

Anti-Forensics with Steganographic File Embedding in Digital Image Using Genetic Algorithm

Amadeus Pondera Purnacandra, Subektiningsih

Informatics Department, Faculty of Computer Science, Universitas Amikom Yogyakarta, Yogyakarta, 55283, Indonesia

ARTICLE INFO

Article history:

Received June 22, 2022
Revised August 11, 2021
Accepted September 16, 2021

Keywords:

Anti-forensic;
Digital forensic;
Steganography;
Cybersecurity;
Genetic Algorithm

ABSTRACT

In this study, a steganography method on digital images as anti-forensics by utilizing genetic algorithms was proposed. Genetic Algorithms are artificial intelligence whose functions are optimization and search. The purpose of this research is to optimize steganography as anti-forensic by applying a Genetic Algorithm and combined with the Hilbert curve, lempel Ziv Markov chain, and least significant bit. The result provides a new steganography method by combining various existing methods. The proposed method will be tested for image quality using PSNR, SSIM, Chi-Squared steganalysis and RS-Analysis, and extraction test. The novelty obtained from the developed method is that the steganography method is as optimal as anti-forensic in keeping confidential data, has a large embedding capacity, and is able to be undetected using forensic methods. The results can maintain data confidentiality, have a large embedding capacity, and are able to be undetected using forensic methods. The proposed method got better performance rather than the previous method because PSNR and SSIM values are high, secret data can be received back as long as the pixel value doesn't change, and the size of the embedding capacity. The proposed method has more ability to embed various types of payload/ secret data because of the way it works, which splits byte files into binary. The proposed method also has the ability not to be detected when forensic image testing is carried out.

This work is licensed under a [Creative Commons Attribution-Share Alike 4.0](https://creativecommons.org/licenses/by-sa/4.0/)



Corresponding Author:

Subektiningsih, Universitas Amikom Yogyakarta, Yogyakarta, 55283, Indonesia
Email: subektiningsih@amikom.ac.id

1. INTRODUCTION

Since society has become more connected and digitized, the need for digital forensic investigations has become important for both civil and criminal purposes [1]. Digital forensics is a branch of forensic science that studies how to detect and observe abnormal conditions in applications, files, and digital devices to be used as strong evidence in the eyes of the law [2]. Disclosure of evidence from digital forensics is to obtain details of the sequence of events in a case so that a conclusion is obtained in law enforcement efforts [3]. Digital forensic investigations can be carried out for internal company investigations, civil investigations, and criminal investigations [4]. The process stages in digital forensics broadly include Collection, Examination, Analysis, and Report [5]. In the forensic process, there is a possibility that evidence can become unidentifiable due to anti-forensic [6]. Anti-forensics is an action to make the examination of the evidence difficult or even impossible to do [7]. There are several categories of anti-forensic methods that are often used. Namely Data Hiding, Artefact Wiping, Trail Obfuscation, and Attack Against The Computer Forensic Process or Tools [8]–[10]. Data hiding is a technique for hiding secret data either explicitly or implicitly. Examples are cryptography and steganography [11], [12]. Steganography is the science of embedding secrets in digital media, such as images, audio, and video files, to be invisible [13]. The main problem of steganography is how to communicate securely with a large embedding capacity, processing resistance, and imperceptibility [14]–[17]. As a scientific method, there are no studies that directly state how dangerous steganography is, but steganography can be very

dangerous when used by criminal or terrorist groups in communicating [18]–[20]. Apart from being used for crime, steganography is also used in other important things such as military purposes, medical purposes, industrial purposes, to system authentication methods [21]–[23]. However, there is a lack of academic research on anti-forensics compared to research on digital forensics, and only 2% of 500 digital forensics research papers focus on anti-forensics [24]. Anti-forensics is not always defined as a criminal endeavor but can be understood as input to forensic practitioners, experts, and investigators to develop outdated forensic methods [10]. Kadhim et al. [25] summarize steganography in digital images, which can be implemented in several parts of the file, such as; End of the File, Spatial Domain, and Adaptive. In this case, the adaptive methods are methods that directly affect the embedding process and are also used to optimize the embedding process, such as the use of machine learning or artificial intelligence.

This research is based on related research that applies genetic algorithms as an optimization effort. Genetic algorithms can be used in two types of areas for embedding, namely, spatial domain (based on pixel values) and transform domain (based on frequency components). Genetic algorithms are used to generate chromosomes that contain the best solution to a problem and utilize the Least Significant Bit embedding method on pixel values in the spatial domain area named SDMS-FC (Secret Data Modification Based Image Steganography - Flexible Chromosome) [26]. While in the area of the transform domain [27], a new method that can map the suitable frequency between the secret data with the least significant bit belonging to the frequency coefficient of the cover image in the best way, while the genetic algorithm is used to find the most optimal frequency transformation parameters. In [28], the use of a genetic algorithm that produces chromosomes that are used to set certain parameters, the result is a high embedding capacity and is able to set the embedding location automatically, the result is a high embedding capacity and is able to set the embedding location automatically.

In an effort to uncover confidential information on steganography, steganalysis techniques were developed as digital forensic techniques. Steganalysis and steganography are two contradictory things. Steganography aims to hide confidential information, while steganalysis aims to reveal confidential information [29]. According to [29], the steganalysis method used by the forensic examiner is divided into 6 categories, namely; visual steganalysis, signature or specific steganalysis, Statistical steganalysis, spread spectrum steganalysis, transform domain steganalysis, universal or blind steganalysis. Statistical steganalysis using Chi-square or Regular/Singular (RS) has a good performance when embedding is done in the spatial domain [30]–[32].

In this study, the genetic algorithm is proposed as a method of finding the most optimal value of the existing parameters, namely the Hilbert-Curve, as a visual cryptography effort, reversing the direction of secret data, inversion of secret data, and compression of secret data using the Lempel Ziv Markov Chain algorithm then data The secret is embedded in the Least Significant Bit (LSB). The proposed method is tested for image quality using PSNR and SSIM. Then forensic image testing is performed using Chi-Squared steganalysis and RS-Analysis.

The purpose of this study is to obtain a steganographic method as an optimal anti-forensic in keeping confidential data, large embedding capacity, and being able to be undetected using the forensic method. Visual cryptography attempts, reversal of secret data direction, inversion of secret data, and compression of secret data using the Lempel Ziv Markov Chain algorithm, then the secret data is embedded in the Least Significant Bit (LSB). The proposed method is tested for image quality using PSNR and SSIM. Then forensic image testing is performed using Chi-Squared steganalysis and RS-Analysis.

2. METHOD

The research method used is shown in the following Fig. 1. A literature study was conducted to find current research trends so that the research carried out was relevant and obtained maximum results. After getting the latest research trends, the existing steganographic methods were obtained. From the existing methods, improvements were made to the method to obtain the proposed method. The proposed method will be used to embed confidential data with the same dataset in previous studies in the literature study section.



Fig. 1. Research Method

The image results from the proposed method will be assessed for quality using the test method used in previous studies. To confirm the purpose of steganography as anti-forensic, a steganalysis test was carried out

to find out whether the image resulted from a method that was able to keep the data confidential. After obtaining the results from the series of tests, the results of the previous method tests are compared with the proposed method to assess whether the proposed method is better than the existing method. The results will be explained in the form of tables, graphs, and narratives.

2.1. Purposed Method

The genetic algorithm is an optimization used to find the best solution for steganography problems. The Peak Signal Noise Ratio (PSNR) value is the main value that becomes the fitness value of this genetic algorithm. The genetic algorithm will produce chromosomes that represent the solution to the problem.

2.1.1. Chromosomal Representation

The representation of chromosomes in the proposed method will look like in Table 1.

Table 1. Chromosomal Representation

Hilbert Curve Space-Filling		Secret Data	Embedding	Secret Data
X Value	Y Value	Inversion	Direction	Modification
8 Bit	8 Bit	1 Bit	1 Bit	1 Bit
Chromosomal example: 19 Bit				
0 1 1 0 0 1 0 1 1 0 1 1 1 0 0 1 0 1 0				

2.1.2. Visual Cryptography Hilbert Curve Space filling

In the representation of the X and Y chromosomes, these values are used for encryption purposes. The digital image will be made into a stego sequence, which is a 1-dimensional array using the Hilbert Curve depicted in Fig. 2 Hilbert Curve 4x4, and Fig. 3 Hilbert Curve 8x8. The flow of changing images into sequences is visualized in Table 2. According to [33], the Hilbert curve has better performance for steganography than raster order and Z-scan. The use of the Hilbert Curve gets less distortion, which means it is possible to get a higher PSNR value. The condition for using the Hilbert Curve is that the dimensions of the digital image must be 2^n ($2 \times 2, 4 \times 4, 8 \times 8 \dots n \times n$).

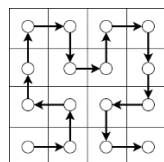


Fig. 2. Hilbert Curve 4x4

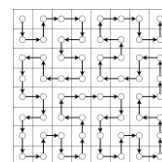


Fig. 3. Hilbert Curve 8x8

Table 2. The flow of changing 4x4 images into stego sequences

Image 4x4				Stego Sequence	Hilbert Curve 4x4 Flows Visual
12	15	5	0	[12, 3, 11, 15, 5, 0, 7, 3, 5, 2, 8, 6, 7, 3, 9, 4]	
3	11	3	7		
9	3	5	2		
4	7	6	8		

2.1.3. Secret Data Inversion

Chromosomal representation Secret data inversion is the process of creating a secret sequence and determining whether the secret data value needs to be inverted or not.

2.1.4. Embedding Direction

The chromosomal representation of the embedding direction is used to determine the embedding direction. In the previous process, after the stego sequence is created, it will be determined whether the embedding occurs from the index $\alpha \rightarrow \Omega$ or vice versa $\Omega \rightarrow \alpha$

2.1.5. Modification of Confidential Data using Lempel Ziv Markov-Chain Compression

Chromosome Representation Confidential Data Modification is used to set whether a secret file is better compressed or not. Lempel-Ziv Markov-Chain Algorithm (LZMA) is a lossless sequential data compression technique created by Abraham Lempel and Jacob Ziv [34], which is modified using the Markov chain. This method focuses on the integrity of the data that will not be reduced by a single bit after the return process. An example of the data compression process using LZMA is shown in Table 3.

Table 3. Lempel Ziv Markov chain compression method

byte stream:	0100100011100110111101										
The encoding process starts from the leftmost bit, looks for bits, and puts them into the Dictionary:	0 100100011100110111101										
Then search for the next phrase that is not in the Dictionary.	0 1 00100011100110111101										
	0 1 00 100011100110111101										
	0 1 00 10 0011100110111101										
The next phrase that is not in the dictionary is 00, and so on:	0 1 00 10 001 1100110111101										
	0 1 00 10 001 11 00110111101										
	0 1 00 10 001 11 0011 0111101										
	0 1 00 10 001 11 0011 01 11101										
Because all the bytes have been exhausted, the last phrase will repeat itself, the previous 01 we have found.	0 1 00 10 001 11 0011 01 111 01										
The next process is indexing the Dictionary, then the encoding process and the last line is the result of encoding.	1	2	3	4	5	6	7	8	9	10	Dictionary number
	0	1	00	10	001	11	0011	01	111	01	Encoding Process
	00	01	10	20	31	21	51	11	61	8	Encoding Results

2.1.6. Least Significant Bit Embedding

After the Stego sequence and Secret sequence are finished, the embedding process will be carried out by replacing the LSB value in the Stego sequence with the Secret sequence value. The example is in Table 4.

Table 4. Least Significant Bit (LSB) embedding

Stego Sequence	
[12, 3, 11, 15, 5, 0, 7, 3, 5, 2, 8, 6, 7, 3, 9, 4]	
Dalam bentuk biner:	
[00001100 00000011 00001011 00001111 00000101 00000000 00000111 00000011 00000101 00000010 00001000 00000110 00000111 00000011 00001001 00000100]	
Secret Sequence	
[1, 2, 3]	
In binary form:	
[00000001 00000010 00000011]	
Embedded Sequence	
In binary form:	
[00001100 00000000 00001000 00001100 00000100 00000000 00000110 00000011 00000100 00000010 00001000 00000110 00000110 00000010 00001001 00000100]	
In decimal form:	
[12, 0, 8, 12, 4, 0, 6, 3, 4, 2, 8, 6, 6, 2, 9, 4]	

2.2. Image Quality Test

2.2.1. Peak Signal to Noise Ratio (PSNR)

The peak signal-to-noise ratio (PSNR) is a measure of how much distortion occurs in an image caused by image processing. PSNR is usually expressed on the decibel scale as

$$PSNR = 20 \log_{10} \left(\frac{MAX_f}{\sqrt{MSE}} \right) \tag{1}$$

where MSE is

$$MSE = \frac{1}{m n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|f(i, j) - g(i, j)\|^2 \quad (2)$$

Where f is the data matrix of the original image, g is the matrix data of the degraded image, m is the number of rows of image pixels, i represents the row index, n is the number of image pixels column, and j represents the index of that column, and MAX_f is the maximum signal value present in the original image, which is not suspicious.

Assessment of the visual quality of digital images can be subjective. Then it is necessary to use quantitative/empirical measures to compare. By comparing the original image with the processing results, the results obtained whether the steganography algorithm causes a lot of damage or not. The PSNR value will be in the range of 100 to 0, where the higher the PSNR value means, the less noise is produced. In other words, the higher the PSNR value, the better the image quality. PSNR value is obtained from Equation (1), where MSE is Equation (2). PSNR is used because it has been proven to be accurate for assessing noise caused by data embedding and is used by many studies, including [26], [28], [35].

2.2.2. Structural Similarity Index Measure (SSIM)

Structural Similarity Index Measure (SSIM) is a method to measure the similarity between two images by working like the Human Visual System (HVS). SSIM is a method of comparing the structural features of an image, and image quality is described by structural similarity. The SSIM calculation is based on a three-factor calculation; luminance (l), contrast (c), and structure (s). First coined by [36]. SSIM obtained from Equation (3) where $[l(x, y)]^a \times [c(x, y)]^b \times [s(x, y)]^g$ is Equation (4), Equation (5), Equation (6) and its simple form becomes Equation (8). SSIM is

$$SSIM(x, y) = [l(x, y)]^a \times [c(x, y)]^b \times [s(x, y)]^g \quad (3)$$

Luminance is

$$l(x, y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \quad (4)$$

Contrast is

$$c(x, y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (5)$$

Structure is

$$s(x, y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \quad (6)$$

Constants C_1 , C_2 , and C_3 are entered to avoid instability when $\mu_x^2 + \mu_y^2$, $\sigma_x^2 + \sigma_y^2$, $\sigma_x\sigma_y$ close to 0, then become Equation (7).

$$C_1 = (K_1L)^2, C_2 = (K_2L)^2, C_3 = C_2/2 \quad (7)$$

Or, in a simple form, SSIM will become

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_x\sigma_y + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (8)$$

Where x is the original image, y is the stego image, μ_x, μ_y is image average, σ_x, σ_y is the standard deviation of the image, σ_{xy} is image covariance x and y / cross-covariance, α, β, γ determine the weight given to each model, namely luminance, Contrast, and Structure

The SSIM value has a range of 0 to 1, where getting closer to 1 means an image is said to be structurally similar. SSIM is used because it has been proven to be good at assessing the structural similarity of images and is used in various studies, including [26], [28], [35].

2.2.3. Image Transmission and Extraction

Steganography is used as a host for data that is transmitted through communication networks such as the internet, intranets, communication media, or social media. This test is intended to test that the steganographic

image transmitted through the communication media is not damaged, data loss, or damage. The test will be carried out using two communication media, namely Whatsapp and Telegram, both of which are able to send images. The original image and the image sent through the communication media will be checked and analyzed for hexadecimal values to see if there is any damage or changes to the data. The last step is data extraction which is the main step to ensure the secret data is receivable. The purpose of this test is to see the robustness of steganographic images to image processing is, and able to receive the secret data without any damage or loss.

2.3. Steganography and Steganalysis

In this section, forensic image testing will be carried out with two methods based on statistics to test whether the secret data embedded in the steganographic image can be detected or not.

2.3.1. Chi-Squared Steganalysis

One of the statistical steganalysis techniques is the χ^2 or Chi-Squared test, which was introduced by Andreas Westfeld and Andreas Pfitzmann [37]. χ^2 test is very popular because it does not require the original cover image for comparison, considering that steganalysis rarely have access to the original image. Main focus of χ^2 test is to calculate the Pairs of Values generated from the embedding method. This technique is not only able to detect whether an image is a steganographic image but also can estimate the number of embedded secret bits.

The work steps of detecting steganographic images using chi-squared include determining the Pair of Value values from steganographic images and ordinary images, calculating the actual PoV frequency from the stego image and the expected frequency from ordinary images, then calculating the chi-square value by comparing the actual frequency distribution and expected frequency with Equation (9) as

$$\chi^2 = \sum_{i=1}^{v-1} \frac{(e_i - E(e_i))^2}{E(e_i)} \quad (9)$$

If distribution $E(e_i)$ (actual frequency) is equal to e_i (expected frequency) then χ_{PoV}^2 will approach 0, which means there is a small probability that an embedding has occurred. On the other hand, if the value of p the closer to 1, the greater the probability that there has been a secret message embedding.

2.3.2. Regular/Singular (RS) Steganalysis

The RS Steganalysis method was developed by Jessica Fridrich [39]. This technique is able to detect random embedding accurately by utilizing the correlation of pixel values in the image. The way this technique works is by partitioning the given image into groups n pixel next door ($x_1 \dots x_n$).

To be able to explain how the Steganalysis Hospital works in a coherent manner, previously, we will describe how the embedding and grouping used by Jessica Fridrich works. To get the correlation of pixel values, the discrimination function f is used, which is the absolute value of the average difference between adjacent pixels. The equation of the discrimination function f can be expressed in Equation (10).

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \quad (10)$$

The greater the value of the function f , it can be concluded that a group is getting noisy. The implication of embedding LSB will increase the noise of the image, so the value of the function f will increase. The LSB insertion performed by Jessica Fridrich can be described by the flipping function F_1 and the dual-flipping function F_{-1} shown in Equation (11) & Equation (12):

$$F_1 : 0 \leftrightarrow 1, 2 \leftrightarrow 3, \dots, 254 \leftrightarrow 255 \quad (11)$$

$$F_{-1} : -1 \leftrightarrow 0, 1 \leftrightarrow 2, \dots, 255 \leftrightarrow 256 \quad (12)$$

The functional relationship between *flipping* F_1 and *dual flipping* F_{-1} shown in Equation (13):

$$F_{-1} = F_1(x + 1) - 1 \text{ for all } x \quad (13)$$

The pixel group (G) can be classified into three different types, namely R, S, and U:

1. *Regular* $G \in R \Leftrightarrow f(F(G)) > f(G)$ Groups
2. *Singular* $G \in S \Leftrightarrow f(F(G)) < f(G)$ Groups
3. *Unusable* $G \in U \Leftrightarrow f(F(G)) = f(G)$ Groups

Where $f(G)$ is the flipping function of each group component $G = (x_1 \dots x_n)$. In general, different flipping operations are in groups. The pattern of pixels to be flipped will be called a mask. $F(G)$ group, which has gone through the defined flip process $(F_{M(1)}(x_1), F_{M(2)}(x_2), \dots, F_{M(n)}(x_n))$, where $M(i = 1, 2 \dots, n)$ is the mask element M , and its value is -1, 0, 1.

After defining the term for the embedding process, it is time to define how the steganalysis process works. Henceforth the Regular Group for mask M will be symbolized as R_M , as well as the Singular Group symbolized as S_M . $R_M + S_M \leq 1$ dan $R_{-M} + S_{-M} \leq 1$ is owned to negative mask. Expected value of R_M is the same as $(\cong)R_{-M}$, and also applies to S_M and S_{-M} defined in Equation (14).

$$R_M \cong R_{-M} \text{ and } S_M \cong S_{-M} \tag{14}$$

Based on the classification that has been done, an RS diagram like Fig. 4 sample diagram taken from J. Fridrich, et al. [39] where the image is taken using a digital camera.

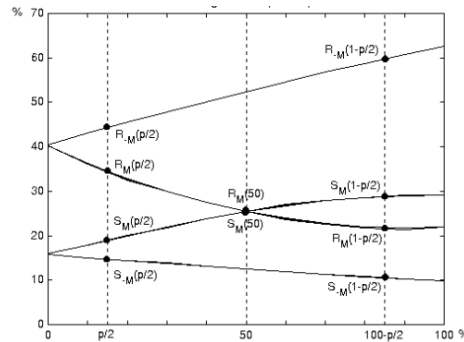


Fig. 4. An example of an RS diagram is taken from J. Fridrich et al.

The diagram shows R_{-M} , S_{-M} , R_M and S_M as the number of pixels with the LSB that have been flipped, where the abscissa represents the LSB pixels that have been flipped, at the same time, the ordinate is the relative number of groups R and S with masks M and $-M$, when the example $M = 0 1 1 0$. Then step to get secret message length (p) by re-adjusting the x-axis or abscissa so that $p/2$ becomes 0 and $100 - p/2$ becomes 1, the x-coordinate of the intersection is the root of the following quadratic equation to Equation (15). Then thus, the length of the secret message (p) can be obtained using Equation (16).

$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0 \tag{15}$$

Where d_0, d_1, d_{-0} , and d_{-1} is

$$\begin{aligned} d_0 &= R_M(p/2) - S_M(p/2) \\ d_1 &= R_M(1 - p/2) - S_M(1 - p/2) \\ d_{-0} &= R_{-M}(p/2) - S_{-M}(p/2) \\ d_{-1} &= R_{-M}(1 - p/2) - S_{-M}(1 - p/2) \\ p &= x/(x - 1/2) \end{aligned} \tag{16}$$

2.4. Method Comparison

The proposed method will be compared with existing methods by comparing the PSNR and SSIM values using the same dataset and the same secret data as used in previous studies. The next comparison is to compare the results of steganalysis testing using Chi-Squared and RS-Analysis with popular steganography programs. The steganalysis testing process is based on Chi-Squared, and RS-Analysis using Benedikt Boehm's StegExpose [40].

3. RESULTS AND DISCUSSION

3.1. Literature Study

The literature study in this study was conducted to obtain the latest research trends so that the research results can produce quality research. Previous studies that have been used as references are [26][27][28] as a reference for the use of genetic algorithms in steganography, [30]–[32] as a reference for forensic image

research using the steganalysis method, and [33] as a reference for research trends in steganography. From the results of the literature study, it was also found that the datasets used in previous studies were passed down from generation to generation to measure the quality of the proposed method.

3.1.1. Dataset Collection Method

In this study, the source comes from <http://sipi.usc.edu/database/database.php>, belonging to the Signal and Image Processing Institute (SIPI), University of Southern California. This dataset is a dataset that has been used in previous studies so that the proposed method can be measured and evaluated appropriately.



Fig. 5. Dataset 1 Lena



Fig. 6. Dataset 2 Jet



Fig. 7. Dataset 3 Pepper

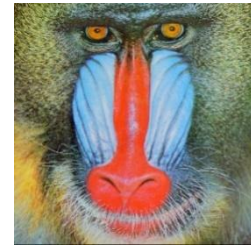


Fig. 8. Dataset 4 Baboon



Fig. 9. Dataset 5 Living Room

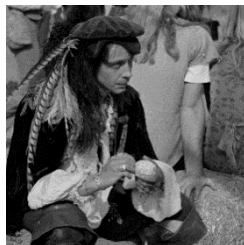


Fig. 10. Dataset 6 Pirate



Fig. 11. Dataset 7 Boat

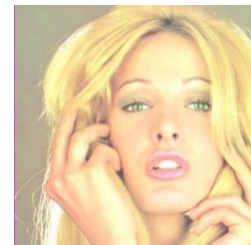


Fig. 12. Dataset 8 Blonde

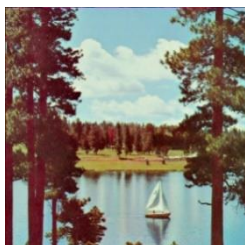


Fig. 13. Dataset 9 Lake

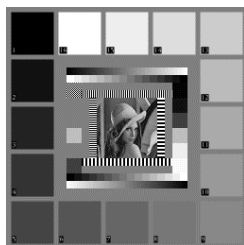


Fig. 14. Dataset 10 Test Pattern



Fig. 15. Dataset 11 Cameraman

The dataset can be used as a cover image or as a secret file to be embedded. Although the contents of the dataset have 24 bits of color (RGB), in this study, only 8 bits of color (Grayscale) will be used following previous research. Fig. 5, Fig. 6, Fig. 7, Fig. 8, Fig. 9, Fig. 10, Fig. 11, Fig. 12, and Fig. 13 are images with a size of 512×512, while Fig. 14 and Fig. 15 are 256×256 images.

3.2. Image Quality Test Results

Fig. 16, Fig. 17, Fig. 18, Fig. 19, and Fig. 20 are stego images that have embedded secret data in Fig. 21. Result in Table 5 shows that the stego image has a PSNR value above 50 dB and an SSIM value of 0.99. A high PSNR value indicates that the stego image quality gets less distortion or damage. A high SSIM indicates that the image visually does not change. Despite having the same high value, PSNR and SSIM do not have a correlation.

Fig. 23, Fig. 24, Fig. 25, and Fig. 26 are stego image that has embedded secret data in Fig. 27. Result in Table 6 shows that the stego image has a PSNR value above 50 dB as well. And the SSIM value is 0.99, which means the quality of the embedding process causes a little distortion and visual changes. But in Fig. 22, the PSNR value does not reach a value of 50 dB. This is because the size of the cover image is only 256×256 pixels. The size of the cover image and confidential data greatly affects the PSNR value.

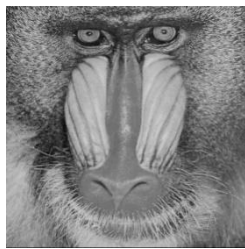


Fig. 16. GA.bmp (Mandrill/ Baboon)

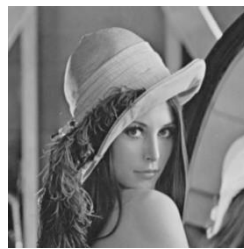


Fig. 17. GA.bmp (Lena)



Fig. 18. GA.bmp (Airplane)



Fig. 19. GA.bmp (Lake)



Fig. 20. GA.bmp (Pepper)

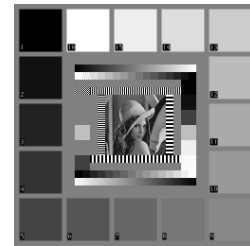


Fig. 21. testpat.bmp

Table 5. PSNR and SSIM test results with secret data testpat.bmp

Secret: testpat.bmp		
Cover Image	PSNR	SSIM
Baboon / 4.1.03	58.88	0.99
Leno / 4.1.04	57.36	0.99
Airplane / 4.1.05	58.87	0.99
Lake / 4.1.06	58.91	0.99
Pepper / 4.1.07	57.35	0.99



Fig. 22. 4.1.02 (Living Room)



Fig. 23. 5.3.01 (Pirate)



Fig. 24. 4.2.05 (Airplane)



Fig. 25. boat.512

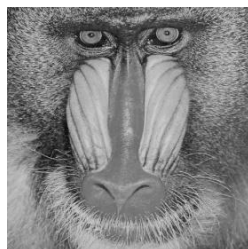


Fig. 26. 4.2.03 (Baboon/ Mandrill)



Fig. 27. cameraman.bmp

Table 6. PSNR and SSIM test results with secret data cameraman.bmp


Secret: cameraman.bmp		
Cover Image	PSNR	SSIM
Living Room / 4.1.02	43.00	0.99
Pirate / 5.3.01	54.13	0.99
Airplane / 4.2.05	54.2	0.99
Boat / boat.512	54.05	0.99
Mandrill / 4.2.03	53.83	0.99

3.2.1. Transmission and Extraction Results

Delivery and extraction tests are carried out to prove that the stego image processed using the proposed method is able to maintain the robustness of confidential data. The test was carried out using social media Telegram and Whatsapp. These two social media were chosen because Whatsapp uses image compression when sending, while Telegram does not use compression.

Based on the test, the data on Table 7 image that was sent via Telegram, shown in Fig. 28 no change, as evidenced by HexDump, shown in Fig. 29. While the image sent via Whatsapp, shown in Fig. 30, subjected to compression and changes as evidenced by HexDump shown on Fig. 31. The changed image cannot keep the data confidential/payload, this means that the proposed method does not meet the Robustness aspect (resistance) to data processing. Meanwhile, Citra, which has not changed, is still able to maintain its secret data properly, as evidenced by when Fig. 32 is HexDumped and shown in Fig. 33, the result is the same as the Payload before embedding, and when a hash comparison is made between Fig. 32 with Payload before embedding the result is identical and shown on Fig. 34.

Table 7. Delivery and extraction testing

Telegram	WhatsApp
 <p>file name: 4.2.04GA.bmp mime type:</p> <pre> 0000-0010: 42 4d 36 04-04 00 00-00 00 36 04-00 00 28 00 BMG.....6...(. 0000-0020: 00 00 00 02-00 00 00-00 00 01 00-08 00 00 00 0000-0030: 00 00 00 00-00 00 00-00 00 00 00-00 00 00 00 0000-0040: 00 00 00 00-00 00 00-00 00 01 01-01 00 02 02 0000-0050: 02 00 03 03-03 00 04 04-04 00 05 05-05 00 06 06 0000-0060: 06 00 07 07-07 00 08 08-08 00 09 09-09 00 0a 0a 0000-0070: 0a 00 0b 0b-0b 00 0c 0c-0c 00 0d 0d-0d 00 0e 0e 0000-0080: 0e 00 0f 0f-0f 00 10 10-10 00 11 11-11 00 12 12 0000-0090: 12 00 13 13-13 00 14 14-14 00 15 15-15 00 16 16 0000-00a0: 16 00 17 17-17 00 18 18-18 00 19 19-19 00 1a 1a 0000-00b0: 1a 00 1b 1b-1b 00 1c 1c-1c 00 1d 1d-1d 00 1e 1e 0000-00c0: 1e 00 1f 1f-1f 00 20 20-20 00 21 21-21 00 22 22 0000-00d0: 22 00 23 23-23 00 24 24-24 00 25 25-25 00 26 26 0000-00e0: 26 00 27 27-27 00 28 28-28 00 29 29-29 00 2a 2a 0000-00f0: 2a 00 2b 2b-2b 00 2c 2c-2c 00 2d 2d-2d 00 2e 2e 0000-0100: 2e 00 2f 2f-2f 00 30 30-30 00 31 31-31 00 32 32 0000-0110: 32 00 33 33-33 00 34 34-34 00 35 35-35 00 36 36 0000-0120: 36 00 37 37-37 00 38 38-38 00 39 39-39 00 3a 3a </pre>	 <p>file name: WhatsApp Image 2022-01-09 at 2.25.49 PM.jpeg mime type:</p> <pre> 0000-0010: ff d8 ff e0-00 10 4a 46-49 46 00 01-01 00 00 01JF IF..... 0000-0020: 00 01 00 00-ff e2 02 28-49 43 43 5f-50 52 4f 46(ICC_PROF 0000-0030: 49 4c 45 00-01 01 00 00-02 18 00 00-00 00 04 50 FILE..... 0000-0040: 00 00 6d 6e-74 72 52 47-42 20 58 59-5a 20 00 00mtrRG B,XVZ... 0000-0050: 00 00 00 00-00 00 00-00 00 61 63-73 70 00 00acscp... 0000-0060: 00 00 00 00-00 00 00-00 00 00 00-00 00 00 00 0000-0070: 00 00 00 00-00 00 00-00 01 00 00-f6 d5 00 01 0000-0080: 00 00 00 00-d3 2d 00 00-00 00 00 00-00 00 00 0000-0090: 00 00 00 00-00 00 00-00 00 00 00-00 00 00 0000-00a0: 00 00 00 00-00 00 00-00 00 00 00-00 00 00 0000-00b0: 00 00 00 00-00 00 00-00 09 64 65-73 63 00 00desc... 0000-00c0: 00 f0 00 00-00 74 72 58-59 5a 00 00-01 64 00 00trXVZ...d... 0000-00d0: 00 14 67 58-59 5a 00 00-01 78 00 00-00 14 62 58gXVZ...x...bX 0000-00e0: 59 5a 00 00-01 8c 00 00-00 14 72 54-52 43 00 00YZ.....rTRC... 0000-00f0: 61 a0 00 00-00 28 67 54-52 43 00 00-01 a0 00 00(GT RC..... 0000-0100: 00 28 52 54-52 43 00 00-01 a0 00 00-00 28 77 74(bTRC.....(wt 0000-0110: 70 74 00 00-01 c8 00 00-00 14 63 70-72 74 00 00cprT... 0000-0120: 01 dc 00 00-00 3c 6d 6c-75 63 00 00-00 00 00<ml uc..... 0000-0130: 00 01 00 00-00 0c 65 6e-55 53 00 00-00 58 00 00en US...X... 0000-0140: 00 1c 00 73-00 52 00 47-00 42 00 00-00 00 00s.R.G .B..... </pre>
 <p>file name: output mime type:</p> <pre> 0000-0010: 89 50 4a 47-0d 0a 1a 0a-00 00 00-0d-49 48 44 52 PNG.....INDR 0000-0020: 00 00 01 00-00 00 00 00-00 00 00 00-00 c1 de e8 0000-0030: 06 00 00 41-8d 49 44 41-54 78 9c 05-fd e9 b7 67A.IDA Tk.....g 0000-0040: 50 75 10 00-c6 39 d7 de-e7 0e 08 07-65 be ac 50 [.....] 0000-0050: a5 5a 24 a5-94 08 c9 60-91 20 04 08-81 6d c0 06 ZS.....m... 0000-0060: 59 b0 c0 c3-d8 c3 40 09-a6 3c f4 36-36 76 99 b2 V.....\,66v... 0000-0070: 4c 51 d5 50-58 46 00 00-09 61 44 63-23 0c 96 68 LQXXF...adov,h 0000-0080: 24 48 34 02-04 02 f5 29-29 d5 66 a6-9a 6c of 7b 804.....)f..l.(0000-0090: 99 2f 5f 17-f1 e2 fe ce-09 80 ce fa-70 6e 08 fe /.....k..p... 0000-00a0: 67 8a 00 31-22 6e 7c b5-11 bf 73 f6-de 60 ad 09]..... 0000-00b0: 6d fe 99 4a-97 2b 21 48-c0 d3 f4 58-d3 96 8b 9d m...L.H.....X... 0000-00c0: 81 28 11 80-c6 80 28 b3-cb 15 c8 b2-92 81 44 65 (.l.(.....De 0000-00d0: 81 00 05 ac-32 09 78 50-32 34 99 4a-43 0c 53 602..Wk 24..CJ'S 0000-00e0: 47 40 b3 96-ca d5 a0 01-81 ac b9 50-6a 32 a3 c7 00.....Ph2... 0000-00f0: 8a 12 c0 5a-c5 86 c2 16-6d ae e2 31-90 05 0c 072.....m..l... 0000-0100: c2 aa 05 41-48 00 0c 5a-04 ac 6a 39-15 36 e1 f0BM;Z...9..6... 0000-0110: 98 05 07 18-00 00 0f 84-ae 94 03 ba-e7 ba 00 97].....g... 0000-0120: 63 42 e3 48-a5 02 aa 3b-4e a4 d8 5a-70 2a a9 eb cb.H.....;F..Zp... 0000-0130: 98 87 29 20-49 a9 40 0e-5e e1 fc 24-06 70 a0 14)I..B...;S.p... 0000-0140: 21 46 16 52-86 48 cc 00-5a 41 37 3a-90 2f 34 15 IF.R.....;2P..A... 0000-0150: c3 69 28 2b-70 1a 61 6a-4b 8e 79 70-c4 b3 a8 54 i(ep;a] K.y.p...T 0000-0160: 40 50 2a 00-66 20 10 a9-c3 12 00 05-b0 6a 60 ac K]P...e..3k... 0000-0170: 35 00 18 63-56 91 88 5c-12 c7 64 c6-00 05 4a a6 6 c(x).....).....2... 0000-0180: 3c b4 84 95-59 01 e9 51-9c 35 66 03-e9 31 50 00 <...Y..Q 5f..3P... 0000-0190: 54 a4 aa a0-35 09 c6 22-ae a2 40 80-92 07 c4 26 T...5'1'..b...& 0000-01a0: fb 00 ca 50-00 90 6c 37-92 95 00 60-a0 22 00 13T..l37...h... 0000-01b0: 6d 1a 14 38-c0 16 9c 0e-28 a0 c4 54-a1 08 e9 2a m..8.....(LT... 0000-01c0: 8a 29 80 05-73 10 62 81-61 ef e4 3c-66 16 75 74)..s.b..a..cfut 0000-01d0: cc 2a 00 60-20 43 23 13-4e 3c 05-05 92 ba f7(c) W... 0000-01e0: c2 28 a5 8c-b5 8e ee 04-b4 da ce 3a-c2 b5 12 a3(..... </pre>	

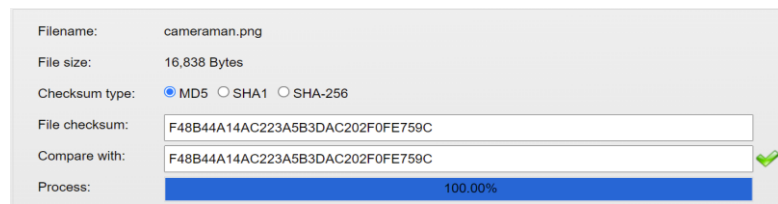


Fig. 34. Hash Comparison Result

3.3. Image Steganalysis Test Results

In Table 8, the results show that the proposed method is able to maintain confidential data and is not detected as a steganography file when steganalysis testing is carried out.

Table 8. Steganalysis results on stego image testing

File name	Above the stego threshold? True = Detected	Secret message size in bytes (ignore for clean files)	Chi-Square	RS analysis	Fusion (mean)
4.2.03GA.bmp	FALSE	5527	8.37E-04	0.102852993	0.062989607
4.2.04GA.bmp	FALSE	2005	0.001293948	0.022336234	0.022852045
4.2.05GA.bmp	FALSE	1940	0.004505766	0.026006712	0.02211449
4.2.06GA.bmp	FALSE	1420	4.19E-08	0.023825325	0.016187578
4.2.07GA.bmp	FALSE	730	2.84E-06	0.008238846	0.00831912

3.4. Method Comparison Results

In the results section of this comparison, the proposed method is compared with the results from the previously existing methods [2], [26], [28], [41]–[45]. Other popular methods used are Robin David's LSB-Steg and Georgeom's StegOnline.

Based on the results of the comparison in Table 9, which uses Testpat.bmp as secret data, the proposed method has a better PSNR value than the previous method and the LSB-Steg method in Fig. 35. Likewise in the comparison results in Table 10, which uses Cameraman.bmp as its secret data. The proposed method still has a slightly higher PSNR value than the previous method Fig. 36. Except for Fig. 22 PSNR value does not reach 50 dB. This is because the size of the cover image is only 256×256 pixels. However, the SSIM value in each method is the same Fig. 37 which means all methods do not change the image visually.

Table 9. Comparison of methods on secret data testpat.bmp

Cover Image	Secret: Testpat.bmp							
	PSNR							
	Lin and Tsai's method [41]	Yang et al.'s method [42]	Chang et al.'s method [44]	Wu et al.'s method [45]	Kanan's technique [28]	Pratik Shah's technique [26]	LSB-Steg	Purposed Method
Airplane/ 4.2.05	39.25	41.66	40.73	43.53	45.18	46.37	43.5	58.87
Lake / 4.2.06	39.18	41.51	38.86	43.55	45.1	46.42	43.51	58.91
Pepper /4.2.07	39.17	41.56	39.3	43.56	45.13	46.39	43.49	57.35
Mandrill/4.2.03	39.18	41.55	39.94	43.54	45.12	46.42	43.49	58.88
Lena/ 4.2.04	39.2	41.6	40.37	43.54	45.12	46.43	43.5	57.36

Table 10. Comparison of methods on secret data cameraman.bmp

Cover Image	Secret: Cameraman.bmp					
	PSNR		SSIM			
	LSB	Pratik Shah's technique [26]	Proposed Method	LSB	Pratik Shah's technique [26]	Purposed Method
Living Room / 4.1.02	51.12	52.17	43.00	0.99	0.99	0.99
Pirate / 5.3.01	51.14	52.41	54.13	0.99	0.99	0.99
Airplane / 4.2.05	51.14	52.21	54.20	0.99	0.99	0.99
Boat / boat.512	51.12	52.35	54.05	0.99	0.99	0.99
Mandrill / 4.2.03	51.13	52.13	53.83	0.99	0.99	0.99

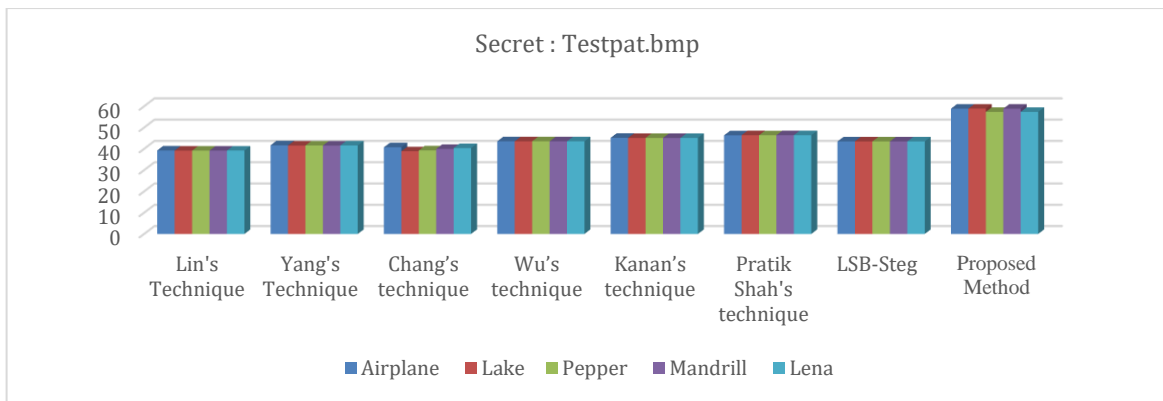


Fig. 35. Method comparison graph on testpat.bmp secret data

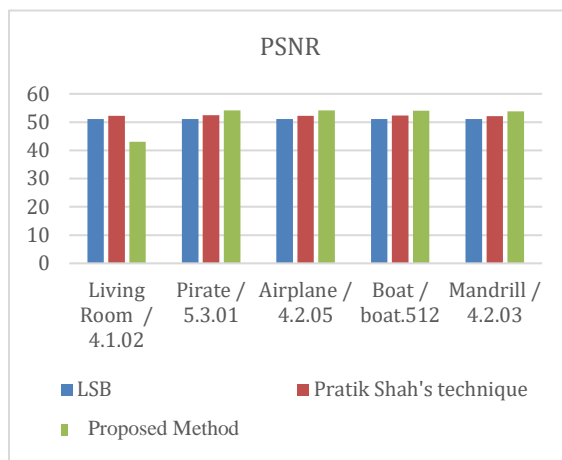


Fig. 36. Comparison graph of psnr method on cameraman.bmp rahasia secret data

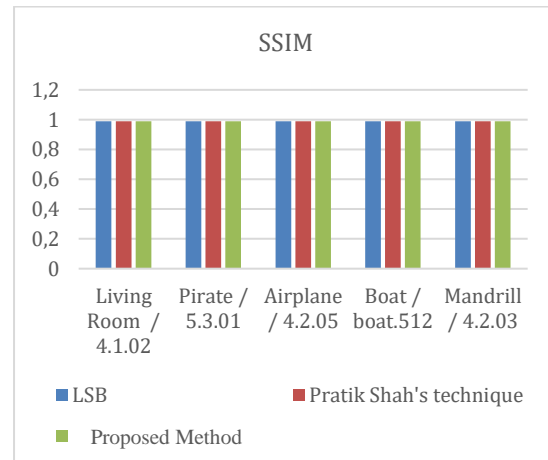


Fig. 37. Comparison graph of SSIM method on secret data cameraman.bmp

Statistical steganalysis test results in Table 11 proved that the proposed method proved undetectable using statistical attacks with the chi-squared in Fig. 38 and RS analysis in Fig. 39. Confidential Data Assumption Embedded in Fig. 40 shows that the proposed method is not statistically detectable by the steganalysis technique.

Table 11. Comparison of steganalysis test results

File name	Above the stego threshold? True= Detected	Secret message size in bytes (ignore for clean files)	Chi-Square	RS analysis	Fusion (mean)
4.2.03GA.bmp	FALSE	5527	8.37E-04	0.102852993	0.062989607
4.2.03_LSB-Steg.png	TRUE	82023	0.44761641	0.410052685	0.401045038
4.2.03_StegOnline.bmp	TRUE	54699	0.411640243	0.409821311	0.398655132
4.2.04GA.bmp	FALSE	2005	0.001293948	0.022336234	0.022852045
4.2.04_LSB-Steg.png	TRUE	54492	0.109431763	0.448458811	0.336423872
4.2.04_StegOnline.bmp	TRUE	36233	0.089003766	0.440266831	0.320810262
4.2.05GA.bmp	FALSE	1940	0.004505766	0.026006712	0.02211449
4.2.05_LSB-Steg.png	TRUE	55129	0.264528786	0.445139875	0.380177097
4.2.05_StegOnline.bmp	TRUE	35425	0.169685238	0.44433494	0.34712031
4.2.06GA.bmp	FALSE	1420	4.19E-08	0.023825325	0.016187578
4.2.06_LSB-Steg.png	TRUE	64635	0.167365533	0.46399416	0.356971206
4.2.06_StegOnline.bmp	TRUE	46088	0.21947907	0.465481233	0.373559561
4.2.07GA.bmp	FALSE	730	2.84E-06	0.008238846	0.00831912
4.2.07_LSB-Steg.png	TRUE	68589	0.311341214	0.466841773	0.416350521
4.2.07_StegOnline.bmp	TRUE	40247	0.142343695	0.461474496	0.350743584

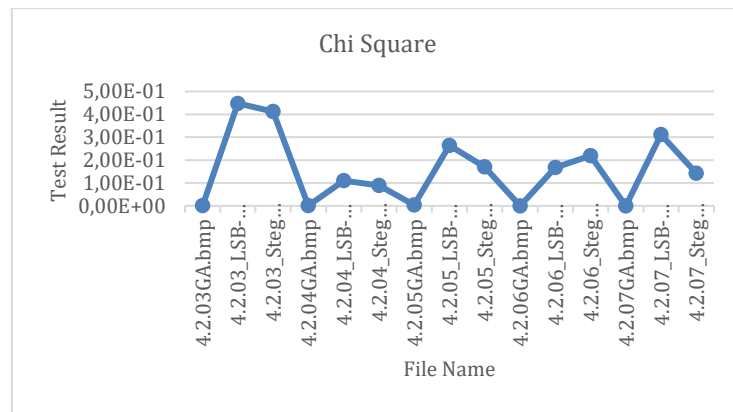


Fig. 38. Comparison graph of chi-square test results

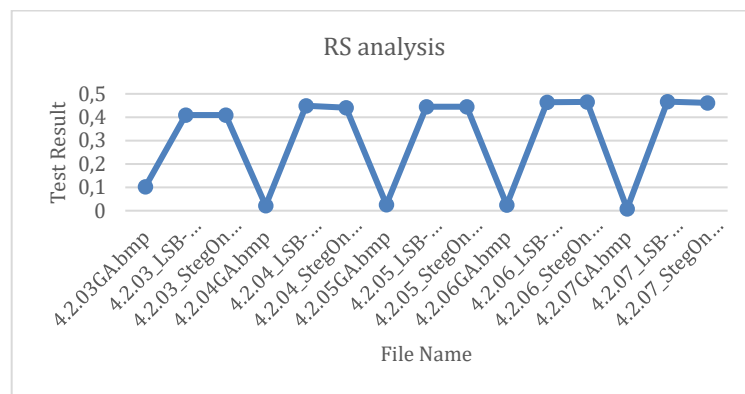


Fig. 39. Comparison graph of RS analysis test results

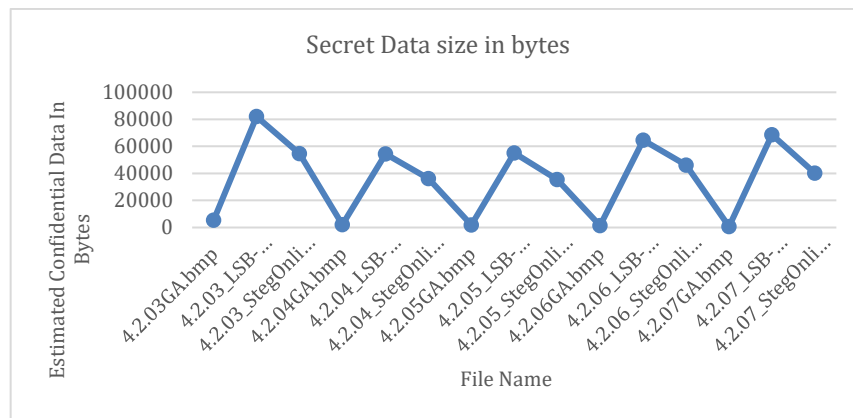


Fig. 40. Comparison graph of embedded secret data estimate results

At the forensic investigation stage, if the evidence is found with the type of digital image during the evidence collection process, it will be carried out using procedures that are in accordance with image forensics based on the National Institute of Standards and Technology (NIST) [46]. When the digital image generated from the proposed method is tested forensically using statistical methods (chi-squared and RS-Analysis), it is able to retain its confidential data. The proposed method also gets a higher PSNR value than the previous method, which means the proposed method gets less damage to the cover image. However, the proposed method has a weakness in the robustness aspect of image processing which causes changes in the spatial domain.

4. CONCLUSION

The proposed method is by utilizing genetic algorithm chromosomes in steganography techniques to control the parameters. It can be a steganographic method as an effective anti-forensic technique. The proposed method can maintain data confidentiality well, as evidenced by a high PSNR value, as evidence which shows the average PSNR value resulting from the proposed method is more than 50 dB, the SSIM value is close to 1, and confidential data can be received back by the intended party intact without being damaged if the pixel value of the steganography image does not change-

The magnitude of the embedding capacity can also be proven by the proposed method based on the results of the comparison of the methods carried out and proven. The cover image and secret image are the same as those used in previous studies. The proposed method gets a higher PSNR value than the previous method. The high PSNR value is obtained because there is less distortion in the steganographic image due to the smaller size of the secret/payload data due to data compression using the Lempel Ziv-Markov Chain Algorithm.

The proposed method can also produce steganographic images with the ability to keep confidential data from being detected during forensic image testing with statistical steganalysis techniques, as proven, and when compared to the general method, the proposed method has better undetectability.

With this, the proposed method can be an effective steganographic method because it is able to maintain data confidentiality, has a large embedding capacity, and has the ability not to be detected during forensic image testing. The proposed method has more ability to embed various types of payload/ secret data because of the way it works, which breaks the byte file into binary.

However, the proposed method still has drawbacks. When there is a change in the pixel value, the secret data will not be accepted again. Transmission and extraction results in those who use Whatsapp fail to be accepted again because, at the time of transmission, the steganographic image is compressed, which results in a change in the pixel value in the steganographic image

REFERENCES

- [1] V. R. Kebande, S. O. Baror, R. M. Parizi, K.-K. R. Choo, and H. S. Venter, "Mapping digital forensic application requirement specification to an international standard," *Forensic Sci. Int. Reports*, vol. 2, p. 100137, Dec. 2020, <https://doi.org/10.1016/j.fsir.2020.100137>.
- [2] V. M. Potdar, M. A. Khan, E. Chang, M. Ulieru, and P. R. Worthington, "E-Forensics steganography system for secret information retrieval," *Adv. Eng. Informatics*, 2005, <https://doi.org/10.1016/j.aei.2005.04.003>.
- [3] A. B. J. Humaira Arshad, "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence," *J. Inf. Process. Syst.*, vol. 14, 2018, <https://doi.org/10.3745/JIPS.03.0095>.
- [4] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. J. Cano, "Digital Forensic Analysis of Cybercrimes," *Int. J. Inf. Secur. Priv.*, vol. 11, no. 2, pp. 25–37, Apr. 2017, <https://doi.org/10.4018/IJISP.2017040103>.
- [5] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, and I. Mavridis, "D4I - Digital forensics framework for reviewing and investigating cyber attacks," *Array*, vol. 5, p. 100015, Mar. 2020, <https://doi.org/10.1016/j.array.2019.100015>.
- [6] K. Hausknecht and S. Gruicic, "Anti-computer forensics," in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, May 2017, <https://doi.org/10.23919/MIPRO.2017.7973612>.
- [7] G. Horsman and D. Errickson, "When finding nothing may be evidence of something: Anti-forensics and digital tool marks," *Sci. Justice*, vol. 59, no. 5, pp. 565–572, Sep. 2019, <https://doi.org/10.1016/j.scijus.2019.06.004>.
- [8] G. C. Kessler, "Anti-Forensics and the Digital Investigator," *Proceedings of The 5th Australian Digital Forensics Conference*, 2007, <https://doi.org/10.4225/75/57ad39ee7ff25>.
- [9] H. Majed, H. N. Noura, and A. Chehab, "Overview of Digital Forensics and Anti-Forensics Techniques," in *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, Jun. 2020, <https://doi.org/10.1109/ISDFS49300.2020.9116399>.
- [10] M. Gul and E. Kugu, "A survey on anti-forensics techniques," in *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, Sep. 2017, <https://doi.org/10.1109/IDAP.2017.8090341>.
- [11] A. K. Singh, "Data Hiding," *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 16, no. 3s, pp. 1–16, Jan. 2021, <https://doi.org/10.1145/3382772>.
- [12] K. Cabaj, L. Caviglione, W. Mazurczyk, S. Wendzel, A. Woodward, and S. Zander, "The New Threats of Information Hiding: The Road Ahead," *IT Prof.*, vol. 20, no. 3, pp. 31–39, May 2018, <https://doi.org/10.1109/MITP.2018.032501746>.
- [13] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, 2010, <https://doi.org/10.1016/j.sigpro.2009.08.010>.
- [14] S. Kaur, S. Bansal, and R. K. Bansal, "Image steganography for securing secret data using hybrid hiding model," *Multimed. Tools Appl.*, vol. 80, no. 5, pp. 7749–7769, Feb. 2021, <https://doi.org/10.1007/s11042-020-09939-7>.
- [15] 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, <https://doi.org/10.1109/ACCESS.2020.3022779>.
- [16] 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, <https://doi.org/10.1109/ACCESS.2021.3053998>.
- [17] A. M. Alhomoud, “Image Steganography in Spatial Domain: Current Status, Techniques, and Trends,” *Intell. Autom. Soft Comput.*, vol. 27, no. 1, pp. 69–88, 2021, <https://doi.org/10.32604/iasc.2021.014773>.
- [18] B. Haloiseau, “Terrorist use of the internet,” in *Cyber Crime and Cyber Terrorism Investigator’s Handbook*, Elsevier, 2014, <https://doi.org/10.1016/B978-0-12-800743-3.00010-4>.
- [19] M. Dalal and M. Juneja, “Steganography and Steganalysis (in digital forensics): a Cybersecurity guide,” *Multimed. Tools Appl.*, vol. 80, no. 4, pp. 5723–5771, Feb. 2021, <https://doi.org/10.1007/s11042-020-09929-9>.
- [20] C. Yakar and S. Ozdemir, “Steganography Application for UTF8 Encoded Texts,” in *2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, Dec. 2018, <https://doi.org/10.1109/IBIGDELFT.2018.8625308>.
- [21] S. Karakus and E. Avci, “A new image steganography method with optimum pixel similarity for data hiding in medical images,” *Med. Hypotheses*, vol. 139, p. 109691, Jun. 2020, <https://doi.org/10.1016/j.mehy.2020.109691>.
- [22] M. Hassaballah, M. A. Hameed, A. I. Awad, and K. Muhammad, “A Novel Image Steganography Method for Industrial Internet of Things Security,” *IEEE Trans. Ind. Informatics*, vol. 17, no. 11, pp. 7743–7751, Nov. 2021, <https://doi.org/10.1109/TII.2021.3053595>.
- [23] T. Kalaichelvi and P. Apuroop, “Image Steganography Method to Achieve Confidentiality Using CAPTCHA for Authentication,” in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, Jun. 2020, <https://doi.org/10.1109/ICCES48766.2020.9138073>.
- [24] I. Baggili, A. BaAbdallah, D. Al-Safi, and A. Marrington, “Research Trends in Digital Forensic Science: An Empirical Analysis of Published Research,” *International Conference on Digital Forensics and Cyber Crime*, 2013, https://link.springer.com/chapter/10.1007/978-3-642-39891-9_9#citeas.
- [25] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, “Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research,” *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019, <https://doi.org/10.1016/j.neucom.2018.06.075>.
- [26] P. D. Shah and R. S. Bichkar, “Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure,” *Eng. Sci. Technol. an Int. J.*, vol. 24, no. 3, pp. 782–794, Jun. 2021, <https://doi.org/10.1016/j.jestch.2020.11.008>.
- [27] A. Miri and K. Faez, “Adaptive image steganography based on transform domain via genetic algorithm,” *Optik (Stuttg.)*, vol. 145, pp. 158–168, Sep. 2017, <https://doi.org/10.1016/j.ijleo.2017.07.043>.
- [28] H. R. Kanan and B. Nazeri, “A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm,” *Expert Syst. Appl.*, vol. 41, no. 14, pp. 6123–6130, 2014, <https://doi.org/10.1016/j.eswa.2014.04.022>.
- [29] K. Karampidis, E. Kavallieratou, and G. Papadourakis, “A review of image steganalysis techniques for digital forensics,” *J. Inf. Secur. Appl.*, vol. 40, pp. 217–235, Jun. 2018, <https://doi.org/10.1016/j.jisa.2018.04.005>.
- [30] I.-H. Pan, K.-C. Liu, and C.-L. Liu, “Chi-Square Detection for PVD Steganography,” in *2020 International Symposium on Computer, Consumer and Control (IS3C)*, Nov. 2020, <https://doi.org/10.1109/IS3C50286.2020.00015>.
- [31] S. Chutani and A. Goyal, “A review of forensic approaches to digital image Steganalysis,” *Multimed. Tools Appl.*, vol. 78, no. 13, pp. 18169–18204, Jul. 2019, <https://doi.org/10.1007/s11042-019-7217-0>.
- [32] W.-B. Lin, T.-H. Lai, and C.-L. Chou, “Chi-square-based steganalysis method against modified pixel-value differencing steganography,” *Arab. J. Sci. Eng.*, vol. 46, no. 9, pp. 8525–8533, Sep. 2021, <https://doi.org/10.1007/s13369-021-05554-2>.
- [33] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K.-H. Jung, “Image steganography in spatial domain: A survey,” *Signal Process. Image Commun.*, vol. 65, pp. 46–66, Jul. 2018, <https://doi.org/10.1016/j.image.2018.03.012>.
- [34] J. Ziv and A. Lempel, “A universal algorithm for sequential data compression,” *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 337–343, May 1977, <https://doi.org/10.1109/TIT.1977.1055714>.
- [35] D. R. I. M. Setiadi, “PSNR vs SSIM: imperceptibility quality assessment for image steganography,” *Multimed. Tools Appl.*, vol. 80, no. 6, pp. 8423–8444, Mar. 2021, <https://doi.org/10.1007/s11042-020-10035-z>.
- [36] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image Quality Assessment: From Error Visibility to Structural Similarity,” *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004, <https://doi.org/10.1109/TIP.2003.819861>.
- [37] A. Westfeld and A. Pfitzmann, “Attacks on Steganographic Systems,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1768, 2000, https://doi.org/10.1007/10719724_5.
- [38] J. R. Lucas, “Minds, Machines and Gödel,” *Philosophy*, vol. 36, no. 137, pp. 112–127, Apr. 1961, <https://doi.org/10.1017/S0031819100057983>.
- [39] J. Fridrich, M. Goljan, and R. Du, “Reliable detection of LSB steganography in color and grayscale images,” in *Proceedings of the ACM International Multimedia Conference and Exhibition*, 2001, pp. 27–30, doi: <https://doi.org/10.1145/1232454.1232466>.
- [40] B. Boehm, “StegExpose - A Tool for Detecting LSB Steganography,” *arXiv preprint*, pp. 1–11, 2014, <https://doi.org/10.48550/arXiv.1410.6656>.
- [41] C.-C. Lin and W.-H. Tsai, “Secret image sharing with steganography and authentication,” *J. Syst. Softw.*, vol. 73, no.

- 3, pp. 405–414, Nov. 2004, [https://doi.org/10.1016/S0164-1212\(03\)00239-5](https://doi.org/10.1016/S0164-1212(03)00239-5).
- [42] C.-N. Yang, T.-S. Chen, K. H. Yu, and C.-C. Wang, “Improvements of image sharing with steganography and authentication,” *J. Syst. Softw.*, vol. 80, no. 7, pp. 1070–1076, Jul. 2007, <https://doi.org/10.1016/j.jss.2006.11.022>.
- [43] C.-M. Wang, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, “A high quality steganographic method with pixel-value differencing and modulus function,” *J. Syst. Softw.*, vol. 81, no. 1, pp. 150–158, Jan. 2008, <https://doi.org/10.1016/j.jss.2007.01.049>.
- [44] C.-C. Chang, Y.-P. Hsieh, and C.-H. Lin, “Sharing secrets in stego images with authentication,” *Pattern Recognit.*, vol. 41, no. 10, pp. 3130–3137, Oct. 2008, <https://doi.org/10.1016/j.patcog.2008.04.006>.
- [45] C.-C. Wu, S.-J. Kao, and M.-S. Hwang, “A high quality image sharing with steganography and adaptive authentication scheme,” *J. Syst. Softw.*, vol. 84, no. 12, pp. 2196–2207, Dec. 2011, <https://doi.org/10.1016/j.jss.2011.06.021>.
- [46] K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to Integrating Forensic Techniques into Incident Response,” *Tech. Rep.*, 2006, <https://doi.org/10.6028/NIST.SP.800-86>.

BIOGRAPHY OF AUTHORS



Amadeus Pondera Purnacandra received his bachelor's degree in Informatics from the faculty of Computer Science, Universitas Amikom, Yogyakarta, in 2022. His research interests include computer networks, data security, cyber security, and digital forensics, in particular. Email: amadeuspondera@gmail.com.



Subektiningsih is Lecturer at Informatics Department, Faculty of Computer Science, Universitas Amikom Yogyakarta. Have an interest in information security and digital forensics. Like the sound of the camera shutter when capturing, and likes to write on a personal blog. Can be contacted via email at subektiningsih@amikom.ac.id.