4

by Alam Syah

Submission date: 11-Jun-2021 11:11AM (UTC+0700)
Submission ID: 1604481212
File name: 11Vol82No1-jatit.pdf (506.2K)
Word count: 3430
Character count: 17464

Journal of Theoretical and Applied Information Technology
10th December 2015. Vol.82. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DATA HIDING SECURITY USING BIT MATCHING-BASED STEGANOGRAPHY AND CRYPTOGRAPHY WITHOUT CHANGE THE STEGO IMAGE QUALITY

[1]ALAMSYAH, [2]MUCH AZIZ MUSLIM, [3]BUDI PRASETIYO

[1,2,3]Departmen of Computer Science, Semarang State University, Indonesia

Email: [1]alamsyah@mail.unnes.ac.id, [2]a212muslim@yahoo.com,
[3]budipras@mail.unnes.ac.id

ABSTRACT

This research discussed about the data hiding information using steganography and cryptography. New method are discussed to secure data without change the quality of image as cover medium. Steganographic method is used by find the similarity bit of the message with bit of the MSB (Most Significant Bit) image cover. Finding of similarity process is done by divide and conquer method.The results are bit indexposition, thenthenencrypted using cryptographic. In this paper we using DES (Data Encryption Standard) algorithm. We use data information as message, images, and key as an input. Then, we use our method to secure message. The output is encrypted bit index which containt data hiding information and can be used to secure the messages. To reconstruct the contents, we require the same image and same key.

Outcomes of our method can be used to secure the data. The advantages of this method are the capacity of stored data hiding of messages can be larger than the image. The image quality will not change and the capacity of stored messages can be larger than the image. Acoording to the research, both gray scale and colorful images can be used as image cover, except the image contains 100% black and 100% white. Bit matching process on image which have much variety of color takes less time. The damage of messages due to the addition of "salt and pepper" noise starts from 0.00049of MSE.

Keywords: bit index, bit matching, cryptography, divide and conquer, MSB, steganography.

1. INTRODUCTION

These recent years, the human need for information is increasing. In the midst of rapid development of information technology, the internet is no longer providing secure information. The development of search-engine coupled with the development of virus, bugs, spam and hackers who can steal confidential data [1]. To solve this problem, various ways have been developed to improve data security, such as cryptography and steganography. For example, [2] using steganography Techniquesin the study of Distributed XML.

Steganography is the art and science of hiding data in other media as a cover in order to makethe data looks sketchy [3]. Cryptography is the art and science of maintaining the confidentiality of data [4]. In cryptography, the original data is converted into another form that can not be read. The combination of steganography and cryptography can simultaneously increase the security of the data [5].

Method for combining steganography and cryptography has been developed. In general, the mostly used technique is message encrypting first (cryptography), then hiding it into media cover (steganography)[6]. However, the embedding process can affect the quality of the cover media. A data hiding method by improved LSB substitution process is proposed by [7]. The quality of stego-image can be greatly improved with low computational complexity.

Efforts to minimize the quality changes of cover image can be done by embedding the data in the least significant bit. Changes in the quality of cover is invisible [8], but the embedding of cover into the least bit tends to make the cover prone to robust. Robust resistance can be done by embedding the data in the first bit (most significant bit), but it will change the quality of the cover and it will look suspicious. Primitive structural method was proposed by [9] for improve capacity text steganography can be embed. Each bit of secret text will be placed at corresponding place in the cover text.

Journal of Theoretical and Applied Information Technology
10th December 2015. Vol.82. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Other studies conducted by [10] developed a new way of merger steganography and cryptography without changing the media cover. The technique is performed by matching the message bits on the cover, and then continue the process of encryption (cryptographic). One well-known cryptographic algorithms since 1977 and became a worldwide standard is the Data Encryption Standard (DES) .

This research willcombine steganography and cryptography without changing the media cover. The steganography method used is a method based on bit matching in the first bit (most significant bit) and the cryptographic method used is the DES algorithm.

2. REVIEW OF LITERATURE

Various methods have been developed for data security. In general,the techniques use this encrypting themes sage first (cryptographic process), and then embedding it into theme diacover (steganography process)[6].

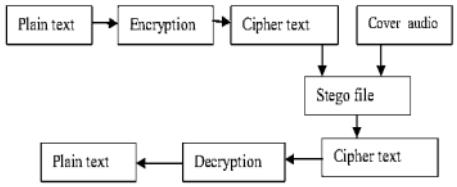

Figure 1.Combination Of Steganography And Cryptography[6].

Combination technique is not only limited as shown inFigure1. Research [11] examines two approach estosecure steganography mediacover (image). Securing steganography imageis done by encrypting. The first method, steganography image is directly encrypted with S-DES, the result is a ciphertext. The second method, the image is encrypted then ciphertext from encryption will be embedded ona nother image.

One of the easiest methods of steganography is LSB (Least Significant Bit). The procedure to perform this method is to embedthe least bit at each pixel with the message bits. Terminology LSB is reviewed by [12]. The LSB embedding will change the bit value, but it will be invisible, so that the third party does not know the existence of the secret message behind the media cover [7].

The use of LSB on the combination of steganography and cryptography was done in a research conducted by[12]. The process consists of three stages, namely encryption, steganography and decryption. Encryption and decryption is done with DES algorithm (Data Encryption Standard). The use of LSB can minimize the image quality changes, but the capacity of messages that can be accommodated is due to the size of the image. Kekre, et al. [13] conducted a LSB steganography study to increase the messages capacity with PVD approach (Pixel value differencing). LSB insertion is based on comparison of the MSB bit value. If the value of the first 4 MSB bits is "1", then embed it on the last 4 bits. If the first 3 bits MSB is " 1 ", then embed it on the last 3 bits. If the first 2 MSB bit is " 1", then embedit on the last 2 bits. If the value is outside the criteria, then the embedding is done on the last bit (least).

Image quality is an important component in steganography. Challita and Farhat [10] developed another way to combine both steganography and cryptography without changing the image quality. The technique is performed by matching the message bits on the cover, the results is in the form of bit position index. Index is then encrypted. The output is bit index ciphertext.

Bit matching is done by divide and conquer[14] that consist of three processes, namely divide, conquer, and combine. Arrangement of long bits is splitting it into two smaller parts (divide), then match each section (conquer). The results of each part of the solution then combined into a total solution (combine).

3. RESEARCH METHOD

Solving a problem begins with the development of software in the process of combining steganography and cryptography used Agile Method as seen in Figure 2.

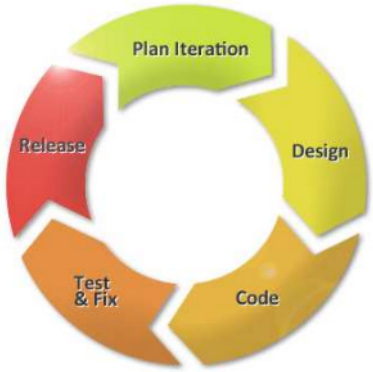

Figure 2. Agile Method

Journal of Theoretical and Applied Information Technology
10th December 2015. Vol.82. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Agile method is methodology development of software based on short-term development system that require adaptation rapidly than the developer to changes of any form [15].The step of method: planning, design, code, test & fix, and release.

The combination of stego-crypto in this caserequired 4 processes, they are bit matching, encryption, decryption and reconstruction. The details are as follow.

3.1. Matching Bit

In this study the method of matching is done with divide and conquer[14]. The matching bit process is as follows.

Input: secret message and image
Output: secret bit position

Procedure:
Step 1: Convert the message and image in binary.

Step 2: Put the value of MSB image.

Step 3: Perform the matching messages on MSB image. If the bit message is contained in the MSB image, then proceed to save the position of the bit index. Index saving consists of index position of the first (start) and the position index of the last bit (end). If the matching process does not occur, continue the process step 4 as follows.

Step 4: Divide the message into two parts of equal length of the left (L [i]) and right (R [i]).

Step 5: Repeat the same steps as instep 4), with L [i] and R [i] as input. If all the bit message are contained in the image, the matching process is completed and continue to step 6). If not, repeat step 3) with L [i] and R [i] as any step .

Step 6: Keep all bit index from matching results.

Step 7: The output is a vector that contains the index structure of bit position.

3.2. *Encryption*

Secret bit position then encrypted by cryptography algorithm (DES) shown at Figure 3.

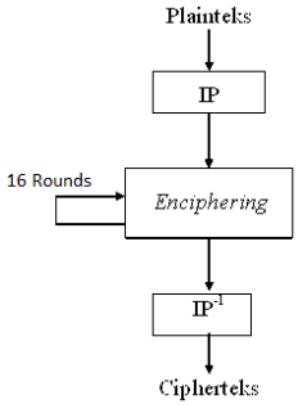

Figure 2a..Des Algorithm

The ecryption process is as follows.
Input: secret bit position (plaintext) and key.
Output: chipertext of bit position.

Procedure:
Step 1: Broke the 64-bit plaintext into L (32 bit) R (32 bit).

Step 2: Perform initial permutation (IP).

Step 3: Encrypt in 16 rounds (enchipering). Internal locks on each different lap.

Step 4: Invert the initial permutation (IP^{-1}).

3.3. *Decryption*

The decryption process is as follows.
Input: chipertext of bit position and key
Output: Plaintext.

Decryption of the ciphertext is the inverse of the encryption process. DES uses the same algorithm for encryption and decryption. In the process of decryption, the key sequence used is the inverse one namely K16, K15, ...,K1. For each round of 16, 15, ...,1, the output a teach round of deciphering is

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i).$$

3.4. Reconstruction

Reconstruction aims to restore the message to its original form.

Input: text file (that consists of bit and image index location)
Output: composition of bit meggase.

Journal of Theoretical and Applied Information Technology
10th December 2015. Vol.82. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Procedure:
Step 1: Convert the image in binary form and take the bit of MSB image.

Step 2: Read the contents of two index vectors. The first index is a bit's early position (start) and the second index is the bit's end position (end).

Step 3: Taking the value of bit image based on step 2).

Step 4: Repeating the process step 2) and step 3) until the last index position.

Step 5: The composition of the bits will create an output in the form of bit message

3.5. Combination Steganography and Cryptography

3.5.1.Overview

Combination of steganography and cryptography in this research consists of two main processes: embedding and extraction which is generally shown in Figure 4.

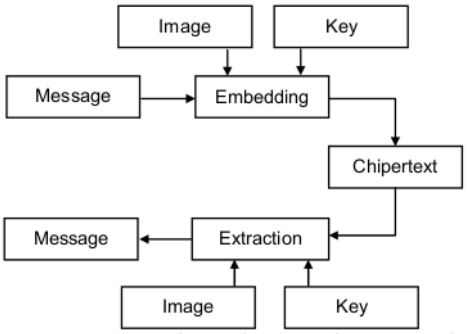

Figure 4.Overview The Combination Of Steganography And Cryptography

Embedding process (Figure 5) consists of bit matching and encryption, the result is ciphertext. Extraction process (Figure 6) consists of decryption and reconstruction; the results are in the form of a message.

3.5.2. Embedding Process

Embedding process aims to generate bit index position as shown in the Figure 5.

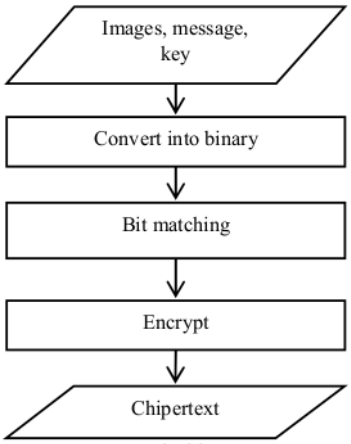

Figure 5.Embedding Process

Input: secret messages, images, andkey.
Output: ciphertext.

Algorithm of embedding steps as follows.
Step 1: Read input information: images, messages, and key.

Step 2: Convert the message and image in binary form.

Step 3: Match the bit message with the bit of MSB image. The same bit positions are stored in the bit vector index.

Step 4: Encrypt the bit vector index with DES algorithm.

Step 5: The output is ciphertext. The ciphertext contains a bit vector that has been encrypted.

3.5.3. Extraction process

Extraction process as shown in the Figure 6 store the message to its original for min order to maintain the original contents.

Journal of Theoretical and Applied Information Technology
10th December 2015. Vol.82. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

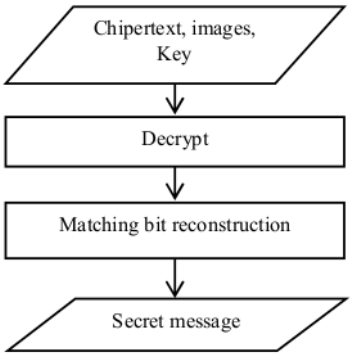

Figure 6.Extraction Process

Input: ciphertext vector, a key, and image.
Output: original message.

Algorithm of extraction process steps are as follows.

Step 1: Input key, ciphertext vector, and image.

Step 2: Decrypt the vector with the key, the decrypted plain text is in the form of bit index.

Step 3: Do a message reconstruction by matching bit of MSB image based on bit index vector.

Step 4: The output isthe message.Finish.

4. RESULTS AND DISCUSSIONS

The result is application programs of stego-crypto which has developed using the programming language MATLAB R2009 a then use it forsecure the data.

Experiment 1: Testing the image color

Selecting the secret messages in file transfer.txt. Then Choosing a cover imageJet.bmp (Figure 7).

Figure 7. Cover Image

Typing key as the encryption key for DES, for example key: 1234567.The output of embedding is bit index position (Figure 8).

vÀáÞhsÂ«A°9üª ànÕsm7-y4fé>>²å #¶i<`~¡*Z g?.a¦«¥¦è~Ã\þ+|Í$I3M"Ú_x6¶zø±ä-U2¿ï^«üu¥Dy VhIOvA0ÊFÁ];p¢f<ú4½ëaK«ø:XkÄ+m{ú7zè/8( \Gêéª Z~µ}êË 0k{ Ü|DHÛZ é£[;ÿÅÀu/¶äN §oKqÂð¨¤.Ð#¥ûR#á¢'ø|þX kMO{ªÙý¤;®iùröÂ 8,ÐýXUjD ®G[Ü®{<y6WLõwÝåXô¤á71F|6D Oxo LóÛy¥ÅÀ ïhi*7}GÑ>ñ,yX8È8äY5ÆÛMñ 7°çdÅ<pdÃ×v£¢`äiJ¦÷H±áL*<«¡¡dÆÎg|_Aª4±k¡ æGäñýjÛê0uX³¹x=IÊ Kï¬·L=?óK×úR¦zZV\dÝr°ê èJ!¶ÂP fta[)a¼ç ÷Fæú·»ÝzÒäíÒS¯ ³Ë$8õùÔþUÖ#És

Figure 8. Encrypted bit index.

Experiment 2: Experiment in Different Size Resolution

The application was also tested with different image sizes, ranging from 512px, 256px, 128px, to 64px. The test result (Table 1 and 2) shows that the larger the image resolution, the longer the bit matching process will take. The bit matching time of "Jet" is 0.729 sec.

Table1.The test results embedding process

Image	Resolution (px)	Embedding time ('s)		
		Matching	Encrypt	Total
"Jet"	512 x 512	2,038	12,186	14,713
	256 x 256	0,567	11,341	12,095
	128 x 128	0,221	10,714	11,039
	64 x 64	0,089	10,734	10,902
	Average	0,729	11,244	12,187

Table 2.The test results reconstruction process

Image	Resolution (px)	Reconstruction ('s)		
		Decrypt	Recons-truction	Total
"Jet"	512 x 512	10,564	0,181	10,900
	256 x 256	11,099	0,267	11,574
	128 x 128	10,704	0,183	11,503
	64 x 64	10,575	0,179	10,946
	Average	10,736	0,203	11,231

Experiment 3: Testing with Giving Noise

Noise 'salt and pepper' was given to the image in the next embedding process. The image was given noise 'salt and pepper' with standard deviation, d=0.001; 0.005, 0.01; 0.05. The image has been given a noise then tested in the extraction process store cover the messages. Then computing then PSNR that can computed by:

$$PSNR = 20.\log_{10}\frac{R}{MSE}$$

Where R is the maximum fluctuation in the input image data type.R=255. Then, MSE computing by as follows.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left|f(x,y) - g(x,y)\right|^2$$

where f(x,y) and g(x,y) denote pixel value of original and the reconstructed image at the position (x,y), respectively. The Test results with Noise shown in the Table 3.

Table3.The Test Results With Noise

Citra	Salt & pepper (d)			
	d	MSE	PSNR	Message
"Jet"	0,001	0,00014	61,398	Fine- readable
	0,005	0,00056	55,936	Fine- readable
	0,01	0,00123	52,807	Fine- readable
	0,05	0,00515	46,077	Damage-readable
"Lenna"	0,001	0,00030	34,987	Fine- readable
	0,005	0,00140	28,435	Fine- readable
	0,01	0,00310	25,014	Damage-readable
	0,05	0,01400	18,282	Damage-readable
"Pepper"	0,001	0,00010	67,295	Fine- readable
	0,005	0,00483	50,094	Damage-readable
	0,01	0,00094	57,320	Damage-readable
	0,05	0,00483	50,094	Damage-readable
"Baboon"	0,001	0,00013	67,773	Fine- readable
	0,005	0,00049	60,369	Damage-readable
	0,01	0,00091	57,660	Damage-readable
	0,05	0,00494	50,410	Damage-readable

Test results of message reconstruction on a black and white image with the addition of salt & pepper noise remains good. Messages can be read, but there was one image which was damaged. While most of the colorful images were damage, except the image of "Jet" and "Lenna" which only suffer from a little damage. Both "jet" and "lenna" images have the highest MSE value 0.014. Damage to colorful image occurred from 0.00049 MSE on image "Baboon" which incidentally has a fairly simple color variations. The result of message reconstruction will produce the changed message as well.

5. CONCLUSION

Step of hiding data security in this study consists of two processes. First, the embedding process which includes the process of matching the same bit thenencrypt it. Secondly, the extraction process which includes the decryption process then construct bit position to restore the message.The advantages of this method are the capacity of stored data hiding of messages can be larger than the image. the image quality will not change and the capacity of stored messages can be larger than the image

The experiment with addition noise to the image causes some changes in the message content. In the black and white image, the changes are not significant, while in the colorful imagethe message content changes a lot. Damage occurred on the addition of salt and peper noise start from MSE 0.00049.

6. REFERENCES

[1] Kautzar, M.G., 2007, *Studi Kriptografi Mengenai Triple DES and AES*, ITB, Bandung.

[2] Memon, A. G., Khawaja, S. & Shah, A., 2008, Steganography: A New Horizon for Safe Communication Through XML. *Journal of Theoretical and Applied Information Technology (JATIT), 4*, 187-202.

[3] Provos, N., and Honeyman, P., 2003, Hide and Seek: An Introduction to Steganography, *IEEE Security & Privacy Vol. 1(3)*, 32-44.

[4] Schneier, B., 1996, *Applied Cryptography 2nd Edition*, Wiley & Sons. Inc., New York.

[5] Krenn, R., 2004, *Steganography and Steganalysis*, Whitepaper.

[6] Raphael and Sundaram, A.J., and Sundaram, V., 2011, Cryptography and Steganography – A Survey, *International Journal Comp. Tech. Applied Vol. 2 (3)*, 626-630.

[7] Sharma, V. K., Shrivastava, V., 2012, A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection, *Journal of Theoretical and Applied Information Technology (JATIT) Vol. 36 No.1*, 1-8.

[8] Chan, C. K., and L.M. Cheng, 2004, Hiding Data in Images by Simple LSB Substitution, *Pattern Recognition Vol. 37(3)*, 469–474.

[9] Roslan, N. A., Mahmod, R., Udzir, N. I., and Zurkarnain, Z. A, 2014, Primitive Structural Method for High Capacity Text Steganography, *Journal of Theoretical and Applied Information Technology (JATIT),Vol. 67 No.2.*

[10] Challita, K., andFarhat, H., 2011, Combining Steganography and Cryptography: New Directions, *International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1),* 199-208.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[11] Narayana, S., and Prasad, G., 2010, Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions, *Signal & Image Processing: An International Journal (SIPIJ) Vol. 1(2)*, 60-73.

[12] Sharp, T., 2001, An implementation of Key-based Digital Signal Steganography, *Proc. Information Hiding Workshop Vol. 2137, Springer LNCS*, 13–26.

[13] Kekre, H.B., Archana A., and Pallavi N.H., 2012, Comparison between the basic LSB Replacement Technique and Increased Capacity of Information Hiding in LSB's Method for Images, *International Journal of Computer Applications (0975 – 8887) Vol .45 (1)*, 33-38.

[14] Cormen, T.H., Leiserson C.E., Rivest R.L., and Stein D., 2009, *Introduction to Algorithms, Third Edition*, The MIT Press, England.

[15] Gandomani, T.J., H. Zulzalil, A.Z.A. Ghani & A.A.MD. Sultan. 2013. Important Considerations For Agile Software Development Methods Governance. *Journal of Theoretical and Applied Informations Technology (JATIT),* Vol. 55 No. 3.

ORIGINALITY REPORT

11%	9%	10%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Omar A. Dawood, Abdul Monem S. Rahma, Abdul Mohsen J. Abdul Hossen. "The New Block Cipher Design (Tigris Cipher)", International Journal of Computer Network and Information Security, 2015 Publication	4%
2	Ali Akbar Lubis, Ronsen Purba, Irpan Adiputra Pardosi. "Combination of Steganography with K Means Clustering and 256 AES Cryptography for Secret Message", 2019 Fourth International Conference on Informatics and Computing (ICIC), 2019 Publication	1%
3	Ali Ikhwan, Rafikha Aliana A. Raof, Phaklen Ehkan, Yasmin Yacob, M. Syaifuddin. "Data Security Implementation using Data Encryption Standard Method for Student Values at the Faculty of Medicine, University of North Sumatra", Journal of Physics: Conference Series, 2021 Publication	1%

4	ijarcsse.com Internet Source	1 %
5	journal.unnes.ac.id Internet Source	1 %
6	pnrsolution.org Internet Source	1 %
7	sinta3.ristekdikti.go.id Internet Source	1 %
8	www.ime.cas.cn Internet Source	1 %
9	bear.buckingham.ac.uk Internet Source	1 %
10	Jin, Renchao, Enmin Song, Lijuan Zhang, Zhifang Min, Xiangyang Xu, Chih-Cheng Huang, and Josien P. W. Pluim. "", Medical Imaging 2008 Image Processing, 2008. Publication	<1 %
11	documents.mx Internet Source	<1 %
12	iugspace.iugaza.edu.ps Internet Source	<1 %
13	www.mdpi.com Internet Source	<1 %

14 Harianto Antonio, P. W. C. Prasad, Abeer Alsadoon. "Implementation of cryptography in steganography for enhanced security", Multimedia Tools and Applications, 2019
Publication

<1%

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	On		

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7