International Journal of Information System & Technology
Akreditasi No. 158/E/KPT/2021 | Vol. 6, No. 2, (2022), pp. 213-218

Maximum Security of Login Pin Data by Combining the Gifshuffle Algorithm and TCC Algorithm

Rivalri Kristianto Hondro

Universitas Budi Darma, Medan, Indonesia

rivalryhondro@gmail.com

Abstract

System or data security is very important in today's digital era. Various kinds of security techniques used, one of these techniques is the encoding technique by applying a number of cryptographic algorithms. The durability of cryptographic algorithms must of course be known before the algorithm is used and applied to a system or data to be secured. This study discusses the combination of the gifshuffle algorithm and the TCC algorithm for securing login pin characters.

Keywords: *Cryptography, Gifshuffle, TCC, Login Pin, Combination*

1. Introduction

Data is an object that is used and processed to produce useful information to others. The form of information that needs to be secured is confidential information, meaning that not everyone can access it. There are many data security techniques including encryption techniques (cryptography) and concealment techniques (steganography)[1][2]. The durability of cryptographic algorithms must of course be known before the algorithm is used and applied to a system or data to be secured.

Cryptographic technique is an encoding technique in which data objects that are encoded/secured can be known to exist, but the meaning or information contained in the encoded/secured data (cannot be understood), with a form like this can raise suspicions by other parties that the data is confidential. , then the intention to know the contents of the encoded information will be higher[3][4][5].

The importance of data encoding is not only changing the shape of the data or information content, but also being able to eliminate the meaning of information from the data itself even the existence and form of the data itself when unauthorized parties access or use it[6][7], it is necessary to combine data security using cryptography and steganography techniques. Fulfilling the security techniques described above, the authors choose algorithms related to cryptography and steganography, namely the triangle chain cipher algorithm and the gifshuffle algorithm.

2. Research Methodology

2.1. Cryptography

Cryptography was originally described as the study of how to hide the meaning of messages. In accordance with the modern generation of cryptography, cryptography is a science based on mathematical techniques related to information security that maintains the confidentiality, integrity, and authentication of data. So the application of cryptography is not just how to hide the meaning of the message but rather a set of techniques that provide information security[8][9].

2.2. Steganography

Steganography is the science and art of hiding secret messages in other messages so that the existence of these secret messages cannot be known. Steganography has two

ISSN : 2580-7250

properties, namely container media and secret messages[10][11]. The container media that can generally be used are text, images, sound, or video. While messages that can be hidden are articles, pictures, lists of items, passwords, program codes, or other types of secret messages[12].

2.3. Algorithm Triangle Chain Cipher

Algorithm The triangle chain cipher algorithm has a process rule with caesar cipher which shifts letters based on predetermined key numbers. The key number values used are natural numbers such as 1, 2, 3, 4, ... and so on. In addition to the primary key that has been determined, the second strength lies in the process of multiplying the sequence of numbers multiplied by the key. The value of the number line can be an even number, a Fibonacci series, a prime number series, and a number series that we can determine ourselves [13][14][7].

2.4. Algorithm Gifshuffle

Algorithm is one of the steganographic algorithms, where this algorithm works by hiding messages in gif images by doing a shuffle color map. gifsuhuffle algorithm can work on all gif images both in the form of transparency and animation[12]. The gifshuffle algorithm makes use of a gif file header that performs media insertion in a color palette. gif images contain a clourmap of up to 256 entries and produce a maximum storage capacity of 1683 bits[15].

The process of applying these two algorithms is carried out in parallel, namely where the triangle chain cipher cryptographic algorithm is first applied to encrypt data, then the results of the encryption process will be inserted into the image using the gifshuffle algorithm. The following is a schematic of the process of applying the two algorithms.

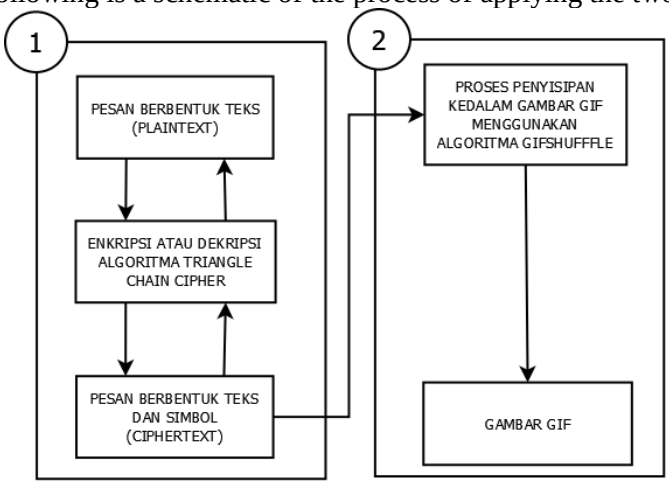

Figure 1. Deployment Process Scheme

In accordance with the scheme of the application process as shown above (1) first, the encryption process is carried out on the text, then (2) the second is the ciphertext insertion process into the GIF image.

The discussion carried out in this study tells about how to combine the triangle chain cipher algorithm for the message encryption process and the gifshuffle algorithm for the embedding process (hidden file) encrypted into a GIF image.

Meanwhile, when returning the message to its original form, the first processing activity is to **gifshuffle** message *(show file)* algorithm, which then performs the decryption process using a triangle chain cipher.

Two topics of discussion carried out in this study are (1) the encryption process followed by the insertion process and (2) the extraction process followed by the decryption process.

a) The following is the first discussion scheme

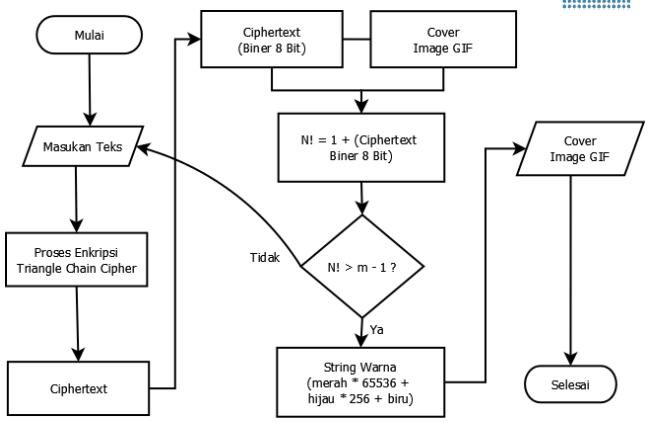

Figure 2. Message Encryption and Insertion Schemes

b) Scheme The following is the second discussion scheme

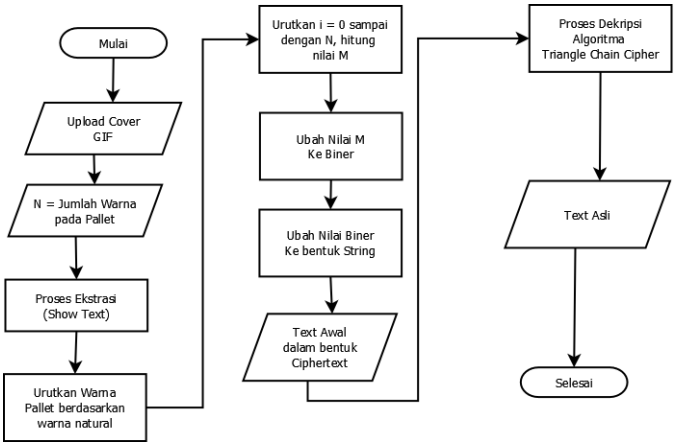

Figure 3. Message Extraction and Decryption Scheme

4. Result and Discussion

The process of testing the triangle chain cipher algorithm and the gifshuffle algorithm is carried out by encrypting the message text to be inserted on a digital image in GIF format as a cover where the encrypted message text is inserted. The display of the initial form of the encryption process and the embedding process can be seen in the following image.

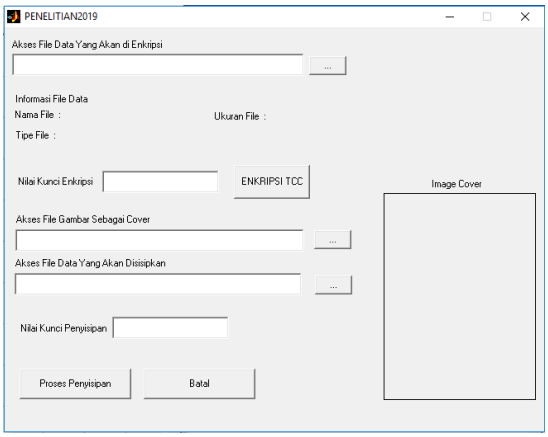

Figure 4. Encryption and Insertion Process Form Display

Testing process for the encryption and insertion form is carried out by:

a) Perform the process of uploading a data file containing text to be encrypted,
b) After the upload process runs successfully, information about the uploaded data file will appear including the name , type, file size,
c) Enter the crypto key value,
d) then click the "TCC ENCRYPTION" button to carry out the encryption process.
e) Save the encrypted file.
f) After the encryption process is done, the next step is to carry out the file insertion process
g) Click the upload image file button as a cover image,
h) Click the upload button for encrypted data files,
i) Enter the stego key value,
j) Click the "Insertion Process" button to carry out the insertion process, Click the "Cancel" button if you want to cancel the insertion process.

In accordance with the description above, the encryption and decryption testing process can be seen more clearly in the following picture.

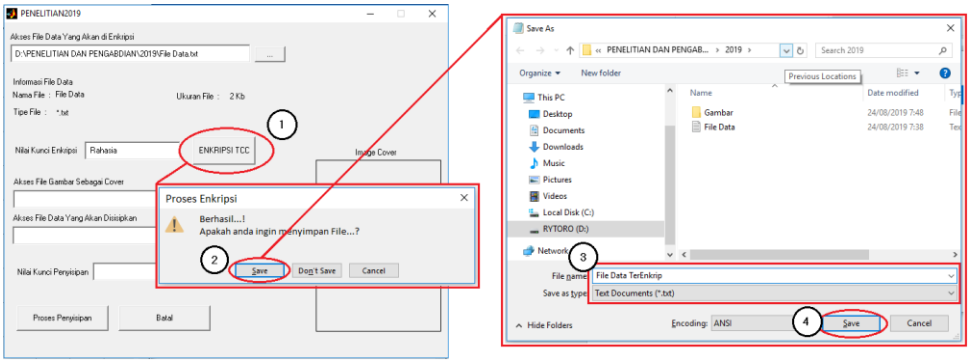

Figure 5. Encryption Process

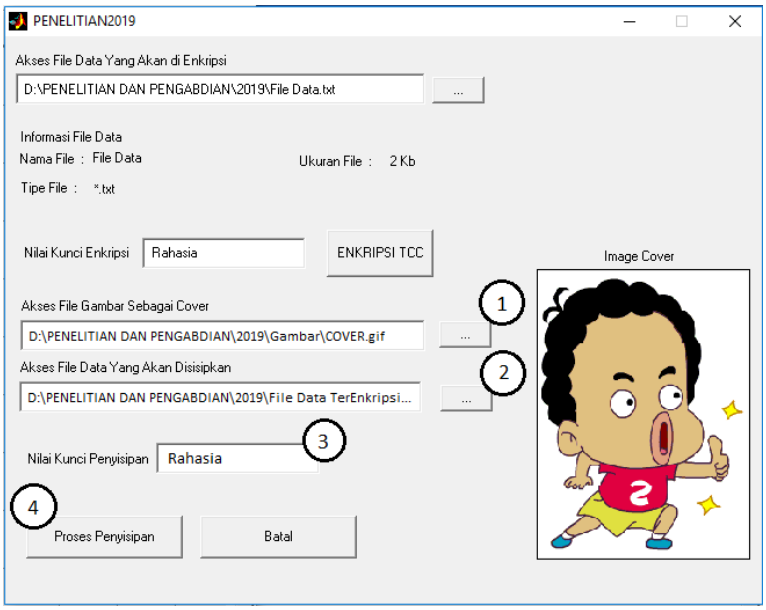

Figure 6. Insertion Process

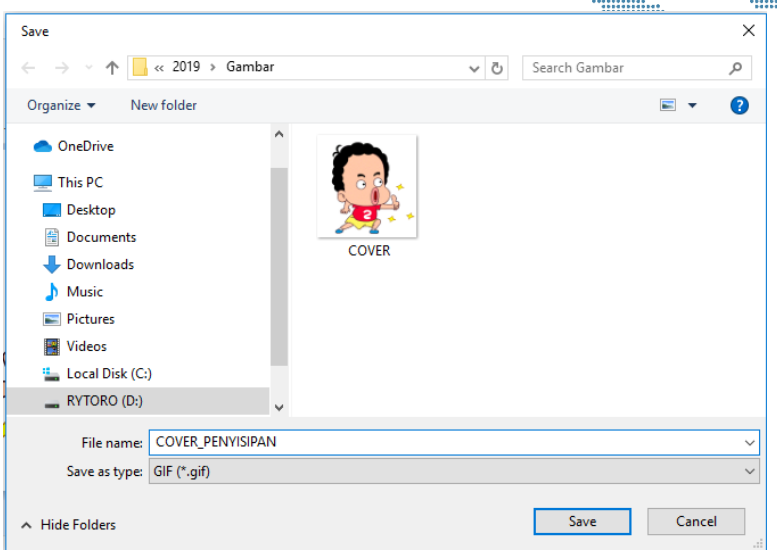

Figure 7. Process of Saving File Cover

Based on the tests carried out, the following results were obtained related to the application of the triangle chain cipher algorithm and the gifshuffle algorithm consisting of the

a) Confusion aspect
   Has a fairly good confusion value, so it is difficult for cryptanalysts to hack the ciphertext, meaning that it takes a long time to get the encrypted key.
b) Imperect (Vision Aspect)
   At this stage related to the difference in the appearance of the original image with the cover image (stego image) in accordance with the vision, testing was carried out by giving questions to 10 respondents. According to the responses of respondents assessing the difference between the original image and the stego image, 20% said it was different and 80% said it was the same.

4. Conclusion

After the process of analysis, discussion and testing of the application of the triangle chain cipher algorithm and the gifshuffle algorithm in securing files, the following conclusions are drawn from the research. The combination of cryptographic and steganographic security techniques is very appropriate to make people unable to access information without even knowing the existence of information from the data that has been secured. The tests carried out on the triangle chain cipher algorithm and the gifshuffle algorithm run successfully, resulting in a cover stego object that cannot be distinguished from the original image.

References

[1] L. J. Pangaribuan, "Kripografi Hybrida Algoritma Hill cipher dan Rivest Shamir (RSA) Sebagai Pengembangan Kriptografi Kunci Simetris," *J. Teknol. Inf. dan Komun.*, 2018.
[2] A. Hariati, K. Hardiyanti, and W. E. Putri, "Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks," *Sinkron*, 2018.
[3] R. Arifin and L. T. Oktoviana, "Implementasi Kriptografi Dan Steganografi Menggunakan Algoritma RSA Dan Metode LSB," *J. Din. Inform.*, 2013.
[4] D. Lombu, S. D. Tarihoran, and I. Gulo, "Kombinasi Mode Cipher Block Chaining Dengan Algoritma Triangle Chain Cipher Pada Penyandian Login Website," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, 2018, doi: 10.30645/j-sakti.v2i1.51.

[5] "Perancangan Perangkat Lunak Steganografi Menggunakan Least Significant Bit Dengan Enkripsi Vigenere Cipher," *e-Jurnal JUSITI (Jurnal Sist. Inf. dan Teknol. Informasi)*, 2020, doi: 10.36774/jusiti.v9i1.643.

[6] Z. Sun, H. Wu, Z. Zhou, and H. Kang, "On steganography detection of palette based images," *J. Inf. Comput. Sci.*, 2008.

[7] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020, doi: 10.1109/ACCESS.2020.2968985.

[8] Febriansyah, "Analisis dan Perancangan Keamanan Data Menggunakan Algoritma Kriptografi DES (Data Encyption Standard)," *Skripsi*, vol. XV, no. November, pp. 1–2, 2022.

[9] Z. Basim and P. Painem, "Implementasi Kriptografi Algoritma RC4 Dan 3DES dan Steganografi Dengan Algoritma EOF Untuk Keamanan Data Berbasis Desktop Pada SMK As-Su'udiyyah," *Skanika*, vol. 3, no. 4, pp. 45–52, 2020, [Online]. Available: http://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/1739

[10] D. Anggara and A. S. Sembiring, "Peningkatan Keamanan Data Teks Terenkripsi Algoritma Luciver Menggunakan Steganografi Gifshuffle Pada Citra," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, 2019, doi: 10.30865/komik.v3i1.1626.

[11] S. Rohayah, G. W. Sasmito, and O. Somantri, "Aplikasi Steganografi Untuk Penyisipan Pesan," *J. Inform.*, 2015, doi: 10.26555/jifo.v9i1.a2038.

[12] D. Andika and D. Darwis, "Modifikasi Algoritma Gifshuffle untuk Peningkatan Kualitas Citra pada Steganografi," *Program*, vol. 1, no. 2, pp. 1–9, 2020.

[13] P. Tarigan, H. Sunandar, B. Sinuraya, Z. Arizona Matondang, and G. Ginting, "Implementation of Triangle Chain Cipher Algorithm in Security Message of Social Media," *J. Phys. Conf. Ser.*, vol. 1573, no. 1, 2020, doi: 10.1088/1742-6596/1573/1/012024.

[14] C. H. Bennett, "Quantum cryptography: Public key distribution and coin tossing," *Int. Conf. Comput. Syst. Signal Process.*, vol. 1999, no. December, pp. 1–6, 2006.

[15] R. A. Larasati, "Analisis Teknik Steganografi pada Data di Dinas Komunikasi dan Infomatika Penajam Paser Utara Menggunakan Openstego dan Hex Editor Neo," *Repos. Itk*, vol. 1, no. 1, 2021, [Online]. Available: http://repository.itk.ac.id/id/eprint/17276