I'(x,y)]^2$$

Where: MSE = Mean Square Error Stego-Image Value , M = Length of cover image (pixel), $I(x,y)$ = ixel value from cover image, N = Width of stego-image (pixel) , $I'(x,y)$ =

pixel value from stego-image, MAX = the maximum value of the image pixel used in the picture is 255.

Table 1: PSNR Storage and Calculation Capacity

Image	Number of Pixel Images	Storage Capacity in Characters	PSNR
Image 1	40000	4999	57.23
Image 2	183750	22967	63.13
Image 3	249696	31211	64.63
Image 4	262144	32767	64.94
Image 5	607500	75936	68.38
Image 6	798201	99774	69.50
Image 7	1048576	131071	70.84
Image 8	2457600	307199	74.60

From the above table, it can be concluded that by using the PVD-DE method, larger storage capacity will result in a higher PSNR value as well.

3.8 Evaluate Storage Capacity With Encryption Time

This evaluation is intended to determine whether differences in the size of the image affect the time of the encryption process.

Table 2: Storage Capacity and Encryption Time

Image	Storage Capacity in Characters	Encryption Processing Time (ms)
Image 1	4999	22
Image 2	22967	22
Image 3	31211	23
Image 4	32767	21
Image 5	75936	23
Image 6	99774	22
Image 7	131071	22
Image 8	307199	22

From the above table, it can be concluded that by using the PVD-DE method and encrypting the process with the same secret message, the amount of storage capacity does not affect the encryption process time.

3.9 Evaluate Decryption Times and Hidden Messages

This evaluation is done to get the time needed to get the hidden message in the image that has undergone the encryption process and to find out whether the word is inserted = with the message obtained for each image.

Table 3: Decryption Times and Hidden Messages

Image	Decryption Process Time (ms)	Hidden Message = Inserted message
Image 1	23	yes
Image 2	22	yes
Image 3	21	yes
Image 4	22	yes
Image 5	23	yes
Image 6	21	yes
Image 7	21	yes
Image 8	22	yes

From the above table, it can be concluded that by using the PVD-DE method, all images can return secret messages that have been encrypted correctly, and the amount of storage capacity does not affect the decryption process time.

4. CONCLUSION AND SUGGESTION

4.1 Conclusion

Some conclusions obtained from the writing of this thesis are as follows:

1. The design of image steganography applications with the Pixel Value Differencing and Diamond Encoding methods can answer the user's need to insert messages into the image without making changes to the image and the embedded secret message.
2. Pixel Value Differencing and Diamond Encoding can perform encryption and decryption processes at speeds that are not affected by image file size accompanied by good PSNR.
   In 8 times, the test results with different file sizes obtained an average time for the encryption and decryption process that is evenly distributed.
   The good stegano image quality can be seen from the PSNR value were from 8 times the test results obtained the average PSNR value of 66.65625db. With a PSNR ratio of> 30dB, the stegano image quality can be said to be good.
3. Images generated after the encryption process using the steganoscrip application do not have significant differences with the pictures before the encryption process.
4. In the application of android-based steganography applications, this application already uses the features available in android smartphones such as camera, gallery, and share features. Where the camera and gallery features are used to take cover images, then the sharing feature is used to send pictures resulting from the encryption process. The gallery feature is also used to select the image that will be used for the decryption process.

4.2 Suggestion

Some suggestions made with the possibility of further development are as follows:

1. Further development is recommended to add data types that will be used as secret messages. For example, this method can also be inserted in the audio type data.
2. Develop this method so that you can insert secret messages with higher capacity.
3. Development of Pixel Value Differencing and Diamond Encoding methods in order to insert secret messages into colored image files, because in this application the image must be changed first to the greyscale.
4. Develop this PVD-DE application on a different operating system.

REFERENCES

[1] H. . Yang, C.H., Weng, C.Y., Wang, S.J., Sun, "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 3, pp. 488–497, 2008.