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/ijeter155892020.pdf
https://doi.org/10.30534/ijeter/2020/155892020

Steganography Using Android-Based Five Pixel Pair Differencing and LSB Substitution Method

Albert Hero Tanasal[1,2], Rojali[3], AfanGalih 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

FPPD and LSB Substitution modified method are development of FPPD and LSB Substitution method. The modification of FPPD and LSB Substitution is located at the pixel block that is going to be used to insert the secret message. The pixel block being used is 2x2. The LSB Substitution method is a method to insert the data by changing the last bit of the pixel into the byte of the hidden message. FPPD uses data blocks and calculates the capacity of each blocks, then inserts the hidden message in accordance to the capacity of each blocks. The development of this method is expected to increase the capacity of the plain text without reducing the quality of the data produced. To help users in hiding and sending data, a steganoskrip application using improved PFFD and LSB Substitution method will be developed on Android smartphone.

Key words : FPPD method, hidden message, LSB Substitution, pixel

1.INTRODUCTION

The development of technology and information is currently developing very rapidly, one indicator that proves this is the use of internet media that is multiplying along with the development of technology and information.The development provides many benefits that can facilitate every activity in everyday life[1]. In 2016 Indonesian internet users were recorded as many as 132.7 million users, while in 2017 internet users in Indonesia had reached 143.2 million users, just for information the total population of Indonesia's population was 262 million. This proves that more than half of Indonesia's population are internet media users.

One of the essential uses of internet media is communication. With the internet, we can communicate with other users without the limitations of distance, time, and place. Many companies, governments, or individuals use the internet to exchange information[2]. That is why the security of the information sent is fundamental. It is this information security that can guarantee that information sent via the internet as intended. One way that can be used to ensure the safety of information or data is to secure data using steganography [3].

There are various methods of steganography that are used to ensure data security, one of which is Tri-way Pixel Value Differencing (TPVD)[4]. This method converts the plaintext in the form of an image into pixel blocks of data. After that, the data blocks will be inserted hidden messages that you want to hide. In addition to the TPVD method, there are also the Least Significant Bit (LSB) methods. In this method, the last bit of the plaintext will be changed to the bit of the hidden sent message. In the development of TPVD and LSB, Gulve and Joshi developed the Five Pixel Pair Differencing (FPPD) and LSB Substitution. In this method, Gulve and Joshi make images (where these images become plaintext) into 2x3 data blocks that do not coincide with hiding messages in the data blocks[5]. So the message you want to hide is contained in the data blocks.

In 2017, Tzu and Yu made a more in-depth study of FPPD and LSB Substitution developed by Gulve and Joshi in the An Improved Data Hiding Method of Five Pixel Pair Differencing Journal and LSB Substitution Hiding Scheme. Tzu and Yu used the FPPD and LSB Substitution method into data blocks 1x3, 2x2, 3x3 and 2x3 (FPPD). And the results obtained, Tzu and Yu wrote that 2x2 data blocks could produce better performance compared to other data blocks[6]. Although the PSNR value of the 2x2 data block is smaller than 2x3, the hiding capacity of the 2x2 block is higher than the 2x3 block. The experimental results also show that 2x2 data blocks can produce higher hiding capacity in complex and smooth images.

The scope of this thesis is using the steganography method of modifying five-pixel pair differencing and LSB substitution, plain text in the form of images, and chipper text in the form of writing.

The primary purpose of doing this thesis is how to apply the modification method of five-pixel pair differencing and LSB substitution to get the results of a good encryption process, and the image of the encryption process does not have a significant difference with the cover image.

2.RESEARCH METHODOLOGY

The frameworkfor this research is the development of the waterfall model flow in creating a process.

The framework has several steps:

1. Problem Analysis and Identification

At this stage the authors analyze the problem, including in the communication stage of the waterfall model, where an increasing number of mobile phone users, especially smartphones accompanied by developments in internet technology that is increasingly developing so that it can reach the wider community, the more data or information will be sent through the internet media. So that various problems arise as follows:

1. How do you increase the security of data to be transmitted over the internet so that it reaches the recipient safely?
2. How do you design an application using the Five Pixel Pair Differencing and Least Significant Bit Substitution methods to improve data security, especially for Android-based smartphones?

2. Literature Study and Learning

Of the problems that arise, the next stage, the authors do a literature study. Where at this stage, the authors study and understand the steps of steganography, especially the Five Pixel Pair Differencing and the Least Significant Bit. Where before the above method was developed first through the Tri-way Pixel Pair Differencing method. Afterward also developed Improved Method of Five Pixel Pair Differencing and Least Significant Bit Substitution where the technique is applied to several different data blocks and produces 2x2 data blocks as data blocks that produce better steganographic results Gupta. As well as in the study of literature, the authors also learn about the java programming language, which will be implemented on an android application system. At this stage, the author also schedules and outlines a flow in this writing. This includes writing theses and making applications.

3. Mathematical Modelling and Model Test

At this stage, including in the Modeling stage of the waterfall model, the authors do mathematical modeling. Where determined mathematical modeling following the modification method of FPPD and LSB Substitution to do the encryption and decryption process. After that, the model test is also done to ensure the encryption and decryption process runs well.

And at this stage also made the design of UML diagrams of the application including use case diagrams, sequence diagrams, activity diagrams, and class diagrams. Lastly, make the design of the display (user interface) of this application.

4. Software Design

After conducting mathematical modeling and model testing, then proceed to the software design stage. This stage includes in the Construction stage of the waterfall model, which means that at this stage, it is the stage of building the application following the plan made at the previous step. The idea is implemented using the help of Android Studio software using the Java programming language.

5. Testing and Evaluation

After designing the software, including in the deployment of the waterfall model, the testing and evaluation stages are also carried out. At this stage, the application will be tested for its ability to secure data using the Modified FPPD & LSB substitution method. As well as an evaluation of the results of the data security process.

6. Finish

At this stage, it is ensured that the steps of developing a mobile steganoscrip application using the Android-based FPPD & LSB Modification method have been completed.

3. RESULT AND DISCUSSION

3.1 Modification of Five Pixel Pair Differencing and LSB Substitution

After the FPPD method proposed in 2015 by Gulve and Joshi[1], T.C. Lu and Y.C. Lu tried using this method by using different pixel block sizes. In the FPPD method, a 2x3 block pixel block is used, while Tzu and Yu apply the technique into 1x3, 2x2, 2x3 and 3x3 pixel blocks to get the best performance from the data hiding process[2].

The conclusions obtained by Tzu and Yu show that experiments on 2x2 data arrays have better results or performance[2]. The PSNR evidence this results greater than 37,916 db and the effects of BPP (Bits per pixel) that exceed 3. Although the PSNR results from pixel blocks are 2x3 larger, but the size of the data can be modified to hide messages on 2x2 larger pixel blocks. Besides, the results of the study also revealed that 2x2 pixel blocks get a large storage capacity for information or data that can be hidden in complex or smooth images.

3.2 Encryption Algorithm

How the FPPD and LSB substitution modification works:

1. Read the pixel value of the cover image
2. Change the cover image RGB pixel value to Grayscale
3. Read secret message inputted by the user
4. Change the value of secret message to binary called hiding bit(b)
5. Retrieve 2x2 array data from cover image

Px_1	Px_0
Px_2	Px_3

6. Use the LSB Method which is to replace the last 3 bits of Px_0 with 3 bits from b to be $\overline{px_0}$
7. Shape 3-pixel pairs, and count each of the differences
   $d_0 = Px_1 - \overline{px_0}$
   $d_1 = Px_2 - \overline{px_0}$
   $d_2 = Px_3 - \overline{px_0}$
8. Using the following table range

Table 1: Range Table

[li, ui]	[0,7]	[8,15]	[16,32]	[33,63]	[64,127]	[128,256]
Hiding Bits (K)	$\log_2 8 = 3$	$\log_2 8 = 3$	$\log_2 16 = 4$	$\log_2 32 = 5$	$\log_2 64 = 6$	$\log_2 128 = 7$
Range	R1	R2	R3	R4	R4	R5

li is the lower value for range table i, and ui is the upper value for range table i.

Determine the Ki value of each pixel pair. Then calculate the average of the K values$avg = \frac{\Sigma k_i}{3}$, if the value of k is a fraction, then k is rounded down.

9. Calculate value dl_i
$$dl_i = d_i \, mod \, 2^{avg}$$
Using the table ranges above, determine the hidding bits and lower bit capacities for each dl_i.
10. Taking value b_i following the capacity for each value dl_i and change into decimal.
11. Calculate the value of *Offset different* from $d_i$and dl_i
$$OD_i = |d_i| - |dl_i|$$
12. Calculate the new different value using the following formula
$$d'_i = \begin{cases} OD_i + l_i + b_i, jika\ d_i \geq 0 \\ -(OD_i + l_i + b_i), jika\ d_i < 0 \end{cases}$$
13. Calculate the value of m_i
$$m_i = d'_i - d_i$$
14. Calculate a new value for each pixel pair
$$(pu_i, pd_i) = (\overline{px_0} - \left\lceil \frac{m_i}{2} \right\rceil, px_i + \left\lfloor \frac{m_i}{2} \right\rfloor)$$
15. Calculate the difference in value between $\overline{px_0}$ dan pu_i. $\overline{px_0} - pu_i$. To determine the smallest distraction value between stego-pixel and original pixel to be used as a reference pixelpu_{min}.
16. Revised the value of $pd'_i$to each pixel
$$pd'_i = pd_i + pu_{min} - pu_i$$
17. Calculate a new value for each pixel px'i
$$px'_i = pd'_i + (\overline{px_0} - pu_{min})$$
So the new pixel value is

Px'_1	$\overline{px_0}$
Px'_2	Px'_3

18. If there is a value px'_i out of bounds $0 < px'_i < 255$ then
18.1 If there is a value $px'_i > 255$ then all the pixels in the block are reduced by 8.
18.2 If there is a value $px'_i < 0$ then all the pixel values in the block are added by 8.
18.3 If steps 18.1 and 18.2 have been carried out and there are still values px'_i that exceeds the limit $0 < px'_i < 255$ then it can be concluded the image is not suitable for the process of hiding the message.
19. If the b value still exists, repeat steps 5-18 until all b values of secretMessage have been hidden
20. Display images from the encryption process as steganoImage.

3.3 Decryption Algorithm

Retrieval of secret messages from steganographic images that have been inserted data with modifications to the FPPD and LSB Substitution can be done by:

1. Read the value of pixel from steganoImage
2. Gathering data array 2x2 from steganoImage

Px'_1	$\overline{px_0}$
Px'_2	Px'_3

3. Shape 3 pixel pairs, and calculate the difference in each pixel pair.
$d'_0 = Px'_1 - \overline{px_0}$
$d'_1 = Px'_2 - \overline{px_0}$
$d'_2 = Px'_3 - \overline{px_0}$
4. Determine the value of k'_i from each pixel pair. Then calculate the average of the values of k' and the value of $avg = \frac{\Sigma k'_i}{3}$, if value k' in the form of fractions, then k' round down.
5. Calculate the value of dl'_i
$$dl'_i = d'_i \, mod \, 2^{avg}$$
By using the table range above, lower bits for each dl'_i.
6. Perform the extraction process on $\overline{px_0}$ by using LSB in the last 3 bits $\overline{px_0}$.
7. Calculate the value of hiding bits
$$b_i = dl'_i - l'_i$$
After getting the bi value in decimal, change it to binary
8. The message that is hidden is the result of LSB in step 6 added to the binary value of b_i into step 7.
9. Repeat rare to 2-8 until all messages that have been hidden.
10. After all the binary values from the Secret Message are read, change the binary value into the alphabet using code ASCII
11. Shows the secretMessage.

3.4 Example of the Encryption Process using the modification method of FPPD and LSB Substitution

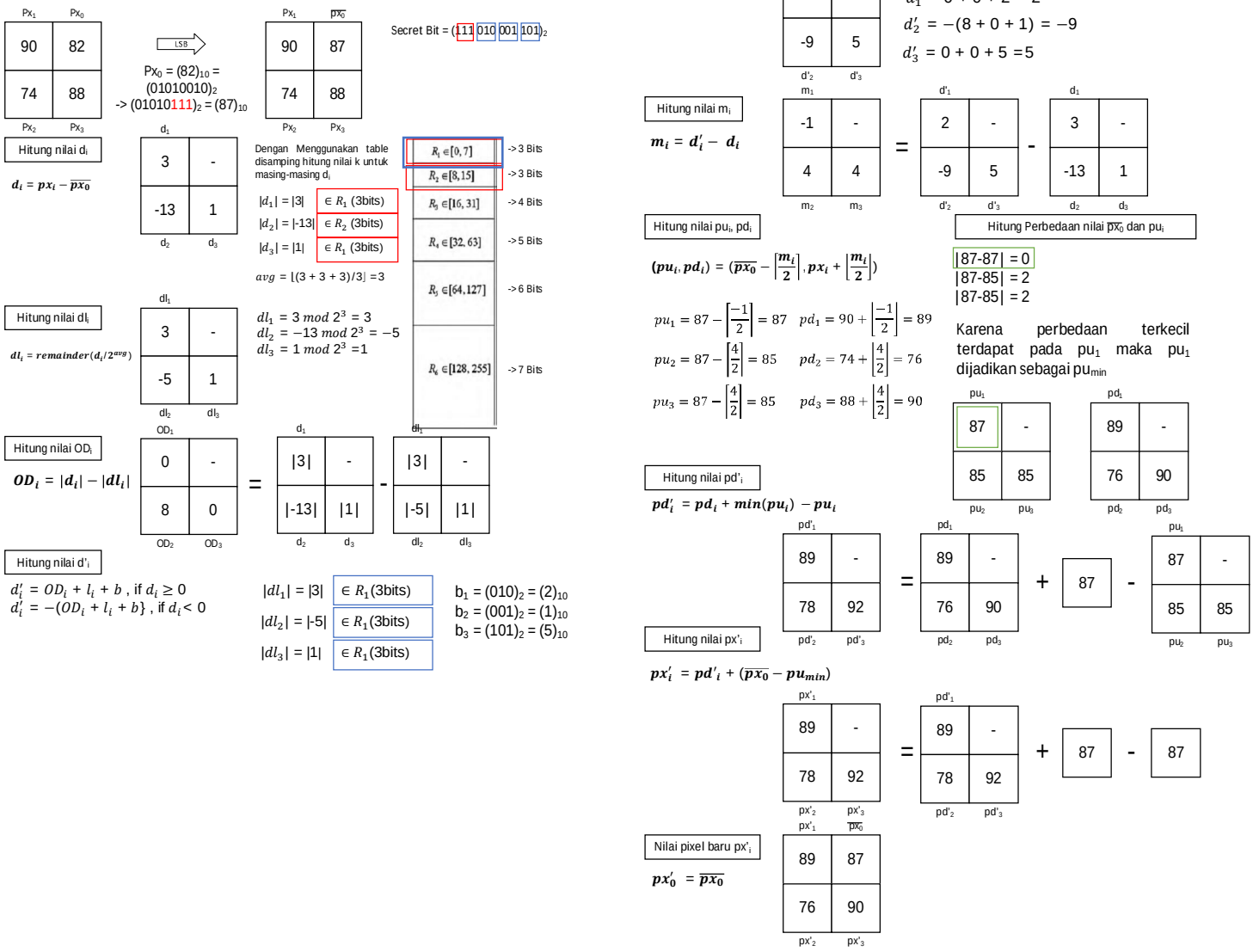

Figure 2: Encryption Process

3.5 Example Decryption Process using the modification method of FPPD and LSB Substitution

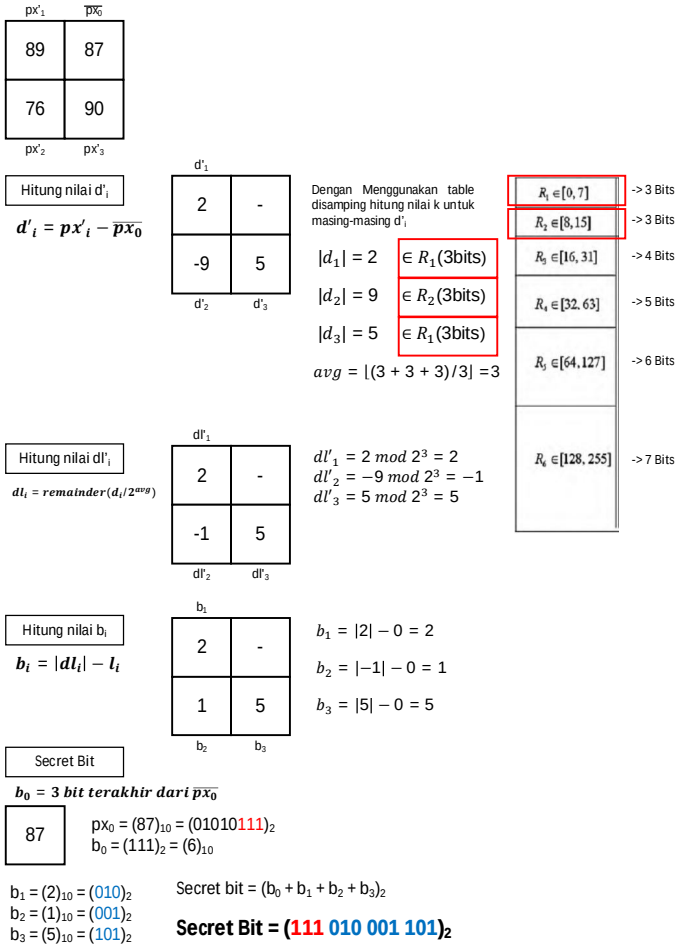

Figure 3: Description Process

3.6 Analysis

In conducting experiments, carried out trials on 8 images that are used as cover image of the image :

Figure 4: Cover Image and Image Size

3.7 Evaluation of Bit Per Pixel Calculations

This evaluation is intended to determine the average secret bit storage capacity in each pixel in the image. The calculation formula for bpp is:

$$Bpp = \frac{capacity}{w\ x\ h}$$

Where w is the width of the image and h is the length of the image.

Following are the results of the bpp calculation

Table 2: Calculation of BPP

3.8 Evaluate PSNR Calculation and Encryption Time

Figure	Storage capacity in bits	Value of Bpp
Figure 1	178866	2.98009
Figure 2	391863	2.99521
Figure 3	3150144	3.00422
Figure 4	788094	3.00639
Figure 5	795006	3.03275
Figure 6	197772	3.01794
Figure 7	196812	3.0033
Figure 8	787287	3.00331

This evaluation is intended to determine the PSNR results that show whether the resulting image is good or not, the indicator that says the results of a good encryption image is an image that has a PSNR value> 30 and the time needed to run the encryption process. This evaluation was carried out on the eight images above, and the message entered was 316 characters..

Calculation Formulas of PSNR

$$PSNR = 10.\log\left(\frac{MAX^2}{MSE}\right) MSE$$

$$= \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - I'(x,y)]^2$$

Where: MSE = Value of *Mean Square ErrorStego-Image* , M = Length of *cover image* (pixel), $I(x,y)$ = pixel value from *cover image*, N = Width *stego-image* (pixel) , $I'(x,y)$ = Pixel value to *stego-image*, MAX = the maximum value of the image pixel used in the picture is 255.

Table 3: Encryption and Calculation Time PSNR

Figure	Time of Encryption Process (ms)	PSNR (db)
Figure 1	1105ms	50.9208
Figure 2	2111ms	60.5076
Figure 3	16173ms	68.3967
Figure 4	4044ms	63.0394
Figure 5	4146ms	61.8971
Figure 6	1082ms	56.9395
Figure 7	1099ms	56.5717
Figure 8	4121ms	61.5175

3.9 Evaluate Decryption Times and Hidden Messages

This evaluation is intended to get the time needed by this application to get hidden messages in images that have

undergone an encryption process and find out whether the messages that are inserted = with the messages obtained for each model.

Table 4: Decryption Time and Hidden Messages

Figure	Time Decryption Process (ms)	Hidden Message = Inserted message
Figure 1	7847ms	Yes
Figure 2	7734ms	Yes
Figure 3	7765ms	Yes
Figure 4	7783ms	Yes
Figure 5	7630ms	Yes
Figure 6	7880ms	Yes
Figure 7	7770ms	Yes
Figure 8	7329ms	Yes

4. CONCLUSION AND SUGGESTION

4.1 Conclusion

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

1. The design of steganoscrip application with the modification method of Five Pixel Pair Differencing and LSB Substitution can answer the user's need to insert a message into the picture and maintain the quality of the image produced after going through the encryption process.
2. Modification of Five Pixel Pair Differencing and LSB Substitution by using 2x2 data blocks can produce a better secret message storage capacity that is accompanied by a good PSNR value.
   An excellent secret message storage capacity can be seen from the BPP value were from 8 times the test results obtained an average BPP value of 3.005401 interpreted as 1 pixel of the cover image can store a minimum of 3 bits of secret message.
   Good stegano image quality seen from the PSNR value were from 8 times the test results obtained the average PSNR value of 59.97381db. With a PSNR ratio of> 30dB, the stegano image quality can be said to be good.
3. The time needed to run the average encryption process is 4235,125 ms.
4. The time required to run the average decryption process is 7717.25 ms.
5. Images generated after the encryption process using the steganoscrip application do not have significant differences with the photos before the encryption process.
6. Steganography can be applied together with smartphone features such as camera, memory, gallery, and share features. Where each of these features is used to take pictures as cover images and stegano images for camera and gallery features and sharing features are used to send images resulting from the encryption 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 plain text. For example, this method can also be inserted in the data type of video or voice recording.
2. Further development is also recommended to add data types that will be used as secret messages.
3. Develop this method so that you can insert and retrieve messages in a faster time.
4. Add a password feature that makes the results of the decryption process read only by people who have the same password.
5. The process of taking pictures through the gallery and turning them into grayscale also needs to be further developed so that the time required to take and convert images to grayscale is not long.
6. Developing this steganoscrip application on different operating systems

REFERENCES

[1] A. A. I. K. G.Dewi, and A. N.Fajar, "**Analysis and Design of KOMINFO Mail Handling System Based on Mobile Application**," International Journal of Emerging Trends in Engineering Research, vol. 8 no. 3, pp 747 – 751, 2020

[2] R. C. Gustilo. R. M. Castillo, N. A. Gonzales, J. G. Raz, and T. J. Tejones. **"Android-based Image and Video Steganography System,"** International Journal of Emerging Trends in Engineering Research vol. 7 no. 9, pp. 346-352, 2019.

[3] H.C Wu, N.I. Wu, C.S. Tsai, and M.S. Hwang, "**Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods,"** Image and Signal Processing, 152, 611–615, 2005

[4] Y.P. Lee, L.C. Lee, W.K. Chen, I.J. Chen, C.P. Chang, and Chang, **"High Payload Image Hiding with** Quality Recovery using Tri-way Pixel-Value Differencing," Information Sciences, 191, 514–225, 2012

[5] A.K. Gulve and M.S. Joshi, **"An Image Steganography Algorithm with Five Pixel Pair Differencing and Grey Code,"** Int. J. Image, Graph. Signal Process., vol. 6, pp. 12–20, 2014.

[6] Tzu-Chuen Lu, and Yu-Ching Lu, **"An Improved Data Hiding Method of Five Pixel Pair Differencing and LSB Substitution Hiding Scheme,"** Adv. Intell. Inf. Hiding Multimed. Signal Process., pp. 67–74, 2016

[7] S. Gupta, **"Information Hiding Using Least Significant Bit Steganography and Cryptography,"** Int. J. Modern Education and Computer Science, Vol.6, pp.27-34, 2012.