International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 1, 2020
ISSN: 1475-7192

Pixel Value Differencing and Modulus Function Method for embedded message in Digital Images

Candra Zonyfar[1] Kiki Ahmad Baihaqi[2], Annisa Bela Pertiwi[3]

Abstract---*Image steganography is technique hiding messages into digital images so that secret message unvisually. This research discusses of steganography apply by modulus function algorithm and pixel value differencing (PVD) algorithm. We carried out public datasets image 256x256 and 512x512 constituent. Messages could be embedded in the form of text characters of a certain length. Modulus function and pixel value differencing algorithm manages to hide the message so that no change is seen between the cover object and the cross-sectional image. This research was proven to be successful in the process of recovering secret messages. Evaluation were made using peak signal to noise ratio, mean square error, normalized cross correlation and structural content. From the experimental results, measurement value is based on the level of similarity between cover image and stego object with modulus function method is better with an average normalized cross correlation and structural content 1.0000 and 0.999543 respectively.*

Keywords---*Steganography, Pixel Value Differencing, Modulus Function, Peak Signal to Noise ratio, Mean Square Error, Normalized Cross Correlation, Structural Content*

I. Introduction

Information privacy and security are the most important things in digital communication. The internet is a vast network which can be accessed by anyone from all over the world. This allows one to commit cyber-crimes such as data theft and data manipulation. Therefore steganography is the choice to overcome these problems (Setiadi et al, 2017)

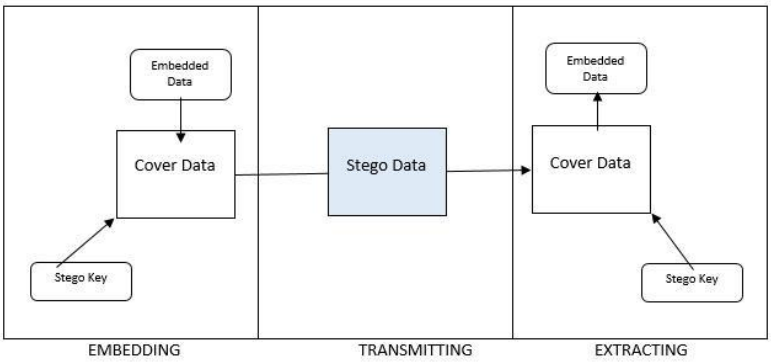
According to (Nurtantio, 2017) that steganography is described as a technique of hiding messages in a container both image and other media such as text, audio media or digital video media. The goal is that other people do not realize there is a message in the media.

An image is one of the media storage of steganography and will be discussed in this study. Experiments were conducted to compare several steganographic algorithms, namely the modulus function algorithm and pixel value differencing by focusing on the element of recovery. An objective assessment is carried out using the Peak Signal to Noise Ratio, Mean Square Error, Normalized Cross Correlation, Structural Content.

II. LITERATURE REVIEW

Universitas Buana Perjuangan Karawang[1,2]
Widyatama University[3]
[1]candra@ubpkarawang.ac.id [2]kikiahmad@ubpkarawang.ac.id

Steganography can be applied to all types of file formats with high level redundancy. Without changes that are easily detected, bits that can be changed are redundant bits. There are four types of file formats used for Steganography as shown in Figure 2.1.



Picture 2.1 Block Diagram Steganography (Hsieh, 2011)

According to Al-azawi (2010), the steganography protocol could be used in OSI model network and thus, the information would be embedded and used in the transmission known as Steganography protocol.

Mean Square Error, Peak Signal to Noise Ratio

Peak signal to noise ratio (PSNR) is the ratio between the maximum value of the measured signal and the amount of noise that affects the signal. PSNR is usually measured in decibels (dB). PSNR is used to compare the quality of the original image before and after the message is inserted. To determine the PSNR, you must first determine the value of the MSE (Mean Square Error). MSE is the average square value between host images and stego images. The smaller the MSE value, the better the steganography product used. That is, the quality of the image after the secret message is inserted is almost the same as the quality of the original image before the secret message is inserted. MSE results are inversely proportional to PSNR results. If the MSE value gets smaller then the PSNR value will be even greater. MSE is defined as follows:

$$\text{MSE} = \frac{1}{MN} \sum_{x=1}^{M} \cdot \sum_{y=1}^{N} (Sxy - Cxy)^2$$

Where x and y are the coordinates of the image, M and N dimensions of the image, Sxy states Stego-image and Cxy is the host-image. In the development and implementation of image reconstruction requires a comparison between Stego-Image and Host-Image (Shi et al., 2019).

$$\text{PSNR} = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

A higher PSNR value indicates that the image is not damaged. So for PSNR values close to 50, the algorithm tested is good and feasible to implement. PSNR can be stated in the formula above.

III. RESULT

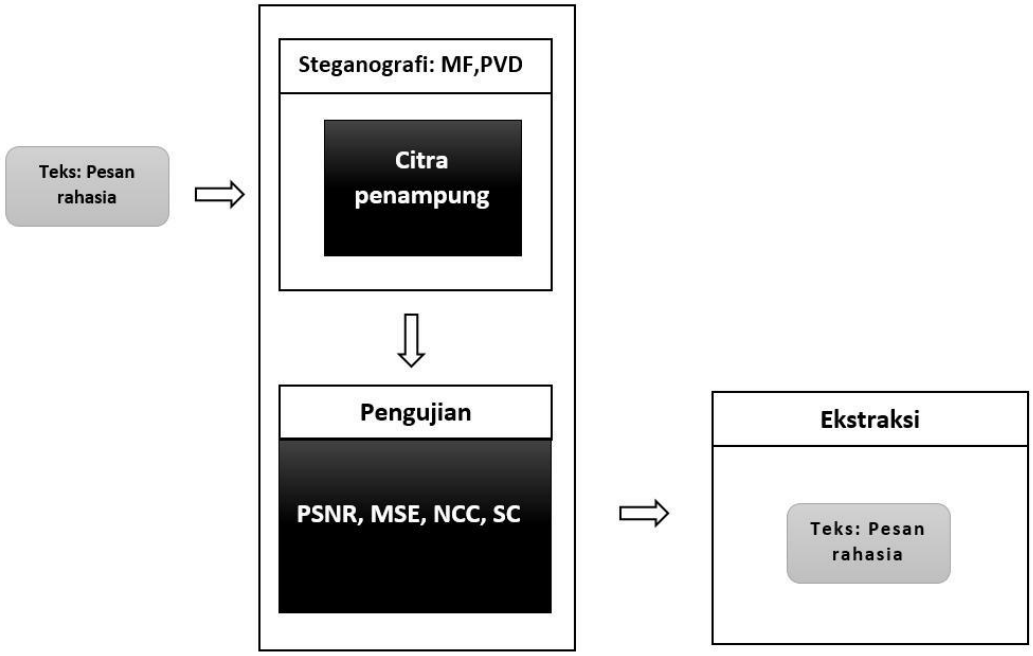
A. Instrumentation and Data

The research instrument consists of software and hardware. The software used includes the Windows 10 Pro 64bit Operating System and MATLAB 2019a for writing code and proving the function modulus algorithm and Pixel Value Differencing whereas the device used is a computer device with Intel i5-7200U specifications and 4GB of memory.

Datasets image source of this research came from sipi.usc.edu. In the form of colour images and gray-scale images, namely: house image, tree image, jelly bean image, moon surface image, air plane image, clock image, chemical plant image that has dimensions: 256 x 256 and 512x512 with tiff format. The secret message that will be inserted is the alphabet text with a range of up to 100 characters.

B. Embedded Message and Extraction

Experiments carried out on the image data that has been acquired. Implementation of steganography algorithm is done by making modeling as shown in the flow chart in Figure 3.2.



Picture 3.1 Method Embedded Message

Host Image	Properties	Stego Image	Properties
	Size: 64,7KB		Size: 64,7KB Embedded message: text alphabet 209 character.

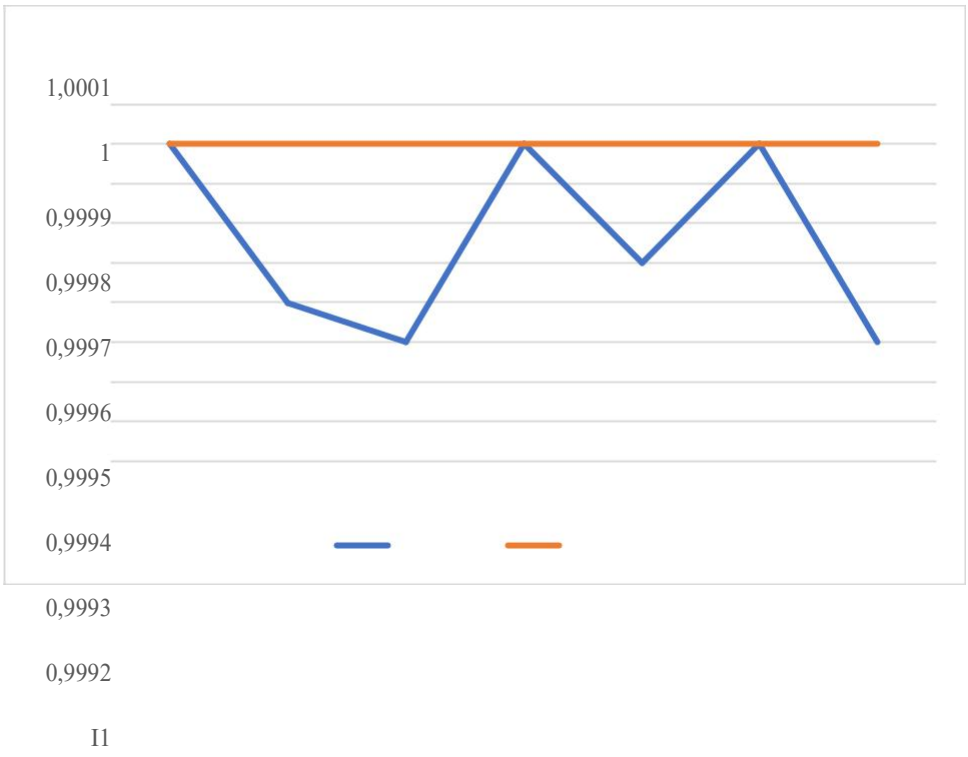
IV. RESULTS

Table 3.1 Results of evaluation of cover image and stego image from message insertion using Pixel value differencing and modulus function methods.

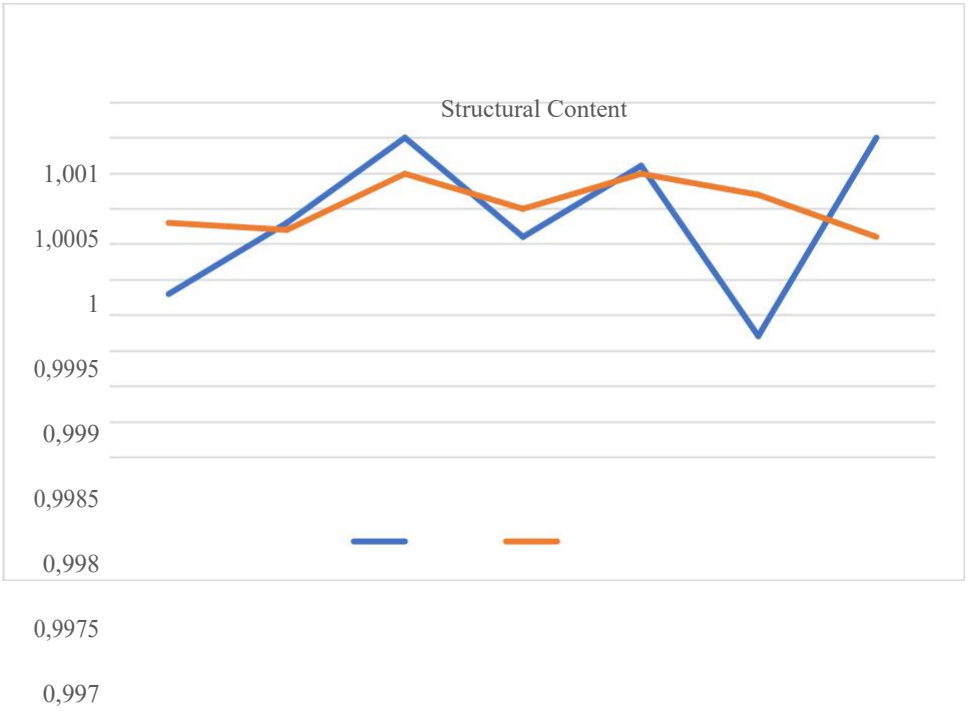
Table 3.1 Result Evaluation

DATA	MSE		PSNR		NCC		SC	
	PVD	MF	PVD	MF	PVD	MF	PVD	MF
I1	63495	30952	0,1034	3,2239	1,0000	1,0000	0,9983	0,9993
I2	63495	23649	0,1034	4,3927	0,9996	1,0000	0,9993	0,9992
I3	63495	255	0,1034	24,0654	0,9995	1,0000	1,0005	1,0000

I4	63495	31501	0,1034	3,1476	1,0000	1,0000	0,9991	0,9995
I5	63495	3623	0,1034	12,5401	0,9997	1,0000	1,0001	1,0000
I6	63495	36944	0,1034	2,4554	1,0000	1,0000	0,9977	0,9997
I7	62575	20379	0,1668	5,039	0,9995	1,0000	1,0005	0,9991



Performance evaluation similarity based Normalized Cross Correlation



0,9965

0,996

I1 I4

SC MF

Performance evaluation similarity based Structural Content

V. Conclusion

The experiments in this study showed the results of steganography using the modulus function and pixel value differencing techniques successfully inserted secret messages in the form of characters well on a cover image. The secret messages can be recovered. The measurement table shows that the modulus function technique has a better similarity than the pixel value differencing technique by looking at the average normalized cross correlation and structural content 1.0000 and 0.99954 respectively. Modulus function and pixel value differencing algorithm manages to hide the message so that no change is seen between the cover object and the cross-sectional image.

REFERENCES

[1] Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida
[2] extensions with huffman code. J. Applied Sci., 10: 436-439.
[3] D. Wu and W. Tsai, “A steganographic method for images by pixel-value
[4] differencing,” vol. 24, pp. 1613–1626, 2003.
[5] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi dan C. A. Sari, “A Performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size,” in International Seminar on Technology for Technology of Information and Communication (iSemantic), Semarang, 2017
[6] Hsieh, Jun-Yi & Pei Wen, Liao. (2011). Antecedents and Moderators of Online Shopping Behavior in Undergraduate Students. Social Behavior and Personality: an international journal. 391271-1280.
[7] 10.2224/sbp.2011.39.9.1271.
[8] Pulung Nurtantio Andono, T.Sutojo, Muljono. (2017). Pengolahan Citra Digital. Andi Offset Yogyakarta ISBN: 9789792963700
[9] https://www.mathworks.com/matlabcentral/answers/59061-how-can-i-embedd-data-to-an-image?s_tid=srchtitle
[10] R. J. Anderson and F. A. P. Petit colas, “On the limits of steganography”. IEEE Journal on Selected Areas in Communications, pages 474–481, 1998
[11] Sembiring, S. (2013). Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File. Pelita Informatika Budi Darma, 4(2), 1–7. http://doi.org/ISSN: 2301-9425 http://sipi.usc.edu/
[12] Shi, X., Dini, A., Shao, Z., Jabarullah, N.H. & Liu, Z. (2019) Impacts of photovoltaic/ wind turbine/ microgrid turbine and energy storage system for binding model in power system, *Journal of Cleaner Production*, 226, 845-857.
[13] Nagaraj, V. Vijayalakshmi dan G. Zayaraz, “Modulo Based Image Steganography Technique against Statistical and Histogram Analysis,” International Journal of Computer Applications (IJCA), vol. 4, no. Network Security and Cryptography, pp. 34-39, 2011