Jurnal CoreIT, Vol.8 No.2, December 2022
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

Combination RC4 Algorithm and Base64 Encryption on The Least Significant Bit Method

Soleman[1], Dendi Budiman[2], Sefty Mubaroq[3]
[1]Faculty of Computer Science, Borobudur University, Jakarta – Indonesia
[2]Faculty of Computer Science, Budi Luhur University, Jakarta – Indonesia
[3]Faculty of Computer Science, Mercu Buana University, Jakarta – Indonesia
solemediagrafik@gmail.com

Abstract – Steganography is an art form of hiding data or information on a medium. Steganography was created as a way to secure data by hiding it in other media so that it is "invisible". In steganography, secret data is hidden in a carrier such as sound, image or video. Securing messages using steganography is still vulnerable to third parties because the message inserted is still the original message, so that when it is successfully deleted from the message carrier it can be immediately identified. Given these problems, the steganography method needs to be combined with other methods to strengthen the level of data security, in this case a combination of steganography and cryptography will be carried out so that the embedded message will be different from the original message. Even if the data is deleted from the user, the message cannot be known immediately. In this trial, the RC4 cryptographic method which has a symmetric key and also Base64 will be implemented in the PHP and Android programming languages using the Least Significant Bit (LSB) steganography method which will create encrypted secret messages embedded in JPG format, JPEG image media formats on each the last bit of a pixel so that the eye does not see the difference between the inserted and non-inserted images with the original image variable/result of 131.91KB after the Encryption process the amount of data is 31.92KB with very small differences so that data security is maintained without being visible to the naked eye.

Keywords: Base64, Encryption, JPG, Least significant Bit, RC4, Steganography

Received November 2022 / **Revised** December 2021 / **Accepted** December 2022

INTRODUCTION

New technologies that are rapidly developing are very fast, effective and efficient. Technology makes it easier to communicate socially via SMS, BBM, Facebook, Line, Whatsapp, Email, etc. With ease of communication, it is necessary to have secret security, so that in communicating there are no leaks or our secrets are not detected or known by others. On internet social media, many things can be done by various groups, both small children, teenagers, and parents. Many people use the internet in negative terms, even current events, in the form of messages via social media that mention the name of someone whose veracity is still doubtful.

Given these problems, researchers use several references that are similar to previous studies including: The RC4 algorithm operates with the XOR method so that the XOR encryption operation is carried out very quickly assisted by the Base64 encoding algorithm in handling 0x00 [NUL] data reading in image files[1]. The encryption process method is easy to use and can also protect the confidentiality of data or information with cryptographic applications using the RC4 and Base64 methods[2]. Combining steganography techniques with cryptographic techniques where messages are encrypted first before being inserted into the file[3]. The combination of the RC4 and Base64 algorithms has a higher level of security than using only the RC4 algorithm[4]. The security system uses RC4 and Base64 Cryptographic Algorithms to ensure the security of online payment transaction data[5]. The encryption and decryption process using the RC4 algorithm is carried out 10 times from a total of 100 to 1000 characters, so that the resulting image has an error value and a quality value that is not much different[6]. Securing messages into images and changing the contents of messages from known meanings to unknown meanings[7]. Application of the rsa algorithm for instant message security on android devices[8]. The use of encryption with Base64 Encode is implemented in the PHP programming language, both the use of encryption and decryption of data, URL addresses and images[9]. Securing exam document files with image steganography using the physics method [10]. Review of the use of human senses and capabilities in cryptography [11]. Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome

DOI: 10.24014/coreit.v8i2.20106

structure [12]. Based on the background and results of previous research, data is converted into strings. It can be concluded that in the development of communication technology, security is needed to maintain the confidentiality of a message sent. Messages via cell phones or internet networks are vulnerable to eavesdropping. So that the message can only be accessed by the person we are aiming for, a secret message delivery technique is needed. Therefore, this study uses Steganography techniques, namely the technique of inserting secret messages into a media, digital data in computer files, images, articles, shopping lists, or other messages, so that other people do not know that the media contains messages. confidential. Secret messages in insertion steganography are not scrambled when the message is sent.

METHODS

A. Steganography

Steganography is the art of hiding messages within other messages in various ways so that other people do not realize there is something in the message. The word steganography (steganography) comes from the Greek, namely steganos which means hidden or veiled and graphein which means to write, so more or less means "to write hidden or veiled writing" [13].

This steganography technique has existed for 4000 years ago in the city of Menet Khufu, Egypt. Initially using hieroglyphics, namely writing using characters in the form of pictures. Scribes used this ancient Egyptian writing to relate the life of their master. This ancient Egyptian writing became the idea for today's secret messages. For this reason, ancient Egyptian writing using pictures is considered the world's first steganography [14]. The steganography process can be seen in Figure 1 below:

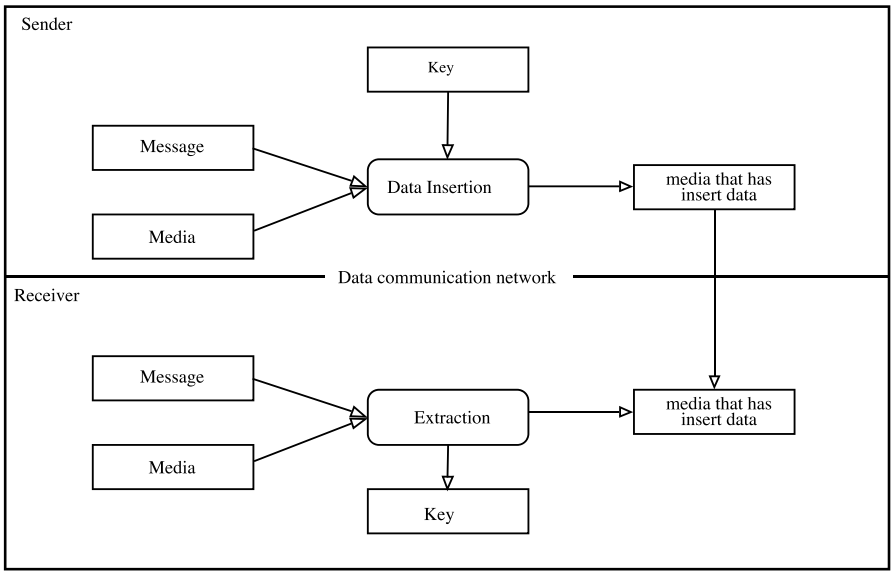

Figure 1. Steganography Process

In general, there are two processes in steganography namely the embedding process to hide messages and extraction to extract secret messages hidden in the messenger media.

B. Cryptography

Cryptography is a science that relies on mathematical techniques to deal with information security such as confidentiality, data integrity and entity authentication. Cryptography is part of a branch of mathematics called i. Cryptography aims to maintain the confidentiality of the information contained in the data so that the information cannot be known by other parties.

In maintaining data confidentiality, cryptography changes clear data (plaintext) into unrecognizable ciphertext data. This ciphertext is then sent by the sender to the recipient. After arriving at the recipient, the ciphertext is converted back into plaintext so that it can be recognized.

C. Least Significant Bit (LSB)

LSB is a technique commonly used in encryption and decryption of confidential information. The way the LSB method works is by changing the redundant cover image bits which have no significant effect on the secret message bits. The mechanism of the LSB method on 8-bit images using 4-bit LSB can be seen in Figure 2 below:

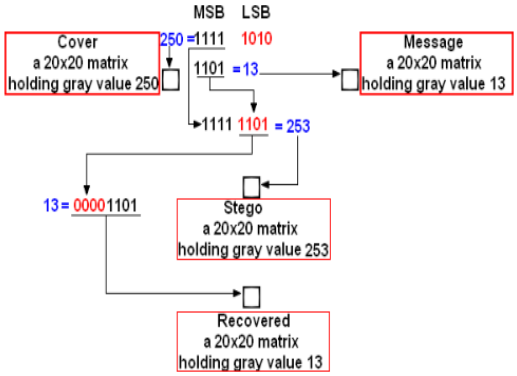

Figure 2. LSB mechanism

Figure 2 shows the implementation of LSB using pixel-based image media with an 8-bit value (gray value). Each pixel which consists of 8 bits is divided into 2 parts, namely 4 bits MSB (most significant bit) and 4 bits LSB (least significant bit). This is the LSB part that is converted into the value of the message to be inserted. After being tagged with a secret message, each pixel is reconstructed into a complete image that is similar to the original image media.

D. RC4 Cryptographic Algorithm

RC4 is a code flow type which means that the encryption operation is performed per 1 byte of characters for one operation. The Rivest Code 4 (RC4) cryptographic algorithm is a symmetric key algorithm created by RSA Data Security Inc (RSADSI) in the form of a stream chipper. [15]. This algorithm was invented in 1987 by Ronald Rivest and became the security symbol of RSA (which is an abbreviation of the names of the three founders: Rivest, Shamir, and Adleman).

RC4 uses key lengths from 1 to 256 bytes which are used to initialize tables that are 256 bytes long. This table is used for next generation pseudo random which uses XOR with plaintext to generate ciphertext. Every element in the table is swapped at least once. RC4 is a type of stream cipher so that RC4 processes units or input data, messages or information at one time. Units or data are generally bytes or sometimes even bits (a byte in the case of RC4) so that in this way encryption or decryption can be done with variable length.

This algorithm does not have to wait for some input data, messages or information before processing, or adding additional bytes to be encrypted. RC4 is widely used in several applications and is generally stated to be very secure, because RC4 is included in the symmetric algorithm, the key secrecy must be maintained and sent on a secure communication channel.

Until now it is known that no one has managed to crack or disassemble it, only the 40-bit export version which can be disassembled by brute force (trying all possible keys). The RC4 algorithm uses two Substitution Boxes (S-Boxes), namely an array of length 256 containing permutations from 0 to 255, and a second S-Box, which contains permutations which are function keys of variable length. The following RC4 cryptographic mechanism can be seen in Figure 3 below:

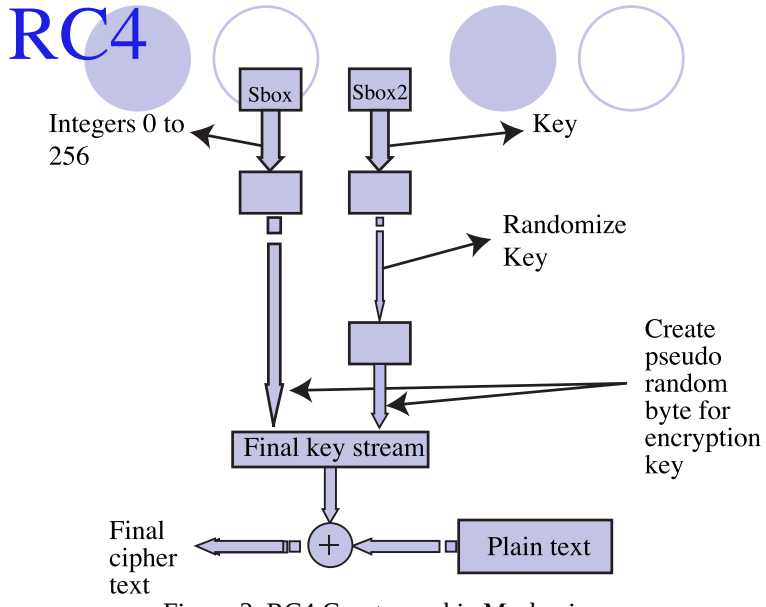

Figure 3. RC4 Cryptographic Mechanism

The way the RC4 algorithm works is the first S-Box initialization, S[0], S[1], …….., S[255], with numbers from 0 to 255. Fill in the first one in order S[0]=0, S[1]=1, …., S[255]=255. Then initialize another array (another S-Box), for example array K with length 256. The contents of array K with key are repeated until the entire array K[0], K[1], ……., K[255] fully charged.

E. Base64 Cryptographic Algorithm

Base64 comes from electronic mail (e-mail). When an email is sent using the SMTP (Simple Mail Transfer Protocol) protocol to our email server, it is then delivered to the intended person's mailbox on the destination email server. Protocols are procedures for computer machines to communicate with each other over a network. In order for the email to reach the intended person, he must first download it. The email download process uses the POP (Post Office Protocol) protocol. Currently POP has reached version 3 so it is called POP3. A better alternative to POP is IMAP (Internet mail access protocol). How base64 cryptography works can be seen in Figure 4 below:

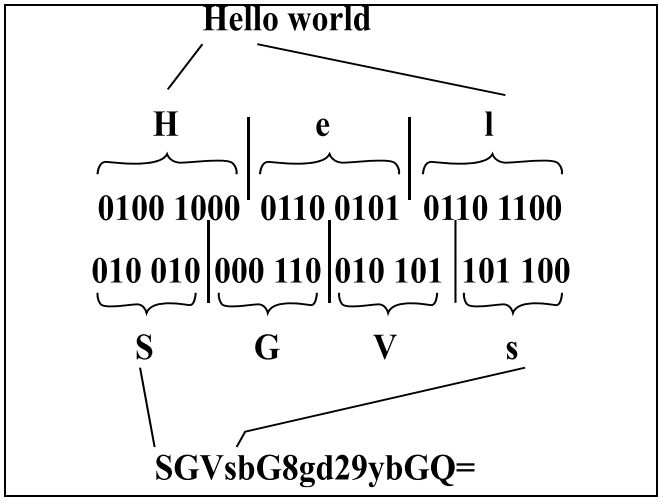

Figure 4. How base64 cryptography works

The following way of converting Base64 can be seen in table 1 below:

Table 1. Base64 conversion

Binary	Decimal	Character	Binary	Decimal	Character
000 000	0	A	100 000	32	g
000 001	1	B	100 001	33	h
000 010	2	C	100 010	34	I
000 011	3	D	100 011	35	J
000 101	4	E	100 100	36	k
000 110	5	F	100 101	37	l
000 110	6	G	100 110	38	m
000 111	7	H	100 111	39	n
001 000	8	I	101 000	40	o
001 001	9	J	101 001	41	p
001 010	10	K	101 010	42	q
001 011	11	L	101 011	43	r
001 100	12	M	101 100	44	s
001 101	13	N	101 101	45	t

The following stages of encryption and their descriptions can be seen in table 2. Base64 conversion below:

Table 2. Base64 conversion

No.	Encryption Stages	Description Stages
1.	Group messages in every 3 characters (3 bytes = 24 bits). If there is a remainder at the end, add (padding '=') bit 0 so that the length is even 24 bits.	Cipher text is converted into an array of 6 bit patterns
2.	Break the 24 bits into 4 groups of 6 bits each.	The 6 bit bit pattern is grouped into an 8 bit / binary bit pattern
3.	Then map each group with the characters in the table.	Binary is converted again to ascii and finally it will return to plain text

F. Hypertext Preprocessor (PHP)

Stating that "PHP (PHP: hypertext preprocessor) is a programming language used to translate program code base into computer understandable machine code that is added server side to HTML "[16]. Hypertext preprocessor (PHP) is a programming language for creating dynamic websites, which are able to interact with visitors or users.

G. Android

Android-based smartphone and tablet PC mobile application programming [17]. Android is an operating system for Linux-based mobile devices. Android provides an open platform for developers to create their own applications to be used for various mobile devices. Android 8.0 is the latest version released by Google in 2017. In this study the authors used Android version 8.0 or also called the Android Oreo version.

H. Joint Photographic Experts Group (JPEG)

JPEG is a bitmap file (file) compression method that is capable of storing digital photos that were previously large in size to small. Image generating devices with the JPEG extension still produce image sizes that are large enough to allow users to compress them [18].

RESULT AND DISCUSSION

A. Knowledge Base Analysis

In the encryption process, the user enters a secret key, a secret message and an image file as the messenger. The system will check the image file extension, if it is not in jpg format the system will ask the user to re-enter the image file. If the input is in jpg format, the system will start encrypting using the RC4 method where the secret message is encrypted together with the secret key.

RC4 encryption results (chippertext RC4) are then re-encrypted using the base64 method. After the RC4 chippertext is successfully encrypted, the system embeds it into the image file using the Least Significant Bit (LSB) method, which places the binary value of the encrypted secret message in the last bits of the image pixels. After the insertion process is complete, the system will return the image file to the user for download. In the decryption process, the user enters a secret key along with an image file that has been embedded with a secret message. The system will check the image file extension, if the format is invalid the system will prompt the user to re-enter the image file. If the image is valid (image file with jpeg extension) the system will extract the image to retrieve the secret message in it.

The message extracted from the image is then decrypted using the base64 method, then the results of the base64 decryption are again decrypted using the RC4 method with a secret key. Then the results are displayed to the user. If the image and key entered match then the message will match what was entered during encryption, but if it does not match the message will remain random and meaningless.

1. Use Case Diagram

Use case is a sequence of transactions or processes carried out by the system, which produces something that can be seen and observed by certain actors. The steganography system usecase diagram with the RC4 and Base64 algorithms can be seen in Figure 5 below:

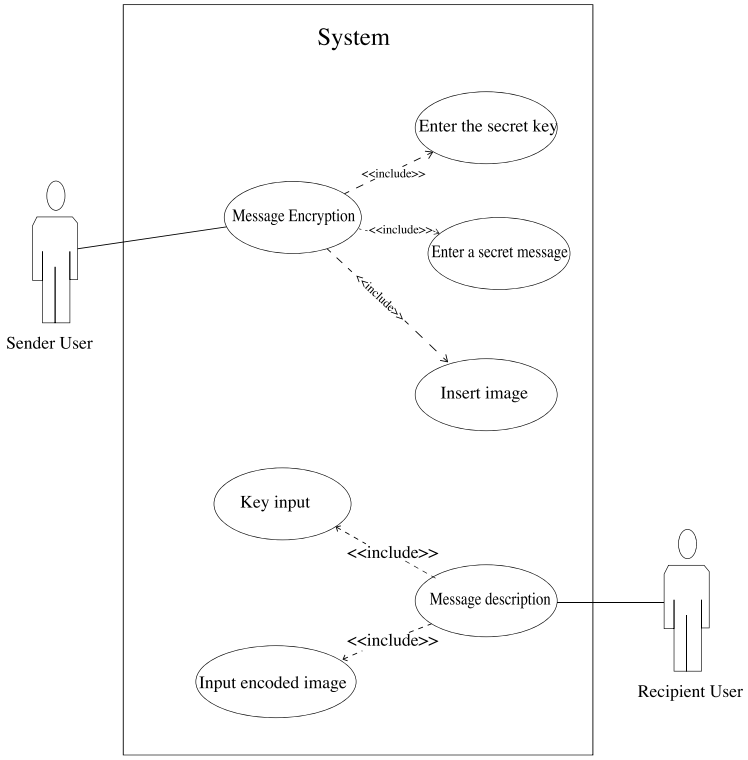

Figure 5. Use Case Diagram

Table 3. Identification of Actors with Descriptions

No.	Actor	Description
1.	Sender User	Encrypt images by filling in secret keys, secret messages, and uploading images in jpg format. then the image will be encrypted by the system based on the methods and algorithms running on the system.
2.	Recipient User	Do the decryption by filling in the secret key and uploading the encrypted image which is changed to jprg format which will open the secret message, then the image will be extracted based on the methods and algorithms running on the system.

2. Activity Diagram

Activity diagrams are one way to model the events that occur in a use case. The following is a diagram of the steganographic system encryption activity with the RC4 and Base64 algorithms which can be seen in Figure 6 below:

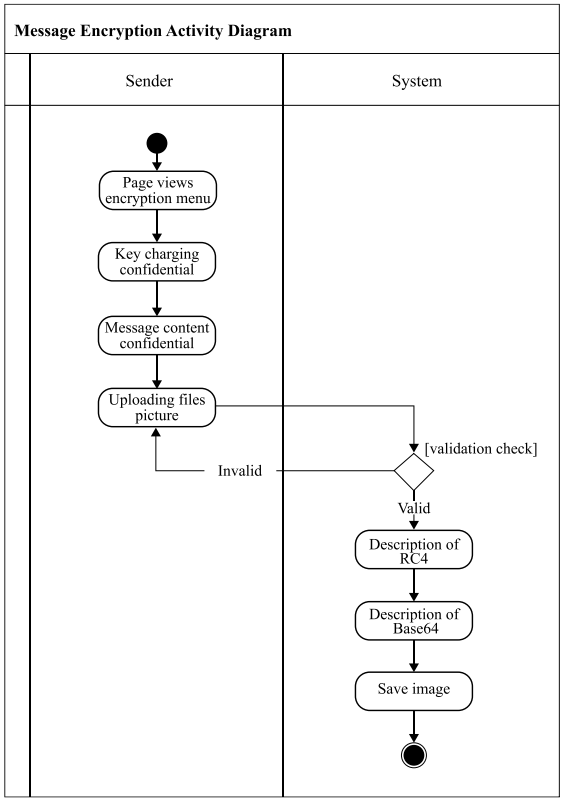

Figure 6. Encryption Activity Diagram

The following is an overview of the steganography system activity diagram with the RC4 and Base64 algorithms which can be seen in Figure 7 below:

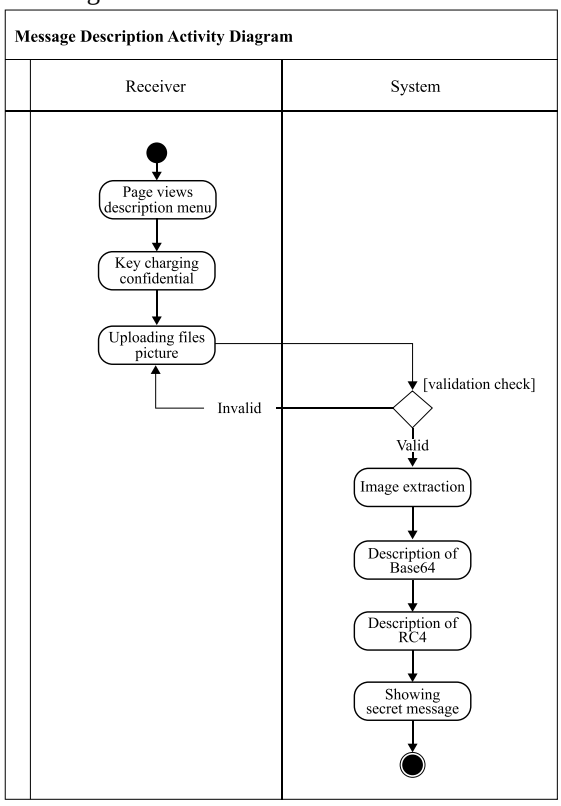

Figure 7. Description of Activity Diagram

3. Implementation and testing

The implementation phase is the stage where the program that has been created and designed is implemented. The following are the implementation stages that will be discussed:

Hardware Implementation (Hardware)

The hardware used to implement this system is as follows:

1) Processor: Intel® Core™ i5-4210U CPU 1.70GHz ~ 2.40GHz
2) RAM: 8GB
3) Harddisk: 500GB
4) 14" monitor with screen resolution of 1366 x 768 pixels
5) Keyboard and Mouse

Software Implementation (Software)

The software used in building this system is as follows: Windows 10 Operating System.

1) XAMPP 1.7.3 for localhost server and database (MySQL).
2) Macromedia Dreamweaver 8 to design the display.
3) Notepad++ is used as a script editor in making a web server.
4) Mozilla Firefox as a browser, media to run the program.
5) Android Studio 3.0 is used for the script editor.
6) Genymotion is used for Android emulator.

Program Implementation

The following is the implementation of the program according to the screen design that was previously designed, including:

a) Encryption page is a page for entering secret messages into images and consists of three columns, namely: key column, secret message, and file column for selecting an image file as the messenger. The key in question is the keyword to open the secret message during the decryption process as shown in Figure 8 below:

Figure 8. Encryption Menu Page

b) The decryption page is a page for opening secret messages contained in an image and consists of two columns, namely: the key column and the file column for selecting the messenger image file. The key column in question is the key to open encrypted secret messages. As is known, before the secret message is inserted into the image, the secret message is encrypted first, which can be seen in Figure 9 below:

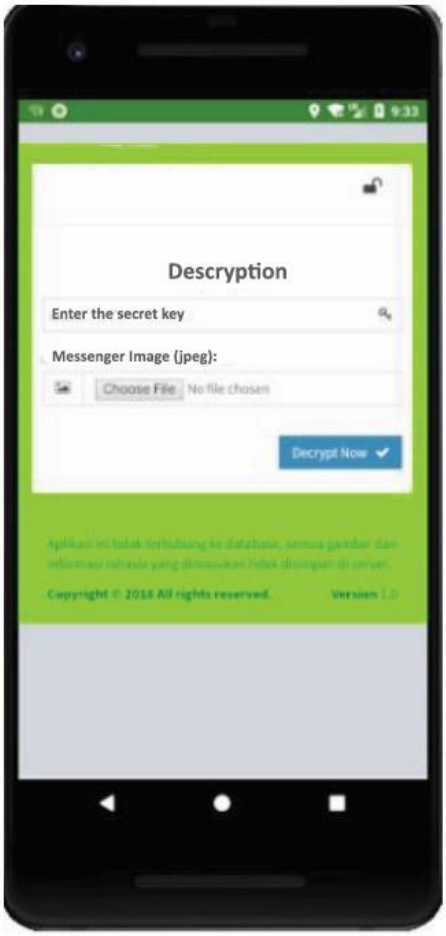

Figure 9. Decryption menu page

Application Testing

1) Encryption Testing

To test whether the system is running properly, the author tries the application by filling in the encryption column as shown in Figure 10 as follows:

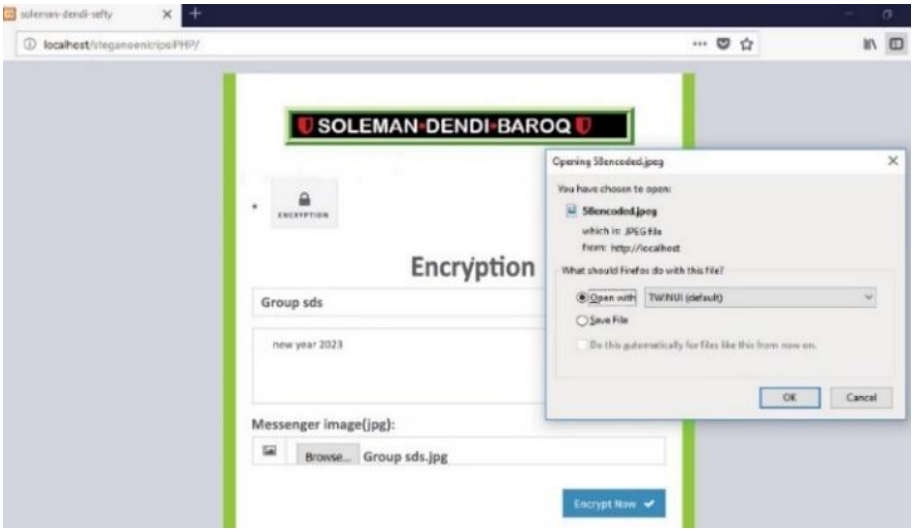

Figure 10. Filling in the encryption column

The secret message that will be inserted is 'new year 2023' with the 'sds group' encryption key. For images used "group sds.jpg" as a message storage medium can be seen in Figure 11. as follows:

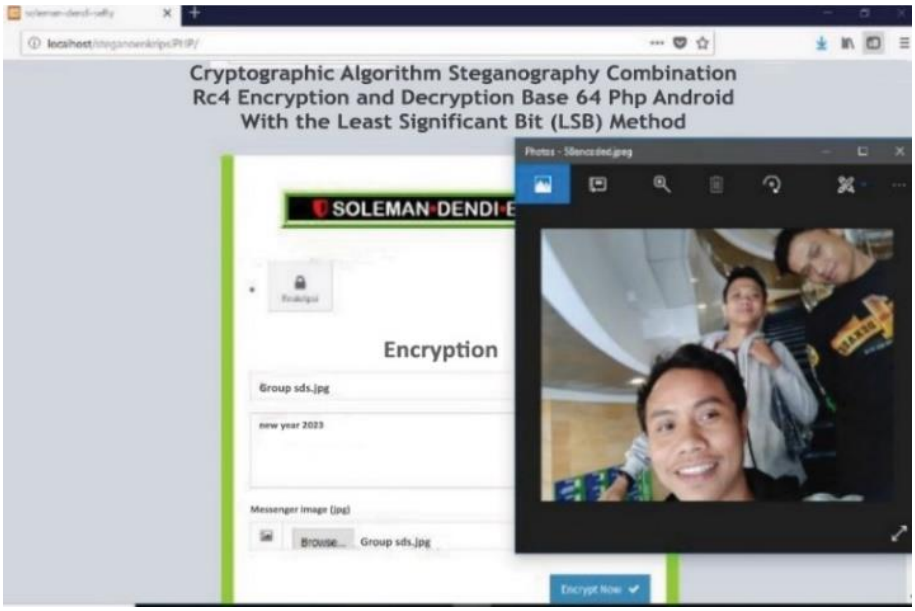

Figure 11. Encryption results

2) Testing Decryption
Testing the application system by filling in the description column can be seen in Figure 12 below:

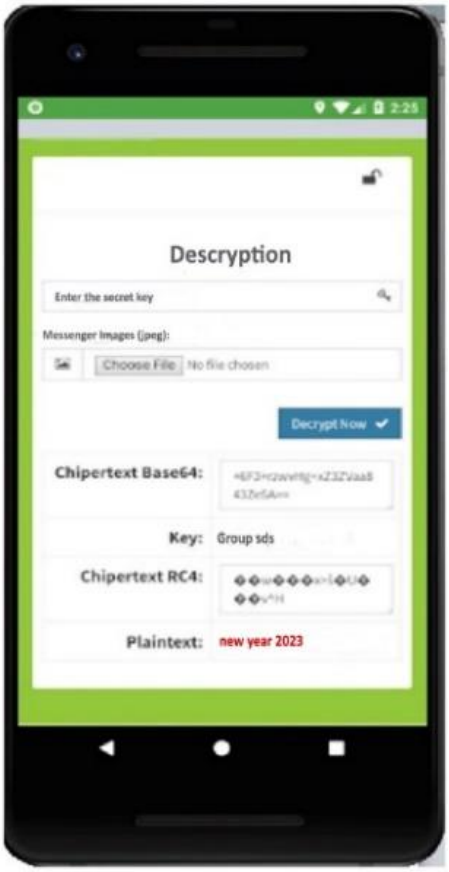

Figure 12. Test decryption

B. Black box testing

The black box method is used in system testing to find out which application systems can run abilities that match the expectations of researchers. The test in question consists of several scenarios to test the authentication, encryption and decryption functions along with other supporting functions. The results of the black box evaluation of the application can be seen in table 4. These results state that the application has met the expectations of the researchers as follows:

Table 4. Blackbox Application Testing Results

Activity Testing	Input scenario testing	Expected output	Results Testing	Accuracy
Encryption menu page	Keyword to unlock secret messages during the decryption process	▪ Displays the encryption menu, which is a page for inserting secret messages into images. ▪ Displays the lock field, secret messages, and the file field to select an image file as a messenger.	Accepted	100%
Description menu page	Keyword to open encrypted secret messages	▪ Displays a page to open a secret message contained in an image. ▪ Show key field and file field to select messenger image file.	Accepted	100%
Test encryption	View encryption test results	▪ Displays a secret message to be inserted.	Accepted	100%
Test description	See description test results	▪ Show results chipertext Base64, key, chipertext RC4 and Plaintext	Accepted	100%

Table 5. Evaluation Results of Encryption and Decryption Process Testing

Document	Document Size (KB)			Difference	Duration (Seconds)	
File image	Original	Encryption	Decryption	Size	Encryption	Decryption
Group sds.jpg	131.91	131.92	131.91	0.01	16,945	15,3682
Group sds1.png	140.11	142.12	140.11	2.01	37.941	31.2386
Group sds2.jpeg	136.11	138.39	136.11	2.28	34.911	29.0127
Group sds3.tiff	164.12	167.01	164.12	2.89	61.120	53.101

The secret key used is 'group sds' to open encrypted messages on images. For images as message storage media, the author uses an example of an image with the group name sds.jpg. The results before and after image extraction can be seen in Table 6 below:

Table 6. Results before and after encoding

Variabel/Images		
	Before the encoding process	**After the encoding process**
Average	131.91KB	131.92KB

From the results of the comparison of the images above, the differences between the before and after images are explored, the contents of the message can be seen through the system that displays the contents of the message, if the message key used matches the incoming secret key.

CONCLUSION

Based on the results of the testing and implementation of this study it can be concluded that: RC4 and Base64 cryptographic algorithms can be combined in a system to provide two layers of security in hiding secret messages. Based on steganography techniques, the Least Significant Bit (LSB) method can be used to hide secret messages in images in JPG or PNG format and the LSB steganography method can be implemented using the Hypertext PreProcessor (PHP) programming language. the difference in the size of the data before and after the decryption shows the addition of data with the smallest difference of 0.01 KB is a jpg file.

REFERENCES

[1] M. D. Putra dan M. Hayaty, "Enkripsi dan Dekripsi gambar dengan menggunakan perpaduan algoritma Base 64 dan Rc 4," pp. 1–6, 2018.

[2] A. Kodir dan W. Pramusinto, "Implementasi Kriptografi dengan menggunakan metode Rc 4 Dan Base 64 Untuk mengamankan database Sekolah pada Sdn. Grogol Utara 10," vol. 4, no. 1, pp. 7–14, 2021.

[3] Soleh, F. Alfiah dan B. Yusuf, "Perancangan Aplikasi Steganografi Dengan Teknik LSB dan AlgoritmaRC4 & Base64 Encoding," *Technomedia Journal (TMJ)*, vol. 3, no. 1, 2018.

[4] N.Taliasih dan I. Afrianto, "Sistem Keamanan Basis Data Klien P.T. Infokes Menggunakan Kriptografi Kombinasi RC4 Dan Base64," *Jurnal Nasional Teknologi dan Sistem Informasi*, vol. 06, no. 01, pp. 9–18, 2020.

[5] F. Wahyu, A. P. Rahangiar dan F. de Fretes, "Penerapan algoritma gabungan RC4 dan Base64 pada sistem keamanan e-commerce," vol. 2012, no. Snati, pp. 15–16, 2012.

[6] Ellya Helmud, "Kombinasi Kriptografi RC4 dan Steganografi LSB Pada Citra Digital Dengan Format Bitmap untuk Menjaga Keamanan Pesan," vol. 2, no. 2, pp. 20–27, 2017.

[7] I. Rizqa, A. N. Safitri dan I. Harkespan, "Kriptostegano Menggunakan Data Encryption Standard dan Least Significant Bit dalam Pengamanan Pesan Gambar," vol. 13, no. 2, pp. 111–120, 2022.

[8] M. A. Zainuddin dan D. I. Mulyana, "Penerapan algoritma rsa untuk keamanan pesan instan pada perangkat Android," vol. 9, no. 2, pp. 105–114, 2016.

[9] D. I. Mulyana, "Kajian penerapan encode data dengan base64 pada pemrograman php," vol. 9, no. 1, pp. 47–52, 2016.

[10] S. Abdurrahman and A. Prapanca, "Pengamanan File Dokumen Ujian Dengan Image Steganography Metode Lsb," vol. 03, pp. 186–192, 2021.

[11] K. Halunen and O. Latvala, "Review of the use of human senses and capabilities in cryptography," *Computer Science Review*, vol. 39, p. 100340, 2021.

[12] P. D. Shah and R. S. Bichkar, "Engineering Science and Technology , an International Journal Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure," *Engineering Science and Technology, an International Journal*, vol. 24, no. 3, pp. 782–794, 2021.

[13] Sellars, *Steganografi : menulis tulisan yang tersembunyi atau terselubung*. 1996.

[14] Ariyus, *Teknik steganografi : tulisan Mesir kuno yang menggunakan gambar dianggap sebagai steganografi pertama di dunia*. 2009.

[15] Ariyus (2008:250), *Algoritma kriptografi Rivest Code 4 (RC4) merupakan salah satu algoritma kunci simetris dibuat oleh RSA Data Security Inc (RSADSI) yang berbentuk stream chipper*. 2008.

[16] Supono dan Putratama, *"PHP (PHP: hypertex preprocessor) bahasa pemrograman yang digunakan untuk menterjemahkan basis kode program*. 2018.

[17] N. Safaat, *Pemrograman aplikasi mobile smartphone dan tablet PC berbasis android*. 2012.

[18] Mawati Zalukhu, "Jurnal KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer) JPEG merupakan sebuah metode kompresi berkas (file) bitmap," *Jurnal KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, 2021. .