Published *online* on the journal's web page : http://innovatics.unsil.ac.id

Innovation in Research of Informatics (INNOVATICS)

| ISSN (Online) 2656-8993 |

Hybrid Cryptosystem Using RC5 and SHA-3 with LSB Steganography for Image Protection

Adisti Dwi Susanti[1], Asep Id Hadiana[2], Fajri Rakhmat Umbara[3], Hidayatulah Himawan[4]

[1,2,3]Informatics Study Program, University Jenderal Achmad Yani, Jl Terusan Jend. Sudirman, Cibeber, Cimahi 405314, Indonesia
[4]Faculty of Information and Communications Technology, Universiti Teknikal Malaysia Melaka, 76100 Durian Tunggal, Malaysia
[1]adistids08@gmail.com, [2]asep.hadiana@lecture.unjani.ac.id, [3]fajri.rakhmat@lecture.unjani.ac.id, [4]P031920047@student.utem.edu.my

ARTICLE INFORMATION

Article History:
Received: June 18, 2024
Last Revision: September 24, 2024
Published *Online*: September 30, 2024

KEYWORDS

Encryption,
Steganography,
RC5,
SHA3-256,
LSB

CORRESPONDENCE

Phone: +6285156755623

E-mail: adistids08@gmail.com

ABSTRACT

The rapid development of internet technology has been accompanied by a significant increase in information security threats. Ensuring the security of confidential information transmission is crucial. Cryptography and steganography are among the most efficient techniques for safeguarding data. Both fields focus on information concealment. This paper proposes a hybrid approach to protect confidential multimedia data, specifically image media, by using LSB steganography techniques in combination with the RC5 encryption algorithm and the SHA3 hashing algorithm to provide dual-layer protection for information. In the proposed method, image data is first encrypted using the RC5 encryption algorithm with a specified key. Subsequently, a hashing function using SHA3 is applied for dual protection, ensuring data authenticity and integrity. Finally, steganography is performed using the LSB technique to embed the hashed information into the image media. This study aims to enhance the security of information in digital image media, providing a reliable solution to address security challenges. The results indicate that data confidentiality was successfully achieved, with an average PSNR of 52.509 dB and an MSE of 0.3829. Tests were conducted using a dataset of images with various dimensions.

1. INTRODUCTION

In the rapidly evolving digital era, information security has become one of the major issues receiving significant attention. Data breaches, particularly those involving personal information, are increasingly rising due to unauthorized access on the internet, causing substantial losses and leading to calls for the criminalization of such acts. Furthermore, crimes related to image data breaches have also increased with the advancement of sophisticated image editing software, spurring a surge in digital crimes. With the growing reliance on information technology and the internet, the risks to data security have likewise escalated [1]. To solve security issues, it is necessary to apply methods that can ensure data security [2].

To protect digital data from unauthorized parties, steganography and cryptography techniques can be used, which are two methods that can ensure the security of digital information. The primary objective of cryptography is to transform confidential data into cipher text that cannot be read by unauthorized individuals. A steganography involves the protection of additional information embedded within a cover object, which includes the secret message or information itself as well as the cover object that conceals it. This cover object can take various forms of digital media. Advancements in steganographic techniques necessitate enhancements in imperceptibility, data capacity, and robustness. Various types of digital formats, including images, videos, text, audio, network protocols, and DNA, can be utilized for this purpose [3].

The main idea of steganographic methods is to make the embedded information invisible to attackers, thereby emphasizing the importance of the image quality of the stego image [4]. One of the techniques to embed information in steganography is the Least Significant Bit (LSB) method, LSB is the most popular steganography approach. In this technique, the least significant bit of the image pixels is replaced with the bits of the hidden data.

The resulting image after embedding remains largely like the original image, as the pixel changes do not significantly alter the overall appearance of the image [5].

Other methods include the Most Significant Bit (MSB) and New Hybrid (NHB) techniques. In research [6] comparing the LSB, MSB, and NHB embedding techniques using Peak Signal to Noise Ratio (PSNR) calculations to measure the quality of images that have undergone steganography and Mean Squared Error (MSE) calculations to measure the level of valid pixel distortion from the original image to the stego image. Four tests were conducted, yielding average PSNR values of 55.41dB for the LSB method, 47.65dB for the NHB method, and 13.31dB for the MSB method, with corresponding average MSE values of 0.21 for LSB, 1.042 for NHB, and 3381.97 for MSB. Therefore, the LSB method demonstrates superior performance compared to the other two algorithms, with higher PSNR and lower MSE values. However, the study also indicates that in terms of security, all three methods still require enhancements by leveraging cryptographic algorithms.

Research from B. Karthikeyan, et al. the proposed method combines cryptography and steganography, utilizing the Data Encryption Standard (DES) algorithm for encryption and the Least Significant Bit (LSB) steganographic insertion technique on digital image objects. The results of the research indicate an average Mean Squared Error (MSE) value of 0.00199 and a Peak Signal-to-Noise Ratio (PSNR) value of 53.3153 dB [7]. Research from Rituraj Gaur, et al. proposing a dual-security method by implementing both cryptographic and steganographic techniques, specifically the DES encryption algorithm and the Secured Hash Algorithm (SHA), with a focus on digital image objects using the LSB embedding method. The results of the study indicate an average MSE value of 0.0126 and an average PSNR value of 60.45 dB from testing five image objects. These results show a lower MSE value by 0.0084 and a higher PSNR value by 10.266 dB [8].

Research [7] implemented security using the DES encryption algorithm and LSB steganography technique. Subsequently, research [8] employed a dual approach by using the DES encryption algorithm, SHA3 hashing algorithm, and LSB steganography technique. The results indicated that research [8] achieved better test outcomes even after the images were attacked. However, despite being relatively strong, the DES algorithm has a weakness related to its short key length 56 bits and a fixed number of rounds 16, making it more vulnerable to brute force attacks[9], [10], [11]. RC5 and DES are both encryption algorithms used to secure data transmission and storage. DES, or Data Encryption Standard, is a symmetric key algorithm that transforms plaintext into ciphertext using a fixed key length, making it vulnerable to brute force attacks due to its small key size. On the other hand, RC5 is a symmetric key block cipher that allows for variable key lengths, providing enhanced security compared to DES. Both algorithms have been widely used in cryptography, with DES being older but widely used and while RC5 flexibility and resistance to attacks [9], [10], [12].

Research from Harsh Kumar V et al. it is mentioned that RC5 is 1.54 times faster than Blowfish and 2.57 times faster than DES, with each algorithm's parameters observable in Table 1. From the perspective of resource utilization, RC5 consumes an additional 13.9 MB of memory compared to Blowfish and an extra 37.46 MB of memory compared to DES, while CPU usage is approximately the same for all three algorithms. RC5 has variable block size, key size, and number of rounds. Therefore, the RC5 block cipher algorithm is faster and simpler compared to Blowfish & DES block cipher algorithms [12].

TABLE 1. PARAMETERS RC5, BLOWFISH, DES

Tab	Algorithm Type		
Parameters	RC5	Blowfish	DES
b (key length in *bytes*)	0 - 255	16, 24, or 32	8
r (no of rounds)	0 – 255 (standard 16)	16	16
No of round keys	2r+2	r+2	r
Block size in words	16, 32, 64 (standard 32)	16, 32, 64 (standard 32)	16, 32, 64 (standard 32)
w (word size in bits)	32, 64, 128 (standard 64)	32, 64, 128 (standard 64)	32, 64, 128 (standard 64)
Used Operation	+, -, ⊕, <<<, >>>	+, -, ⊕, <<<, >>>	+, -, ⊕, <<<, >>>

In the hybrid approach we propose, we utilize the RC5 algorithm and SHA3-256 to secure images while preserving their original quality, without restricting the length of the message characters. This approach was tested using the PSNR and MSE metrics. Implementing a hybrid approach that combines cryptographic encryption algorithms with LSB insertion techniques may not fully or entirely secure data, but it can slow down adversaries' efforts to penetrate the encryption when they attempt to decrypt it.

2. RELATED WORK

Several studies have implemented hybrid approaches, such as in research from B.Karthikeyan et al. which applied the use of the DES cryptographic algorithm combined with LSB steganography techniques, with the research object being a secret text message to be concealed within an image. A transposition of ASCII values in the secret message was performed by adding 2 to each character, which was done to strengthen the encryption technique. Subsequently, double encryption was carried out using the DES algorithm with a fixed 16 rounds and an 8-byte key length. After obtaining the ciphertext, it was inserted using LSB steganography techniques. The hiding of information was accomplished by encoding bits at the LSB position of the carrier image, converting information into an 8-bit sequence. This sequence was divided into substrings containing 2 bits, and then these two bits replaced the last two bits of pixels in the carrier image. The results of the study indicated an average MSE value obtained was 0.00199 and a PSNR value of 53.1153dB [7].

Research from Rituraj Gaur et al. the encryption algorithm DES and the hashing algorithm SHA3 were utilized, focusing on digital image objects using the LSB insertion method. The secret image was encrypted using the DES algorithm, resulting in ciphertext, which was then hashed using SHA3/Keccak to produce a hexadecimal hash value. The hash values generated in this study had predetermined character lengths of 50, 100, and 200, which were embedded into the cover image. The results from the stego images showed an average MSE value obtained of 0.0126 and an average PSNR value of 60.45 dB from five tested image objects [8].

3. METHODOLOGY

The flow of this research begins with the transformation of an image into ciphertext using the RC5 algorithm, followed by conversion into a hash value with SHA3-256/Keccak 256, which is then embedded into a cover image using LSB steganography techniques. The research flow is illustrated in Figure 1.

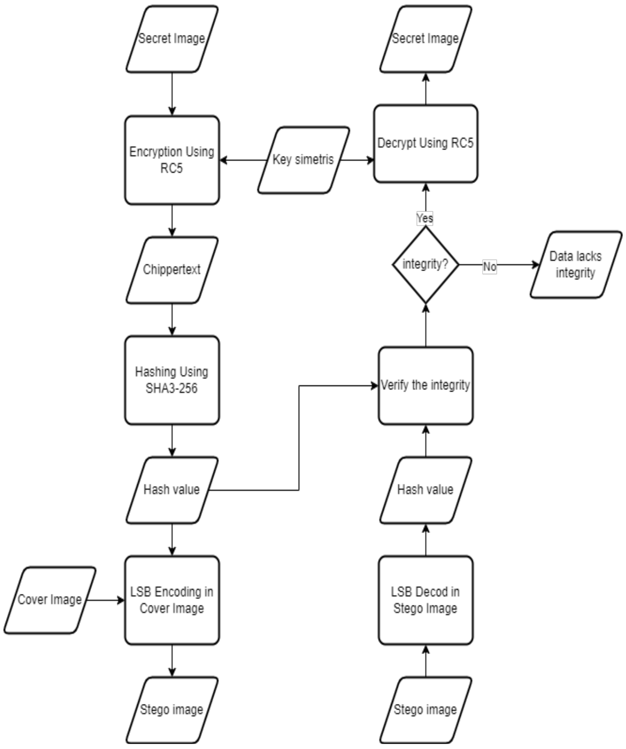


FIGURE 1. FLOW OF THE METHODOLOGY

3.1 Secret Image

In the context of steganography, images serve as a medium to conceal secret mess ages without significantly altering their visual appearance[13]. This technique leverages the characteristics of digital images, which contain information in the form of pixels. During the steganographic process, the secret message is embedded into the image pixels by utilizing the color components or numerical values of those pixels [14].

The objects utilized in this research are digital images, which allow for clear testing and comparison of the proposed method's results. We do not limit the type of extension and depth dimension of images used for the secret image and cover image.

3.2 Algorithm RC5

Image encryption is conducted through the utilization of the RC5 algorithm, which implements arithmetic operations and rotations in accordance with the data quantity. The RC5 algorithm has stipulated allowable values for each of its parameters, which can be observed in Table 2 [15][16].

TABLE 2. PARAMETERS RC5

Parameters	Symbol	Allowed Values
Block Size (in bit)	w	$16, 32, 64$
Number of Rounds	r	$0, 1, \dots, 255$
Length of External Key K (in *byte*)	b	$0, 1, \dots, 255$

In RC5, there are 2r+2 internal keys, each stored in an array element labeled as S [0], S[1],…,S[t-1] with t= 2r+2, where each array element is 1 word in length. During the key generation process, K[0…b-1] is copied into array L[0…c-1], with padding rules involving the character ‘0’ until the size of L[i] becomes w/2 bit. The algorithm for forming internal keys utilizes hexadecimal constants Pw and Qw, which vary based on w. Constants Pw and Qw are derived from functions involving irrational numbers as shown in equation (1).

$$P = Odd\ [(e-2)\ 2w]$$
$$Q = Odd\ [(f-1)2w] \qquad (1)$$

Note:
e = 2.718281828459
f = 1.618033988749

The RC5 encryption process is executed with each round from 1 to r involving operations such as XOR, circular left shifts, and addition in modulo with the internal key. The pseudocode for the encryption process can be viewed in the following pseudocode:

```
$A = A + S[0];$
$B = B + S[1];$
$\boldsymbol{for}\ i \leftarrow 1\ \boldsymbol{to}\ r\ \boldsymbol{do}$
    $A \leftarrow ((A \oplus B) <<< B) + S[2i]$
    $B \leftarrow ((B \oplus A) <<< A) + S[2i+1]$
$\boldsymbol{endfor}$
```

To perform encryption, this algorithm takes an input from a plaintext block divided into two parts, A and B. Encryption utilizes internal keys that are used for each round, with the internal key formation algorithm employing constants Pw and Qw as per equation (1). Subsequently, the encryption process is carried out using pseudocode as depicted in figure 3 to iterate rounds from 1 to r with XOR operations, until the ciphertext from the final round is stored within A and B. The combination of both constitutes the ciphertext block.

3.3 Base64

The encrypted data is stored in a binary buffer, which is then entirely encoded into Base64. Base64 is an encoding scheme that converts binary data into a text format, specifically an ASCII string (American Standard Code for Information Interchange), by translating it into a radix-64 representation [17]. In the Base64 algorithm, a sequence of plaintext bits is divided into several equally sized blocks, typically using 64 bits represented by ASCII characters [18].

The encrypted data is stored in a binary buffer, and then the entire buffer is encoded to Base64. Base64 encoding allows encrypted data to be stored in text files, which are easier to manage and transmit than binary data. Base64 encoding ensures that encrypted data can be transmitted and stored across multiple platforms without worrying about byte order or character encoding issues. Base64 encoded data can be easily transmitted over networks, email, or other communication channels without worrying about data corruption or loss. By using Base64 encoding, encrypted data can be easily stored and transmitted as text strings, making it easier to use than raw binary data.

3.4 Hashing SHA3

In hashing algorithms, the hash output follows a standard instance output with a predetermined number of bits, which is determined by the specific algorithm used, as depicted in the table.

TABLE 3. The Parameters of The Standard Fips 202 and Sp 800-185 Instances

Name Hash	r	c	Output length (bits)	MBits	d
SHAKE128	1344	256	Unlimited	1111	0x1F
SHAKE256	1088	512	Unlimited	1111	0x1F
SHA3-224	1152	448	224	01	0x06
SHA3-256	1088	512	256	01	0x06
SHA3-384	832	768	384	01	0x06
SHA3-512	576	1024	512	01	0x06
cShake128	1344	256	Unlimited	00	0x04
cShake256	1088	512	Unlimited	00	0x04

This research employs the SHA-3 hashing algorithm with a 256-bit output. In the SHA-3 algorithm, the sponge function based on f is depicted in figure 2, where these two sponge functions operate as follows. The input is a message M, which is a bitstring of arbitrary length. M is padded appropriately so that its length becomes a multiple of r. The padded message is then divided into blocks of length r. Initially, the state is a bitstring of length b consisting of zeros. The first block of the padded message is exclusively ORed with the first r bits of the state. Then, the function f is applied, which updates the state. This process is then repeated with the remaining blocks of the padded message. Each block, in turn, is exclusively ORed with the first r bits of the current state and then function f is applied to update the state. This constitutes the absorption phase of the sponge function [19].

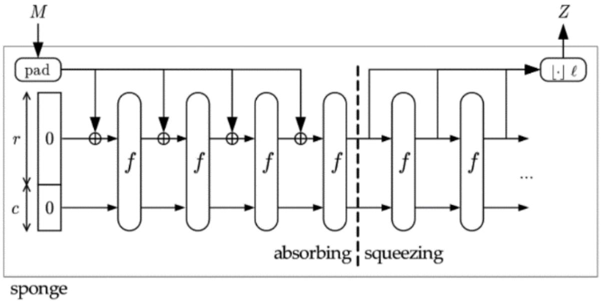


FIGURE 2. Function Sponge

The encrypted output from the RC5 algorithm will be used as input for the SHA-3 algorithm. The RC5 encryption result will be absorbed using the absorbing function. If the data length is not compatible with the block size, padding will be added to adjust it. Padding is done by XOR-ing the last byte of the buffer with 0x80. After absorbing and processing all the data, the final hash is generated by reading from the buffer and performing any necessary permutations.

Leveraging the progressively longer and more varied outputs generated by RC5 encryption significantly enhances the security of the resulting hash code. In this study, we integrate the SHA-3 algorithm, with a bit size of 256, designed to accommodate varying character lengths. This allows the SHA-3 output length to dynamically adjust based on the dimensions of the secret image utilized, ensuring that the encryption process remains robust and adaptable to different input sizes. The combination of RC5 and SHA-3 ensures a more secure and flexible cryptographic solution tailored for advanced encryption scenarios involving sensitive images.

3.5 Least Significant Bit

The hash code result from the SHA-3 implementation is then embedded into a cover image using the Least Significant Bit (LSB) technique. In this LSB watermarking technique, the last bits, which fall into the category of least significant bits and are thus of lesser importance, are altered. By changing the value of these bits to one higher or one lower than their previous value, such modifications do not significantly alter the color.

The LSB technique can be readily comprehended through the example depicted in Figure 3 [20].

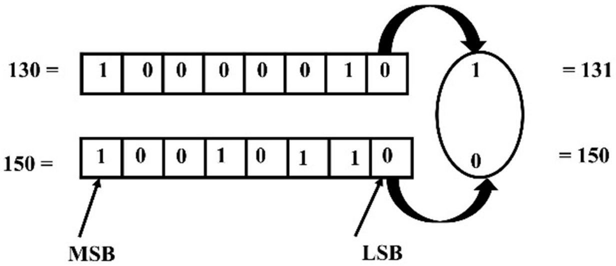


FIGURE 3. Lsb Technique

In figure 3, two-pixel values in an image are represented by the arrangement of bits within a byte (1 byte = 8 bits). Thus, with 130 bytes having a bit arrangement of 10000010 and 150 bytes having a bit arrangement of 10010110, the LSB technique is employed. If the embedded stego image has a value of 10, then the marked pixel values will become 131 (10000011) and remain at 150 (10010110). The LSB technique will be utilized to carry out the embedding process, which involves inserting the stego image into the cover image, and for the extraction process of retrieving the stego image from the cover image.

According to research [8] the following steps are undertaken for the embedding process or message insertion procedure:

1. Calculate the image pixels.
2. Create a loop through the pixels.
3. Retrieve the red, green, and blue values of each pixel in the loop.
4. Set the LSB or each RGB pixel to zero.
5. Obtain the character to be concealed in binary form and hide the-8-bit binary code in the pixel's LSB, as calculated in Figure 2 and exemplified.

6. Repeat this process until all characters of the image are concealed within the image.

3.6 Decoding and Decryption Process

To extract the message contained within a stego image, the following message extraction process is initiated:

1. Calculate the image pixels.
2. Iterate over the image pixels until eight consecutive zeros are found.
3. Select the LSB form each pixel element and then convert it into characters

Once the secret message is successfully extracted, the system reads data from the encrypted file and computes its hash using the Keccak algorithm. This hash is then compared with the hidden message extracted from the image to verify the integrity of the encrypted file. It checks whether the hash of the encrypted image matches the hidden message extracted from the encoded image. If they match, it ensures the integrity of the encrypted file is maintained. Upon confirmed integrity, the encrypted image is decrypted using the RC5 algorithm with a secret key, resulting in the revelation of the secret image.

3.7 Evaluation

The final stage of model evaluation is critical to ensure the accuracy of predictions. Common metrics used include PSNR (Peak Signal-to-Noise Ratio), and MSE (Mean Squared Error). PSNR is often utilized to assess the quality of image recovery or reconstruction after compression or processing, by measuring the ratio between the signal strength and noise energy within that signal. A higher PSNR value indicates a better quality of image reconstruction. PSNR is calculated by comparing pixel values between the original and reconstructed images, then computing the ratio of maximum signal energy to MSE. MSE measures the average squared difference between pixel values in the original and reconstructed or predicted images. A lower MSE value suggests fewer errors or discrepancies between the two images. MSE is calculated by summing the squared pixel differences between both images and dividing by the total number of pixels [21].

We utilize the PSNR and MSE metrics for the evaluation process. PSNR is used to measure the quality of images that have undergone the steganography process with equation (2). Meanwhile, in the context of digital image research, MSE is used to determine the degree of deviation of pixel values after the insertion process of data bits that have been transformed into them with the calculation of equation (3). The higher the PSNR value, the better the quality of the inserted image.

$$MSE = \frac{1}{H*W} \sum_{1}^{H} \left(p(i,j) - S(i,j)\right)^2 \quad (2)$$

H and W represent the height and width, respectively, and P(i, j) denotes the original image while S(i,j) represents the image (stego or reconstructed image).

$$PSNR = 10 \log 10 \; \frac{L^2}{MSE} \quad (3)$$

L is the maximum value that can be accepted by a pixel (for example, 255 for grayscale images or 1 for binary images). MSE, which is the mean square difference between the pixels of the original image and the pixels of the reconstructed image.

4. RESULT AND DISCUSSION

Based on the proposed method described, the input secret image will be converted into ciphertext following the RC5 encryption process. Table 4 presents an example of the resulting ciphertext from the input secret image with dimensions 400x348.jpeg.

TABLE 4. CHIPPER TEXT FROM IMAGE 400X300.JPG

Chipper Text
SmpF+Hh+kBVzqKq5+4m/WmDu2tvgvJ7mF/j4dTNkpvXqe2VG0j IX/B+784Hc7oNh0eMOMQ4JGEowYFDYn3HMdWAkYsG6o07T 9PiI7hkoFDTRdXZyaYU6X7SttSQ2qHMx7gtp8YpiMqP5dfqVWql nE0CZ41RrwlyNRpDgRJRI91X/cqnIJYBxr0gutyMHCqnCafuc9rE G1obIpEs0bOqoo2IZ/IxuKyaxHuGN+fNtITNwnxxS+3DNVWiWy 4Tv9n5WKUEUfj6EkLaeaTXfRM/DTczrAohucp7fI7DncHylRTVd efIyQvH4mgR6GB+masYAlVnT5L2kA0G1YOVetqzmlY7xklfkVA Id7/n8DRg+Mf5eU4cNaldTyoln7R6jiAQyBtd7H7cnNdkPz0M91/h Hi+Y9lZBZS+LjATQB5nNV9aSck0X0l6jFzGTHGLw6JkTKqShm Oo5fRxb6G2Mh919WI3dAFZukOZvyXlJaXcyTBMEiMxzcGJnU5 uNLZg/ckhF0GdQbimcsOovTOCSLmhopRkutfXKyuKmtzsJknTtc GpRNntXF8yCfpIwv4jXzNQbAsXRkjVpAFQOcm1d3HlyfDuYgN g01T8K+c1dMmzcCG9weAot042sDJeFuI8MLbUUwc2cFnMd3DjJ Jk7K73WUyNmq4QPF1AV7Yf99pB0pykdkmMDaTrNDUFtm4gG 8I6zpRAvk+LFM3aXLGgzEMmzQbdZBOaufcwapIC6h3LNuCd+r pJHq/BSNh5sHZV6Ey6wpVi+lkMNjTUYVGEmgJ79qzB2IzSIMO/ 5yi4UpyqmnjaG/opvEU8ayN6SW91HzsECFuVY+OXdxxJIPnsptw dZTriYRGNkMyJ0nhD1x0k9pVYKScFkF7vISYLAkhXVOrnk6Iv Y7lI2lxzYlB3K3vnkWgzj7pRs9g5xzx280fKC3HmWPDhwsRLJ2Rt yvHPZsgy4T5179Ing89RVDQ7j5i7UPYIAf1o0UnMH8xXcz1qP/U 5T+WDRQgDV+3ApCi4rS1bHJfXgjnnmR23IUoEtp+gdtujAqnjaW UXdY6uTuq44VsA+zNUwcfYkQou69JGKBDmnzK4K7Ak3q+UT BEVd7sQpi2yzjbT39mJllKTO2Kf7KyrG6EyLhf1SB/KnkbzHRnao 6Mw8WclaARMk70Z/HsCZMt7Aw4BjUtiMkR5Ysm0hn5NEIyzQ 9YcqOJ1MMFtW9IrQeEGhfmbCqS/gDIoEXrdmEw7O49ZK84uro9 K3ThSw62l6OBlmXC9s3A+ICt9XZahubOcImgNIl0PkxtpKd5ja3T 1ipOD+nxkcY/Yk03gK/7uyxYVy9wlN5dZAU/EKN7b0wPniBGtvk HeqwN79aWJCVdSvwJpZ61JDukPIzJJZcSZV8hpj5t0RVSRzHGc mGFjTiFxS46qXjF8f5E5l7sScTSUavPYUvCX/xom/7TkUBnaC9ae W9lA72/ecKb8LTa6jsi3JRbanMqHS21YRvyWmn88wsYsJFq+sJlI PMv8bUjtKUK7xQvPwQSyxtwFJxU9Ij7c+2FDDf9ZTQ+X5a2W5t PUtQeA+kOQRN5AdlaHdHBgNW/yDias9lUI/lHx6d1NS+Cn3TpZ gIvdVH6OYRUAjnECugPksXl5pn5UayXbr4fong5Zvlg472VCbIb4 bDBQxYth4P1nOwziSoQmRg16hc6s3Toe5QjRLs/tFUPKGWYU8 XHtz4Hajxi7E5e38gDa5sTcQu7uS6njl5FcTc/jnZHxMNvtXGzKCj3 vgt700lKiHHI3JGsBRjAKNcdMg937LLuA3hyd0pcRrA5gjFQ1rny a29DPPZj7pdQSArVKR7MeKpIklo1DLrL9MCLUy7Qe5RuzQ/Vz StRTv9XvpRSMVkeTQWTq8DOFYdIJ4PLWiL6LfF5aDq+eEWZ ZSYhg4PWPXpiA2jyhOwBjiipbSWmHtWULPeVKJPdF3cMh/C59 w5I4l6wRZiGHHG0TBpIrDkpMbuYnkuQKfkHDU1udscrA10U/0P rP/ItdEjFWPmY6AtdvZA64hAb427MJgiCDnrDb5opSD31nrCd9vP OXHN4OUh6G9cO/Q41oUFWtZ+dgJ4qoE/GScFHXYTIYHeR6do 3N9WNoor/NHFie+wsWa95AOf5BijQkWShRa2pnr6jGlHS0naEAn NA8dUDrvOPu5NX1vND/MNsJb9cKjHDbuU4vZznF8TxPfsJG951 iV8Hc0mvlSr95DU6CjAGK+aI5SSO+BtF0t7TuDIVo8YcXKWNU 2mbuBMqsO+mW7Ly5LsKBe8adfI2H2yEIA8ssrfA4h8MMiw9GU o5CEVcgMaQ/ZrFlilqik5//TfbrzdXZs8rDN2Zml+NDGS7cKGnL73 jnuNM7DJbNG9iYG3b9ioXGZROzpOyVIix1Xqn/SN/JBWNFot7n n4ykVunOvNGpNWxjewWKpAR+ekyJIkMw0naIemvnABeME2S/ dKH/k2cT/VOMIbL8iuQEODyxg/28w0UVajLiunU5rpIj2igzI64Q9 NCPyMBWmyoXTjmEZewAduNqybALvzzo23XAjQtdyB0K/Diyc 9Y9Vev+Xcn/WwOf6LbMC9Wi3m3FefCw7+tO7 ...

TABLE 5. HASH VALUE FROM IMAGE 400X300.JPEG

Hash Value
a5d594d309d8a94028b5fc2a48b1d80580b2733120abfd5734c371cef 3df45e6

The generated hash value is then carefully embedded into a cover image of identical dimensions, ensuring no visible distortion. Below are the results of the stego image obtained after successfully implementing the proposed method, clearly demonstrating its effectiveness and maintaining image quality while securing the data.

TABLE 6. TESTING WITH THE SAME SECRET IMAGE AND COVER IMAGE

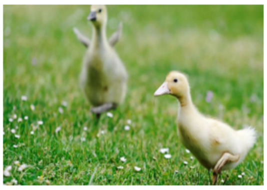
Secret Image	Cover Image
	

TABLE 7. EVALUATION RESULTS FROM FIGURE 4

Image	Inputted Characters	Evaluation Matrix	
		PSNR	MSE
Flower 200x200.jpg	17436 char (256 bit)	38.41788	0.93603
Child 400x348.jpeg	31628 char (256 bit)	52.10952	0.40006
Tiger 500x500.jpg	106648 char (256 bit)	51.81572	0.42806
Duck 734x435.jpeg	61664 char (256 bit)	54.15989	0.24951

The diagram presented in Table 6 highlights the comparison of results between two methods: Method A, which refers to the approach employed in previous research, and Method B, the newly proposed method in this study. The Y-axis of the diagram showcases three different metrics: Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and the number of characters processed. The X-axis, on the other hand, represents the input of the tested image, varying across different image sets. This comparison aims to illustrate the performance improvement of the proposed method over the existing one in terms of image quality and data capacity, which is evident through higher PSNR values and a lower MSE, suggesting superior performance. Additionally, Method B demonstrates better character-handling capacity across all image inputs, emphasizing its efficacy in real-world applications.

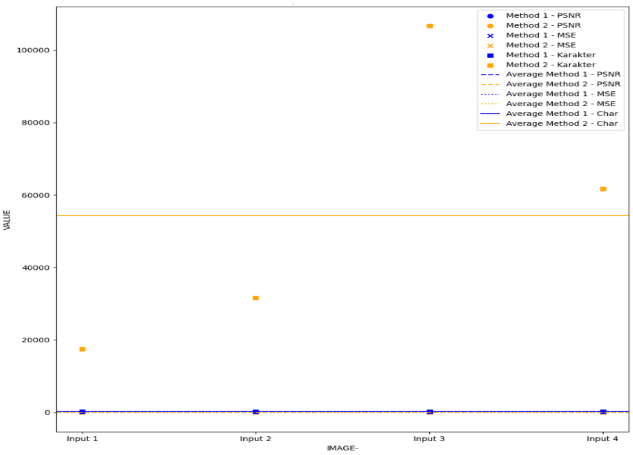


FIGURE 4. DIAGRAM COMPARISON RESULT WITH PREVIOUS RESEARCH

Based on the average PSNR and average MSE results, method A shows better performance than method B. However, method B is better in the number of characters that can be hidden. This research does not aim to compare existing methods, but rather to show that the application of the RC5 algorithm as a replacement for DES, with the ability to hide unlimited characters, can also produce satisfactory PSNR and MSE values, with an average PSNR of 49.125 and an average MSE of 0.503 based on the results in Table 6. We also conducted tests on the secret image that was embedded into a different cover image, and with varying dimensional sizes.

TABLE 8. TESTING WITH VARYING SECRET AND COVER IMAGES

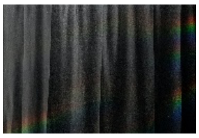
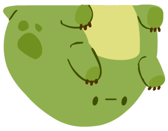
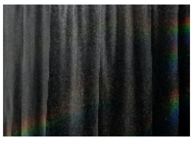
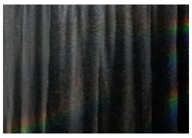
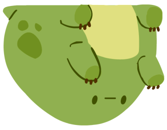
Secret Image	Cover Image	Stego Image
		
		
		

TABLE 9. EVALUATION RESULTS FROM FIGURE 5

Image	Secret Image	Cover Image	Evaluation Matrix	
			PSNR	MSE
01	1200x800.jpeg	256x256.tiff	51.07329	0.50786
02	256x256.tiff	512x512.tiff	57.28583	0.12147
03	800x600.gif	1200x800.jpeg	63.10335	0.03182
04	3024x4032.heic	1200x800.jpg	52.91793	0.33211
05	800x600.gif	256x256.tiff	51.70082	0.43953

The test results indicate that the resolution difference between the secret image and the cover image can affect the reconstruction outcome. Pairs with more similar resolutions tend to yield better results. The combination of image formats also influences the outcome, with gif and jpeg formats as secret and cover images showing very good results in Table 9 testing.

Based on the results and discussion above, this research has the potential to be applied in the real world, where such as the utilization of the application of SHA3 which can ensure that the hidden data remains intact during transmission. If there are any changes or manipulations to the image, the integrity of the data can be easily checked with the hash, which allows the system to detect and prevent manipulation attacks. Furthermore, the technique can now be used to hide secret messages in images sent over open communication channels, such as for Intellectual Property Rights (IPR) protection, with this technique Copyright owners can ensure that their work is protected and any modification to the image can be easily detected through the utilization of SHA-3 hash, and protection with RC5 encryption algorithm.

5. CONCLUSIONS

A steganography technique can be considered successful when the quality of the stego image remains largely indistinguishable from the original cover image. To enhance security, hybrid methods incorporating encryption and hashing algorithms are often employed, though these methods may raise concerns about potential degradation of image quality. However, several tests have shown that the proposed hybrid approach using the RC5 encryption algorithm and the SHA3 hashing technique can effectively conceal secret messages without significantly altering image quality. The size and complexity of the hidden message, as well as the resolution and format of the cover image, can greatly impact the outcome. Tests indicate that using images with similar resolutions and compatible formats improves the reconstruction quality, yielding optimal results. Looking ahead, combining this method with image compression techniques could help further reduce quality changes in the stego image. Additionally, this technique can be extended to other types of data, such as embedding image-to-image, where hash values could be converted into images before being embedded into the cover image. This opens new possibilities for secure data transmission.

REFERENCES

[1] B. S. Shishodia and M. J. Nene, “Data Leakage Prevention System for Internal Security,” in *2022 International Conference on Futuristic Technologies, INCOFT 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/INCOFT55651.2022.10094509.

[2] D. Teguh Yuwono *et al.*, “DETEKSI SERANGAN VULNERABILITY PADA OPEN JURNAL SYSTEM MENGGUNAKAN METODE BLACK-BOX,” 2021. [Online]. Available: http://e-journal.stmiklombok.ac.id/index.php/jireISSN.2620-6900

[3] H. Alatawi and C. Narmatha, “The Secret image hiding schemes using Steganography- Survey,” in *2020 International Conference on Computing and Information Technology, ICCIT 2020*, Institute of Electrical and Electronics Engineers Inc., Sep. 2020. doi: 10.1109/ICCIT-144147971.2020.9213764.

[4] O. Evsutin, A. Melman, and R. Meshcheryakov, “Digital steganography and watermarking for digital images: A review of current research directions,” *IEEE Access*, vol. 8, pp. 166589–166611, 2020, doi: 10.1109/ACCESS.2020.3022779.

[5] S. A. Jebur, A. K. Nawar, L. E. Kadhim, and M. M. Jahefer, “Hiding Information in Digital Images Using LSB Steganography Technique,” *International Journal of Interactive Mobile Technologies*, vol. 17, no. 7, pp. 167–178, 2023, doi: 10.3991/ijim.v17i07.38737.

[6] Y. Y. Wai and E. Myat, “Comparison of LSB, MSB and New Hybrid (NHB) of Steganography in Digital Image,” *International Journal of Engineering Trends and Applications (IJETA)*, vol. 5, 2014, [Online]. Available: www.ijetajournal.org

[7] P. L. N. Ramesh, M. Moorthi, Prathyusha Engineering College, and Institute of Electrical and Electronics Engineers, *A Combined Approach of Steganography with LSB Encoding technique and DES Algorithm*. 2017.

[8] Rituraj Gaur, Dr. RekhaVig, and Ms. AmanpreetKaur, “An Effectual Hybrid Approach Using Data Encryption Standard (DES) and Secured Hash Algorithm (SHA) for Image Steganography,” 2018, [Online]. Available: http://www.ijritcc.org

[9] R. Bhanot and R. Hans, “A review and comparative analysis of various encryption algorithms,” *International Journal of Security and its Applications*, vol. 9, no. 4, pp. 289–306, 2015, doi: 10.14257/ijsia.2015.9.4.27.

[10] N. Advani, C. Rathod, and A. M. Gonsai, “Comparative Study of Various Cryptographic Algorithms Used for Text, Image, and Video,” in *Advances in Intelligent Systems and Computing*, Springer Verlag, 2019, pp. 393–399. doi: 10.1007/978-981-13-2285-3_46.

[11] A. Jain and D. Bhatnagar, “A Comparative Study of Symmetric Key Encryption Algorithms,” *IJCSN International Journal of Computer Science and Network*, vol. 3, no. 5, 2014, [Online]. Available: www.IJCSN.org

[12] H. K. Verma and R. K. Singh, “Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms.”

[13] S. Atawneh, A. Almomani, and P. Sumari, “Steganography in Digital Images: Common Approaches and Tools.”

[14] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[15] Tishk International University, Erbil Polytechnic University, Institute of Electrical and Electronics Engineers, and Institute of Electrical and Electronics Engineers. Iraq Section, *Proposed Parallel Algorithms to Encryption Image Based on Hybrid Enhancement RC5 and RSA*. 2019.

[16] J. S, M. C, S. S, J. P, and S. S, "The Role of AES and RC5 Algorithm: A Cryptosystem Model to Secure Information in the Image based Steganography along with Watermarking," *Webology*, vol. 18, no. 05, pp. 1158–1167, Oct. 2021, doi: 10.14704/web/v18si05/web18296.

[17] Somchai Wen Dong and Wen Dang, *Research on Base64 Encoding Algorithm and PHP Implementation*. Institute of Electrical and Electronics Engineers, 2018.

[18] Institute of Electrical and Electronics Engineers. Indonesia Section and Institute of Electrical and Electronics Engineers, *Stegocrypt Sceheme Using LSB-AES Base64*. 2019.

[19] B. Schneier, *Applied cryptography : protocols, algorithms, and source code in C*. Wiley, 1996.

[20] M. Begum and M. S. Uddin, "Digital image watermarking techniques: A review," Feb. 01, 2020, *MDPI AG*. doi: 10.3390/info11020110.

[21] P. V. Sanivarapu, K. N. V. P. S. Rajesh, K. M. Hosny, and M. M. Fouda, "Digital Watermarking System for Copyright Protection and Authentication of Images Using Cryptographic Techniques," *Applied Sciences (Switzerland)*, vol. 12, no. 17, Sep. 2022, doi: 10.3390/app12178724.

AUTHORS

Adisti Dwi Susanti

She is currently a dedicated student in the Informatics Study Program at Jenderal Achmad Yani University, where she is developing her skills in computer science, programming, and data analysis. Her passion for technology drives her academic success.

Asep Id Hadiana

He currently serves as the Chairman of the Department of Informatics at Jenderal Achmad Yani University. With extensive experience in the field, he holds a prestigious PhD from Universiti Teknikal Malaysia Melaka (UTeM). His expertise includes research in computer science, data analysis, and information systems management. Additionally, he actively contributes to academic conferences and publications, enhancing the university's reputation both locally and internationally.

Fajri Rakhmat Umbara

Currently a Lecturer in the Department of Informatics at Jenderal Achmad Yani University. With a strong academic background, he actively contributes to the department through teaching, research, and involvement in various academic initiatives. His areas of expertise include software engineering, data science, and system development. Fajri is also passionate about mentoring students and fostering innovation within the field of informatics, helping to drive the university's mission of academic excellence and technological advancement.

Hidayatulah Himawan

He is a senior lecturer in the Informatics Engineering Department at UPN Yogyakarta, where he has been actively involved in teaching and research for several years. Currently, he is pursuing his PhD at Universiti Teknikal Malaysia Melaka (UTeM), focusing on cutting-edge advancements in information systems research, data communications, and information technology. His work delves into areas such as system optimization, network infrastructure, and the integration of emerging technologies within information systems. Over the course of his academic career, he has contributed to various research projects, published papers in international journals, and presented at conferences. In addition to his academic commitments, he collaborates with industry professionals to bridge the gap between theoretical research and practical applications in IT and data communication systems. His dedication to research and education positions him as a key figure in shaping the future of informatics and technology in the region.