Darwis2019-ANA_steganography_CST.pdf
Jan 11, 2022
2626 words / 13446 characters

Akmal Junaidi

Darwis2019-ANA_steganography_CST.pdf

Sources Overview

72%

OVERALL SIMILARITY

1	D Darwis, A Junaidi, Wamiliana. "A New Approach of Steganography Using Center Sequential Technique", Journal of Physics: Confere... CROSSREF	66%
2	Sriwijaya University on 2019-10-26 SUBMITTED WORKS	4%
3	debian.mirrors.tds.net INTERNET	<1%
4	latel.upf.edu INTERNET	<1%
5	www.nrc.gov INTERNET	<1%

Excluded search repositories:

None

Excluded from document:

Bibliography
Quotes
Citations
Small Matches (less than 10 words)

Excluded sources:

None

A New Approach of Steganography Using Center Sequential Technique

D Darwis[1,a], A Junaidi[2] and Wamiliana[3,b]

[1]Faculty of Engineering and Computer Science, Universitas Teknokrat Indonesia, Indonesia
[2]Department of Computer Science, Universitas Lampung, Indonesia
[3]Department of Mathematics, Universitas Lampung, Indonesia

[a]darwisdedi@teknokrat.ac.id; [b]wamiliana.1963@fmipa.unila.ac.id

Abstract. The quality of steganographic images can be determined from several aspects. One of the testing techniques on steganography is cropping which is part of robustness testing. Under cropping process, it is possible that the secret message cannot be extracted from the stego-image. This happen because the pixels values on the stego-image embedded message changed and the message content on the stego-image will be lost. In this research we propose a new approach for solving that problem by using the algorithm based on Sequential Technique where the input process starts from the center of the cover. The secret information in the form of image and the cover image is also an image. By using this method, the secret image is safe although the cropping is done from left, right, above or bottom of the stego image.

1. Introduction

Steganography is the science and art of hiding messages that involves two procedures. First process is insertion of the message. In this process a message is hidden in a certain media, such as images, sounds, text, video, audio, the media to hide the message is called steganography cover. The second procedure is to send the Steganography cover to the recipient without arousing suspicion, and also how the recipient can extract the secret message.

Steganography can be applied to digital technologies such as audio, images, videos and every file which are stored in bits [1, 2]. Utilization of Steganography in everyday life can be applied in data exchange over the internet, exchange of data via short messages, social media and data hiding on Personal Computers (PC).

The media of steganography in this study is image. The image quality of steganography is determined from the reliability of the algorithm or technique used during the insertion and extraction process [3]. There are several methods of testing image quality from steganography :

1) Fidelity, refers to the ability to process an image accurately, without any visual distortion or loss of information by measuring values *Peak-Signal to Noise-Ratio* (PSNR) [4].
2) *Robustness*, this method performs attacks in the form of steganalyst or image manipulation by attacking the Stego-image with image processing attacks such as cropping, blur, noise and others [5, 6].

Robustness is a big problem in steganography because in general the stego-image is not resistance to image manipulation attack or the message will be damaged when extraction is done after (Robustness manipulation) [7]. One way to test robustness is to crop the image. The cropping will cause damage to the secret message when the extraction process is carried out because the pixels value in the stego-image change in value. According to previous research, that attacks carried out on the stego-image can make the hidden message on the cover corrupt [8, 9]. One of the most effective attacks on stego-image is cropping attacks. Cropping is one image processing that removes some or pieces of a particular image. In general, the messages hidden in stego-image are at the last bit and are located in the upper left corner of the image. So, when a stego-image is cropped, the message hidden in the image will be difficult to be extracted [10].

The paper is organized as follows: after Introduction given in Section 1, Data dan Methods will be given in Section 2. In Section 3 the Results and Discussion will be provided, followed by Conclusion in Section 4.

2. Data and Methods

2.1. Data

The steganography covers and secret images used for the testing in this study are images with several extension formats namely jpg and png with various sizes and dimensions of pixels. Based on the distribution of color types in the image, for this study only grayscale type images have 256 intensity values [11] to be used. If the image is used as a cover or secret image in RGB format, the image will automatically be converted into a gray scale image.

2.2 Research Methods

2.2.1 Research Framework

The research framework is basically a framework of the relationship between concepts that will be observed or measured through research that will be conducted. Several steps taken to complete this research are Identification Problems, Opportunity, Theory, Approach, Identification & Assessment, Proposed, Validation and Result. More details the concept of the research framework can be seen in figure 1.

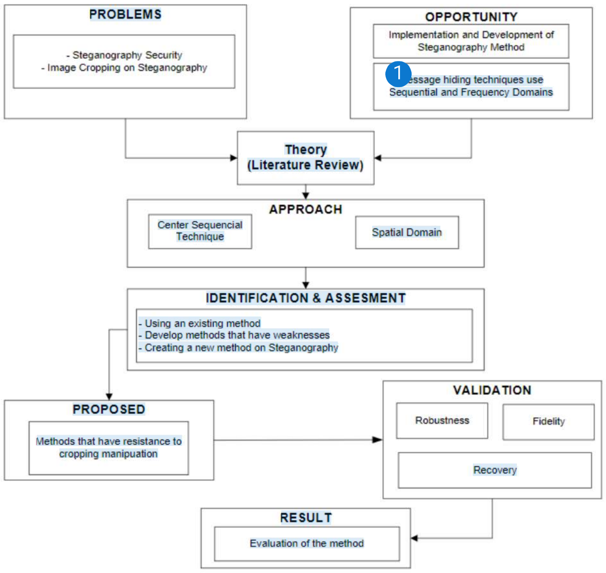

PROBLEMS
- Steganography Security
- Image Cropping on Steganography
OPPORTUNITY
Implementation and Development of Steganography Method
Message hiding techniques use Sequential and Frequency Domains
Theory (Literature Review)
APPROACH
Center Sequencial Technique
Spatial Domain
IDENTIFICATION & ASSESMENT
- Using an existing method
- Develop methods that have weaknesses
- Creating a new method on Steganography
PROPOSED
Methods that have resistance to cropping manipuation
VALIDATION
Robustness
Fidelity
Recovery
RESULT
Evaluation of the method

Figure 1. Research Framework

2.2.2 Center Sequential Technique

Basically there are two ways of inserting messages through pixels on Steganography. First technique is using random pixels where bit of secret data is randomly embedded into cover pixels of Steganography; the second technique is using sequential pixels where the bit of the secret data is inserted sequentially according to how the algorithm works and the method used [12]. This research is introducing a message insertion in a sequential way, where the bit of secret message is inserted from the center of the cover image. In general, the procedure of the Center Sequential Technique algorithm are as follows:

1. Read the size of cover images and secret images.
2. Check whether the message size is larger than the size of the cover image.
3. Map pixels from both images.
4. Make a temporary image to use as an output image.
5. Change the values of each pixel in the cover image and message into binary form as shown in figure 2.

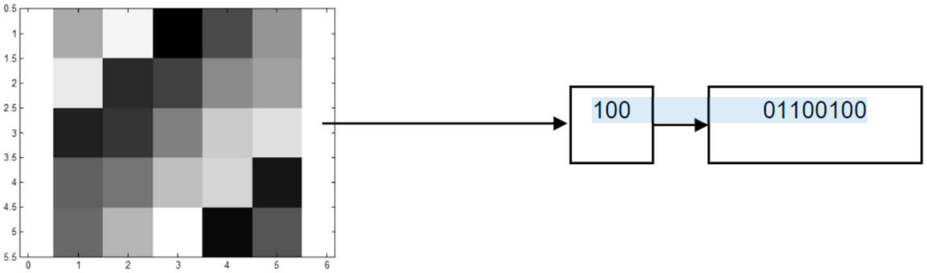


Figure 2. Changing Pixel Values in Binary Form

6. Determine the coordinates of the message image planting to the center position of the cover image.
7. The message image size must be smaller than the size of the cover image.
8. Determine the value X_{start},X_{end},Y_{start}, and Y_{end} through the width and height of the cover image (W, H) and the message image (x, y).
9. Determine the position of the message image that will be placed on the cover image by using the functions in equations (1) and (2).

$$X_{start} = \left(\frac{1}{2} \times W\right) - \left(\frac{1}{2} \times x\right) \ , \ X_{end} = \left(\frac{1}{2} \times W\right) + \left(\frac{1}{2} \times x\right) \qquad \text{...............} \ (1)$$

$$Y_{start} = \left(\frac{1}{2} \times H\right) - \left(\frac{1}{2} \times y\right) \ , \ Y_{end} = \left(\frac{1}{2} \times H\right) + \left(\frac{1}{2} \times y\right) \qquad \text{...............} \ (2)$$

$W =$ width of the cover image

$H =$ height of the cover image

$x =$ width of the message image

$y =$ height of the message image

$X_{start} =$ the message start point is inserted from the width of the cover image

$X_{end} =$ the message endpoint is left out of the width of the cover image

$Y_{start} =$ the starting point of the message is inserted from the height of the cover image

$Y_{end} =$ the endpoint of the message is inserted from the height of the cover image

3. Results and Discussion

3.1 Algorithm Model Center Sequential Technique

Each Steganography algorithm must have its own model to process the insertion and extraction of data into the cover. This will later determine the quality of the image used as Stego-image. This research proposes a new model and technique on Steganography by placing a secret image pixel in the middle position of the cover image. Although Stego-image trimming has been done the secret image will remain intact during the recovery process.

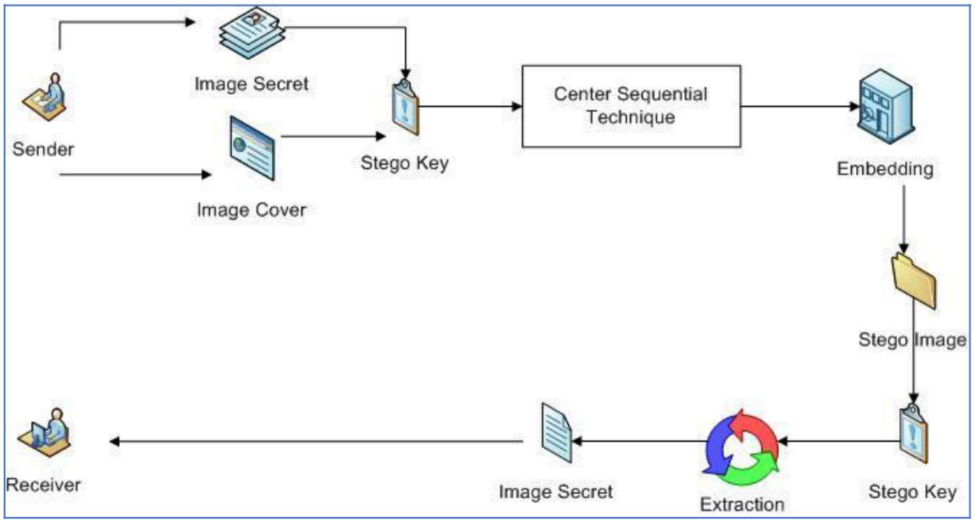


Figure 3. Algorithm Model Center Sequential Technique

Figure 3 is a process model in Center Sequential Technique. The following is insertion process of center sequential algorithm:

1. The sender prepares an image cover and secret image where the image secret should be a smaller size than the cover image, while for the image format can be JPG and PNG.
2. Determine the Stego-key that is used as a reference during the extraction process. The Stego-keys used are based on the dimensions of the cover image.
3. After determining the stego key the next process is to implement the Center Sequential Technique algorithm to combine cover images and secret images. This process will produce a Stego-image with a design simulation in figure 4.

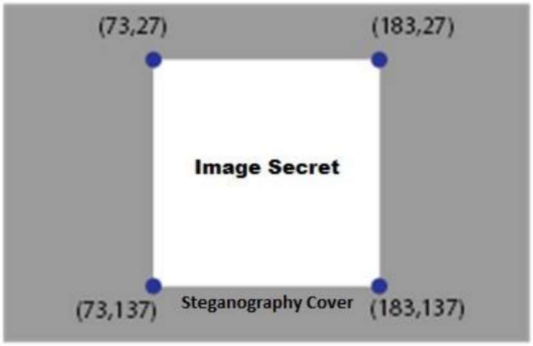


Figure 4. Stego-image simulation using Center Sequential Technique

4. The Extraction process is done by reading the Stego-key, if appropriate, it will produce the Secret Image according to the one sent from the sender.

3.2 Test Results

3.2.1. Fidelity

Fidelity testing is used to measure the quality of the Stego-image and test the reliability of the Steganography algorithm used by calculating the value of Mean Square Error (MSE) and Peak-Signal to Noise-Ratio (PSNR). MSE and PSNR values can be calculated using equations (3) and (4) [4].

$$MSE = \frac{1}{M.N}\sum_{x=1}^{M} \sum_{y=1}^{N}(Sxy - Cxy)^2 \qquad \dots\dots\dots\dots\dots\dots(3)$$

$$PSNR = 10_{log10}\left(\frac{Cmax^2}{MSE}\right) \qquad \dots\dots\dots\dots\dots\dots(4)$$

X and Y	= Point coordinates on the image.
M and N	= Image Dimension.
S	= Inserted Image (Stego-Image).
C	= Original Image (Cover Image).
Cmax	= The Largest Pixel Value in the Overall Image.

Table 1. PSNR Value Testing Results

Cover Steganography		Secret Image		Stego-Image		PSNR (db)
File Name	Size (KB)	File Name	Size (KB)	File Name	Size (KB)	
Cover1.jpg	1.202	Secret1.png	9	Stego1.png	1.174	51.140
Cover2.jpg	446	Secret2.jpg	11	Stego2.png	873	51.992
Cover3.jpg	190	Secret3.jpg	3	Stego3.png	112	51.107
Cover4.jpg	157	Secret4.jpg	7	Stego4.png	190	51.164
Cover5.png	3.070	Secret5.jpg	4	Stego5.png	482	51.146
Cover6.png	138	Secret6.jpg	3	Stego6.png	58	51.187
Cover7.png	133	Secret7.png	3	Stego7.png	52	51.140
Cover8.png	125	Secret8.png	8	Stego8.png	47	51.139

From the test results in table 1, showing a good PSNR value of more than 40 db. The format also affects the Stego-image file size, the png cover format will produce a smaller stego-image size than the cover, while the jpg format produces more file sizes big of cover.

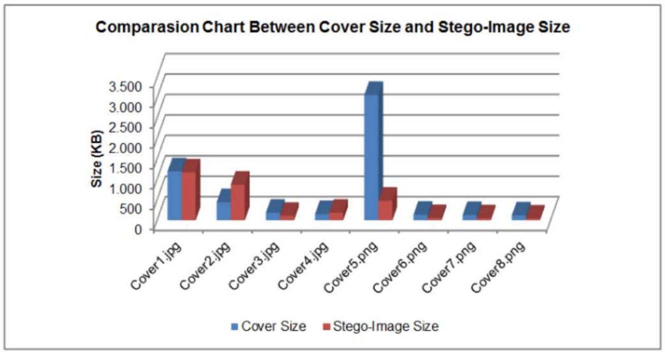


Figure 5. Comparison of File Cover Size and Stego-Image Size

Figure 5 shows that the size of the stego-image file resulting from insertion of cover images and secret images can have larger and smaller stego-image file sizes, depending on the size of the secret image. Whereas for cover images with png format will produce stego-images with a lower size because of the influence of conversion to grayscale.

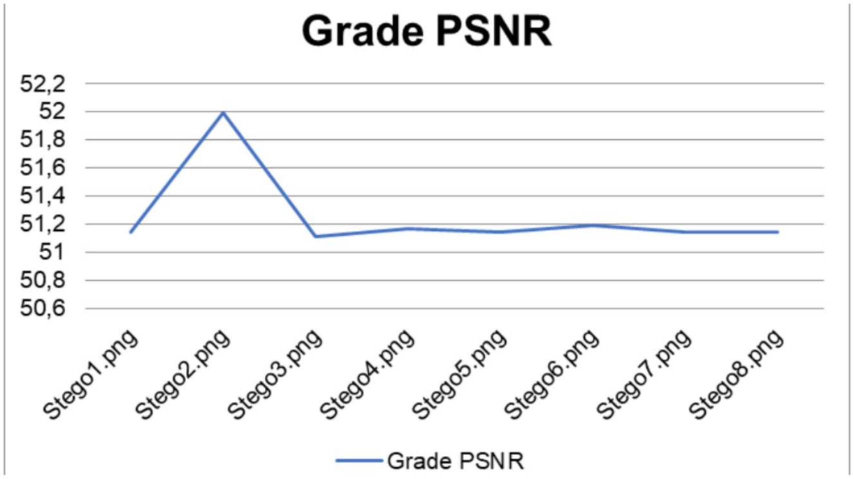


Figure 6. Results of Calculation of PSNR Value

The PSNR of the stego-image generated by the Center Sequential Technique method produced PSNR more than 40 db. From figure 6, the highest PSNR value is almost 52 db and the lowest value is not below 51 db. This shows that the Stego-image generated by the Center Sequential Technique method to produces a good image quality, so that the image does not change significantly.

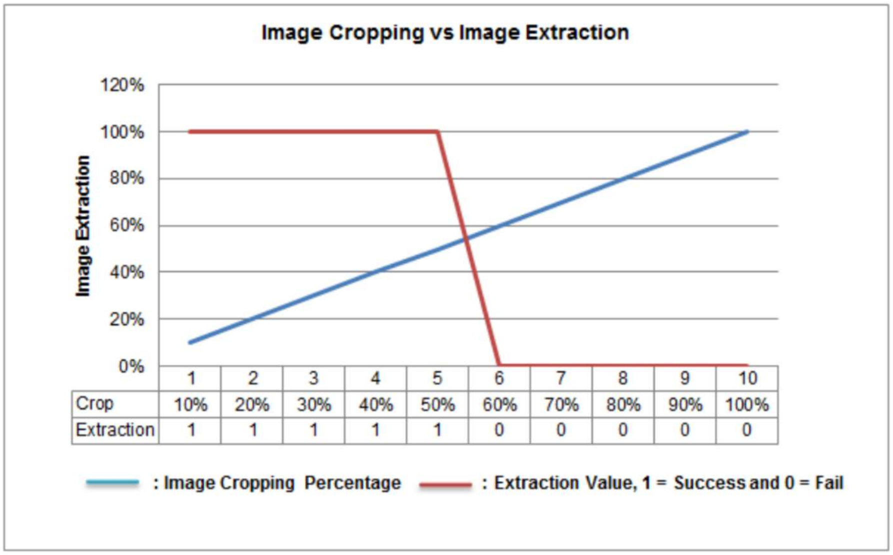
3.2.2. Robustness

Trials in this section are the core of the research. Robustness trials are carried out by attacking the Stego-image through cropping from various positions and then extracting the Stego-image to see whether the secret image can still be reproduced or not.

Table 2. Cropping Testing Results

Stego-image	Crop Position	% Crop	Extraction
Stego1.png	Left	10	Success
Stego1.png	Right	10	Success
Stego1.png	Bottom	10	Success
Stego1.png	Top	10	Success
Stego1.png	All Position	10	Success
Stego1.png	Left	30	Success
Stego1.png	Right	30	Success
Stego1.png	Bottom	30	Success
Stego1.png	Top	30	Success
Stego1.png	All Position	30	Success
Stego1.png	Left	50	Success
Stego1.png	Right	50	Success
Stego1.png	Bottom	50	Success
Stego1.png	Top	50	Success
Stego1.png	All Position	50	Success

Stego-image	Crop Position	% Crop	Extraction
Stego1.png	Left	>=60	Failed
Stego1.png	Right	>=60	Failed
Stego1.png	Bottom	>=60	Failed
Stego1.png	Top	>=60	Failed
Stego1.png	All Position	>=60	Failed



	1	2	3	4	5	6	7	8	9	10
Crop	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
Extraction	1	1	1	1	1	0	0	0	0	0

Figure 7. Cropping Test Results

Test results in table 2 and figure 7 show that images on the stego-image can be trimmed from left, right, top, bottom and all trimming positions. The proposed new method can prove that the Stego-image uses the Center Sequential Technique method to extract the process even though the Cropping attack has been done up to 50%, but the extraction process cannot be done if the Cropping attack is up to more than 60% this is due to the image the message planted on the Steganography Cover is in the middle position so that the message image will be cut off and cannot be extracted.

4. Conclusion

Based on the discussion and testing carried out, it can be concluded:

1. Image quality generated from the Center Sequential Technique Method has a PSNR value with an average of more than 50 db.
2. The Center Sequential Technique Method has resistance to Cropping attacks from the left, right, center, top and all positions and has a cropping ratio resistance of more than 50%.

References

[1] Desoky A 2012 *Noiseless Steganography: The Key to Covert Communications* (Florida: CRC Press)

[2] Prajapati A and Chitaliya G 2015 Secured and robust dual image steganography : A survey *International Journal of Innovative Research in Computer and Communication Engineering* **3** 1 pp 30–37

[3] Kumar V and Kumar D 2010 Digital image steganography based on combination of DCT and DWT *Communications in Computer and Information Science* **101** pp 596–601

[4] Silverstein D A and Farrell JE 1996 The relationship between image fidelity and image quality, *IEEE* **1** pp 881–884

[5] Mishra M and Mishra P 2012 Digital image data hiding techniques *ANSVESA* **7** 2 pp 105–115

[6] Mishra B and Singh V P 2013 Information security through digital image steganography using multilevel and compression technique **3** 1 pp 26–29

[7] Singh S and Siddiqui T J 2013 Robust image steganography using complex wavelet transform, *Impact-2013* pp 56–60

[8] Sandoval J, O Espejel-Trujillo, Angelina Nakano-Miyatake, Mariko Perez-Meana, Hector. 2014 Cropping and noise resilient steganography algorithm using secret image sharing *Sixth International Conference on Graphic and Image Processing* **1** pp 543-551

[9] Sur A R V and Mukherjee J 2012 Secure Steganography Using Randomized Cropping **7110** pp 82-95

[10] Potdar V M, Han S and Chang E 2005 Fingerprinted secret sharing steganography for robustness against image cropping attacks *3rd IEEE International Conference on Industrial Informatics (INDIN)* pp 717–724

[11] Kumar M and Yadav M 2014 Image steganography using frequency domain *International Journal of Scientific & Technology Research* **3** 9 pp 226–230

[12] Rejani R, Murugan D and Krishnan V 2015 Pixel pattern based steganography on images *ICT ACT Journal on Image and Video Processing* **05** 3 pp 991-997