

Available online at <http://www.mecs-press.net/ijmsc>

An Approach of Securing Data using Combined Cryptography and Steganography

Rosalina, Nur Hadisukmana

Faculty of Computing, President University, Indonesia

Received: 05 August 2019; Accepted: 11 August 2019; Published: 08 February 2020

Abstract

The recent advance in information technology field forcing us to ensure the privacy of the digital data. It is very important to develop the method that may satisfy the needs. Many methods/techniques applied to reach that goal. One of efficient way to reach that secrecy can be achieved by combining Cryptography and Steganography. In this paper, a new RGB shuffling method proposed. The concept of encryption using RGB Shuffling is shuffling all of RGB element to distort the image. RGB Shuffling method will shuffle the RGB each pixel of image depends on the input password from user. The basic step of RGB shuffling is adding RGB element with ASCII password, invers and shuffle it.

Index Terms: RGB Shuffling, Cryptography, Steganography, Securing Digital Data

© 2020 Published by MECS Publisher. Selection and/or peer review under responsibility of the Research Association of Modern Education and Computer Science

1. Introduction

Cloud computing is a technology that utilizes internet services using a virtual server for the purpose of maintaining data and applications. The existence of cloud computing has lead to changes in an organization as through the concept of virtualization, standardization and other fundamental features in cloud computing could reduce the cost of Information Technology (IT), simplify the management of IT services, and speed up the delivery of services. Cloud computing enable users to transmit their data to cloud servers, users could access those data remotely over the Internet. It is also known for its flexibility and cost saving. The company can freely choose the appropriate services and that services can be changed as needed at any time and they don't need to care with the complexities of managing servers directly. The critical aspect related with the importance of data that is transferred on the cloud is the security of the data, since the data can be confidential. Thus, the data security should be enhanced and the data is protected from malicious attracts.

* Corresponding author.
E-mail address:

Deputy Chief of police of the Republic of Indonesia, Commissioner General Syafruddin [1] said that cybercrime vulnerability in Indonesia is number two highest in the world after Japan. The type of cybercrime that mostly did spreading hoax and stealing of secret personal data like document or photo. Data usually were stolen in a process of data transfer through email or file transfer. It usually happened because there is lack of data protection or security method in that process.

Cryptography and Steganography are technique that could be used as a data protection method. Cryptography is a technique to protect a data by changing the content of that data into a character that could not be understandable by the other person, while steganography is a technique of hiding a data inside another data. The uses of steganography technique makes the other people do not realize that there is a confidential data in the data transfer. Media that commonly used to carry the secret message or data are image or audio.

2. Literature Review

Many researches have been conducted to secure the data by combining cryptography and steganography, combining these two techniques could enhanced the security [2,3,4,5]. A new approach was proposed [6] to encrypt the image by shuffling the RGB pixels, in that research, the cipher image were retrieved by extracting the RGB pixels of the input image, and then the RGB values were swapped by changing the position and the values of the RGB pixels. [7] also proposed encryption technique by shuffling the RGB pixel values by displacing the RGB pixels and also interchanging the RGB pixel values, and at the end the total image size before encryption is the same as the total image size after encryption. While [8] proposed on key generation on a 2D graphics using RGB pixel shuffling and transposition, it fetched the RGB pixel values from cipher algorithm of $m*n$ size image. Securing image digital data could be done using ANN Method [9]. Combination of cryptography and steganography were used to secure digital data by combining three techniques: image compression, cryptography, and steganography [10]. [11] Conduct a research on video steganography using Arnold Scrambling and DWT, in [12] using block matching in DWT domain to improve the quality of the reproduced secret image. In [13] presented combination of cryptography and steganography by using sequential techniques and symmetric XOR technique. In [14] presented another steganography method which is used Least Significant Bit applied in cover image and Most Significant Bit applied in secret image.

3. Research Method

In this section, we will discuss proposed method which combined cryptography and steganography algorithms. In this proposed method first, the message is encrypted by use Message Digest 5 (MD5) Algorithm and for encrypted the image we use RGB Shuffling, then we used the Least Significant Bit (LSB) techniques to embed the encrypted information in image, video or audio. The LSB method works by hiding the information or file into the rightmost bit. With this method, there is not much alteration that affects the carrier file; even it is so close with the original quality. The concern using this method is the message that could be hidden is not much, because of the bit capacity of the carrier file.

A. Encryption and Decryption

In encryption phase, we use MD5 algorithm. The input message in MD5 algorithms is processes into blocks of 512 bit bits, divided into 32 bits of sub-blocks of 16 pieces. The output of the MD5 algorithm is hash value of 4 blocks of 32 bits. While for the encryption of image, we use RGB Shuffling. This method is developed by author. The concept of encryption using RGB Shuffling is shuffling all of RGB element to distort the image. RGB Shuffling method will shuffle the RGB each pixel of image depends on the input password from user. The basic step of RGB shuffling is adding RGB element with ASCII password, invers and shuffle it. The process of RGB shuffling is shown in Figure 1.

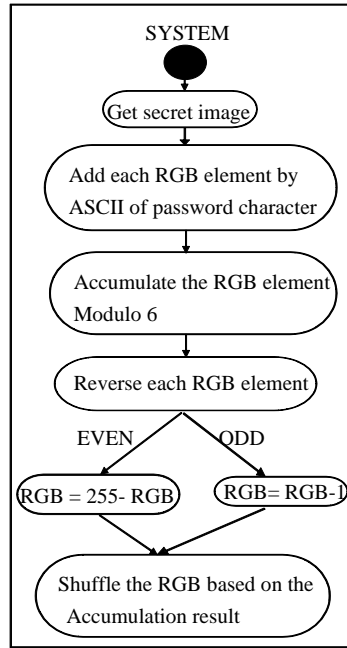


Fig.1. RGB Shuffling Process

Adding each RGB Element in a pixel with ASCII character of password means that each pixel will be added by ASCII character of password. The password will be repeated, this means when adding the RGB element with password and in the last of character of password, the value of ASCII character of password for adding RGB element will be in the first character again until all of RGB element is added. Invers RGB element means that the value of RGB element will be inversed from odd to even and vice versa. After adding with ASCII and Invers is done, the RGB element each pixel will be shuffled. Shuffled means that RGB position will be changed, for example red become green, blue becomes red, and etc. Table 1 shows the result of shuffling RGB element, the result is define to calculate the total of element red, green and blue modulo six. This is used for the main party for encrypting by shuffling the element of RGB.

TABLE 1. SHUFFLING RGB ELEMENTS

Result (Sum of RGB mod 6)	R	G	B
0	R	G	B
1	R	B	G
2	B	G	R
3	B	R	G
4	G	B	R
5	G	R	B

The input of the decryption stage is encrypted secret image and password. Due to the inverse of encryption, first the systems will invers the RGB element, odd to even and vice versa. After that sum all of RGB element modulo six, this step is to recover the shuffled RGB. The last step is adding the RGB element and Password. Therefore, the pixel will be recovered same as the original secret image. If the password is incorrect, the secret image will not be recovered, the output will be distorted image.

After All of RGB element is in their true position; RGB element is added by ASCII character of password. There is a validation for RGB element which is out of range, if more than 255, RGB element is subtracted by 256, if less than zero, RGB element is added by 256.

After the secret image is decrypted, the last phase is recovering the image; the first step is taking the information about the size of secret image which is in the last 8 pixel in red element. After getting the information of the size of secret image, set a pixel of RGB element of secret image from two pixel of cover image.

B. Steganography Phase

The method proposed to hide the information in this research is using Least Significant bit (LSB) method. This method will change the value of the bit in the rightmost position. Because of the value of that bit is low, the file expected did not have affected much by the final bit value that have been altered. LSB algorithm is done by replacing the bits of data that are not too influential in the carrier with the bits in the confidential or secret data. In the arrangement of bits in a byte (1byte=8bits), there is the most significant bit (Most Significant Bit or MSB) and the least significant bit (Least Significant Bit or LSB). LSB has advantage that the image will not change.

The processes of LSB method that take the data that already encrypted and change it into the form of binary. If the carrier is an image, With LSB method, the binary of text can be stored each RGB element of picture using only one LSB.

In this research, if the image is hide in another image. Whether the secret image and cover image have RGB element. Then, the size of secret image cannot be same as cover image. Taking four LSB for storing each bits of RGB element of secret image means that secret image needs cover image that has the size two times from secret image to put the bits of RGB element into cover image.

For example: the segment of image before steganography is processed as follow:

```
00110011 10100010 11100010 10101011 00100110
```

```
10010110 11001001 11111001 10001000 10100011
```

Then the segment of image after the secret message '1010101010' is inserted (1 LSB)

```
00110011 10100010 11100011 10101010 00100111
```

```
10010110 11001001 11111000 10001001 10100010
```

When the carrier is an image, then each RGB element of secret image will be separated into two parts, first bit and second bit. For example in pixel (0, 0), R=245, 245=11110101, first bit of R =1111, second bit of R = 0101. Two pixels in cover image will carry all of RGB element of one pixel of secret image. If the pixel of cover image is more than enough to store the RGB element of secret, the rest of pixel is equal to original pixel of cover image. The size of secret image must be carried by cover image. It store in the last 8 pixel of cover image. Suppose the maximum width and height of the secret image is 65535 or in binary equals 1111111111111111. Fig.2 shows a process of LSB method that takes the encrypted secret image and change and store the bit each RGB element each pixel of secret image in the cover image.

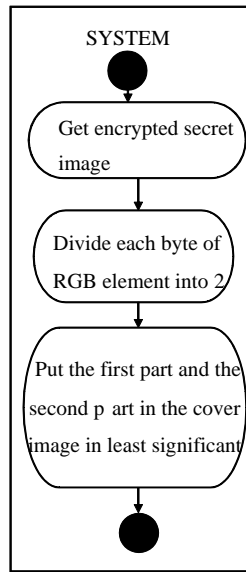


Fig.2 Least Significant Bit Process


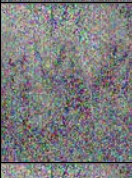
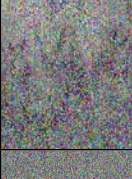

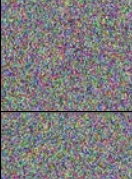

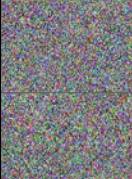

While if the carrier is audio, the first process is initialization of recognizing a signal audio by creating the memory stream and binary writer, then convert it to binary. The data of the wave audio should be converted into binary because when the data of signal audio is still in hex, it cannot be modified with using LSB method. Then, take the information of the leftstream and rightstream of an audio. So the hex of the both stream will be converted into string and after that, the data will be converted into char (example: from 13 14 15 16 into 1 3 1 4 1 5 1 6). The next is converting the stream into binary. For the message that will be embedded, the message will be converted into char and then converted into a binary. The next step is the process of the LSB method. The original leftstream of the wave audio signal will be duplicated to be modified. Then it will count the size of the leftstream available and compare it with the message size that will be hidden. If it satisfied the requirement, then LSB process will start by replacing the last digit of the leftstream with the message. If the leftstream size did not fulfil the requirement, then error message will be displayed. After that, the data of the modified leftstream will be converted again back to string to be replaced the original leftstream.

4. Result and Analysis

To evaluate the performance of the proposed system in this paper, it is tested using Peak Signal Noise Ratio (PSNR). Peak Signal Noise Ratio is used to compare the stego image and the cover image and to measure to quality of the stego image, the higher PSNR means the better the quality of reconstructed image. In this paper, reconstructed image is the stego image. Image application will hide several condition of secret image and password. The main concern for the test is ratio cover image and secret image, and password strength which is can determined by its length, complication and variation. Here are conditions for testing the performance of the system:

1. The resolution of cover image is 512 x 512 pixel
2. The resolution of secret image is 50%, 25%, and 12,5% of cover image
3. The password strength used is low, medium, high
4. The quality of stego image is defined is Peak Signal to Noise Ratio

TABLE 2. THE RESULT OF ENCRYPTED IMAGE AND STEGO IMAGE

No.	Secret Image Resolution	PasswordSt rength*	Encrypted Image	PSNR
1	50% cover image	Low		31.99
2	25% cover image	Low		38.00
3	12,5%cover image	Low		44
4	50% cover image	Medium		31.87
5	25% cover image	Medium		37.87
6	12,5%cover image	Medium		43.90
7	25% cover image	High		37.81
8	12,5%cover image	High		43.87

5. The encrypted image for encryption evaluation.
6. The extension of cover image is bitmap
7. The extension of secret image is jpeg.

Table 2 shows The result of encrypted image and stego image. The highest PSNR is achieved when the percentage of secret image resolution is 12,5% and the password is Low, while the lowest PSNR is achieved when the percentage of secret image resolution is 50% and the password is Medium. The password used to generate this PSNR value is low="computing", medium="itiscomputing2012", high="CoMpUtInG2012!". Determined at www.passwordmeter.com.

Table 3 shows the processing time to hide the secret image in different size of secret image. Processing time depends on the size of secret image and the length of the password. The bigger size of secret image and the longer length of password, processing time will be longer.

TABLE 3. PROCESSING TIME

No.	Secret Image Resolution	Password Length	Time (second)
1	111x74	4	0.489
2	111x74	8	0.547
3	111x74	12	0.6
4	222x148	4	0.707
5	222x148	8	0.889
6	222x148	12	1.09
7	310x206	4	0.945
8	310x206	8	1.311
9	310x206	12	1.77

5. Conclusions

In terms of information encryption, combining cryptography and steganography has proved to be greatly effective in terms of the security analysis. The additional RGB shuffling using least significant bit method contributed to increase the security of the digital image information against every vulnerable attack by the unauthorized access eventhough it is cannot guarantee full data security.

References

- [1] Rizki, Ramadhan. CNN Indonesia. CNN Indonesia. [Online] 7 17, 2018. [Cited: 05 22, 2019.] <https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia>.
- [2] Abdulzahra, Hayfaa, Ahmad, Robiah and Noor, Norliza Mohd "Combining Cryptography and Steganography for Data Hiding in Images" Applied Computational Science,2014, pp. 128-134.

- [3] Poduval, Aditya, et al. "Secure File Storage on Cloud using Hybrid Cryptography" *International Journal of Computer Science and Engineering*, 2019, Vol. 7.
- [4] Garg, Nancy and Kaur, Kamalinder. "Hybrid Information Security Model for Cloud Storage Systems using Hybrid Data Security Scheme", 2016, Vol. 3.
- [5] Rahman, Mohammad Obaidur, et al. "An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Techniques" *International Journal of Computer Science and Network Security*, 2018, Vol. 18, pp. 85-93.
- [6] Navita Agarwal, Prachi Agarwal "An Efficient Shuffling Techniques on RGB Pixels for Image Encryption", *MIT International Journal of Computer Science & Information Technology*, 2013, Vol. 3, No. 2, pp. 77-81
- [7] Quist-Aphetsi Kester, MIEEE "Image Encryption based on the RGB Pixel Transposition and Shuffling" *International Journal Computer Network and Information Security*, 2013, No.7 pp. 43-50
- [8] Londhe Swapnali, Jagtap Megha, Shinde Ranjeet, P.P. Belsare and Gavali B. Ashwini "A Cryptographic Key Generation on a 2D Graphics using RGB Pixel Shuffling and Transposition" *Proceedings of the International Conference on Data Engineering and Communication Technology, Advances in Intelligent Systems and Computing* 469, 2016, Vol. 2, Springer
- [9] Sanjay Kumar Pal, Sumeet Anand, "Cryptography Based on RGB Color Channels using ANNs", *International Journal of Computer Network and Information Security(IJCNIS)*, Vol.10, No.5, pp.60-69, 2018
- [10] Aumreesh Kumar Saxena, Sitesh Sinha, Piyush Shukla, "Design and Development of Image Security Technique by Using Cryptography and Steganography: A Combine Approach", *International Journal of Image, Graphics and Signal Processing(IJIGSP)*, Vol.10, No.4, pp. 13-21, 2018
- [11] Hnin Lai Nyo, Aye Wai Oo, "Secure Data Transmission of Video Steganography Using Arnold Scrambling and DWT", *International Journal of Computer Network and Information Security(IJCNIS)*, Vol.11, No.6, pp.45-53, 2019
- [12] Jaeyoung Kim; Hanhoon Park; Jong-Il Park "Image steganography based on block matching in DWT domain" *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, Page(s):1 – 4, Italy 2017
- [13] M. Saritha; Vishwanath M. Khadabadi; M. Sushravya "Image and text steganography with cryptography using MATLAB" *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPEs)* page(s): 584-587, India-2016.
- [14] Nikhil Patel; Shweta Meena "LSB based Image steganography using Dynamic key cryptography" 2016 *International Conference on Emerging Trends in Communication Technologies (ETCT)*, Pages(s): 1-5, India-2016
- [15] Baboon-image. Retrieved from <https://www.npmjs>.
- [16] Retrieved from <http://www.stefaneberube.com/>

Authors' Profiles



Rosalina Received B.Sc and M.Sc from President University. Currently working as a Lecturer in the Faculty of Computing, President University, Indonesia.



Nur Hadisukmana, received Bachelor degree from University of Indonesia ad Master degree from Oklahoma State University. Currently working as a Lecturer in the Faculty of Computing, President University, Indonesia.

How to cite this paper: Rosalina, Nur Hadisukmana," An Approach of Securing Data using Combined Cryptography and Steganography ", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.6, No.1, pp.1-9, 2020. DOI: 10.5815/ijmsc.2020.01.01