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

[1]Candra Zonyfar [2]Kiki Ahmad Baehaki

[12]Buana Perjuangan Karawang University
[1]candra@ubpkarawang.ac.id [2]kikiahmad@ubpkarawang.ac.id

H.S. Ronggo Waluyo Street, East Telukjambe, Karawang District, West Java,
Indonesia Postal Code 41361

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. Message that 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. And 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.

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

I. Introduction

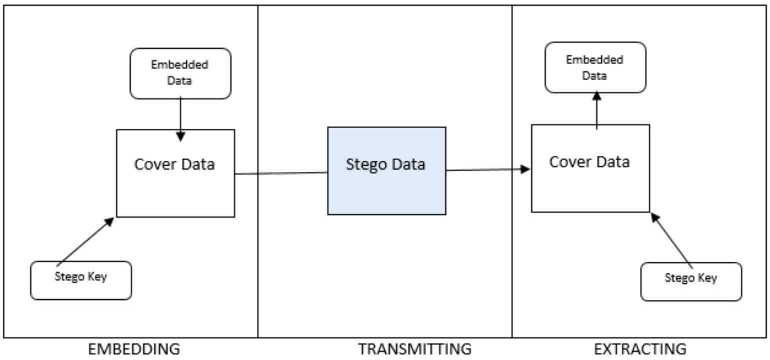
Information privacy and security are the most important things in digital communication. The internet is a vast network which can be accessed by anyone from all over the world. This allows one to commit cyber crimes such as data theft and data manipulation. Therefore steganography is the choice to overcome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

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)

Text messages consist of very little redundant data, so it's not used often. Images are best suited for steganography because they consist of a large number of redundant bits. Audio / video files consist of the same techniques as for image files but there is also a unique technique called masking which hides information that unexpectedly exploits the properties of the human ear. The technique that embeds information in messages and the network control protocol used in network transmission is known as the Steganography Protocol. Steganography can also be used in secret channels in the OSI model network layer (Al-azawi, 2010).

A. Image Steganography

Image Steganography is divided into two categories including different insertion techniques:

Spatial domain: B in BMP: In this technique, the 8th bit is converted into a bit of secret data next to the image. While in a 24-bit image, if a change of bits from each RGB color component is made then 3 bits in each pixel can be saved because it is represented by a byte

LSB in GIF: GIF images require extra attention if used for LSB steganography. The palette approach has the problem that if someone changes the LSB pixels; it produces a completely different color when the index changes to the color palette are made. This problem can be solved by using a gray scale image as an 8-bit gray scale image. GIF provides 256 shades of gray which makes it more difficult to detect color changes.

Transform domain: JPEG compression: In JPEG format, compression is done by changing the RGB color representation into a YUV representation where Y matches lighting (or brightness) and U and V correspond to chrominance (or color). Discrete Cosine Transform (DCT) is used where mathematical transformation will change pixels and spread pixel values to all parts of the new image.

Patchwork: A statistical technique in which excessive pattern coding is used to embed messages in an image. In one patch, pixel intensity increases while the other decreases with the same constant value.

B. 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.

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

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. Instrumentasi dan Data

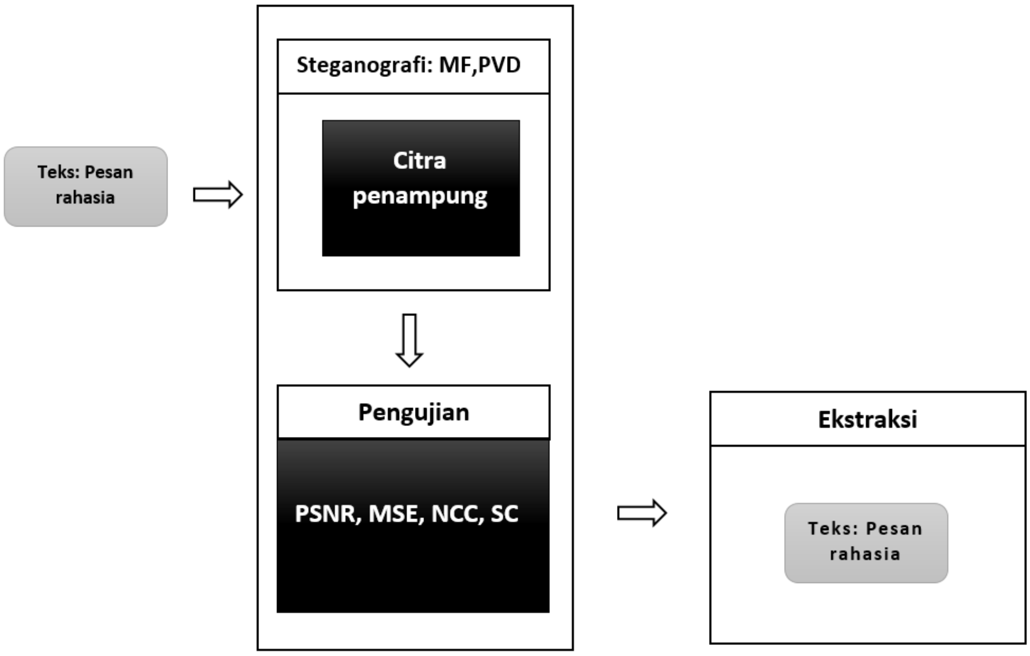
The research instrument consists of software and hardware. The software used includes the Windows 10 Pro 64bit Operating System and MATLAB 2019a for writing code and proving the function modulus algorithm and Pixel Value

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 color images and grayscale images, namely: house image, tree image, jelly bean image, moon surface image, air plane image, clock image, chemical plant image. Has dimensions: 256 x 256 and 512x512 with tiff format. As for 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

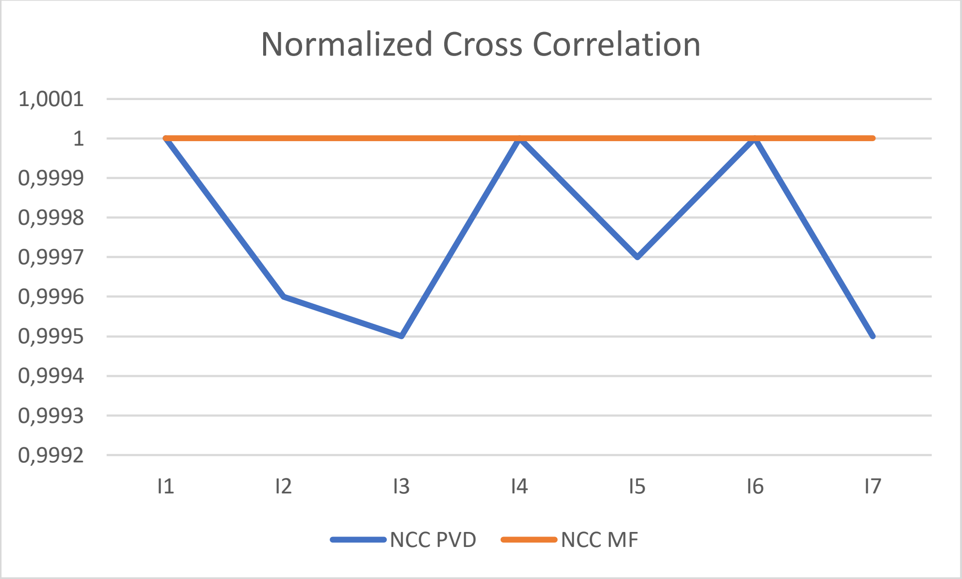
Host Image	Properties	Stego Image	Properties
	Size: 64,7KB		Size: 64,7KB Embedded message: text alphabet 209 character.

C. Evaluation

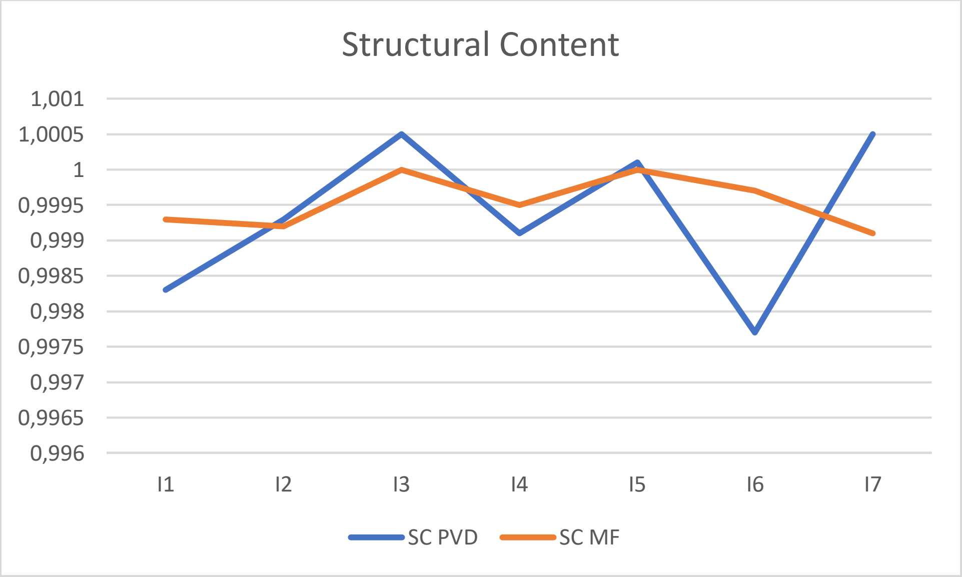
Table 3.1 Results of evaluation of cover image and stego image from message insertion using Pixel value differencing and modulus function methods.

Tabel 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



Performance evaluation similarity based Structural Content

IV. 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. And 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.

DAFTAR PUSTAKA

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

D. Wu and W. Tsai, “A steganographic method for images by pixel-value differencing,” vol. 24, pp. 1613–1626, 2003.

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

Hsieh, Jun-Yi & Pei Wen, Liao. (2011). Antecedents and Moderators of Online Shopping Behavior in Undergraduate Students. Social Behavior and Personality: an international journal. 39. 1271-1280. 10.2224/sbp.2011.39.9.1271.

Pulung Nurtantio Andono, T.Sutojo, Muljono. (2017). Pengolahan Citra Digital. Andi Offset Yogyakarta ISBN: 9789792963700

https://www.mathworks.com/matlabcentral/answers/59061-how-can-i-embedd-data-to-an-image?s_tid=srchtitle

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

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/

V. 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