Color-based microscopic image steganography for telemedicine applications using pixel value differencing algorithm

Budi Santoso

Engineering Faculty, Dr.Soetomo University, Semolowaru 84th Surabaya, Indonesia

*budi.santoso@unitomo.ac.id

Abstract. There are some ethics in the medical world to keep patient information confidential on every result of medical observations and analysis. Therefore, steganography technique is an alternative to conceal sensitive text information on a medical image in the telemedicine system process. Research on steganography using Simple LSB-Substitution and other algorithm has been available but in this study, the implementation of steganography was designed to hide text in color medical images before being sent through the telemedicine system. Sensitive text is hidden in medical images using the Pixel Value Differencing (PVD) algorithm. The main purpose of using this algorithm is to maintain the peak signal to noise ratio (PSNR) and mean square error (MSE) of the steganography image result. As a result, the PSNR value can be maintained at the 57.98dB for 10KB hidden text, and lower MSE at 0.05 for high-density object microscopic image.

1. Introduction

The confidentiality of information, especially the personal data of patients and the results of medical diagnosis, must be maintained, in accordance with the code of ethics in the medical world. Meanwhile, the development of communication technology has made possible the process of diagnosis and remote medical observation, where patients and medical experts are not in one place - or commonly referred to as telemedicine. Because of the range of distance between patients and medical experts, the process of transmitting data from diagnoses or observations through media that are already available in communication technology is needed[1]. Media commonly used in data transmission processes are electromagnetic waves (radio propagation) and internet networks. However, the transmission through both media requires an additional process so the data cannot be tapped and only reaches the specified destination.

There are many ways to secure data that can be done in the data transmission process, such as watermarking[2][3][4], cryptography[5][6], and encryption[7][8]. But steganography is one of the more appropriate ways to do because it can send two data formats both images and text, and also simultaneously encoded. According to T.Morkel et.al[9], steganography is defined as the science and art of hiding secret messages (hiding messages) so that the existence of messages is not detected by the human senses. The media used is generally a different medium from the secret information carrier media, this is the function of steganography as a disguise technique using different media to hide confidential information so it is not clearly visible.
1.1. Pixel Value Differencing

Pixel Value Differencing (PVD) is one method used in steganography and operates in the spatial domain. Early research on PVD algorithms was carried out by Wu et al., 2001, by looking for differences in the value of the two closest pixels. The difference is used to determine the amount of data that can be inserted based on the range of the selected table. Based on an analysis of the human visual system which states that the human eye is not sensitive to changes in pixels that have a high contrast but sensitive to changes in pixels that have low contrast. Through these properties, more bits of confidential data can be inserted in pixels that have high contrast values, and fewer bits that can be inserted in pixels with low contrast. This is the basis of the PVD algorithm on steganography.

The PVD algorithm is a system of two-pixel closest search direction as shown in Figure 1:

![Figure 1. PVD algorithm concept](image)

The insertion process in this method is done by comparing two neighboring pixels $P_i$ and $P_{i+1}$ using equation (1).

$$d_i = |P_i - P_{i+1}|$$  \hspace{1cm} (1)

The results of these comparisons are used to find out how many bits can be inserted into the two compared pixels. This method uses the Wu and Tsai schemes to determine the range of the previous pixel comparison. The Wu and Tsai schemes used are $R = \{[0-7], [8-15], [16-31], [32-63], [64-127], [128-255]\}$.

| Range     | 0-7  | 8-15 | 16-31 | 32-63 | 64-127 | 128-255 |
|-----------|------|------|-------|-------|--------|---------|
| Hiding Capacity | 3    | 3    | 4     | 5     | 6      | 7       |

This scheme is used to find out which range is the difference between the two pixels if it is known where the range is, then we can find the lower limit ($U_i$) and upper limit ($L_i$). After knowing the lower limit and upper limit of the range, we can calculate the width of the optimum range ($W_i$) using equation (2).

$$W_i = U_i - L_i + 1$$  \hspace{1cm} (2)

The next step is to find the number of message bits ($t_i$) that can be inserted through equation (2.3).

$$t_i = \lfloor \log_2 (W_i) \rfloor$$  \hspace{1cm} (3)

Message insertion can be done by taking as many as $i$ bits of the message to be inserted. After knowing how many message bits will be inserted, change the message bits to be inserted into decimal ($b$). Then the new difference value is calculated for insertion into the image using equation (4).

$$d'_i = b + L_i$$  \hspace{1cm} (4)

To determine the value of new pixels that have been inserted messages, there are several rules that must be met with equation 5:
\[
(P_i', P_{i+1}') = \begin{cases} 
(P_i + \frac{m}{2}, P_{i+1} - \frac{m}{2}), & \text{if } P_i \geq P_{i+1} \text{ and } d'_i > d_i \\
(P_i - \frac{m}{2}, P_{i+1} + \frac{m}{2}), & \text{if } P_i < P_{i+1} \text{ and } d'_i > d_i \\
(P_i - \frac{m}{2}, P_{i+1} + \frac{m}{2}), & \text{if } P_i \geq P_{i+1} \text{ and } d'_i \leq d_i \\
(P_i + \frac{m}{2}, P_{i+1} - \frac{m}{2}), & \text{if } P_i < P_{i+1} \text{ and } d'_i \leq d_i 
\end{cases}
\]

Where,

\[ m = d'_i - d \] (5)

These processes are carried out continuously until the message bits are all inserted into the image. The process of extracting messages from the stego image using the PVD algorithm begins by sorting all the pixels in the image that has been inserted into the message, according to the way the message is retrieved. Then the difference in the value of the new difference value \( i \) is calculated. The new difference value is used to determine the continuous ranges (R) value that has been defined using the Wu and Tsai schemes. Thus the message that has been inserted is obtained. Based on this information it can be seen how long the secret data is inserted in both pixels so the secret message that has been inserted is retrieved.

1.2. Least Significant Bit (LSB) Steganography

Least significant bit (LSB) insertion is a simple approach to embedding text in a cover image[10]. The least significant bit or the 8th bit from some of the bytes inside an image is changed to a bit of the secret message. When using a color image, a bit of each of red, green and blue color components can be used, since they are each represented by a byte. In this study, steganography using LSB insertion is used as a comparison of the of the PVD steganography algorithm image output. The results of the PSNR comparison of the two methods are presented in the form of tables and graphs.

2. Result and Discussion

In this study 2 groups of test data were used from the ZN Sputum Smear Microscopy Image Database (ZNSM-iDB). The first group contained 20 microscopic images with 1-10 bacilli (low density bacili image) as a result of the Zielh Nielsen staining process. Whereas the second group contained 20 microscopic images with many bundled bacilli (high density bacili image) resulting from the Zielh Nielsen staining process.

![Figure 2. Low object density microscopic image](image1)

![Figure 3. High object density microscopic image](image2)

In each image the process of hiding data is done with text files size of 10KB, 20KB and 30KB. The original image is treated as a cover image at the steganography process, both for the PVD method and the LSB method as a comparison. In each test calculation of each MSE and PSNR is carried out, as the output image quality parameters for steganography.
2.1. Test Results of High-Density Objects (HDO)
Table 4 shows the overall results of steganography using PVD algorithm experiments for groups of images with high object density both for MSE and PSNR measurement.

|   | PSNR (dB) |   | MSE |
|---|-----------|---|-----|
|   | 10KB      | 20KB| 30KB|
| 01 | 58.0525   | 54.9574 | 53.2387 |
| 02 | 58.3286   | 55.3168 | 53.5693 |
| 03 | 58.0522   | 55.0777 | 53.3029 |
| 04 | 58.2875   | 55.0833 | 53.4023 |
| 05 | 57.7827   | 54.7891 | 53.1601 |
| 06 | 57.9707   | 55.1059 | 53.4114 |
| 07 | 58.1378   | 54.8026 | 53.0383 |
| 08 | 58.3399   | 55.3212 | 53.5255 |
| 09 | 58.2085   | 55.2601 | 53.5348 |
| 10 | 58.0876   | 55.0981 | 53.4004 |
| 11 | 58.2389   | 55.0726 | 53.3555 |
| 12 | 57.8192   | 54.8207 | 53.0956 |
| 13 | 58.0412   | 54.9614 | 53.1687 |
| 14 | 58.1478   | 55.0164 | 53.1872 |
| 15 | 56.4596   | 53.5155 | 51.7487 |
| 16 | 58.2181   | 55.1944 | 53.3865 |
| 17 | 58.0486   | 55.1243 | 53.3479 |
| 18 | 57.8385   | 54.8681 | 53.1697 |
| 19 | 57.7224   | 54.7427 | 53.0455 |
| 20 | 58.2444   | 55.2506 | 53.4722 |

2.2. Test Results of Low-Density Objects (LDO)
Table 3 shows the overall results of experiments for groups of images with low object density both for MSE and PSNR measurement.

|   | PSNR (dB) |   | MSE |
|---|-----------|---|-----|
|   | 10KB      | 20KB| 30KB|
| 01 | 57.3763   | 54.3879 | 52.7102 |
| 02 | 57.5083   | 54.5336 | 52.7643 |
| 03 | 57.5004   | 54.4378 | 52.6857 |
| 04 | 57.9232   | 54.9458 | 53.1905 |
| 05 | 58.1048   | 55.1562 | 53.3953 |
| 06 | 57.5526   | 54.5602 | 52.8391 |
| 07 | 57.9757   | 54.8825 | 53.0688 |
| 08 | 57.3742   | 54.3887 | 52.6122 |
| 09 | 57.2537   | 54.2082 | 52.4063 |
From the test results, it was found that the average MSE and PSNR values in the PVD steganography process are better than the results obtained from the LSB steganography method. Whereas in testing the type of microscopic image groups, it was found that the group of images with a low bacilli density had higher MSE values and a lower PSNR. This is advantageous because in a microscopic image with higher bacilli density requires more observation accuracy as one of the basic diagnoses by the medical expert.

![Figure 4. Graph of PSNR PVD Steganography results on HDO](image)

![Figure 5. Graph of PSNR PVD Steganography results on LDO](image)
Generally, both the PVD and LSB methods, the PSNR value decreases when the size of the message stored in the image increases as shown at Table 4.

**Table 4.** Average results of MSE and PSNR steganography using PVD

|                      | Average of MSE |          |          |
|----------------------|----------------|----------|----------|
|                      | 10kb text      | 20kb text| 30kb text|
| PVD Method (HDO)     | 0.054015       | 0.10802  | 0.16141  |
| PVD Method (LDO)     | 0.058375       | 0.11677  | 0.1754   |
| LSB Method (HDO)     | 0.32186        | 0.64036  | 0.956065 |
| LSB Method (LDO)     | 0.32664        | 0.64282  | 0.96246  |

|                      | Average of PSNR (dB) |          |          |
|----------------------|----------------------|----------|----------|
|                      | 10kb text            | 20kb text| 30kb text|
| PVD Method (HDO)     | 57.98502             | 54.96889 | 53.22805 |
| PVD Method (LDO)     | 57.66059             | 54.66161 | 52.89707 |
| LSB Method (HDO)     | 50.09723             | 47.12932 | 45.40128 |
| LSB Method (LDO)     | 50.149575            | 47.19772 | 45.4311  |

3. Conclusion

Based on the results of steganography testing for microscopic color images using the PVD algorithm, it is found that the PVD algorithm produces a stego image with better PSNR than the comparison method (LSB). The best average value is 57.98 dB in the 10KB text. Besides that, it is found that the MSE measurement results on PVD algorithm steganography output with high object density images are even lower, that is 0.05 in the 10KB text.

References

[1] Sachpazidis D I, 2008 Image and Medical Data Communication Protocols for Telemedicine and Teleradiology September.
[2] Zain J and Clarke M, 2005 Security in Telemedicine: Issues in Watermarking Medical Images in 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications.
[3] Eswaraiah R and Reddy E S, 2015 Robust medical image watermarking technique for accurate detection of tamperers inside region of interest and recovering original region of interest 2 p. 615–625.
[4] Eswaraiah R and Reddy E S, 2014 Medical Image Watermarking Technique for Accurate Tamper Detection in ROI and Exact Recovery of ROI Int. J. Telemed. Appl. 2014.
[5] Al-haj A Abandah G and Hussein N, 2015 Crypto-based algorithms for secured medical image transmission IET Inf. Secur. 9 p. 365–373.
[6] Varsha and Chhillar R S, 2015 Data Hiding Using Steganography and Cryptography Int. J. Comput. Sci. Mob. Comput. 4, 4 p. 802–805.
[7] Syawal M F Fikriansyah D C and Agani N, 2016 Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB 4, 3.
[8] Rahim R, Pixel Image Steganography Using EOF Method and Modular Multiplication Block Cipher Algorithm.
[9] Morkel T Elof J H P and Olivier M ., 2005 An overview of image steganography in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005) July 2005.
[10] Champakamala B S Padmini K Professors R D K A and Bosco D, 2014 Least Significant Bit algorithm for image steganography Overview of Steganography Int. J. Adv. Comput. Technol. 3, 4 p. 5.