

# Dynamic Steganography Least Significant Bit with Stretch on Pixels Neighborhood

Muhammad Khoiruddin Harahap<sup>1)</sup>, Nurul Khairina<sup>2)\*</sup>

<sup>1)</sup>Politeknik Ganesha, Indonesia  
Jl. Veteran No. 194 Manunggal, Medan  
<sup>1)</sup>choir.harahap@yahoo.com

<sup>2)</sup>Universitas Medan Area, Indonesia  
Jl. Kolam No. 1 Medan Estate, Medan  
<sup>2)</sup>nurulkhairina27@gmail.com

---

*Article history:*

Received 2 September 2020  
Revised 7 October 2020  
Accepted 9 October 2020  
Available online 28 October 2020

---

*Keywords:*

Least Significant Bit  
Pixel Neighborhood  
Steganography  
Stretch

---

*Abstract*

**Background:** The confidentiality of a message may at times be compromised. Steganography can hide such a message in certain media. Steganographic media such as digital images have many pixels that can accommodate secret messages. However, the length of secret messages may not match with the number of image pixels so the messages cannot be inserted into the digital images.

**Objective:** This research aims to see the dynamics between an image size and a secret message's length in order to prevent out of range messages entered in an image.

**Methods:** This research will combine the Least Significant Bit (LSB) method and the Stretch technique in hiding secret messages. The LSB method uses the 8<sup>th</sup> bit to hide secret messages. The Stretch technique dynamically enlarges the image size according to the length of the secret messages. Images will be enlarged horizontally on the rightmost image pixel block until n blocks of image pixels.

**Results:** This study compares an original image size and a stego image size and examines a secret message's length that can be accommodated by the stego image, as well as the Mean Square Error and Structure Similarity Index. The test is done by comparing the size change of the original image with the stego image from the Stretch results, where each original image tested always changes dynamically according to the increasing number of secret message characters. From the MSE and SSIM test results, the success was only with the first image, while the second image to the fourth image remained erroneous because they also did not have the same resolution.

**Conclusion:** The combination of LSB steganography and the Stretch technique can enlarge an image automatically according to the number of secret messages to be inserted. For further research development, image stretch must not only be done horizontally but also vertically.

---

## I. INTRODUCTION

Steganography can keep secret messages uniquely by using media such as digital images, audio and video. Research on steganography use in digital image media seek to solve the existing challenges. Normally the length of secret messages that can be embedded into digital images is limitless. However, secret messages that are too long will be difficult to embed into small images. The problem is when the length of the messages is unfit with the size of the image so there is an issue with the dynamics of messages to be hidden. This research seeks to find the ratio length of the message and the size of the image.

Research on steganography conducted by Nurul [1] in 2016 used images with a TIFF extension to increase the capacity of a message storage media with multilayer images. In this study, the number of messages that can be inserted is unlimited. When the image of the first layer is full, then the image will automatically add a second layer, and so on until all messages have been successfully inserted. The weakness of this method is that the file capacity becomes very large after a message insertion process is completed because TIFF extension supports multi-layer images.

---

\*Corresponding author

Antoniya Tasheva [2] combined the Modified LSB Insertion method with Contrast Stretching Image Histogram Modification. This method can produce a secret message storage capacity that is greater than the usual LSB method. The research results also showed that the Steganalysis RS could not detect the presence of secret messages, so this method can offer better secret message security. Anju Asokan [3] enhanced satellite image contrast stretching by using a non-linear transformation method. The Bat algorithm used by Anju is more optimal than other algorithms such as the Ant Colony Optimization (ACO) algorithm and Particle Swarm Optimization (PSO). Wenhui Dong [4] proposed a study using the Stretched Natural Vector (SNV) method to recognize facial patterns. The results showed that the SNV method has better recognition accuracy and efficiency than the Principal Component Analysis (PCA) method, Two-Dimensional PCA (2DPCA), and Two-Dimensional Euler PCA (2D-EPCA). Daryanto [5] researched image enlargement using the Nearest Neighbor Interpolation method. From the test results, there are jaggies (jagged edges) in the enlarged image, so that further better image processing is needed. Dengyong Zhang [6] detected an image damage caused by resizing using the Local Tchebichef Moments method. This study shows that the proposed method has a good detection accuracy for the three image resizing techniques, such as scale and stretch method, seam carving method and scaling method.

Wesam Saqer [7] conducted research to hide secret messages using the Indicators-based LSB steganography method using a Secret Key. The insertion of secret messages using the Indicators-based LSB method using a Secret Key is slightly different from the traditional LSB. In this method, a secret message can be inserted more than one bit in one insertion, depending on the indicators used. The results showed that the security of secret messages can also increase, so it is not easy for steganalysis to find the hidden secret messages. Elshazly Emad [8] conducted research related to the LSB steganography method combined with the Integer Wavelet Transform method. The results showed that this method can increase message hiding capacity and also has a high level of security and invisibility. Kemal Tutuncu [9] combined the LSB steganography method with Chaos Theory and Random Distortion. Tests were carried out on 4 steganographic algorithms, namely Least Significant Bit Embedding, Pseudo Random Least Significant Bit Embedding, EzStego and F5. The results show that the security level of this method is very good, because the index generated is completely unpredictable, making it difficult for steganalysis to guess the secret message that has been inserted. Gandharba Swain [10] used Modified LSB Substitution and PVD against Pixel Difference Histogram Analysis in his research. The results of the study can achieve satisfactory bit rate and distortion size values, as well as the resistance of steganography to RS Analysis.

Based on the previous research, we observed that the Stretch technique was able to enlarge the image well without giving a lot of significant color changes, while the Least Significant Bit (LSB) algorithm is able to minimize image changes when a secret message was inserted. We combined the Least Significant Bit steganography method with the Stretch technique to increase the capacity of secret message storage media, especially in digital images. This study will also compare the size of the original image and the stretching stego image, Mean Square Error (MSE), and also the visual feasibility with Structure Similarity Index (SSIM).

## II. LITERATURE REVIEW

### A. Steganography

Stegano is first discovered in the work of Johannes Trithemius with the title "Steganographia". This word comes from Greek (στεγανό-ς, γραφ-ειν) which has to mean "covered writing" [11]. Steganography is a field of computer science that focuses on data security. In steganography, some media help steganography in hiding secret messages [12], such as in a digital image, audio, and video [13] [14]. The more undetectable a secret message contained in a media the more secure the secret message [15].

### B. Least Significant Bit

The Least Significant Bit (LSB) algorithm is one of the algorithms often used by researchers because of its simplicity and uniqueness [16]. The LSB algorithm used in digital images will insert every secret message bit in every last bit of the image pixel (the 8th bit of the image) [17]. The insertion of a secret message in the 8-pixel bit of this image will minimize color change or visual image damage so that it does not invite suspicion from any party [18] [19].

### C. Stretch

Stretch is an activity to represent and change the original size of the image by increasing or decreasing the number of image pixels. In enlarging the size of an image, of course, we must maintain the image feasibility. Several image processing techniques are continuously being developed to maintain the enlarged image feasibility, including sample-rate interpolation-based techniques (i.e., bilinear, bicubic, box sampling, etc.) [20]. Changes in the original size of an

image or changes in the resolution are often needed to show image details, creating documents needs [5] in science such as astronomy, biology, and medicine [20].

*D. Nearest Neighbor Pixel*

Neighbor pixels is a technique used to determine the value of neighboring pixels based on one reference pixel. For one pixel that is selected as a reference, we can find out 8 neighboring pixels based on the following mathematical formula [1]. If pixel P has coordinates x, y where x is a row, and y is a column, then the relationship of neighboring pixels to P (x, y) can be seen in Fig. 1:

$P_4(x-1, y-1)$	$P_3(x-1, y)$	$P_2(x-1, y+1)$
$P_5(x, y-1)$	$P(x, y)$	$P_1(x, y+1)$
$P_6(x+1, y-1)$	$P_7(x+1, y)$	$P_8(x+1, y+1)$

Fig. 1 Neighbors Pixel Illustration

where :

- P (x,y) = Pixels at coordinates x and y
- $P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8$  = The 8 Neighboring Pixels
- x = Pixel rows
- y = Pixel column

*E. Mean Square Error*

Mean Square Error (MSE) can be used to measure how much damage to a stego image (the image resulting from the insertion of a secret message) against the original image that has not been inserted with a secret message [15] [20]. MSE can be calculated by (1).

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

where:

- $I'(x,y)$  = Stego Image Pixel
- $I(x,y)$  = Original Image Pixel
- M = Colomn Size
- N = Row Size
- x = Coordinate column x
- y = Coordinat row y

*F. Structural Similarity Index (SSIM)*

Structural Similarity Index (SSIM) is one of the perceptual techniques used to measure the visual feasibility that has been lost or has decreased. This can happen when an image is compressed or undergoes image processing with various techniques [19].

III. METHODS

The following is a research methodology to combine LSB steganography and Stretch technique in message embedding and message extraction:

*A. Embedding Process:*

The process of embedding messages using the LSB algorithm is carried out by inserting the message bit on every 8<sup>th</sup> bit of the image pixel. The number of message bits should be equal to the number of image pixels. An image must be able to contain all secret messages. Here are the steps to insert a secret message using a combination of the LSB steganography method and the Stretch technique:

- 1) Count how many pixels of a digital image. For example, the original image has a size of 4 x 3, so there are 12 pixels as in Fig.2 :

203	196	223	220
198	223	215	255
231	223	195	253

Fig. 2 Image Original Pixel

- 2) Convert secret messages into binary (as per ASCII rules)  
 Message : N U  
 ASCII : 01001110 01010101
- 3) Compare the length of the secret message with the size of the digital image  
 Bit of Secret Message : 16 digit  
 The number of image pixels : 12 pixel
- 4) If the message bits are more than the number of image pixels (message bits > image pixels), then perform the Stretch technique on the original image
- 5) Stretch technique can be done by:  
 Identifying the value of x, y, and the number of image pixels:  
 $x = 4; y = 3;$   
 The number of image pixel =  $x * y = 12$
- 6) Deficiency of pixels = Secret message bits - number of pixels  
 $= 16 - 12 = 4$
- 7) Pixel increments = ceil (Deficiency of pixels / y)  
 $= \text{ceil} (4/3) = \text{ceil} (1.3) = 2$
- 8) New Pixel = Pixel increments + x  
 $= 2 + 4 = 6$
- 9) The number of new pixels resulting from the Stretch technique = New Pixel \* y  
 $= 6 * 3 = 18$
- 10) You can see that the original image was originally 4 x 3 in size, now it is 6 x 3 in size.  
 The resulting pixels = 6 x 3 = 18 pixels, where the number of pixels is enough to accommodate 16 bits of secret messages, as in Fig.3:

203	196	223	220		
198	223	215	255		
231	223	195	253		

Fig. 3 Stretch Image Results

- 11) From Figure 3. it can be seen that two-pixel blocks do not contain a value, we can use the Nearest Neighbor Pixel to fill in the pixel value so that the image pixel value can be seen in Fig.4:

203	196	223	220	223	220
198	223	215	255	215	255
231	223	195	253	195	253

Fig. 4 Nearest Neighbor Image Results

- 12) Insert a message using the LSB steganography method, so that the image pixel values in binary and decimal can be seen in Fig.5:

202	197	222	220	223	21
199	222	214	255	214	255
230	223	194	253	195	253

Fig. 5 Stego Image

**B. Extraction Process:**

The process of extracting messages that have been inserted into the image can be done by converting the previously obtained stego image back into binary form. Take every 8<sup>th</sup> bit of the image pixel so that the message bit is obtained and can be seen in Table 1.

TABLE 1  
SECRET MESSAGE EXTRACTION RESULTS

Message	Extraction		
Original Message	01001110	01010101	
	N	U	
Secret Message	01001110	01010101	11
	N	U	-

IV. RESULTS

After carrying out the embedding and extraction process using the LSB steganography method and the Stretch technique, the test results in this study can be seen in Table 2 and Table 3. Table 2 contains the test of the LSB steganography method combined with the Stretch technique. The test is done by comparing the change in the size of the original image with the stego image from the Stretch results, where each original image tested always changes dynamically according to the increasing number of secret message characters that have been inserted. Table 2 also contains the MSE and SSIM test results, wherein the MSE test, the test success was only with the first image. The second image to the fourth image experienced an error because these two images did not have the same resolution. Likewise, with the SSIM test results, the success was only with the first image, while the second image to the fourth image also experienced an error. This also happened because these two images also did not have the same resolution.

The tests in Table 3 are the results of tests carried out based on the visual feasibility. The test results show a very clear comparison of the original image and the stego image. The first image does not change, while the second image until the fourth image is stretched horizontally.



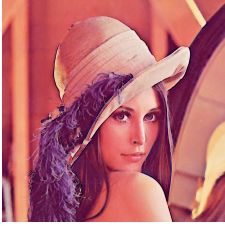





This research shows the dynamization between image size and the size of the secret message to be inserted to overcome the problem of image size limitation that cannot accommodate long messages. The test was measured by the value of MSE, SSIM, and visual feasibility which have been described in Table 2 and Table 3.

TABLE 2  
 LSB STEGANOGRAPHY TEST RESULTS WITH STRETCH TECHNIQUE

No	Message (Character)	Size of Original Image	Size of Stego Image	Image Size Comparison	MSE	SSIM
1	100	50 x 50	50 x 50	1 : 1	0.0	0.99999999
2	500	50 x 50	80 x 50	1 : 1.6	Error	Error
3	1000	50 x 50	160 x 50	1 : 3.2	Error	Error
4	10000	50 x 50	1600 x 50	1 : 32	Error	Error

Note: Error is mean "The images do not have the same resolution"

TABLE 3  
 COMPARISON OF THE VISUAL FEASIBILITY OF THE ORIGINAL IMAGE AND THE STEGO IMAGE

No	Original Image	Stego Image
1		
2		
3		
4		

## V. DISCUSSION

This research is a development of previous research conducted by Nurul [1] [18]. Nurul[1] used the Two-Sided Side Match method with images with the TIFF extension to overcome the problem of the limitations of messages inserted into digital images [1]. The results showed that secret messages can be inserted without a limit. The weakness of this research lies in the large size of the resulting stego image file because the image has many layers (multilayer) and the secret message cannot be retrieved 100%. Nurul[18] used the LSB-2 and LSB-3 methods with images with the BMP extension [18]. The results showed that the inserted secret message is still limited to the size of the digital

image. Therefore, to insert a long secret messages, a large image is needed. The strength of this research lies in the ability of the LSB algorithm to retrieve secret messages exactly 100%. This research uses the LSB method and Stretch technique to solve the problem of secret messages on image size. The results showed that secret messages can be inserted unlimitedly and secret messages can be retrieved 100% intact. The weakness of this research lies in the horizontal stretch if there is a longer message being inserted, so that the original image size will no longer be the same as the stego image size. The difference in the size of the original image and the stego image can raise suspicions that there is a secret message inserted into the digital image.

In terms of data security, this research can be used for both the sender and the receiver of the message, because secret messages can be retrieved 100%. This research can be a variation and can also be a solution in solving the problem of message limitations on the size of digital images.

The strength of this research lies in the ability of the image to accommodate an unlimited number of secret messages, as well as the dynamics between the image size and the length of the secret message. The limitation of this research lies in the size difference between the original image and the stego image, this affects the visual feasibility, the horizontal image widening, and the error value obtained in the MSE and SSIM calculations.

## VI. CONCLUSIONS

This study aims to see the dynamics between the image size and the length of the secret message to be inserted. This study uses a combination of the Least Significant Bit algorithm and the Stretch technique. The results showed that there was a change in the image size horizontally according to the size of the message inserted. The significant difference in the size of the original image and the stego image is very influential on visual feasibility. The more messages inserted, the more visible the difference in the size of the stego image to the original image. The difference in the size of the original image and the stego image also results in an error value in the MSE and SSIM calculations.

This research is able to overcome the problem of the limited length of the secret message to the size of the digital image, where the digital image can accommodate an unlimited number of secret messages. The combination of LSB steganography and the Stretch technique can enlarge an image automatically according to the number of secret messages to be inserted. An image that is stretched will produce an error value in the MSE and SSIM tests because MSE and SSIM only test images that have the same resolution.

For further research development, a stretch on an image must not only be done horizontally but also can be done proportionally both horizontally and vertically. This is expected to minimize the size difference between the original image and the stego image and reduce the suspicion of steganalysis. To increase the resistance of secret messages against steganalysis attacks, in the future this research can be combined with the Modified LSB Insertion Method with Contrast Stretching algorithm.

## REFERENCES

- [1] N. Khairina, "Analisis Steganografi Metode Two-Sided Side Match," *Journal of Computer Engineering, System and Science (CESS)*, vol. 1, no. 2, pp. 7-11, 2016.
- [2] A. Tasheva, Z. Tasheva and P. Nakov, "Image-Based Steganography Using Modified LSB Insertion Method with Contrast Stretching," in *International Conference on Computer Systems and Technologies*, Ruse, Bulgaria, 2017.
- [3] A. Asokan, D. E. Popescu, J. Anitha, and D. J. Hemanth, "Bat Algorithm Based Non-linear Contrast Stretching for Satellite Image Enhancement," *geosciences*, vol. 10, no. 78, pp. 1-12, 2020.
- [4] W. Dong and S. S.-T. Yau, "A Novel Image Description With the Stretched Natural Vector Method: Application to Face Recognition," *IEEE*, vol. 8, pp. 100084-100094, 2020.
- [5] Daryanto, "Aplikasi Pembesaran Citra Menggunakan Metode Nearest Neighbour Interpolation," *Jurnal Sistem dan Teknologi Informasi Indonesia (JUSTINDO)*, vol. 1, no. 1, pp. 31-35, 2016.
- [6] D. Zhang, S. Wang, J. Wang, A. K. Sangaiah, F. Li and V. S. Sheng, "Detection of Tampering by Image Resizing Using Local Tchebichef Moments," *Applied Science*, vol. 9, no. 3007, pp. 1-10, 2019.
- [7] W. Saqer and T. Barhoom, "Steganography and Hiding Data with Indicators-based LSB Using a Secret Key," *Engineering, Technology & Applied Science Research*, vol. 6, no. 3, pp. 1013-1017, 2016.
- [8] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A Secure Image Steganography Algorithm Based on Least Significant Bit and Integer Wavelet Transform," *Journal of Systems Engineering and Electronics*, vol. 29, no. 3, pp. 639-649, 2018.
- [9] K. Tutuncu and B. Demirci, "Adaptive LSB Steganography Based on Chaos Theory and Random Distortion," *Advances in Electrical and Computer Engineering*, vol. 18, no. 3, pp. 15-22, 2018.
- [10] G. Swain, "High Capacity Image Steganography Using Modified LSB Substitution and PVD against Pixel Difference Histogram Analysis," *Security and Communication Networks*, pp. 1-14, 2018.
- [11] Y. Inan, "Assesment of the Image Distortion in Using Various Bit Lengths of Steganographic LSB," in *ITM Web of Conferences*, Polandia, 2018.

- [12] M. Hussain, A. W. A. Wahab, N. Javed and K.-H. Jung, "Hybrid Data Hiding Scheme Using Right-Most Digit Replacement and Adaptive Least Significant Bit for Digital Images," *Symmetry*, vol. 8, no. 41, pp. 1-21, 2016.
- [13] M. Li'skiewicz, R. Reischuk and U. Wölfel, "Security Levels in Steganography Insecurity does not Imply Detectability," *Theoretical Computer Science*, pp. 1-15, 2017.
- [14] A. Pradhan, K. R. Sekhar and G. Swain, "Digital Image Steganography Using LSB Substitution, PVD, and EMD," *Mathematical Problems in Engineering*, pp. 1-12, 2018.
- [15] N. Khairina, M. K. Harahap and J. H. Lubis, "The Authenticity of Image using Hash MD5 and Steganography Least Significant Bit," *International Journal Of Information System & Technology*, vol. 2, no. 1, pp. 1-6, 2018.
- [16] K. Joshi, S. Gill and R. Yadav, "A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image," *Journal of Computer Networks and Communications*, pp. 1-11, 2018.
- [17] J. K. Mandal, *Reversible Steganography and Authentication via Transform Encoding*, Springer, 2020.
- [18] N. Khairina and M. K. Harahap, "Menjaga Kerahasiaan Data dengan Steganografi Kombinasi LSB-2 dengan LSB-3," *Sinkron - Jurnal & Penelitian Teknik Informatika*, vol. 3, no. 1, pp. 286-288, 2018.
- [19] G. Chen, H. Zhao, C. K. Pang, T. Li and C. Pang, "Image Scaling: How Hard Can It Be?," *IEEE Access*, vol. 7, pp. 129452-129465, 2019.
- [20] A. Y. Hindi, M. O. Dwairi and Z. A. AlQadi, "A Novel Technique for Data Steganography," *Engineering, Technology & Applied Science Research*, vol. 9, no. 6, pp. 4942-4945, 2019.