Enhancing Data Security Using DES-based Cryptography and DCT-based Steganography

Achmad Solichin[1], Erwin Wahyu Ramadhan[2]
Informatics Department, Faculty of Information Technology
Budi Luhur University
Jakarta, Indonesia
[1]achmad.solichin@budiluhur.ac.id, [2]erwinwahyuramadhan@gmail.com

Abstract— **The security and privacy of the data transmitted is an important aspect of the exchange of information on the Internet network. Cryptography and Steganography are two of the most commonly used digital data security techniques. In this research, we proposed the combination of the cryptographic method with Data Encryption Standard (DES) algorithm and the steganographic method with Discrete Cosine Transform (DCT) to develop a digital data security application. The application can be used to secure document data in Word, Excel, Powerpoint or PDF format. Data encrypted with DES algorithm and further hidden in image cover using DCT algorithm. The results showed that the quality of the image that has been inserted (stego-image) is still in a good category with an average PSNR value of 46.9 dB. Also, the experiment results show that the average computational time of 0.75 millisecond/byte, an average size increase of 4.79 times and a success rate of 58%. This research can help solve the problem of data and information security that will be sent through a public network like the internet.**

Keywords— data security; application; DES; DCT

I. Introduction (*Heading 1*)

Along with the development of the Internet, the use of digital communication medium for data and information exchange is also increasing. One of the main problems in digital communication is the security of the data was transmitted over the internet network. Data can be stolen or accessed by attackers with the certain techniques. Therefore it is the necessary application of reliable data security techniques for data exchange via internet media. Cryptography and Steganography are two of the most commonly used to secure digital data. Cryptography is a technique for securing data where the original data is randomized in such a way that it is difficult to understand. Original data can only be opened by a specific person using predefined custom keys.

Some of today's popular cryptographic techniques include Advanced Encryption Standard (AES), Data Encryption Standard (DES), RC4 and RSA. All three are often used to secure important data in various applications. Primartha in [1] implements the DES algorithm to develop software that can encrypt and decrypt text and files. Meanwhile, Siswanto et al. in [2] implemented the AES and RC4 algorithms to secure data on the Agricultural Quarantine Agency. Cryptography can also be applied to secure online messaging such as Yahoo Messenger [3].

Meanwhile, steganography is a technique to hide messages on a medium. Messages or confidential data can be hidden in various forms of media, such as text, images, sound, and video. Steganography techniques are widely used such as Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transformation (DWT). Its application is also quite a lot done in various studies. Gunjal and Jha in [4] apply the DWT and Blowfish algorithms to insert messages on digital image media. Fitri in [5] implements the LSB method to secure image data. In addition to using the image media, steganography can also be applied to video media as done on [6] using LSB and Less Significant Frame (LSF) methods to insert messages on video media.

To improve data security, many researchers are currently trying to combine cryptographic and steganographic methods. Research conducted by Yang et al. [7] incorporating the DES cryptography method with LSB steganography. The result stated that the incorporation of the method is better than using only the LSB method. Merging cryptographic and steganographic methods is also performed on [8] to secure image data within other imagery. Meanwhile, [9] conducted a study that incorporated the DES cryptography method with End-of-File (EOF) steganographic method to secure data on audio media.

TABLE I. The Combinations of Cryptographic and Steganographic Methods

#	Cryptographic Method	Steganographic Method	Research
1	DES	LSB	[7], [12], [13]
2	AES	LSB	[14], [15]
3	AES	DCT	[16]
4	AES	DWT	[17], [18]
5	DES	EOF	[9]
6	RSA	LSB	[19]
7	DES	MSB	[20]
8	Blowfish	LSB	[21]

Table I presents several combinations of cryptographic and steganographic methods as summarized in [10], [11] and several other studies. Combining several methods at once can improve data security. However, incorporation will increase the computation time, so a proper merging method is required.

In this study, we combined the DES cryptographic and DCT steganographic method. DES algorithm is an encryption algorithm used in the world's most widely adopted by NIST (National Institute of Standards and Technology) a US Federal information processing standard. The plaintext data are encrypted in 64-bit blocks into 64 bits of ciphertext data using 56-bit keys. DES transforms 64-bit inputs in multiple stages of encryption into 64-bit outputs. Thus, DES includes block cipher. With the same stages and keys, DES is used to reverse encryption. The internal key on the DES algorithm is generated from a 64-bit external key [1]. While DCT (Discrete Cosine Transform) is a mathematical function used to change the signal values of a medium into its basic frequency components. In digital imagery, DCT is used to convert the image spatial domain to its frequency domain. Although originally used as a basic algorithm for image compression, DCT can also be used as a steganographic algorithm [22], [23].

II. The Proposed Method

Data security is an important aspect to be considered, especially when communicating using the internet media. Data can be stolen or accessed by attackers for a particular purpose. Therefore, in this study, we develop an application that applies DES cryptography and DCT steganographic algorithm to improve data security. Figure 1 presents the application architecture of the proposed method in this study. First, the data or documents are encrypted using DES cryptography algorithm so that data are generated in the form of ciphertext. A password is included in the data encryption process. The encrypted data is then inserted in the image media using the DCT steganography algorithm. Inserted images can be sent to destinations through the public network.

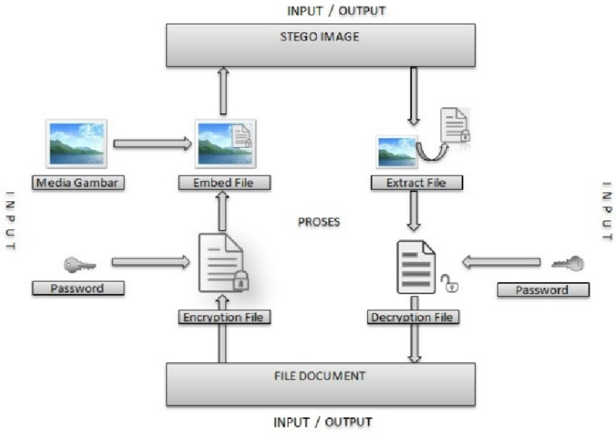


Fig. 1. The application architecture of the proposed method

At the destination, to get back the original data, ciphertext data will be extracted from the stego-image. Next, the ciphertext data is decrypted again with the DES method and the password used in the encryption process. The original data can be reopened by the recipient at the destination.

III. Results and Discussions

A. The Experiments

The experiment was conducted to determine the performance of DES cryptographic and DCT steganographic method. Table II presents the experiment data in the form of the Word, Excel, Powerpoint and PDF format in various sizes. Meanwhile, the image to be used as image cover are shown in Table III. The images used are BMP, PNG, and JPG in various sizes and resolutions. Some experiment scenarios are performed to determine the quality of the inserted image with the value of PSNR, the comparison of file size before and after the process of encryption and insertion, processing time and percentage of success of the proposed method process.

TABLE II. Data for Testing

#	File Name	File Size (byte)	File Type
1	File TA	21,540	PDF
2	File TB	75,726	EXCEL
3	File TC	212,997	DOCX
4	File TD	105,472	PPTX
5	File RA	132,096	PDF
6	File RB	57,344	EXCEL
7	File RC	107,520	DOCX
8	File RD	48,128	PPTX

B. The Experiment Results

After doing a series of experiments, some test results were obtained. Figure 2 shows the PSNR (Peak Signal to Noise Ratio) value for each test. The PSNR is the ratio between the maximum value of the signal as measured by the magnitude of the noise that affects the signal. The PSNR is used to find out the comparison of cover image quality before and after inserted message. Based on the PSNR value of all the experiment obtained the average value of PSNR of 46.9 dB. The value indicates that the image quality of steganographic result or image that has been inserted data is still in the good category. Visually, the original cover image with the inserted image is also no different.

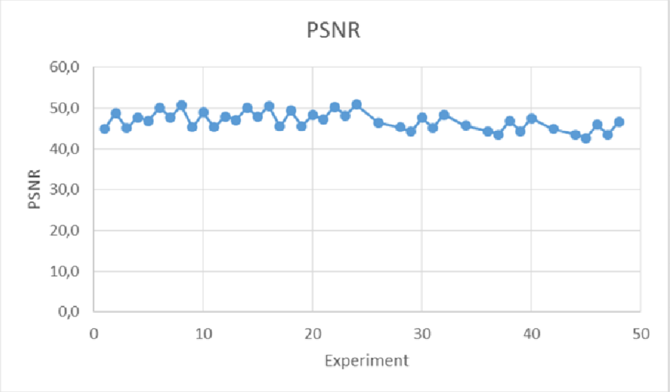
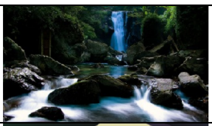
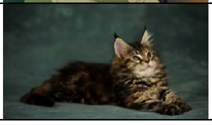
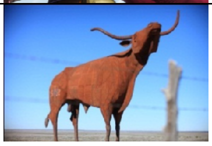
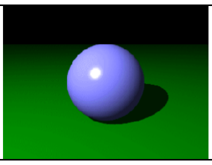


Fig. 2. The PSNR value of Stego-image

TABLE III. IMAGE COVER

#	Image	File Name	Image Resolution	File Size (byte)	File Type
1		Cover TA	1920x1080	393,216	BMP
2		Cover TB	1920x1080	1,075,200	PNG
3		Cover TC	1920x1080	393,216	JPG
4		Cover SA	1080x720	211,968	BMP
5		Cover SB	1080x720	1,146,880	PNG
6		Cover SC	1080x720	97,587	JPG
7		Cover RA	320x240	230,406	BMP
8		Cover RB	500x500	5,443	PNG
9		Cover RC	500x500	110,592	JPG

In this study also seen the comparison of the size between the image and the original data with the stego-image. Figure 3 shows the average rate of incremented image size increments for each original image. In an experiment with a second cover image size of 1,075,200 bytes, the average size of the image was 1.16 times compared to the cover image size plus the original data size. Overall, the average increase in file size before and after insertion is 4.79 times. A large increase in file size occurs in small, low-resolution image sizes. The larger the cover image size and image resolution, the lower the file size increase.

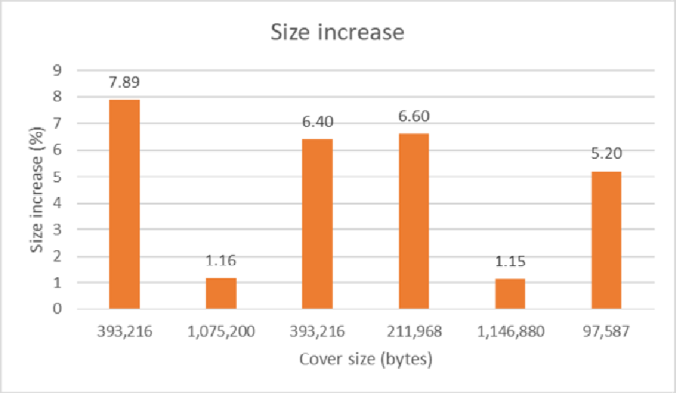


Fig. 3. Size increase of Stego-image

Meanwhile, when viewed from the process time required for insertion obtained an average yield of 0.75 milliseconds/bytes. Thus if the number of cover image size and data of 100 KB then it can be predicted that the required computation process is 100 x 1024 x 0.75 = 76,800 milliseconds or 76.8 seconds. The larger the size of the data or the cover being processed, the longer the computation process is required to do the insertion.

Testing of proposed methods also shows that the success rate of applications in encrypting and inserting messages is 58%. Failure encryption and data insertion process occur on the image cover with a low resolution. The image resolution shows the insertion of data capacity. All of the failed testings occurs on a test with a cover image that has a resolution below 1024x720. It is therefore recommended to use a larger cover image resolution to accommodate large data.

IV. CONCLUSIONS

After testing and evaluation of the program, it can be drawn some conclusions. The applications generated in this research are able to secure data or document files such as word files (.doc, .docx), excel files (.xls, .xlsx), powerpoint (.ppt, .pptx) files, and pdf files. Meanwhile, the combination of the DES cryptographic and DCT steganographic methods proved to improve data security because it has two levels of security. Based on the experiment can also be concluded that the stego-image quality can still be in a good category with an average value of PSNR of 46.9 dB. The combination the two methods resulted in a computation time of 0.75 milliseconds/bytes. The computational time still needs to be improved in the future research. Overall, the success rate of the proposed method in securing the data was 58%. The success of the data security process depends on the resolution of the cover image used. In this study, it is recommended to use a cover image resolution of 1024 x 720 or more.

This research provides a data security application that can be useful for improving the security of data files before being sent over the public network. In the next study, the computation time needs to be optimized again so that it becomes faster. Also, an increase in file size of 4.79 times can be reduced by adding a compression method or optimizing the encryption algorithm used.

References

[1] R. Primartha, “Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma Data Encryption Standard (DES),” J. Sist. Inf., vol. 3, no. 2, pp. 371–387, 2011.

[2] Siswanto, Feriadi, G. P. Utama, and A. F. Achmad, “Pengamanan Data dengan Menggunakan Algoritma Kriptografi AES, RC4 dan Kompresi LZ77 berbasis Java pada Badan Karantina Pertanian,” in Seminar Nasional Telekomunikasi dan Informatika (SELISIK), 2016, pp. 115–120.

[3] A. Pudoli, “Pengamanan Pesan Yahoo Messenger dengan Hybrid Cryptosystem Kombinasi RSA dan Vigenere Double Columnar Transposition Berbasis Android,” J. Telemat. MKOM, vol. 7, no. 1, pp. 86–95, 2015.

[4] M. Gunjal and J. Jha, “Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm,” Int. J. Comput. Trends Technol., vol. 11, no. 4, pp. 144–150, 2014.

[5] S. Fitri, “Implementasi Algoritma Kriptografi DES dan Watermark dengan Metode LSB pada Data Citra,” STMIK Amikom, 2010.

[6] A. Solichin and Painem, “Motion-based Less Significant Frame for Improving LSB-based Video Steganography,” in 2016 International Seminar on Application for Technology of Information and Communication, 2016, pp. 179–183.

[7] R. E. Yang, Z. Zheng, S. Tao, and S. Ding, “Image steganography combined with DES encryption pre-processing,” in 6th International Conference on Measuring Technology and Mechatronics Automation, 2014, pp. 323–326.

[8] S. Sekhon Brar and A. Brar, “Double Layer Image Security System using Encryption and Steganography,” Int. J. Comput. Netw. Inf. Secur., vol. 8, no. 3, pp. 27–33, 2016.

[9] A. Rohmanu, “Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File,” J. Inform. SIMANTIK, vol. 1, no. 2, pp. 1–11, 2017.

[10] V. S. Babu and H. K. J, “A Study on Combined Cryptography and Steganography,” Int. J. Res. Stud. Comput. Sci. Eng., vol. 2, no. 5, pp. 45–49, 2015.

[11] C. P. Shukla, R. S. Chadha, and A. Kumar, “Enhance Security in Steganography with cryptography,” Int. J. Adv. Res. Comput. Commun. Eng., vol. 3, no. 3, pp. 5696–5699, 2014.

[12] N. Manwade and S. Nigam, “LSB Image Steganography with DES Cryptography,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 5, no. 7, pp. 761–764, 2015.

[13] M. Juneja and P. S. Sandhu, “Data Hiding with Enhanced LSB Steganography and Cryptography for RGB Color Images,” in 2nd International Conference on Latest Computational Technologies (ICLCT’2013), 2013, pp. 1–4.

[14] S. P. N., S. A. Hussain, and B. P. M., “Advanced Security Using Cryptography and LSB Matching Steganography,” Int. J. Comput. Electron. Res., vol. 3, no. 2, pp. 52–55, 2014.

[15] S. Panghal, S. Kumar, and N. Kumar, “Enhanced Security of Data using Image Steganography and AES Encryption Technique,” Int. J. Comput. Appl., pp. 1–4, 2016.

[16] D. K. Sarmah and N. Bajpai, “Proposed System for Data Hiding Using Cryptography and Steganography,” Int. J. Comput. Appl., vol. 8, no. 9, pp. 7–10, 2010.

[17] R. N. Ibrahim, “Kriptografi Algoritma Des, Aes/Rijndael, Blowfish Untuk Keamanan Citra Digital Dengan Menggunakan Metode Discrete Wavelet Transformation (Dwt),” J. Comput. Bisnis, vol. 6, no. 2, pp. 82–95, 2012.

[18] S. P. Ravi and L. Dhanalakshmi, “DWT and Modified AES based Secure Image Steganography on ARM A8 Processor,” Int. J. Eng. Res. Technol., vol. 4, no. 5, pp. 1482–1486, 2015.

[19] M. K. Ramaiya, “Improvisation of Security aspect of Steganographic System by applying RSA Algorithm,” Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 7, pp. 245–249, 2016.

[20] Alamsyah, M. A. Muslim, and B. Prasetiyo, “Data hiding security using bit matching-based steganography and cryptography without change the stego image quality,” J. Theor. Appl. Inf. Technol., vol. 82, no. 1, pp. 106–112, 2015.

[21] T. S. Barhoom and S. M. A. Mousa, “A Steganography LSB technique for hiding Image within Image Using blowfish Encryption Algorithm,” Int. J. Res. Eng. Sci., vol. 3, no. 3, pp. 61–66, 2015.

[22] A. Ilhamsyah, “Steganografi pada Citra JPEG dengan Memanfaatkan Koefisien DCT Terkuantisasi,” 2014.

[23] V. M. Amal and A. R. Yohannis, “Aplikasi Steganografi pada Citra Digital Menggunakan Algoritma Discrete Cosine Transform,” J. Sains dan Teknol., vol. 2, no. 1, pp. 77–88, 2015.