Noble Method for Data Hiding using Steganography Discrete Wavelet Transformation and Cryptography Triple Data Encryption Standard: DES

Cahya Rahmad[1], Arief Prasetyo[3], Novriza Arizki[4]
Department of Information Technology
State Polytechnic of Malang
Malang, Indonesia

Kohei Arai[2]
Department of Information Science
Saga University
Saga City, Japan

***Abstract*—Noble method for data hiding using steganography Discrete Wavelet Transformation: DWT and cryptography triple Data Encryption Standard: DES is proposed. In the current era, information technology has become inseparable from human life, especially regarding the processing and dissemination of information. In line with advances in information technology, there are also parties who want to abuse such information by changing information or even damage it. To avoid that happening, then the data needs to be secured first into other media using the DWT method. The choosing of this method is because the image of the data insertion almost resembles the original image. Triple DES methods are also required to encode data and provide additional security so that hidden data will be difficult to solve. The choosing of this method is because it is resistant against brute force, chosen plaintext, and known plaintext attack. Based on the test, image insertion results in 100% immune to the image manipulation of brightness and contrast, but not so resistant to cropped, resized, and rotated image manipulation. Other tests also indicate that the data which is in the picture can be extracted again and will not undergo any changes.**

Keywords—Data hiding; steganography; DWT; cryptography; 3DES

I. Introduction

As the development of the era, the development of technology is also overgrowing, especially information technology. Information technology has become inseparable from human life and helps people in many ways, such as processing and disseminating information. In line with advances in information technology, there are also parties who want to abuse such information by changing information or even damage it.

Data in 2016 showed 1061 reports of cyber-attacks with cybercrime category of 77.4% and 950 reports in 2017 with cybercrime category of 72.1% [1]. By looking at the data, we can know that cybercrime is a serious problem that we must handle and every year the number of cases of cybercrime will remain substantial. It indeed can be a nightmare for companies or even government agencies who want to send data containing confidential information to clients or other companies. The data needs to be secured first using cryptographic and steganographic methods before being sent to avoid that happening.

Data Hiding Based on Wavelet Multi-resolution Analysis is proposed[2] together with Data Hiding Based on Multiresolution Analysis Utilizing Information Content Concentrations using Eigen Value decomposition[3]. Other than these, Information Hiding Method Based on Coordinate Conversion is proposed [4]. Meanwhile, Data hiding based on Multi-Resolution Analysis: MRA taking into account scanning of the embedded image for improvement of invisibility is proposed[5].

Furthermore, Improvement of secret image invisibility in circulation image with Dyadic wavelet-based data hiding with run-length coding is also suggested [6] together with Method for data hiding based on Legal 5/2 (Cohen-DaubechiesFeauveau: CDF 5/3) wavelet with data compression and random scanning of secret imagery data [7] Moreover, Data Hiding Method Replacing LSB of Hidden Portion for Secrete Image with Run-Length Coded Image is proposed[8].

Steganography is a technique to hide messages or information into other media. Therefore, besides the intended person, they will not be aware of any messages or data in that other media and prevent the occurrence of suspicion.

One of the methods in steganography is the DWT method. DWT has advantages over other steganographic methods that is steganographic images almost resemble the original picture[9]. The message needs to be encoded in advance into another form that cannot be understood using a technique called cryptography to provide additional security for the method.

Cryptography is a technique to avoid information being known by unwanted parties and to convert it into an incomprehensible form. The primary purpose of cryptography is to protect data from unauthorized people[10].

In cryptography, there are many methods, and one of them is the Triple DES method (it is referred to 3DES hereafter)1 operates on 64-bit blocks and uses three keys, each of which is 56-bit in size [10]. Those keys are the strengths of the 3DES method. This method has a reasonably fast processing time and has resistance to attacks such as brute force, chosen-plaintext, and known plaintext[11].

In this research, data security application is made using DWT of steganography method and 3DES cryptography method to secure data by inserting data into an image before sending the data.

In the next section, the proposed method is described followed by some experiments. Then, the conclusion is described together with some discussions and future works.

II. Proposed Data Hiding Method

The proposed data hiding method is based on DWT based steganography and 3DES based cryptography.

A. 3DES

The DES algorithm has proved that highly competent algorithms can be considered uncomfortable and unreliable. Therefore, there is a search for a method for using it again by making it stronger and more secure than creating a new algorithm starting from the scratch. Two significant improvements result in double DES and triple DES algorithms (3DES). Double DES repeats the DES process twice using two keys. If the experiment to crack a key in a DES is 256, then the research to break into two different keys of n-bit is 22n. However, all of this is not entirely true since the introduction of the concept of a meet-in-the-middle attack [12].

Given the idea that double DES may not be strong enough to prevent meet-in-the-middle attacks has led to the development of 3DES algorithms developed by IBM in 1999 by a team headed by Walter Tuchman [13]. This kind of attack is one of the main reasons why double DES is replaced by 3DES that DES operation which is repeated three times using three different keys. It's important to avoid using the same key for encryption, as it will only result in a DES process with slower processing time. 3DES has two shapes, the first form uses three completely different keys and the second one uses two completely different keys [12].

According to [14], 3DES has advantages that are fast processing time and a reasonably reliable level of security. Also, 3DES has resistance to several attacks such as brute force, chosen-plaintext, and known plaintext. This method requires three keys that have a 56-bit length per core. The time needed to check all possible keys using 50 million keys per second for each 3DES key is 400 days [15].

The steps in the 3DES process according to [15] shown in Fig. 1 are as follows:

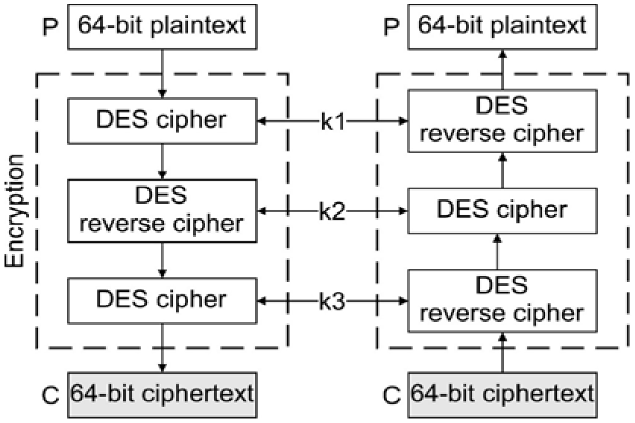

Fig. 1. Encryption and Decryption Process of 3DES.

- Encrypt a message block (plaintext) using a single DES with a K1 key.
- Decrypt the results obtained from step 1 using the K2 key.
- Encrypt the output from step 2 using the K3 key so that it produces ciphertext.
- The decryption process of ciphertext is the opposite of the 3DES Encryption process, which is decryption using K3 keys, encryption using K2 keys, and decryption using K1 keys.

By looking at the advantages of the 3DES algorithm and considering its weakness as well, in this paper, 3DES method is used by using different keys to provide stronger security on the document.

B. DWT

DWT is a method that can divide information from an image into the approach and signal detail. LL bands include low pass coefficients and procedures to a copy as well as more information of other sub-signals indicating vertical, horizontal, or diagonal information or changes in an image [16]. The general equation for DWT can be seen in the equation below [17].

$$DWT\{f\{t\}\} = W_{\emptyset}(j_0, k) + W_{\psi}(j, k) \tag{1}$$

where,.

$$W_{\phi}(j_0, k) \ \ \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[n] \phi_{jo,k}[n] \tag{2}$$

$$W_{\psi}(j, k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[n] \psi_{j,k}[n], \quad j \geq j_0 \tag{3}$$

In the DWT method, there are several techniques for representing images to approach and signal details, one of them is wavelet Haar. Wavelet Haar can be used to describe a picture with a wavelet counting process. The equation of wavelet Haar transform is in the equation shown below [18]:

$$X[2k] = \frac{1}{\sqrt{2}} \ (x[2k] + x[2k + 1] \tag{4}$$

$$X[2k + 1] = \frac{1}{\sqrt{2}} \ (x[2k] - x[2k - 1] \tag{5}$$

The DWT method can represent images into approach and signal details. This method also has advantages compared to other steganography methods, namely the model of steganography results almost resemble the original image [19]. Therefore, in this paper, the DWT method is used to hide the message into the approach and details of the signal, so that the changes that occur in the image will not be too visible in the human vision system.

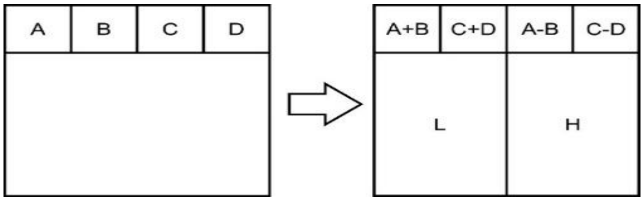

Fig. 2. Horizontal Operation on the First Row.

Haar-DWT is one of the most basic and straightforward transformations in the DWT family. This method reduces the calculation work. Haar-DWT decomposes each signal into two components. The first component is called the average and the second component is called the difference [10]. This process is used to reduce memory requirements and the amount of inefficient Haar coefficient movements. Disadvantages in the sum and subtraction operations can be balanced by decreasing the number of division operations; especially when used at low bit rates, it introduces compression artifacts [19]. A detailed procedure of Haar-DWT 2 dimensions according to [14] described as follows:

Step 1: First, scan the pixels from left to right with the horizontal direction. Then, perform addition and subtraction operations on neighboring pixels. Save the amount on the left and the difference on the right as illustrated in Figure 2. Repeat this operation until the end of the rows. The total pixel represents the low-frequency part (denoted by the symbol L) while the pixel difference represents the high-frequency portion of the original image (indicated by the symbol H).

Step 2: scan the pixels from top to bottom in a vertical direction. Perform the addition and subtraction operations on the neighboring pixels and then store the sums at the top and the difference at the bottom as illustrated in Figure 3. Repeat this operation until the end of the columns. Finally, we will get four sub-bands each denoted as LL, LH, HL, and HH. Sub-band LL is a low-frequency part, so it looks very similar to the original image.

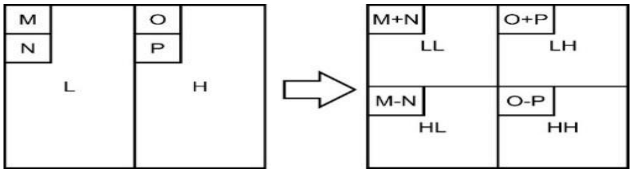

Fig. 3. Vertical Operation.

Haar-DWT is a technique that can be readily applied to get four sub-bands LL, LH, HL, and HH. The processes in Haar DWT are not too complicated to do, but still, represent the frequency of the image. Therefore, in this paper, the Haar-DWT technique is used as an application of the DWT method to get sub-bands of the image and insert the document into the subband.

C. Process Flow of the Proposed Method

The flow of the embedding data and extraction process using the DWT and 3DES methods is explained as follows, Fig. 4:

- Embedding Algorithm

In the insertion process requires a cover image, document (.docx, .xlsx, .pdf, or .txt), and keys (K1, K2, and K3). The following are the steps in the insertion process :

1) Encrypt the document using 3DES with the key, so that it will obtain the ciphertext.

2) Separate ciphertext into three parts that is ciphertext 1, ciphertext 2, and ciphertext 3.

3) Transform the cover image using DWT to get four subbands on the R, G, and B layers.

4) Insert each ciphertext into the HH sub-band at each layer R, G, and B.

5) Image reconstruction uses the IDWT process, resulting in a stego image.

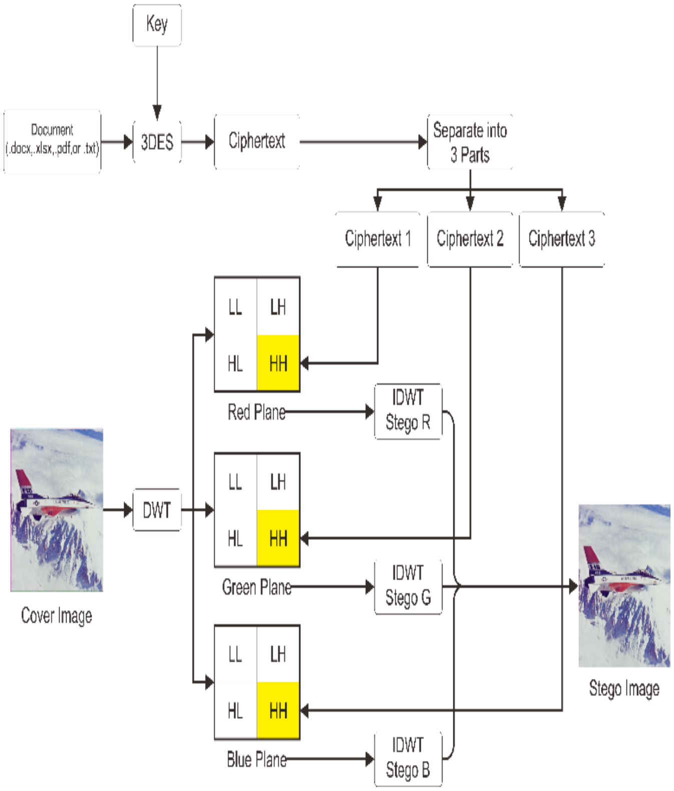

Fig. 4. Embedding Algorithm.

- Embedding Algorithm

In the extraction process requires a stego image and key (K1, K2, and K3). The following are the steps in the extraction process, Fig. 5:

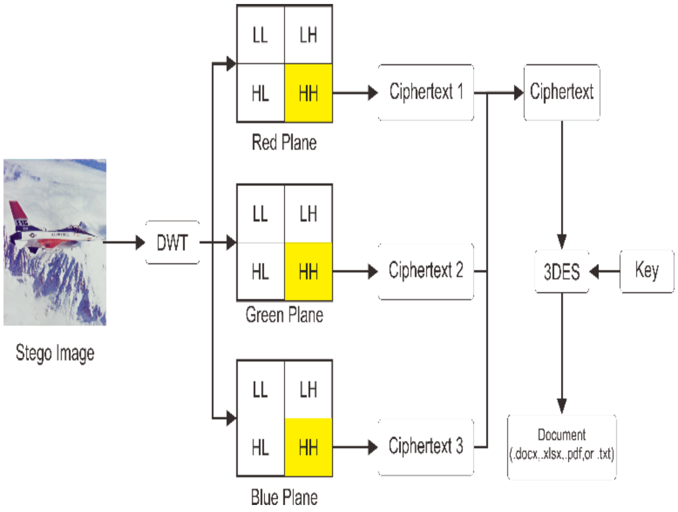

Fig. 5. Extraction Algorithm.

1) Transform the stego image using DWT to get four sub-bands on the R, G, and B layers.

2) Extract information in the HH sub-band on each sheet.

3) Combine the information that has been extracted to get a complete ciphertext.

4) Decrypt ciphertext using 3DES with the key to obtaining the document back.

III. Experiments

In this research, the embedding process uses a few cover images shown in Fig. 6.

(a) (b) (c) (d) (e) (f) (g) (h) (i) (j)

Fig. 6. (a) Airplane.png (b) Arctichare.png (c) Baboon.png (d) Boat.png (e) Boy.bmp (f) Cat.png (g) Fruits.png (h) Frymire.png (i) Lena.png (j) Peppers.png [20].

Those images are the images that will be inserted by the document. The types of support materials and cover images shown in Table 1. Before embedding the document into images, the calculation needs to be done to know the maximum integrated document size. The equation to calculate it shown in the equation below.

$$d = (x * y * 3\ 44000 /)$$

TABLE I. Types of Supported Documents

No	Dokumen	Cover Image
1	Docx	Png
2	Xlsx	Bmp
3	Pdf	Jpeg
4	Txt	Tiff

where,

d = document size (KB), x = image width, y = image height

The first test is the insertion test of the document. Any documents with different extensions shown in Table I will be inserted in each image to compare the time of insertion of each material in each image. The type of paper used in this test is a 12 KB docx, xlsx with a size of 9.67 KB, a pdf with a volume of 22.3 KB, and a txt with a capacity of 161 bytes. The results of this test shown in Fig. 7. Furthermore, the test results of document extraction from the image which contains the document in Fig. 8.

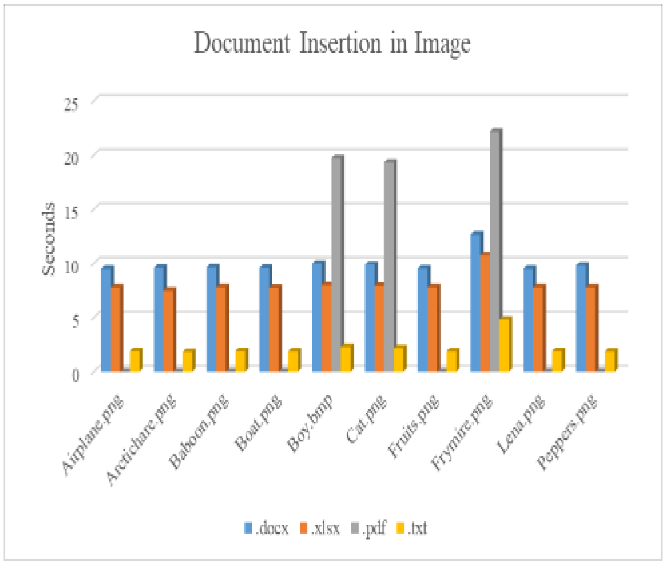

Fig. 7. Graph of Document Insertion in Image.

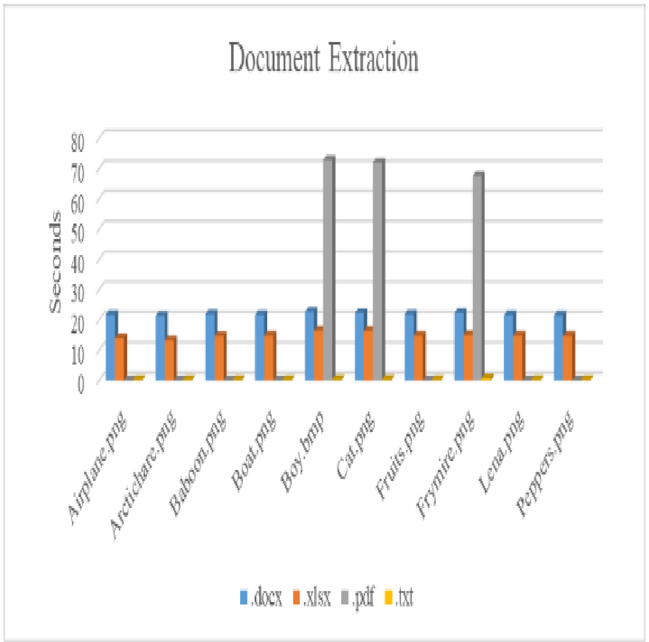

Fig. 8. Graph of Document Extraction.

The next test is testing the image quality on each image of the insertion shown in Table II.

TABLE II. RESULTS OF IMAGE QUALITY TESTING

Images	Image Assesment	Document Types			
		docx	xlsx	pdf	txt
Airplane 512x512	MSE	18	15	-	2
	PSNR	23	25	-	43
Arctichare 512x512	MSE	18	14	-	2
	PSNR	23	25	-	44
Baboon 512x512	MSE	18	16	-	2
	PSNR	23	24	-	42
Boat 512x512	MSE	18	15	-	2
	PSNR	23	25	-	43
Boy 768x512	MSE	14	11	22	1
	PSNR	26	27	21	46
Cat 490x733	MSE	14	12	23	2
	PSNR	25	27	21	45
Fruits 512x512	MSE	17	15	-	2
	PSNR	24	25	-	43
Frymire 1118x1106	MSE	5	5	7	1
	PSNR	34	35	31	52
Lena 512x512	MSE	17	15	-	2
	PSNR	23	25	-	43
Peppers 512x512	MSE	17	15	-	2
	PSNR	23	25	-	43

After testing the image quality has been done, then the next step is insertion testing on the different frequencies shown in Table III.

TABLE III. INSERTION TESTING ON DIFFERENT FREQUENCY

Original Image	Insertion Frequency	Encryption Result	Decryption Result	MSE	PSNR
	LL		Blank Document	11%	27 db
	LH		Original Document	2%	42 db
	HL		Original Document	2%	43 db
	HH		Original Document	2%	43 db

The next test is insertion testing using different insertion values as shown in Table IV.

After that the test of the stego image endurance against some image manipulation attacks shown in Table V.

TABLE IV. INSERTION TESTING ON DIFFERENT INSERTION VALUE

Original Image	Insertion Frequency	Insertion Value	Encryption Result	Decryption Result	MSE	PSNR
Airplane.png	HH	10	airplane.enkripsi.nilai.10.png	*Error*	1%	52 db
Airplane.png	HH	20	airplane.enkripsi.nilai.20.png	*Error*	1%	49 db
Airplane.png	HH	30	airplane.enkripsi.nilai.30.png	*Error*	1%	47 db
Airplane.png	HH	40	airplane.enkripsi.nilai.40.png	*Error*	2%	45 db
Airplane.png	HH	50	airplane.enkripsi.nilai.50.png	Original Document	2%	43 db
Airplane.png	HH	60	airplane.enkripsi.nilai.60.png	Original Document	2%	41 db
Airplane.png	HH	70	airplane.enkripsi.nilai.70.png	Original Document	3%	40 db
Airplane.png	HH	80	airplane.enkripsi.nilai.80.png	Original Document	3%	39 db
Airplane.png	HH	90	airplane.enkripsi.nilai.90.png	Original Document	3%	38 db
Airplane.png	HH	100	airplane.enkripsi.nilai.100.png	Original Document	4%	37 db
Airplane.png	HH	150	airplane.enkripsi.nilai.150.png	Original Document	5%	34 db
Airplane.png	HH	200	airplane.enkripsi.nilai.200.png	Original Document	6%	32 db
Airplane.png	HH	255	airplane.enkripsi.nilai.255.png	Original Document	7%	31 db

TABLE V. TESTING OF STEGO IMAGE RESISTANCE

Original Image	Manipulation	Degree / Area	Encryption Result	Decryption Result
Airplane.txt.png	Brightness	10%	Brightness.10%.png	Original Document
Airplane.txt.png	Brightness	20%	Brightness.20%.png	Original Document
Airplane.txt.png	Brightness	30%	Brightness.30%.png	Original Document
Airplane.txt.png	Brightness	50%	Brightness.50%.png	Original Document
Airplane.txt.png	Brightness	100%	Brightness.100%.png	Original Document
Airplane.txt.png	Brightness	150%	Brightness.150%.png	Original Document
Airplane.txt.png	Brightness	-150%	Brightness.minus150%.png	Original Document
Airplane.txt.png	Contrast	100%	Contrast.100%.png	Original Document
Airplane.txt.png	Contrast	-50%	Contrast.minus50%.png	Original Document
Airplane.txt.png	Crop	Up	UpCrop.png	Original Document
Airplane.txt.png	Crop	Down	Down Crop.png	Blank Document
Airplane.txt.png	Crop	Right	Right Crop.png	“Can’t be Extracted”
Airplane.txt.png	Crop	Left	Left Crop.png	"The Key That You Entered Is Incorrect"
Airplane.txt.png	Resize	400x400	Resize.400x400.png	“Can’t be Extracted”
Airplane.txt.png	Resize	500x500	Resize.500x500.png	“Can’t be Extracted”
Airplane.txt.png	Resize	510x510	Resize.510x510.png	“Can’t be Extracted”
Airplane.txt.png	Resize	514x514	Resize.514x514.png	“Can’t be Extracted”
Airplane.txt.png	Rotate	90^{o} CW	CW rotation.png	Blank Document
Airplane.txt.png	Rotate	90^{o} CCW	CCW rotation.png	“Can’t be Extracted”
Airplane.txt.png	Rotate	180^{o}	Full rotation.png	“Can’t be Extracted”

IV. Conclusions

Based on the results of the previous tests, can be drawn some conclusions that are :

- Encryption and decryption process using pdf documents takes longer than using other materials because it has a bigger size.
- Extraction documents are documents that match precisely the original content.
- The larger the images or, the smaller the document size, the better the quality.
- The insertion of materials in the HL and HH sub-bands produces images of better quality than in the other subbands because they have larger MSE and PSNR values.
- The best insertion value is 50 because it shows minimal MSE values and large PSNR values, as well as documents, can still be extracted.
- The stego image is resistant to brightness and contrast manipulation attacks. As for crop manipulation attacks, stego images cannot always survive. Meanwhile, the stego image cannot withstand the manipulation of resizing and rotate attacks.

Further experimental approaches are required for validation of the proposed data hiding method.

References

[1] P. Passeri, “2017 Cyber Attacks Statistics,” 2017. [Online]. Available: https://www.hackmageddon.com/2018/01/17/2017-cyber-attacksstatistics/. [Accessed: 30-May-2018].

[2] Kohei Arai, Kaname Seto, Data Hiding Based on Wavelet Multiresolution Analysis, Journal of Visualization Society of Japan, Vol.22, Suppl.No.1, 229-232, 2002.

[3] Kohei Arai, Kaname Seto, Data Hiding Based on Multi-resolution Analysis Utilizing Information Content Concentrations by Means of Eigen Value decomposition, Journal of Visualization Society of Japan, Vol.23, No.8, pp.72-79,2003.

[4] Kohei Arai, Kaname Seto, Information Hiding Method Based on Coordinate Conversion, Journal of Visualization Society of Japan, 25, Suppl.No.1, 55-58,(2005)

[5] Kohei Arai, Kaname Seto, Data hiding based on Multi-Resolution Analysis taking into account scanning of the embedded image for improvement of invisibility, Journal of Visualization Society of Japan, 29, Suppl.1, 167-170, 2009.

[6] Kohei Arai and Yuji Yamada, Improvement of secret image invisibility in circulation image with Dyadic wavelet based data hiding with runlength coding, International Journal of Advanced Computer Science and Applications,2,7,33-40, 2011.

[7] Kohei Arai, Method for data hiding based on Legal 5/2 (CohenDaubechies-Feauveau: CDF 5/3) wavelet with data compression and random scanning of secret imagery data, International Journal of Wavelets Multi Solution and Information Processing, 11, 4, 1-18, B60006 World Scientific Publishing Company, DOI: I01142/SO219691313600060, 1360006-1, 2013.

[8] Kohei Arai, Data Hiding Method Replacing LSB of Hidden Portion for Secrete Image with Run-Length Coded Image, International Journal of Advanced Research on Artificial Intelligence, 5, 12, 8-16, 2016.

[9] P. Batarius and M. Maslim, “Perbandingan metode dalam teknik steganografi,” vol. 2012, no. Semantik, pp. 307–313, 2012.

[10] R. Tripathi and S. Agrawal, “Comparative Study of Symmetric and Asymmetric Cryptography,” Int. J. Adv. Found. Res. Comput., vol. 1, no. 6, pp. 2348–4853, 2014.

[11] T. Sobh, K. Elleithy, and A. Mahmood, Novel Algorithms and Techniques in Telecommunications and Networking. 2010.

[12] R. Debnath, P. Agrawal, and G. Vaishnav, “Des , Aes and Triple Des : Symmetric Key Cryptography Algorithm,” Int. J. Sci. Eng. Technol. Res., vol. 3, no. 3, pp. 652–654, 2014.

[13] Y. Dinesh and A. P. Ramesh, “Efficient Capacity Image Steganography by Using Wavelets Yedla dinesh A ddanki purna ramesh,” Int. J. Eng. Res. Appl., vol. 2, no. 1, pp. 251–259, 2012.

[14] A. Noura, “A comparison of the 3DES and AES encryption standards,” Int. J. Secur. its Appl., vol. 9, no. 7, pp. 241–246, 2015.

[15] K. S. Thyagarajan, Still image and video compression with MATLAB. 2011.

[16] N. Kaur and P. Singh, “A New Method of Image Compression Using Improved SPIHT and MFHWT,” Int. J. Latest Res. Sci. Technol., vol. 1,8no. 2, pp. 124–126, 2012.

[17] K. Kaur, “Image Compression using HAAR Wavelet Transform and Discrete Cosine Transform,” vol. 125, no. 11, pp. 28–31, 2015.

[18] P.-Y. Chen and H.-J. Lin, “A DWT Based Approach for Image Steganography,” Int. J. Appl. Sci. Eng. Int. J. Appl. Sci. Eng, vol. 4, no. 4, pp. 275–290, 2006.

[19] D. Coppersmith, “A proposed mode for triple-DES encryption,” IBM J. Res. …, vol. 40, no. March, pp. 253–262, 1996.

[20] https://homepages.cae.wisc.edu/~ece533/images/)

Author’s Profile

Cahya Rahmad: He received BS degrees from Brawijaya University Indonesia in 1998 and MS degrees from Informatics engineering at Sepuluh Nopember Institute of Technology Surabaya Indonesia in 2005. He is a lecturer in The State Polytechnic of Malang Since 2005. He received Doctoral degrees at Saga University japan in 2013, His interest researches are image processing, data mining and patterns recognition.

Kohei Arai, He received BS, MS and PhD degrees in 1972, 1974 and 1982,respectively.He was with The Institute for Industrial Science and Technology of the University of Tokyo from April 1974 to December 1978 also was with National Space Development Agency of Japan from January, 1979 to March, 1990. During from 1985 to 1987, he was with Canada Centre for Remote Sensing as a Post-Doctoral Fellow of National Science and Engineering Research Council of Canada. He moved to Saga University as a Professor in Department of Information Science on April 1990. He was a counselor for the Aeronautics and Space related to the Technology Committee of the Ministry of Science and Technology during from 1998 to 2000. He was a councilor of Saga University for 2002 and 2003. He also was an executive councilor for the Remote Sensing Society of Japan for 2003 to 2005. He is an Adjunct Professor of University of Arizona, USA since 1998. He also is Vice Chairman of the Science Commission “A” of ICSU/COSPAR since 2008 then he is now award committee member of ICSU/COSPAR. He wrote 37 books and published 570 journal papers. He received 30 of awards including ICSU/COSPAR Vikram Sarabhai Medal in 2016, and Science award of Ministry of Mister of Education of Japan in 2015. He is now Editor-in-Chief of IJACSA and IJISA. http://teagis.ip.is.saga-u.ac.jp/index.ht