Modification Of Least Significant Bit Method With Redundant Pattern Encoding For Protection Of Message Integration From Image Modification

Aldi Wiliar Wira Permana , Silvester Dian Handy Permana, Yaddarabullah

Abstract: Steganography is one way to hide messages on a media image. One method used in steganography is the Least Significant Bit (LSB) method. But in the LSB method there are still gaps to damage the message in the image if the image is modified. The most important aspect of steganography is the level of information hiding. Where it refers to how much the inability of a third party to detect the existence of hidden information. There is a way to avoid this gap by modifying the Least Significant Bit method with Redundant Pattern Encoding. With the RPE method, the gap in the LSB method can be overcome, because this method divides the two parts in the image, namely Patch A with Patch B, then incorporates the redundancy (multiplication) of messages into each patch in the image. The results of this study that modify the Least Significant Bit method with Redundant Pattern Encoding, namely, the image can survive if it undergoes Segmentation, Image Compression and Image Enhancement, where in Image Enhancement if the image experiences Sharpness with a maximum level of 25%, the image cannot survive if it is given Color Image Processing and Noise as a whole on both Patches.

Index Terms: Steganography, Message Insertion, Least Significant Bit, Redundant Pattern Encoding, algorithm modification, Protection Message, Image Modification.

1 INTRODUCTION

Steganography is a method of inserting information on a media image, video or sound. Least Significant Bit (LSB) is one of the methods of Steganography, in this method the message will be inserted into the image placed on the rightmost bits in the pixel data that make up the image (Singla & Scarf, 2012). But in this method there are still weaknesses that is if the image is compressed or modified, the message in the image will be damaged. Therefore, this study discusses the modification of the LSB method with the Redundent Pattern Encoding (RPE) method. so this is done to maintain the integrity of the message if the image has been modified. With the RPE method, the gap in the LSB method can be overcome, because the RPE method divides the two patches in the image and redundancy (multiplies) the message to be hidden, then spreads the message throughout the patch. If the image is modified in one patch, then the message in the picture will not be destroyed, because the message is still stored in another patch (Strata et al., 2010). Based on this, if the image has been modified, the message in the picture will not be damaged because the message is stored at every pixel of the image.

2 LITERATURE REVIEW

Research entitled [1], "The Design and Implementation of Steganography Using the Redundant Pattern Encoding Method with the Advanced Encryption Standard (AES) Algorithm" by (M. A. I. Pakereng et al., 2016) which discusses the development of crime in the world of technology. As an example of the case of hiding messages in the form of address data made by employees of a company engaged in the service of sending goods. Image media can be used as an appropriate choice to store confidential data easily and memorable aesthetically. In this research, an application design is done to insert secret files or messages into an image with *. JPEG format by applying the Redundant Pattern Encoding (RPE) method as message insertion so that the results obtained cannot be manipulated and the AES algorithm for data encryption. Research entitled [2], "Comparative Analysis of the Redundant Pattern Encoding and Discrete Consine Transformation Method as a Steganographic Method in Digital Images" by (Strata et al., 2010) which revealed that information and communication technology is developing rapidly, for example the development of internet networks that enable people to exchanging data / messages through the internet network.

Along with the development of technology, communication and information technology crimes are also developing, as we have heard are hackers, crackers, carders, phreakers and so on. Steganography is one technique that can protect messages / confidential data, steganography has many methods such as LSB, RPE, DCT. This study is intended to compare the RPE method with DCT, and explain the general advantages and disadvantages of the several RPE and DCT methods and how to insert or work to improve the message capacity of the method itself. Research entitled [3], "Data Security Using LSB & DCT Steganography in Images" by (Singla & Scarf, 2012). In this study, using two methods of steganography namely DCT and LSB, and also using cryptographic techniques for the process of public key encryption. This study aims to show that the DCT method has a better Peak Signal to Noise Ratio (PSNR) value and higher capacity compared to other techniques such as LSB, modulus arithmetic and SSB4-DCT. This research also maintains satisfactory security as secret messages cannot be extracted without knowing the decoding algorithm. This is achieved by using a public key. This research combines the two features of Steganography and cryptography.

3 ANALYSIS OF LSB METHOD

The LSB method is the simplest and easiest method of steganography to implement. This method uses the last bits in the whole image bits to be inserted, in the order of bits in a byte that is 1 byte = 8 bits in the image pixel, because the last bit does not make a significant change in the results of the

- *Aldi Wiliar Wira Permana, Informatic Engineering, Trilogi University. E-mail: aldiwiliarwira@mail.com*
- *Silvester Dian Handy Permana, Lecture Trilogi University. E-mail: handy@ trilogi.ac.id*
- *Yaddarabullah, Lecture Trilogi University. E-mail : yaddarabullah@trilogi.ac.id*

inserted image (Hidayat & Hastuti, 2013).

The description of the LSB process can be seen as follows:

1. Read the structure and pixel of the image. In this process, the system reads the pixel size of the image where the pixel will later be converted to binary.
2. Convert the RGB value of the image pixel to binary. In the conversion process, the pixel value will be changed to RGB where each RGB has a value of 255 and will be changed to binary where the last bit will be inserted a message.
3. ASCII to binary conversion. This process is to convert ASCII to binary where every bit in ASCII that has been converted to binary will be inserted into the bit value in the RGB image.
4. Spreading stegotext throughout the image. This process will spread stego text throughout the image, for example the following bit order is a byte of an image. (0010011 1101001 01010100) (1010111 1001001 11011100) (0110010 0101011 01010101)

The message to be inserted is the "H" character which has a binary value "010010110", then the bits of the "H" character will be distributed to the last bit of the image and the following results are obtained: (0010010 1101001 01010100) (1010110 1001001 11011100) (0110011 0101011 01010100) The rightmost bit is the result of the insertion of the "H" character. By replacing the rightmost bit in the pixel of the entire image, then the image does not experience significant changes so the changes cannot be seen in plain view. Because the LSB method replaces the rightmost bits in the entire image pixel, the LSB method has a gap to destroy messages by modifying images that contain secret messages. If the image is modified, the bits in each pixel change, so the message will be destroyed because the bits inserted in the message will change.

4 MODIFICATION OF THE LSB METHOD WITH RPE

Based on the analysis of the LSB method, there are still gaps in the method. Therefore, the LSB method will be modified to cover the gaps in the method, namely the Redundant pattern encoding method. The Redundant pattern encoding method spreads the message to each pixel patch in the image. A method for generating sequences of numbers that are close to the nature of random numbers, is used to select two areas of the image (Patch A and Patch B). Patch is a method for marking areas in an image.

4.1 Message Insertion Process

Modification of the LSB method algorithm using the RPE method is done at the image area selection stage, the distribution of Patch A and Patch B and at the message distribution stage, the flow of the LSB method and RPE method modification algorithm can be seen in Figure 1

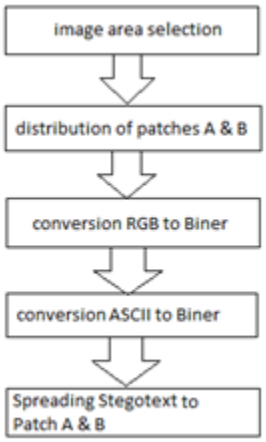

Figure 1 *Insertion Process.*

The description of the process in Figure 1 can be seen as follows:

1. Select pixel size of image. In this process, the system will detect the pixel size in the image, then the system will select the image area into 2 patches.
2. The distribution of Patch A and Patch B. In this process, the Patch will be divided into 2 namely Patch A & Patch B based on the width of the image as a place to store messages as shown in Figure 2. Each box is likened to 1 pixel, each pixel consists of RGB where R has 1 byte, G has 1 byte and B has 1 byte so RGB has a total of 3 bytes. Patch A has 16 pixels, so: 3 bytes x 16 = 48 bytes. 48 bytes results are obtained, which means the size of Patch A, each 1 byte consists of 8 bits so: 48 x 8 = 384 bits. So in Patch A we get 384 bits, where 384 bits is the storage capacity of messages in Patch A. Patch B is the same as the calculation in Patch A which has a message storage capacity of 384 bits.

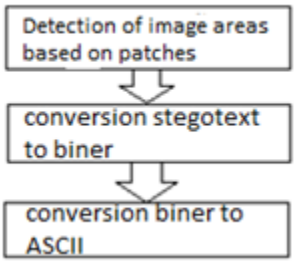

Figure 2. *Distribution of Patches.*

3. Convert RGB values to binary. In the conversion process, the pixel value will be changed to RGB where each RGB has a value of 255 and will be changed to binary where the last bit will be inserted a message.
4. Convert message characters to binary. This process is to convert ASCII to binary where every bit in ASCII that has been converted to binary will be inserted into the bit value in the RGB image.
5. Spread stegotext to Patch A & Patch B. In this process, the system saves every bit of the message character into the rightmost bit in the image such as spreading on the LSB method to 2 Patches namely Patch A & Patch B which have been divided according to step 1.

4.2 Message Extraction Process

The message that is hidden in the image can be revealed

again by extracting it. The position of the byte that stores the message bits can be known from random numbers generated by Peak Signal to Noise Ratio (PRNG). The extraction process can be seen in Figure 3.

***Figure 3**. Extraction Process.*

The description in Figure 3 can be seen as follows:
1. Read the pixel image on Patch A and Patch B.
2. Next change the pixel on each patch to RGB and change RGB into binary form. then take the RGB bits for each pixel in Patch A.
3. Each rightmost bit on the RGB bit will be extracted one by one starting from the bit on R, the bit on G and the bit on B.
After the rightmost bit of each RGB bit is obtained, the next bit will be arranged to form the letters that are inserted in each RGB bit, ie 011100111 The final result "011100111" is the same message segment when hidden in the insertion process. The results are then converted to character form will be the letter "C". The same thing is done to extract the letter "OBA" from the pixel image on Patch A. On Patch B the same thing is done as extraction is done on Patch A.
The secret message bits inserted in the image in Patch A and Patch B can be collected again. Extracted messages have 2 message outputs, namely messages from Patch A and messages from Patch B because at the time of insertion, messages are inserted into Patch A and Patch B.

5 EXPERIMENTAL ANALYSIS

Testing scenarios on the Research Methodology are conducted using 5 ways, namely Image Enhancement, Color Image Processing, Image Compression, Segmentation and Noise with different test variables. The picture that has been inserted message will be tested using these 5 methods, based on the results of the experiment an output will be generated which will determine whether the program is successful or not.

1. Image Enhancement

***Table 1.** Image Enhancement*

No.	Image	Sharpness					Softness					Brightness					Contrast				Grayscale
		5 %	10 %	15 %	20 %	25 %	5 %	10 %	15 %	20 %	25 %	5 %	10 %	15 %	20 %	5 %	10 %	15 %	20 %	
1.	Image A	√	√	√	√	√	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2.	Image B	√	√	√	√	√	X	X	X	X	X	X	X	X	X	X	X	X	X	X
3.	Image C	√	√	√	√	√	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4.	Image D	√	√	√	√	√	X	X	X	X	X	X	X	X	X	X	X	X	X	X
5.	Image E	√	√	√	√	√	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Based on tables 1, Image Enhancement modifications made using the LSB method and the LSB method that has been modified with RPE, the results are obtained that the LSB method cannot protect the message that has been inserted into the image from the Image Enhancement image modification, whereas with the method LSB modified with RPE can still protect the message that is inserted from Image Enhancement image modification if the image experiences Sharpness. The cause of the failure in the modification of Image Enhancement is because the image pixels have changed completely from the lowest level of 5% to 25%, but the LSB method that has been modified with RPE managed to protect the message from Sharpness modification, because the pixels contained in one patch the image does not change so that the message in the Pixel remains intact.

2. Color Image Processing

***Table 2**. LSB & RPE Color Image Processing Results*

No.	Image	*Patch* A Black Block					*Patch* B Black Block				
		10 %	20 %	30 %	40 %	50 %	10 %	20 %	30 %	40 %	50 %
1.	Image A	√	√	√	√	√	√	√	√	√	√
2.	Image B	√	√	√	√	√	√	√	√	√	√
3.	Image C	√	√	√	√	√	√	√	√	√	√
4.	Image D	√	√	√	√	√	√	√	√	√	√
5.	Image E	√	√	√	√	√	√	√	√	√	√

Based on Table 2, the modification of Color Image Processing which is done by using the LSB method and the LSB method that has been modified with RPE, the results are obtained that the LSB method cannot protect the message that has been inserted into the image from the modified Color Image Processing image by giving black block, while the LSB method modified with RPE can protect messages that are inserted from the Color Image Processing image modification both messages that are in Patch A and messages that are in Patch B. In this image modification with LSB method experiencing a total failure, because the message inserted into the entire image so that when the image is modified, the pixel image also changes, therefore the message in the image will disappear.

3. Image Compression

***Table 3.** Image Compression LSB & RPE*

No.	Image	ppi		
		5%	10%	15%
1.	Image A	X	X	√
2.	Image B	X	X	√
3.	Image C	X	X	√
4.	Image D	X	X	√
5.	Image E	X	X	√

Based on Table 3, the modification of Image Compression made using the LSB method and the LSB method that has been modified with RPE, the results are obtained that the LSB method cannot protect the message that has been inserted into the image from the Image Compression image modification with the level of ppi that is different, whereas the LSB method that is modified with RPE can only protect messages that are inserted from Image Compression image modification with a ppi rate of 15%. In the C image modified with a ppi level of 25%, where the results of the ppi level of 25% succeed because the size in the C image is large enough so that it can be modified with a 25% ppi level. In this image modification, the image size changes so that it affects the spread of messages from the LSB method, therefore messages that are

inserted into the image using the LSB method will be destroyed.

4. Segmentation

Table 4. *Segmentation LSB*

No.	Image	*Patch* A	*Patch* B
		Segmentation	*Segmentation*
1.	Image A	√	√
2.	Image B	√	√
3.	Image C	√	√
4.	Image D	√	√
5.	Image E	√	√

Based on Tables 4, the Segmentation modification done using the LSB method and the LSB method that has been modified with RPE, the results are obtained that the LSB method cannot protect the message that has been inserted into the image from the modified Segmentation image by separating objects from the Background, whereas the LSB method that is modified with RPE can protect messages that are inserted from the modified image Segmentation with objects separated from the Background. In this image modification with the LSB method experienced a total failure, because the message is inserted into the entire image so that when the image has been modified Segmentation, there is a loss of pixels in the image, therefore messages in the image will be lost / damaged.

5. Noise

Table 5. *Noise*

No.	Image	*Noise*				
		5%	10%	15%	20%	25%
1.	Image A	X	X	X	X	X
2.	Image B	X	X	X	X	X
3.	Image C	X	X	X	X	X
4.	Image D	X	X	X	X	X
5.	Image E	X	X	X	X	X

Based on Tables 5, Noise modification made using the LSB method and the LSB method that has been modified with RPE, the results are obtained that the LSB method and the LSB method that has been modified with RPE cannot protect the message that has been inserted in the image. In this image modification, giving Noise to the image, can change the arrangement of RGB in the image so that the messages in the picture will be destroyed. Messages that are pasted using the LSB method will also be destroyed, because noise modification greatly damages the overall image.

6 Conclusions And Suggestions

6.1 Conclusions

Based on the discussion that has been explained in the previous chapters, this algorithm modification can survive from some image modifications that have been mentioned in the previous chapters, namely:

1. The picture inserted message with the modification of this algorithm can survive the modification of Image Enhancement if the image only experiences sharpness with a maximum level of 25%.
2. Picture that is pasted by message with modification of this algorithm can survive the modification of Color Image Processing by giving a black color to the image, but cannot survive if giving black color to the image as a whole in Patch A and Patch B.
3. The picture that is pasted message with modification of this algorithm can survive the modification of Image Compression images.
4. The picture inserted in the message with modification of this algorithm can survive the modification of the image segmentation.
5. The picture inserted in the message by modifying this algorithm cannot survive the Noise modification. Based on the above point, it can be concluded that the Algorithm Modification can protect the message from some image modifications that have been tested in the previous chapter, but this Algorithm Modification cannot protect the message from the Noise image modification.

6.2 Suggestions

Based on testing in the previous chapter, the suggestions given for further scientific development are as follows:

1. In future studies, it can modify the LSB method with other methods such as Algorithm and Transformation so that it can better protect the integrity of messages in images that cannot be protected in this study like Noise.
2. In further research, it can add the encryption process so that the security of the message in the picture is more awake. Can be used cryptographic methods such as AES 256 or other cryptographic methods.
3. In future studies it can be to use different generate keys for each file in order to increase the level of security of the message.

ACKNOWLEDGMENT

The authors wish to thank A, B, C. This work was supported in part by a grant from XYZ.

REFERENCES

[1] Anwar., N (2018). Designing Hidden Message Steganography with Matlab Based Least Significant Bit Insertion (LSB) Method.
[2] Arifiansyah, F., Suciati, N., & Wijaya, A.Y. (2012). Implementation of Boosted Steganography Scheme with Image Preprocessing Using Histogram Equalization.
[3] Bhatt, K, R. & Shah, H. (2017). Various Methodologies for Steganography: its Detection and Evaluation.
[4] Champakamala, B.S., Padmini, K., Radhika, D.K (ISSN: 2319-7900) Least Significant Bit Algorithm for Image Steganography.
[5] Elanda, S.K.Y., & Pakareng, M.E.I. (2016). Design and Implementation of Steganography Using the Redundant Pattern Encoding Method with AES (Advanced Encryption Standard) Algorithm.
[6] Hati, K. & Prasetyo, H. Use of the Least Significant Bit (LSB) Method in Making Steganography Applications.
[7] Hashim, M, M., Rahim, M, S, M. (2017). Image Steganography Based on Odd / Event Pixels Distribution Scheme and Two Parameters Random Function.
[8] Hidayat, E.Y. & Hastuti, K. (2013). Steganographic Analysis of the Least Significant Bit (LSB) Method with Quantitative and Random Insertion Quantitative and Visual
[9] brahim, R, N & Ilham, M, S. (2017). Design of Stegagrip

Application with LSB Method Based on RSA Algorithm WEB.
[10] Irvando., Purnama, B., Wijaya, I.S. (2014). Designing of LSB (Least Significant Bit) Technical Steganography in Computer Security.
[11] Jayaram, P., Ranganatha, H, R., Anupama, H, S. (2011). Information Hiding Using Audio Steganography - A Survey.
[12] Juman, K.K. (2008). Steganographic Analysis of Data Security.
[13] Juma'in., Melita, Y. (2011). Image Compression or Image Using Discretecosine Transform.
[14] Jumiran, & Fitri, A. (2014). Insertion of Text In Pictures Using Steganography.
[15] Khan, F., & Gutub, A. A. (n.d.). Message concealment techniques using image based steganography.
[16] Laia, A. (2016). Designing Steganography Learning Applications Using Computer Based Instruction Methods.
[17] Martsanto, S. & Jazuli, W. (2016). Steganography and Document Encryption Techniques to Ensure Information Security and Integrity in Organizational Scope (Case Study at PT Saptawara Teknologi Indonesia).
[18] Nugraha, E.F. (2011) Increasing the Capacity of the Message Inserted by the Redundant Pattern Encoding Method.
[19] Pakereng, M. A. I., Study, P., Informatics, T., Information, F. T., Kristen, U., & Discourse, S. (2016). Design and Implementation of Steganography Using the Redundant Pattern Encoding Method with AES (Advanced Encryption Standard) Algorithm Scientific Article Design and Implementation of Steganography Using the Redundant Pattern Method Encoding with Alg, (672011013).
[20] Pakereng, M. a I., Beeh, Y. R., & Endrawan, S. (2010). Comparison of Steganography Spread Spectrum Method and Least Significant Bit (LSB) Between Processing Time and Image File Size. Spectrum, 6 (1), 68–86.
[21] Saini, G, & Singh, P. (2014). Audio Steganography by LSB Method and Enhanced Security with AES.
[22] Singla, D., & Scarf, R. (2012). Data Security Using LSB & DCT Steganography in Images. International Journal of Computational Engineering Research, 2 (2), 2250–3005.