DOI: 10.14421/ijid.2025.4984 IJID (International Journal on Informatics for Development), *e-ISSN: 2549-7448*
Vol. 14, No. 1, June 2025, Pp.559-574

Implementation and Performance Analysis of PVD Method in Concealing Encrypted Data on Images

Ardhan Hanif
Informatics Department
Ahmad Dahlan University
Yogyakarta, Indonesia
ardhan2100018372@webmail.uad.ac.id

Nur Rochmah Dyah Puji Astuti
Informatics Department
Ahmad Dahlan University
Yogyakarta, Indonesia
rochmahdyah@tif.uad.ac.id

Eko Aribowo
Informatics Department
Ahmad Dahlan University
Yogyakarta, Indonesia
ekoab@tif.uad.ac.id

Article History
Received January 23rd, 2025
Revised April 24th, 2025
Accepted April 25th, 2025
Published June, 2025

***Abstract*—This research aims to secure text data by combining steganography and cryptography. The Pixel Value Differencing (PVD) method allows for higher data insertion capacity with minimal distortion, thereby increasing resistance to steganalysis. However, the PVD steganography method is vulnerable to variation in image areas and to the accuracy of Pixel Difference Histogram (PDH) analysis. In addition, this method is susceptible to statistical tools such as the chi-square and RS, which can be used to analyze the distribution of pixel value differences, allowing data to be detected. To address the limitations of the PVD method, we employed a cryptographic technique called XOR-VLSB, which combines XOR as the primary encryption method, Vigenère Cipher for key generation, and Least Significant Bit (LSB) for key embedding. The results showed that the fully encrypted data could be recovered and had good image quality, as indicated by the metric results, which included a low MSE value, a PSNR above 35 dB, and an SSIM value close to 1. In this study, the process of encrypting text data still uses a simple encryption algorithm, namely XOR. Future research may involve replacing cryptographic algorithms with AES, which offers stronger protection and better resistance to advanced security threats.**

***Keywords*—cryptography; LSB; steganography; XOR; vigenère cipher**

1 INTRODUCTION

Data security is essential in the digital era to maintain integrity and continuity. Maintaining integrity and continuity involves several factors, such as access management, strict identity and the use of technologies, for example, firewalls and data encryption to prevent illegal access into the system. Securing data is very important for several factors, especially since data produced, where collected and exchanged are constantly increasing, as some of these factors can increase the number of data security breaches [1]. Techniques that are often used to solve problems in the data security process are steganography and cryptography methods [2].

Steganography technique is a method used to hide confidential data or messages in digital media, which makes confidential data or messages stored in digital media undetected by others [3][4][5]. The Pixel Value Differencing (PVD) is a steganography method used for hiding confidential data in digital media. This method takes advantage of the comparison of the difference between two-pixel values from the pixel comparison process to know how much data can be hidden in the two pixels. The PVD process has the advantage of being able to store and maintain data with a large capacity in digital media [6][7][8]. The PVD steganography method has several drawbacks that can contribute to the detection of incorrect data. One example is the difference in image intensity that appears in a specific area of the image. It can be analyzed using techniques such as the Pixel Difference Histogram (PDH). This technique allows non-expert individuals to identify the presence of messages by comparing the distribution of pixel differences in the modified image with the original image. In addition, the PVD method is also applicable to many statistical analysis techniques, such as chi-square analysis and regression analysis, which can more thoroughly explain the distribution of sample size differences. Using this method, researchers can identify any anomalies in the image structure that indicate data analysis [9][10].

Cryptography is a method of securing data by using codes, passwords, and encryption techniques that are useful for securely protecting information from unauthorized access [11]. A frequently used Cryptography method in data analysis is the Vigenère Cipher with XOR [12][13]. Vigenère Cipher is a type of encoding based on polyalphabetic substitution, where each character in the plaintext is adjusted to match the character in the key. According to this explanation, the pattern of letters in text is more complex, making it difficult to analyze using frequency analysis techniques. The strength of this method lies in its ability to improve data security, particularly in applications that require protection from any data based on pattern analysis [14][15]. The XOR cryptographic algorithm uses the bitwise XOR operation to encrypt the data by combining the plaintext and the key. This results in a ciphertext that can be easily decrypted with the same XOR operation; the symmetric nature of XOR means that the XOR operation with the same key on the ciphertext will return the original plaintext. The security of this algorithm depends on the key used. Although it is easy to use, its unpredictable nature provides sufficient data communication security [16][17]. The cryptographic process of XOR requires a unique key in the process of encoding data, text, encryption, and decryption [18][19].

Data that is often used in the process of cryptography and steganography is text data, because text data in the process of encoding with cryptography makes the data unreadable because it converts text data into ciphertext to maintain the confidentiality of the data and text data also supports the insertion process in the steganography process because text data can be inserted into the image so that text data cannot be detected, With these advantages, text data becomes an ideal object for steganography and cryptographic processes [20].

In addition to text data that is often used in the steganography process, grayscale images are also often used as cover images in the steganography process because they can effectively conceal text data [21]. Grayscale images have only one channel, in contrast to color images that consist of three channels (blue, green, and red). This structure, in general, facilitates the steganography process and makes data analysis more efficient. Additionally, its complexity makes it easier to manipulate and analyze graphical data, making it more ideal for information gathering purposes [22].

To improve data security and overcome the weaknesses of the Pixel Value Differencing (PVD) steganography method, a cryptographic algorithm-based technique is used. The data is first protected using a cryptographic approach by applying encryption procedures before embedding, which guarantees increased confidentiality and defense against unwanted access. This ensures that, without the proper decryption key, the hidden data content will remain inaccessible if it is discovered. The method used in this study to overcome the weakness in PVD steganography is to use the XOR-VLSB method by relying on unique keys derived from the Least Significant Bit (LSB). The LSB refers to bits in bytes that have the lowest value and are usually located in the last bit in binary representations.

With the solution provided, this research has the main goal, which is to combine steganography and cryptography methods using the PVD scheme combined with XOR and Vigenère Cipher cryptographic algorithms (in loop mode). The unique key used in this process is generated from the LSB. The integration of these two methods is designed to improve the security of data in images through a combination of steganography and cryptography advantages.

2 METHOD

This section discusses three aspects, namely the explanation of the research object used, the research method containing PVD steganography and the XOR-VLSB encryption algorithm and the test method used in this study.

2.1 Research Object

In this study, two objects were used, namely grayscale images and text data.

2.1.1 Grayscale Images: Grayscale images help steganography because they maintain the integrity of the semantic content without considering color distortion. This indicates that hidden messages can be hidden by using the entire cover image. Grayscale images also produce excellent steganography images that are difficult to distinguish from cover images, which increases the security of sensitive data as it prevents damage to luminance channels. Grayscale images are a great choice of objects in the steganography process because they offer a new weight allocation mechanism to achieve a concealment balance [23]. In this study, four grayscale images in BMP, JPG, PNG, and TIFF formats were used as steganography objects. These images are selected to evaluate the effectiveness of the methods used in various image formats. An example of the use of grayscale images in the steganography process can be seen in Figure 1. In Figure 1, a dataset of images with various formats is displayed, namely BMP, JPG, PNG and TIFF with grayscale images. The image shown also has different sizes among the images in Fig. 1, as shown in Table 1.

2.1.2 Text Data: Text data is the object choice for the data to be encrypted and inserted into the object image. The data text used is 8 data texts with the size as shown in Table 2.

2.2 Research Stages

At this stage, this research employs an experimental method that implements the PVD schematic process in hiding data that has been encrypted by the XOR-VLSB cryptographic algorithm process. The flow is as shown in Figure 2.

Figure 1. Grayscale Images

Table 1. Image Size

No	Text Data	Size
1	Couple.bmp	258 KB
2	Couple.jpg	73 KB
3	Couple.png	208 KB
4	Couple.tiff	257 KB

Table 2. Text Data Size

No	Text Data	Size
1	Plaintext 1	10 KB
2	Plaintext 2	20 KB
3	Plaintext 3	30 KB
4	Plaintext 4	40 KB
5	Plaintext 5	50 KB
6	Plaintext 6	60 KB
7	Plaintext 7	70 KB
8	Plaintext 8	80 KB

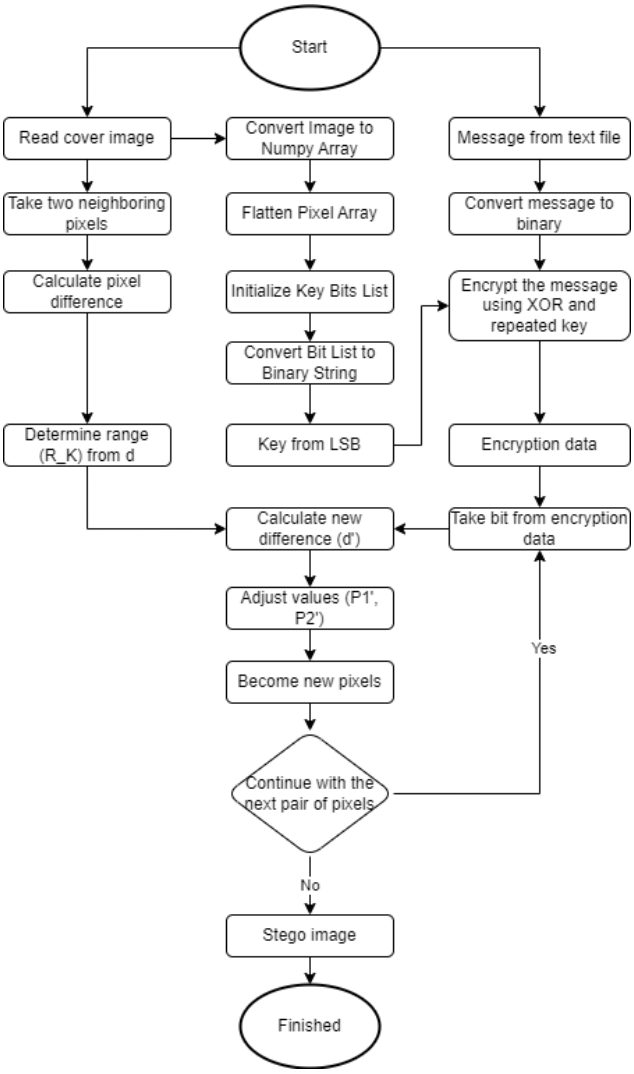

Figure 1. Research Stages

2.2.1 XOR-VLSB: The XOR algorithm is a cryptographic technique that uses XOR (exclusive OR) logic operations on every bit of data to be encrypted. This algorithm encrypts the plaintext by using an XOR key to generate ciphertext, which cannot be read without the available key. For decryption, the same method is used. The ciphertext is re-encoded using the XOR key to retrieve the plaintext. This is due to the nature of XOR's operation, which means that if you apply XOR to the result of encryption with the same key, you will get the original data back. XOR's algorithm is well-known for its simplicity and ease of implementation [16].

Table 3. XOR Equation *[16]*

A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	1

The algorithms used in the encryption and decryption process in this study include several cryptographic algorithms, such as XOR as the main process in data encryption, Vigenère as the key loop process to perform encryption and LSB as the key taken from the Least Significant Bit (LSB) on an image. Binaries in LSB are used to strengthen keys so that encrypted data cannot be cracked because the keys used have a random and long structure.

2.2.2 *Pixel Value Differencing (PVD):* The PVD method takes advantage of the difference in intensity values between adjacent pixels in an image to insert a secret message. The basic principle of PVD is that the greater the difference in intensity values between two adjacent pixels, the more information can be inserted into the image without causing significant distortion. As such, this method allows for a larger amount of data to be inserted in areas of the image that have high contrast, while in areas with small pixel differences, fewer bits are inserted to maintain the visual quality of the image. The main advantage of PVD lies in its ability to balance data insertion capacity with minimal visual distortion, making this technique one of the most effective approaches in image steganography [10] [24]. The PVD process in steganography is based on the difference in pixel values in a block to determine the data analysis capacity. The formula used in this method can be expressed as shown in (1) as follows:

$$d_i = |p_i - p_{(i+1)}| \quad (1)$$

d_i : Difference Between Pixels
p_i : First Pixel
$p_{(i+1)}$: The Second Pixel of the Pair

2.3 Pixel Intensity Testing Methods

The test method used in this study is to calculate the pixel intensity in the image with the results of calculations from MSE, PSNR, SSIM.

2.3.1 *Mean Squared Error (MSE):* Mean Squared Error (MSE) is a metric that measures the level of distortion in an image by comparing the average pixel value of the original image and the processed image [25]. Lower MSE values indicate good quality [26]. MSE is expressed in the form of the following formula in (2).

$$\text{MSE}=\frac{1}{\text{m} \times \text{n}}\sum_{\text{i=1}}^{\text{m}} \sum_{\text{j=1}}^{\text{n}}[\text{I(i,j)-K(i,j)}]^2 \quad (2)$$

m : Number of rows (image height).
n : Number of columns (image width).
$M \times n$: The total number of pixels in the image.
$I(i,j)$: The pixel intensity value of the original image.
$K(i,j)$: Values the pixel intensity of the steganography image.
$[I(i,j)-K(i,j)]^2$: The square of the difference between two pixels.
$\frac{1}{m \times n}$: The average of all the squares of the difference

2.3.2 *Peak Signal to Noise Ratio (PSNR):*To assess image quality, the PSNR, which is calculated in decibel units (dB), is used to compare the original image with the steganography image. A high value of PSNR indicates that the image has very little distortion, which means that the steganography image is preserved during the insertion process[27]. PSNR results above 40 dB are considered good in terms of image quality[28]. The Peak Signal-to-Noise Ratio (PSNR) is expressed in the form of the following formula in (3).

$$PNSR = 10 \times \log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (3)$$

MAX : Maximum value of pixel intensity
MSE : Mean Squared Error
$\log_{10}$: Logarithm line 10

2.3.3 *Structural Similarity Index Method (SSIM):* The Structural Similarity Index Measure, or SSIM, is a method used to determine the degree of similarity between two images that correspond to human visual perception. Since SSIM evaluates the similarity of images based on their structural characteristics, the quality of the images is assessed using the aspects mentioned above. The three main components of SSIM are structure, illumination, and contrast [29]. The SSIM scale runs from 0 to 1, with 1 increasing in value and indicating that the images are structurally very similar [30].

$$\text{SSIM} = \frac{(2_{\mu I \mu K} + \text{C}_1)(2\sigma_{IK} + \text{C}_2)}{(\mu_I^2 + \mu_K^2 + \text{C}_1)(\sigma_I^2 + \sigma_K^2 + \text{C}_2)} \quad (3)$$

μI : The average value of the pixel intensity of the original image.
μK : The average value of the pixel intensity of the stego image.
σ_I^2 : Variation in the original image.
σ_K^2 : Variation in the stego image.
σ_{IK} : the correlation between the original image and the stego image.
C_1 : small constant for stability
C_2 : small constant for stability

3 RESULT AND DISCUSSION

The results of the test during the research process using the PVD scheme combined with the XOR-VLSB cryptographic algorithm are as follows.

3.1 Results of Plaintext Encryption

In the process of encryption and decryption using the XOR-VLSB cryptographic method, the XOR algorithm plays an important role as the main mechanism in data security. Meanwhile, Vigenère functions as a loop on the key used to carry out the encryption process, which is to convert the original data (plaintext) into encrypted data (ciphertext) that cannot be read without the corresponding key. Instead, the same algorithm is used for the decryption process, i.e. it returns the encrypted data to its original data using the same key.

The key used in this process is taken from the LSB (Least Significant Bit) bits of the image that is the object of the steganography. The LSB bits of this image serve as a unique key source, thus adding a layer of security to the encryption process. By utilizing keys derived from the characteristics of the cover image, the encryption and decryption process becomes more difficult to guess or hack without having access to the image used as the key storage medium. The combination of the XOR method with the VLSB approach provides double protection of the data, so that the data inserted into the image becomes safer from exploitation attempts. The results of the encryption and decryption process are as shown in Table 4.

Based on the data presented in Table 2, it can be concluded that the XOR-VLSB cryptographic algorithm process can generate ciphertext that is completely unreadable or recognized by parties who do not have access to the appropriate encryption keys. The encryption process using the XOR-VLSB algorithm works by converting plaintext data into ciphertext form through XOR operations, where the encryption key is retrieved from the LSB bits, and Vigenère serves as a loop so that the key length matches the plaintext. The result of this process is encrypted data that is completely different from the original plaintext, making it difficult to understand or decipher without proper information.

In addition, at the time of the decryption process, the XOR-VLSB algorithm demonstrates its ability to return the ciphertext to its initial plaintext form with a very high degree of accuracy, provided that the correct encryption key is used. This proves that this algorithm is not only effective in protecting data confidentiality during the encryption process, but also reliable in ensuring the integrity and integrity of data during the decryption process. Therefore, the combination of encryption and decryption generated by the XOR-VLSB cryptographic algorithm provides strong protection of the data and guarantees that the data can be returned to its original form without loss of information.

Table 4. Encryption and Decryption Results

Plaintext	Cipher text	Decryption
abcdefghijklnmopqrst uvwxyz_ABCDEFGH IJKLNMOPQRSTUV WXYZ	QSRTTVVXXZZ_]^ @@BBDDFFHHJnqs suuwwyy{{}~|• aacce eggiik	abcdefghijklnmopqrst uvwxyz_ABCDEFGH IJKLNMOPQRSTUV WXYZ

Based on the data in Table 5, the results of the implementation of the PVD method that inserts encrypted data of different sizes show that there are some size changes between the original image and the steganography image. The implementation of the PVD method caused the image size to decrease, increase and remain.

Images with TIFF and BMP formats tend to be stable, even though the amount of data inserted is of different sizes. Images in TIFF and BMP formats have high image quality and are resistant to compression[31]. Images with the PNG format have an increase in size during the implementation process of the PVD method due to the nature of PNG images having lossless compression with which the image becoming larger [32]. While the JPG format has decreased because the implementation process of PVD and LSB schemes can change the characteristics of the JPG format, JPG uses lossy compression, which results in a decrease in image size during the implementation process of the PVD method [26].

3.2 Results of Pixel Intensity Testing Methods

This section presents the results of the evaluation of pixel intensity changes in several image formats, namely BMP, JPG, PNG, and TIFF. Using MSE, PSNR, and SSIM metrics, the study was conducted to analyze the effect of steganography reducers on image quality.

3.3 Mean Squared Error (MSE):

In the calculation of the Mean Squared Error (MSE) image quality metric, this method is used to measure the average difference in pixel values between the original image and the image that has undergone the data insertion process.

The MSE calculation process begins by calculating the difference in pixel values at each position between the original image and the inserted image. This difference is then squared to ensure that all negative values are converted into positives, making them easier to analyze. After that, the sum of all the squared values of this difference is divided by the total number of pixels in the image to get the average value. The final result of the MSE calculation shows the extent to which the inserted image differs from the original image. The smaller the MSE value, the smaller the level of distortion that occurs, thus indicating that the data insertion process is well done without significantly disturbing the visual quality of the image.

The results of this calculation display the MSE values for various data that have been inserted into the image. This table provides a clear picture of how much difference the image embedding process makes to each dataset. Analysis of these results can be used to evaluate the efficiency of the steganography algorithm used, while ensuring that the image

quality is maintained even after the data is inserted into it. The MSE calculation results are presented in Table 6.

The results of the MSE calculation show that the image format used has a significant impact on the level of distortion after the data embedding process. The JPG format has a much higher MSE value than the BMP, PNG, and TIFF formats, which indicates that the embedding method causes larger pixel changes in the JPG format. The lossy compression nature of the JPG format may cause the image quality to become worse after the embedding process.

In addition, the MSE value increases as the plaintext size increases across all image formats. The MSE values increased on BMP, PNG, and TIFF linearly and somewhat slowly, suggesting that the embedding method did not significantly alter the image quality. In contrast, in JPG, although there was a slight increase from 12.60 to 12.70, the distortion remained high from the start, suggesting that lossy compression had a greater influence on the rebuttal.

The results showed that BMP, PNG, and TIFF formats were more suitable for steganography as they exhibited minimal distortion, allowing the inserted images to maintain high visual quality. In contrast, the JPG format is not recommended because high MSE values indicate a greater loss of quality, which can increase the likelihood of being detected by steganography analysis methods.

3.4 Results of Peak Signal-to-Noise Ratio (PSNR)

The calculation of the Peak Signal-to-Noise Ratio (PSNR) metric shows a good quality image with low distortion values and high decibel values, by performing the calculation process. The results are shown in Table 7.

Table 5. Image Size

Size Images	Size	BMP	JPG	PNG	TIFF
Original size		258 KB	63 KB	208 KB	257 KB
1	10 KB	769 KB	42 KB	265 KB	769 KB
2	20 KB	769 KB	42 KB	283 KB	769 KB
3	30 KB	769 KB	42 KB	302 KB	769 KB
4	40 KB	769 KB	42 KB	321 KB	769 KB
5	50 KB	769 KB	42 KB	343 KB	769 KB
6	60 KB	769 KB	42 KB	363 KB	769 KB
7	70 KB	769 KB	42 KB	382 KB	769 KB
8	80 KB	769 KB	42 KB	401 KB	769 KB

Table 6. MSE Calculation Results

Plaintext	Size	BMP	JPG	PNG	TIFF
1	10 KB	0.06	12.60	0.06	0.06
2	20 KB	0.11	12.62	0.11	0.11
3	30 KB	0.17	12.63	0.17	0.17
4	40 KB	0.23	12.65	0.23	0.23
5	50 KB	0.28	12.66	0.28	0.28
6	60 KB	0.34	12.68	0.34	0.34
7	70 KB	0.40	12.69	0.40	0.40
8	80 KB	0.45	12.70	0.45	0.45

Table 7. PSNR Calculation Results

Plaintext	Size	BMP	JPG	PNG	TIFF
1	10 KB	60.64 dB	37.12 dB	60.63 dB	60.63 dB
2	20 KB	57.58 dB	37.11 dB	57.58 dB	57.58 dB
3	30 KB	55.82 dB	37.10 dB	55.82 dB	55.82 dB
4	40 KB	54.55 dB	37.09 dB	54.57 dB	54.57 dB
5	50 KB	53.59 dB	37.07 dB	53.59 dB	53.59 dB
6	60 KB	52.80 dB	37.06 dB	52.80 dB	52.80 dB
7	70 KB	52.13 dB	37.05 dB	52.14 dB	52.14 dB
8	80 KB	51.56 dB	37.04 dB	51.56 dB	51.56 dB

According to the PSNR, the image format used affects the image quality after the data is entered. The BMP, PNG, and TIFF formats have a high PSNR value, which indicates that the image quality remains good after the data is entered. In contrast, the JPG format has a much lower PSNR value, around 37 dB, which indicates a higher level of distortion than the previous JPG format.

However, the PSNR value of JPG usually remains at around 37 dB, indicating that the image quality of the embedding results in this format has deteriorated since the beginning due to lossy compression. In other words, it is not only the embedding process that degrades the quality of the image, but also the innate nature of the JPG format, which results in greater information loss.

Based on the results, it can be concluded that the BMP, PNG, and TIFF formats are better for steganography because of their high PSNR values, which indicate that the embedded images still have good quality and are not as different from the original images. Conversely, the JPG format is not very suitable for steganography because the low PSNR value indicates a higher distortion threshold, which can increase the detection ability through steganographic analysis.

3.5 Structural Similarity Index Method (SSIM)

In the process of calculating the value of image quality metrics from the SSIM with an emphasis on luminance, contrast, and structure. The very good metric value can be seen in Table 8.

Based on the results of the SSIM analysis, it can be shown that the BMP, PNG, and TIFF formats have very high SSIM values, ranging from 0.9998 to 0.9989. This indicates that the image structure is quite good after the data embedding process. On the other hand, the JPG format has a somewhat higher SSIM value, which is stable at around 0.9573. This indicates that there is a more noticeable change in the structure of the image compared to other formats.

Along with the reduction in plain text size, SSIM values in BMP, PNG, and TIFF still have a very high range (above 0.9976) despite slight fluctuations. This suggests that even though there is more data being analyzed, the embedding results still have a structure very similar to the original data, making it difficult to detect visually.

Table 8. SSIM Calculation Results

Plaintext	Size	BMP	JPG	PNG	TIFF
1	10 KB	0.9998	0.9573	0.9998	0.9998
2	20 KB	0.9996	0.9573	0.9996	0.9996
3	30 KB	0.9995	0.9572	0.9995	0.9995
4	40 KB	0.9994	0.9572	0.9994	0.9994
5	50 KB	0.9993	0.9572	0.9993	0.9993
6	60 KB	0.9992	0.9572	0.9991	0.9991
7	70 KB	0.9991	0.9571	0.9990	0.9990
8	80 KB	0.9989	0.9571	0.9987	0.9987

In contrast, the SSIM value for JPG is stable at around 0.9570, which is significantly lower than other formats. This indicates that the structure of the JPG image has undergone significant distortion, which can be attributed to the combination of the embedding process and the lossy compression of the JPG file itself.

Based on the results, it can be concluded that the BMP, PNG, and TIFF formats are better for steganography due to their high SSIM values, indicating that the embedding results rarely change structurally when compared to the original images. In contrast, the JPG format is not suitable because a more accurate SSIM indicates that the structure of the image changes significantly, making it more susceptible to detection by steganalysis techniques.

3.6 Pixel intensity changes

The change in value from the maximum intensity in the pixel occurs due to the process of inserting data using the steganography method. In this process, the pixel values in the image undergo minimal changes that do not significantly affect the visual appearance of the original image. This change results from the insertion of text data using the PVD method, the steganography method employed in this study, which aims to maintain the visual quality of the steganography images without causing significant alterations.

In the PVD method, the difference in the value of the maximum pixel intensity between the original image and the steganography image is the main indicator of the effectiveness of this method. The resulting histogram shows the distribution of the maximum intensity of the pixels for each value in the range of 0–255, where the vertical axis represents the number of pixels at each intensity level, and the horizontal axis represents the pixel intensity level.

As a result, despite a significant increase in data insertion in text data size ranging from 10 to 80 KB, the pixel distribution between the original image and the steganography image still showed a very high degree of similarity, both visually and statistically. This proves that the steganography method with a PVD scheme can insert text data efficiently and safely without being conspicuous, while maintaining the visual quality of the image to remain as it is original.

The following are histogram results showing the distribution of maximum image intensity of the original image and steganography in various formats and sizes. This histogram is used to analyze the differences in data distribution before and after the data analysis process. The histograms for each image format, BMP, JPG, PNG, and TIFF, are displayed in a separate, understandable way to highlight differences in the distribution of image intensity depending on the type of format used.

3.7 Histogram of Pixel Intensity Changes in BMP Format

In this section, the analysis focuses on the changes in pixel intensity distribution in steganographic images embedded with text data using the PVD method. The image format used is BMP (Bitmap), which is known for preserving image quality without compression, allowing clear observation of pixel value changes. The experiments document histogram changes in images embedded with text data ranging from 10 to 80 KB. These changes are analyzed by comparing the histograms of the original and steganographic images, highlighting the extent to which data embedding affects the pixel intensity distribution. The results provide insights into the effectiveness of the PVD method in embedding large amounts of data while maintaining minimal visual disturbance in BMP images.

The histograms in Figures 3 to 10 show the change in the image intensity distribution in BMP steganography images after text data ranging in size from 10 to 80 KB were analyzed using the PVD method. All these analyses were performed in images with BMP extensions, indicating that the format was used consistently during the experiment. Due to the uncompressible nature of the BMP format, changes in the data pixels because of the data analysis process can be clearly and accurately seen through a histogram.

Fig. 3 shows that although the data is about 10 KB in size, the histogram curve of the steganography image is almost identical to the original image, indicating a very high visual quality. Figures 4 and 5 show the results of the data analysis of 20 and 30 KB, respectively. It is evident that there are some fluctuations at some points of intensity, but the entire distribution of the histogram is stable and does not appear to be distorted.

Fig. 6 shows that when 40 KB of data is inserted into the image, a clearer distribution of pixel intensity is seen on the histogram. Nevertheless, the overall distribution pattern remained undisturbed. When the amount of data inserted increases from 50 to 80 KB, as shown in Figures 7 through 10, the histogram begins to show signs of shifting and spreading of intensity values. Fig. 7 shows changes in shifts and widening of distributions, while Fig. 8 indicates a decrease in dominance at a given intensity, reflecting an adjustment to larger data loads.

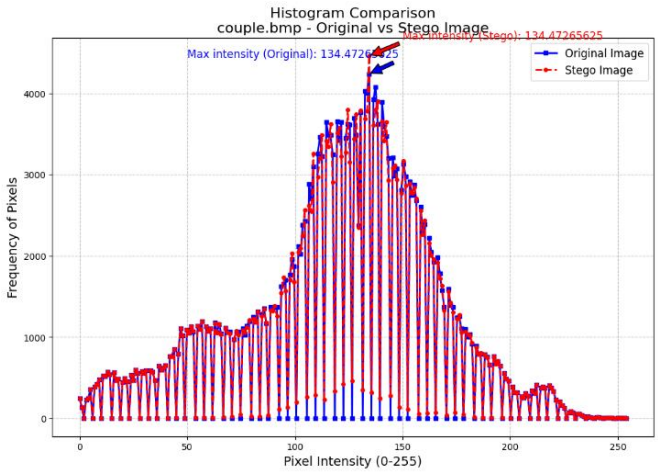

Figure 3. Pixel intensity histogram BMP on plaintext 1

Although the data size continues to increase in Figs. 9 and 10, the steganography histograms are similar to the original histograms of the image. The PVD method remains effective in gradually inserting large data into the BMP image, while maintaining visual quality, as demonstrated by the similarity of the histogram patterns before and after insertion.

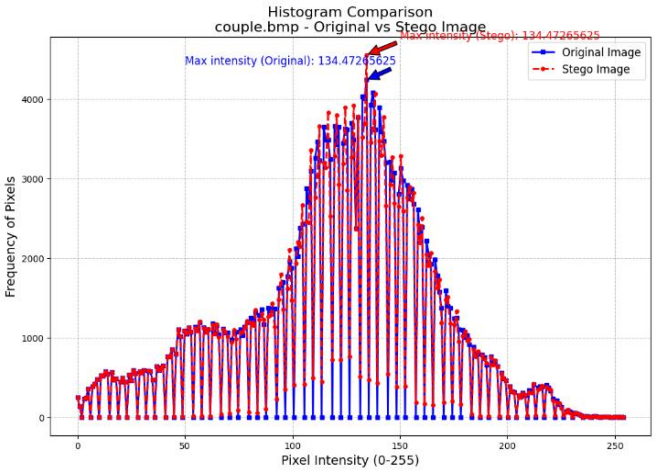

Figure 4. Pixel intensity histogram BMP on plaintext 2

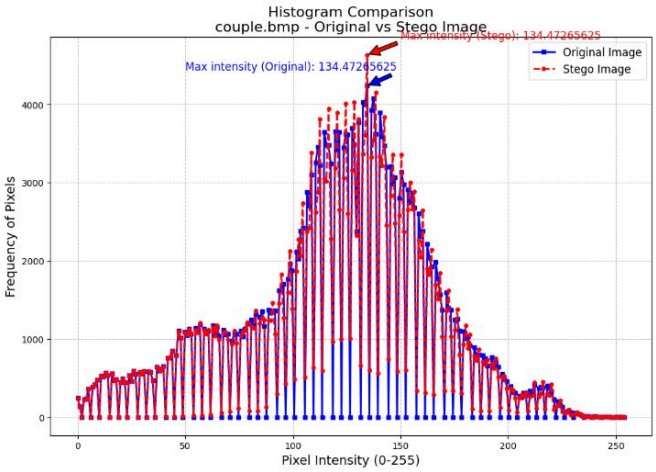

Figure 5. Pixel intensity histogram BMP on plaintext 3

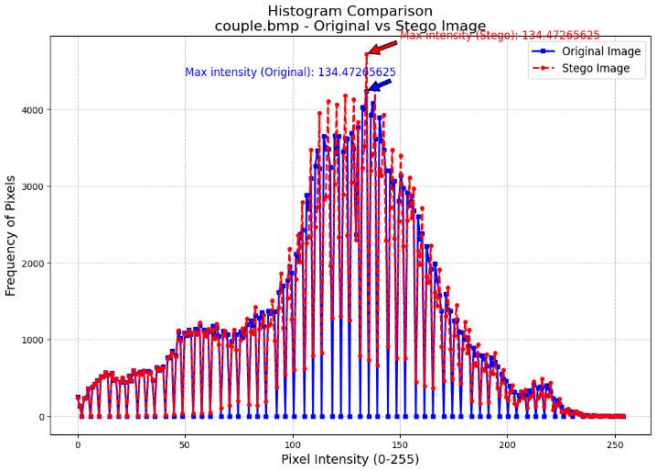

Figure 6. Pixel intensity histogram BMP on plaintext 4

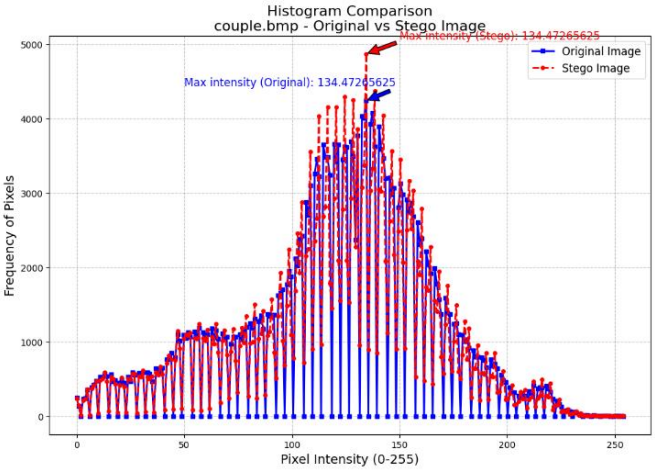

Figure 7. Pixel intensity histogram BMP on plaintext 5

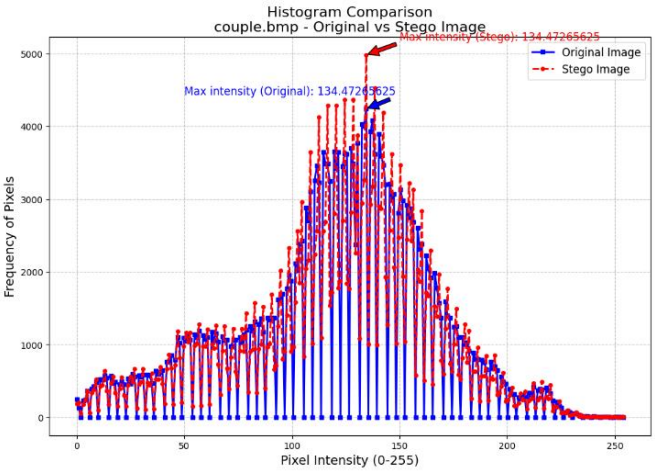

Figure 8. Pixel intensity histogram BMP on plaintext 6

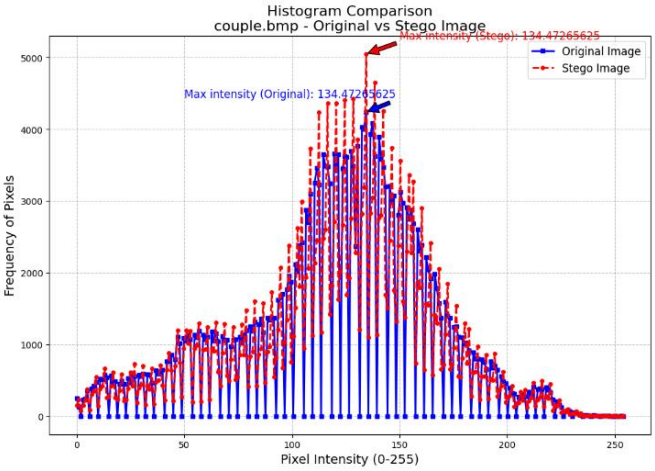

Figure 9. Pixel intensity histogram BMP on plaintext 7

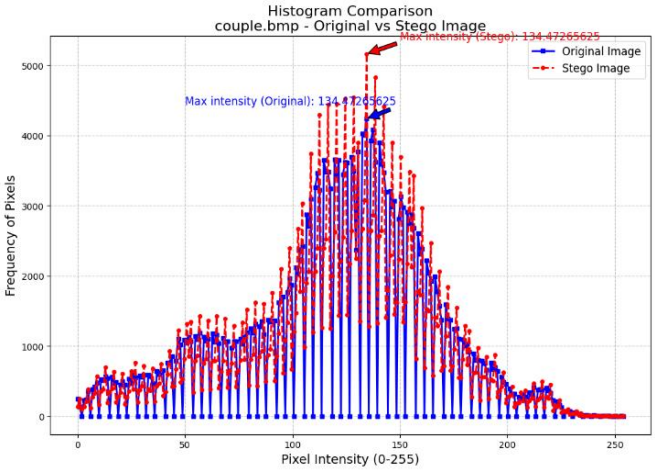

Figure 10. Pixel intensity histogram BMP on plaintext 8

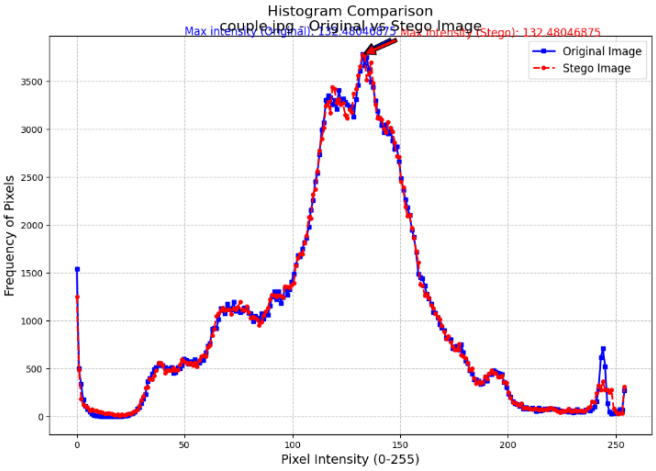

Figure 11. Pixel intensity histogram JPG on plaintext 1

3.8 Histogram of Pixel Intensity Changes in JPG Format

In this section, the analysis focuses on changes in the pixel intensity distribution in steganography images inserted with text data. This was done using the PVD method. The image format used was JPG (JPEG), commonly used for image compression and known for its balance between file quality and size, allowing for the storage of steganography images. This experiment observed changes in histograms in images with text data from 10 to 80 KB. These changes are analyzed by comparing the histogram of the original image with the steganography image, which shows how much the data insertion affects the pixel intensity distribution. These results provide an idea of how effective the PVD method is at inserting a lot of data while maintaining minimal visual interference in JPG images.

The histograms in Figures 11 to 18 show the similarity in pixel intensity distribution between the original image and the JPG format steganography image after inserting text data between 10 and 80 KB using the PVD method. Although the histograms appear similar, the JPG format exhibits a decline in quality as a result of the PVD method's implementation. This is due to the lossy compression properties of the JPG format, which can alter the data characteristics of the image and decrease the size and visual quality during the data insertion process.

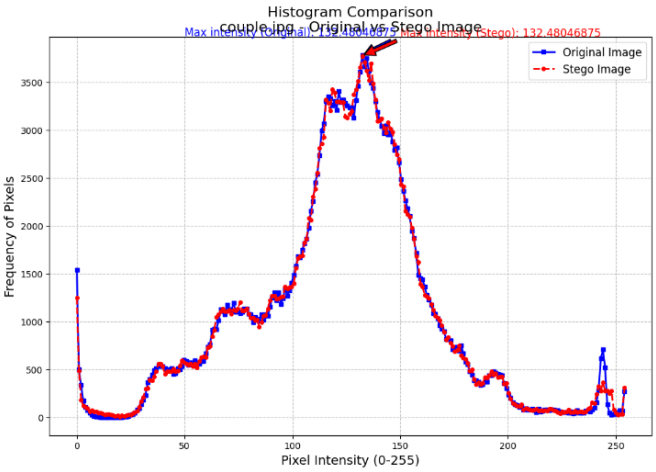

Figure 12. Pixel intensity histogram JPG on plaintext 2

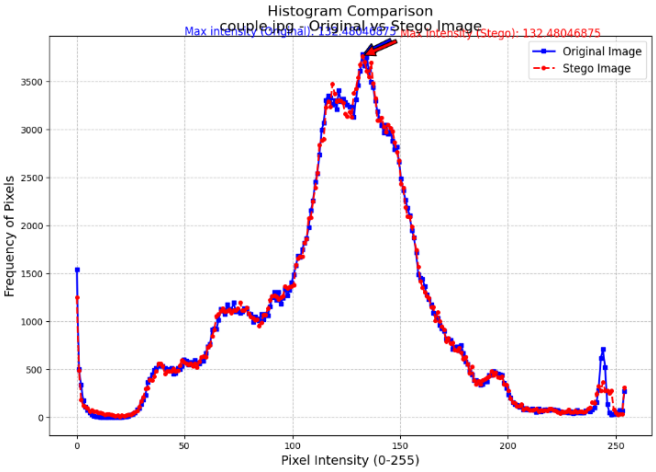

Figure 13. Pixel intensity histogram JPG on plaintext 3

3.9 Histogram of Pixel Intensity Changes in PNG Format

The pixel intensity distribution in steganography images using the PNG format changes after the insertion of text data of various sizes using the Pixel Value Differencing (PVD) method. The PNG format was chosen because it is not corrupted, allowing accurate observation of pixel changes through histograms. To find out the extent to which the steganography process affects the visual quality of the image, an analysis was performed on the image with the insertion of data between 10 and 80 KB.

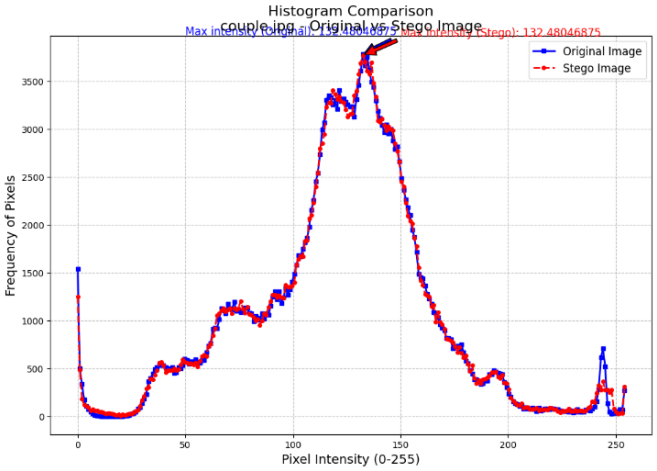

Figure 14. Pixel intensity histogram JPG on plaintext 4

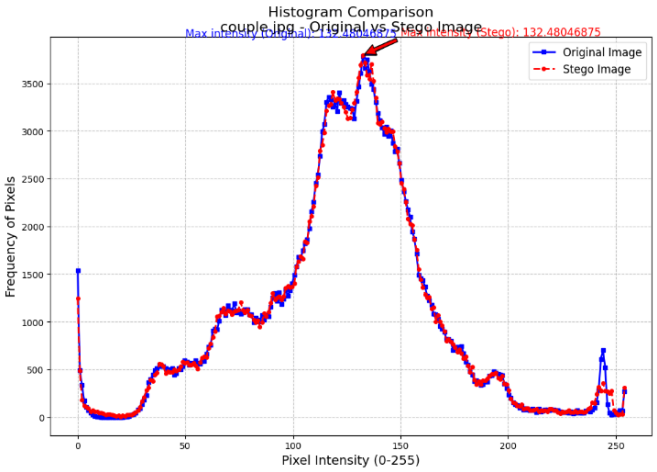

Figure 15. Pixel intensity histogram JPG on plaintext 5

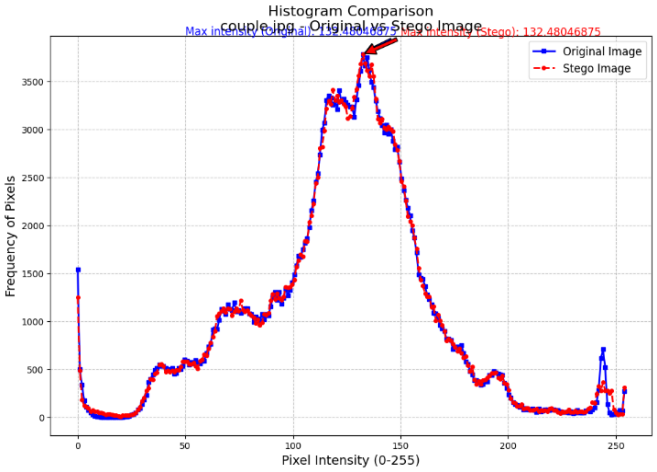

Figure 16. Pixel intensity histogram JPG on plaintext 6

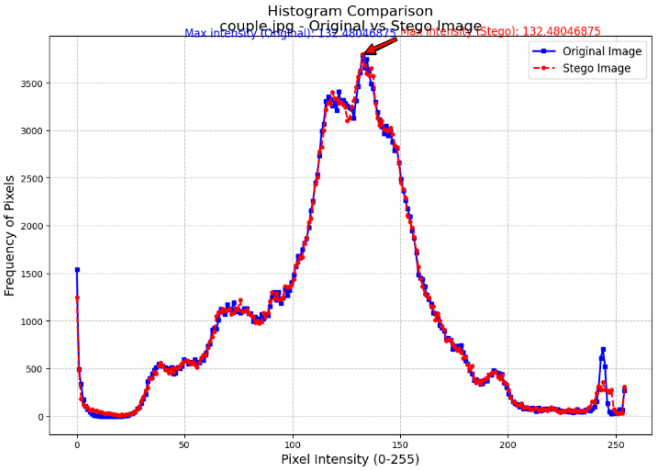

Figure 17. Pixel intensity histogram JPG on plaintext 7

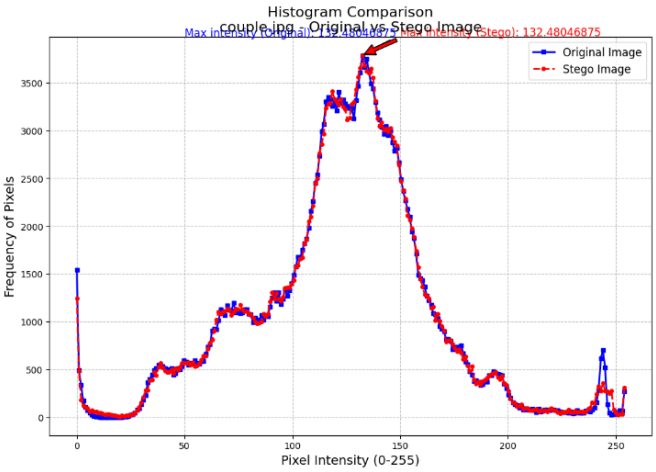

Figure 18. Pixel intensity histogram JPG on plaintext 8

The histogram results in Figures 19 to 26 show a change in the pixel intensity distribution in PNG format steganography images after inserting text data with sizes varying from 10 to 80 KB, using the PVD method. All experiments were consistently conducted using PNG images, as the lossless nature of this format allows accurate visualization of pixel changes through histograms.

In Fig. 19, when data measuring a 10 KB inserted image, the histogram shape of the steganography image is almost identical to the original image, indicating that the visual quality is maintained. In Figures 20 and 21, the data insertion results of 20 and 30 KB differ slightly, but the histogram distribution remains stable and does not experience significant disruption.

In Figures 22 and 23, with image sizes of 40 and 50 KB, the histogram results show changes in the pixel intensity points of the steganography image. However, the histogram distribution remains stable and does not experience any disturbances in the results of the insertion process using the PVD method.

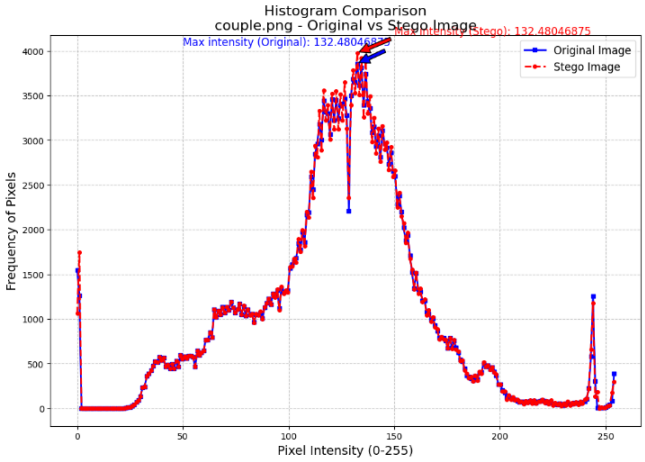

Figure 19. Pixel intensity histogram PNG on plaintext 1

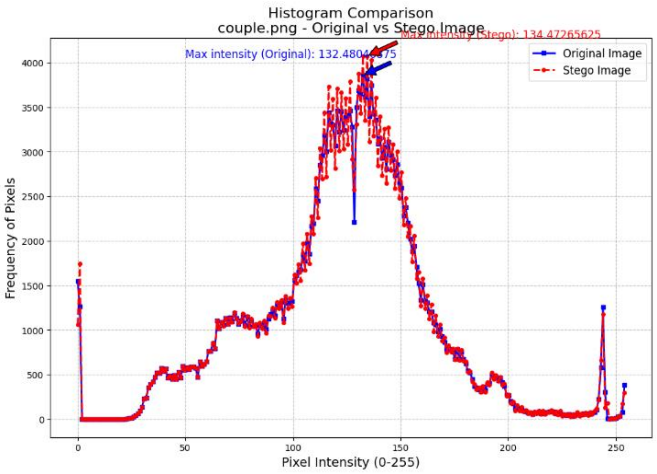

Figure 20. Pixel intensity histogram PNG on plaintext 2

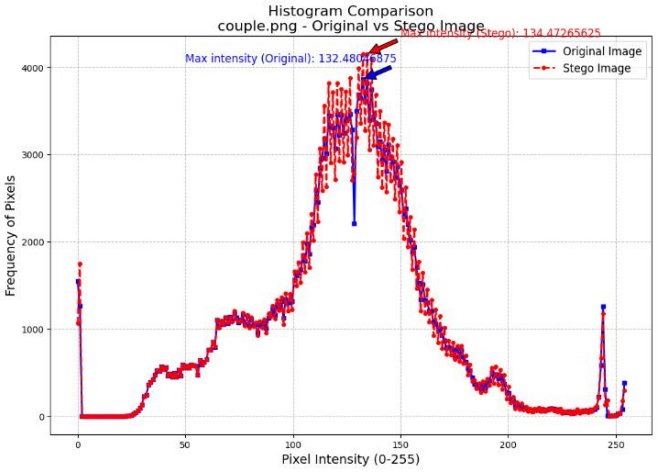

Figure 21. Pixel intensity histogram PNG on plaintext 3

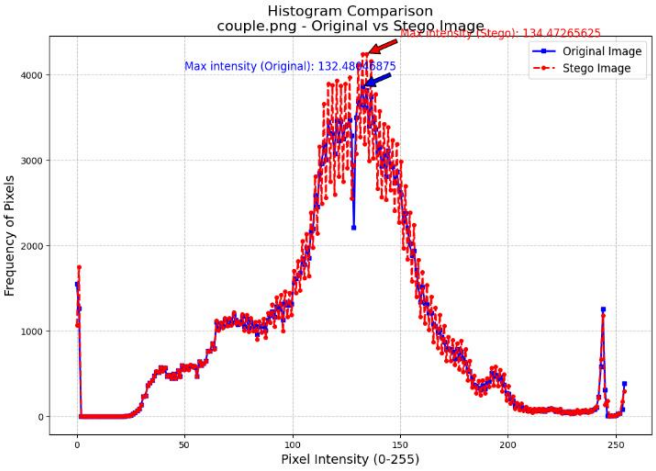

Figure 22. Pixel intensity histogram PNG on plaintext 4

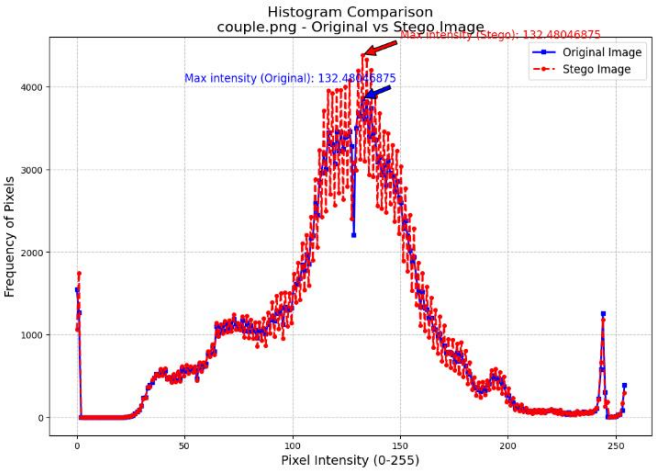

Figure 23. Pixel intensity histogram PNG on plaintext 5

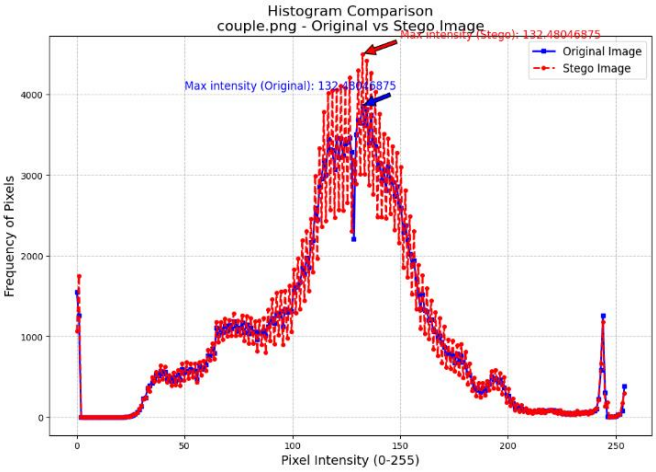

Figure 24. Pixel intensity histogram PNG on plaintext 6

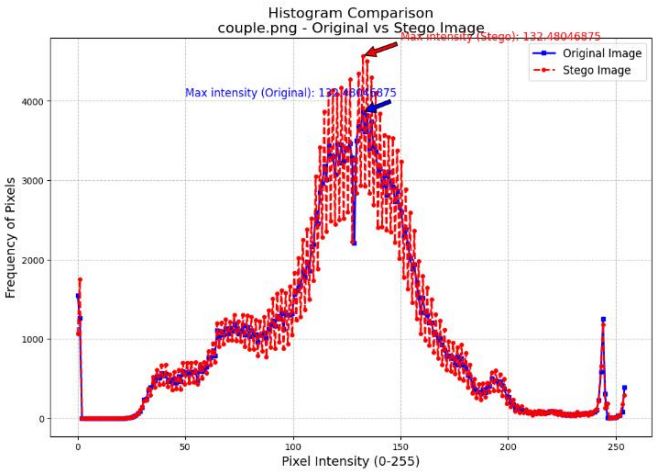

Figure 25. Pixel intensity histogram PNG on plaintext 7

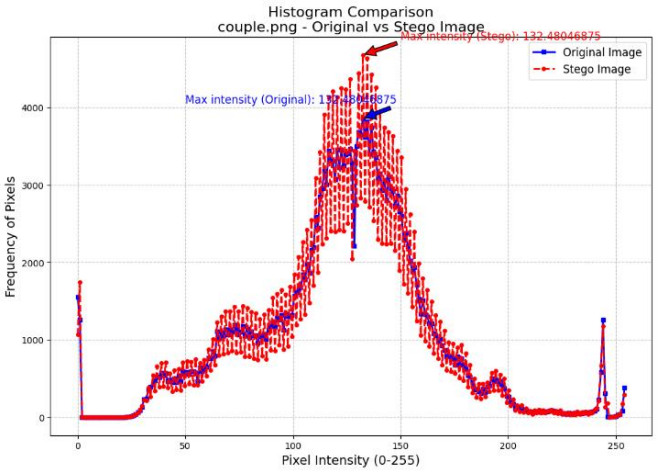

Figure 26. Pixel intensity histogram PNG on plaintext 8

When inserting images with larger sizes, such as 60, 70 and 80 KB as shown in Figures 24 to 26, the pixel distribution histogram remains stable, with no interference from the insertion process using the PVD method. Overall, these results confirm that the PVD method is effective in inserting large data into PNG images without causing significant distortion to the pixel intensity distribution, which demonstrates that the visual quality of the image can still be well maintained.

3.10 Histogram of Pixel Intensity Changes in TIFF Format

In this section, the analysis focuses on changes in the pixel intensity distribution in steganography images embedded with text data using the PVD method. The image format used is TIFF, which is known to maintain image quality through lossless or no compression at all, allowing accurate observation of changes in pixel values. The experiment documented histogram changes in images embedded with text data ranging from 10 to 80 KB. The impact of data embedding on pixel intensity distribution was assessed by comparing the histograms of the original and steganographed images. The results provide insight into the effectiveness of the PVD method in embedding large amounts of data while maintaining minimal visual interference in TIFF images.

The histograms in Figures 27 to 34 illustrate the changes in pixel intensity distribution of steganographic images in TIFF format after embedding text data ranging from 10 to 80 KB, using the PVD method. All analyses were conducted using TIFF images to ensure consistency in file format throughout the experimental process. As a format that supports lossless compression or no compression at all, TIFF allows for accurate observation of pixel-level changes, which can be effectively visualized through histogram analysis.

In Fig. 27, where approximately 10 KB of data was embedded, the histogram of the steganographic image closely resembles that of the original image. This indicates that the embedding process had minimal impact on the visual quality. In Figures 28 and 29, which correspond to 20 and 30 KB of embedded data, respectively, minor fluctuations appear at certain intensity points. However, the overall histogram distribution remains stable and does not exhibit significant distortion.

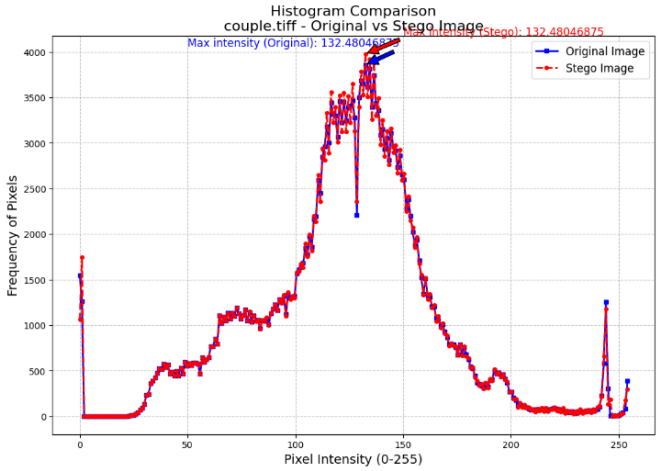

Figure 27. Pixel intensity histogram TIFF on plaintext 1

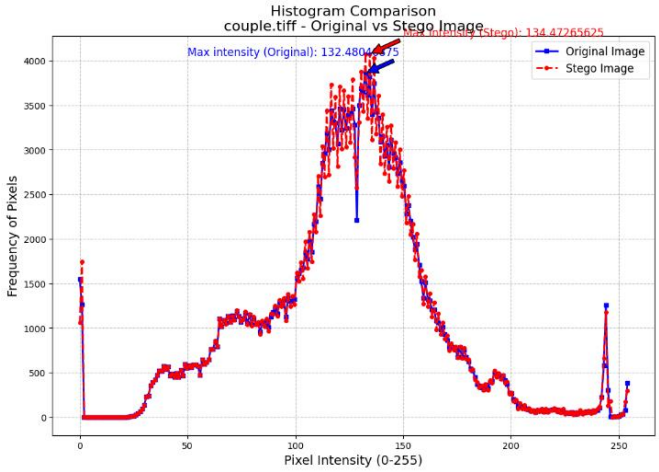

Figure 28. Pixel intensity histogram TIFF on plaintext 2

When the embedded data size reaches 40 KB, as shown in Fig. 30, a more noticeable variation in pixel intensity distribution begins to emerge. Even so, the overall structure of the histogram remains largely undisturbed. As the data volume increases further to 50, 60, 70, and 80 KB, illustrated in Figures 31 to 34, the histograms reveal signs of shifting and spreading intensity values. For instance, Figure 31 shows a shift and broadening of the distribution, while Figure 32 presents a decrease in dominance at specific intensity levels, suggesting an adaptation to the larger data load.

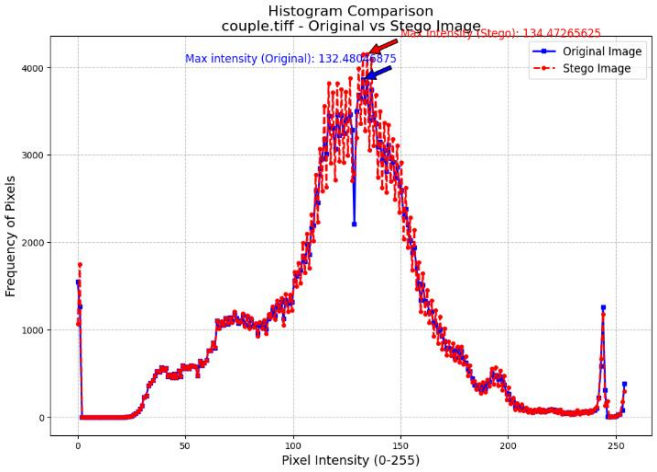

Figure 29. Pixel intensity histogram TIFF on plaintext 3

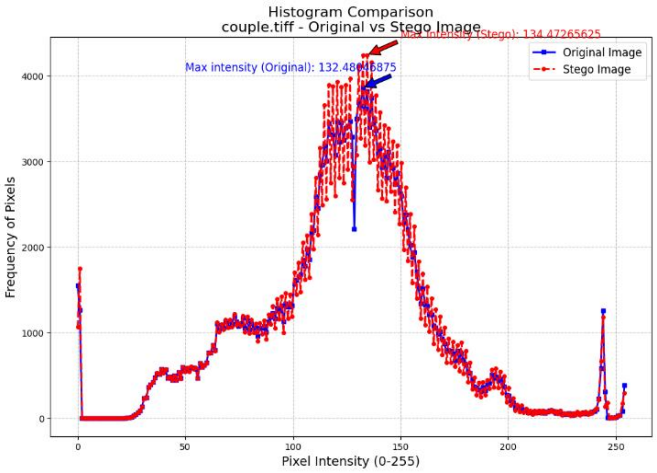

Figure 30. Pixel intensity histogram TIFF on plaintext 4

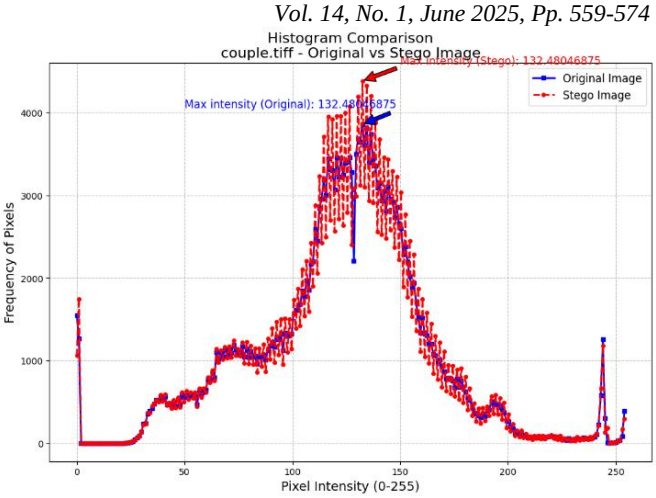

Figure 31. Pixel intensity histogram TIFF on plaintext 5

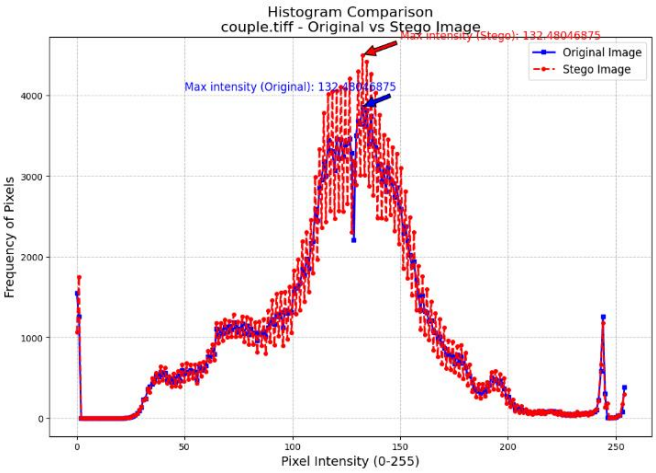

Figure 32. Pixel intensity histogram TIFF on plaintext 6

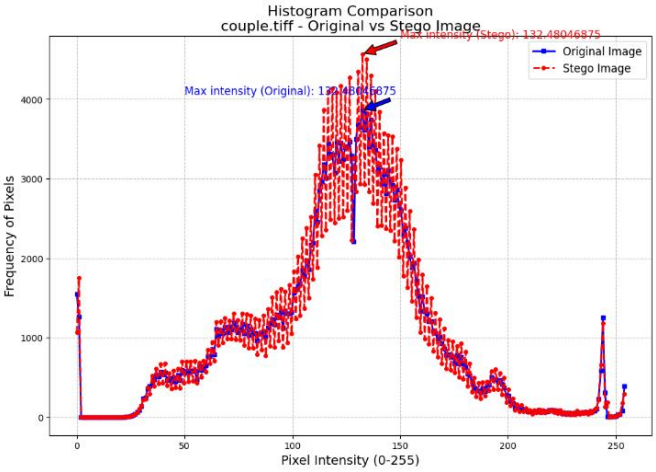

Figure 33. Pixel intensity histogram TIFF on plaintext 7

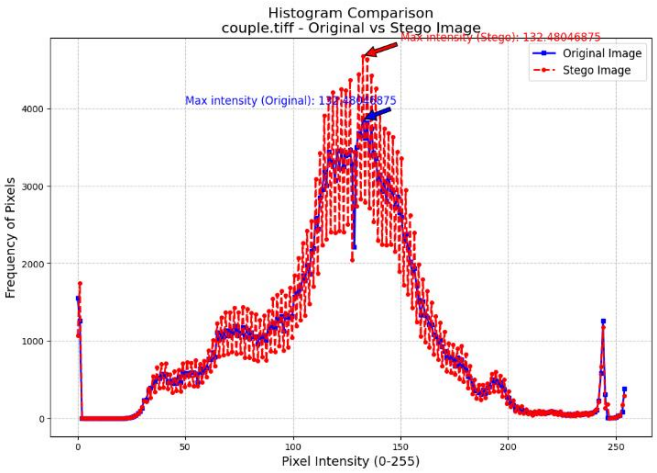

Figure 34. Pixel intensity histogram TIFF on plaintext 8

Despite the increase in embedded data size, the histograms in Figures 33 and 34 still maintain an overall resemblance to the histograms of the original images. These results demonstrate that the PVD method is capable of effectively embedding large volumes of data into TIFF images while preserving visual quality. This is evidenced by the consistent similarity in histogram patterns before and after the data embedding process.

3.11 Image Extraction Evaluation Analysis

The data extraction evaluation analysis was carried out to find out whether the encrypted text data inserted into the image could be extracted again and decrypted again. The analysis using pixel quality metrics revealed the effectiveness of text extraction from images, with results indicating which images successfully extracted text data and which did not, as summarized in Table 9.

The results presented in Table 9 show that images in JPG format cannot extract the data that has been declared in the data, and images in BMP, PNG, and TIFF formats can extract text data well that has been inserted into images. Images with the JPG format cannot extract encrypted data because the nature of images with the JPG format has lossy compression, so they cannot withstand compression during the process of inserting encrypted data with the PVD method [26].

Table 9. Successful extraction

Plain-text	Size	BMP	JPG	PNG	TIFF
1	10 KB	Successful	Unsuccessful	Successful	Successful
2	20 KB	Successful	Unsuccessful	Successful	Successful
3	30 KB	Successful	Unsuccessful	Successful	Successful
4	40 KB	Successful	Unsuccessful	Successful	Successful
5	50 KB	Successful	Unsuccessful	Successful	Successful
6	60 KB	Successful	Unsuccessful	Successful	Successful
7	70 KB	Successful	Unsuccessful	Successful	Successful
8	80 KB	Successful	Unsuccessful	Successful	Successful

4 CONCLUSION

This study successfully implements the XOR-VLSB encryption and decryption algorithm in the process of encoding and decrypting text data before it is inserted into steganography images. This study employs Pixel Value Differencing (PVD) as the steganography technique, which enables flexible analysis of text data by leveraging the differences in pixel values between image blocks. With this approach, the insertion power can be increased without significantly degrading the visual quality of the image.

The results showed that the quality of steganography images was well preserved after the research process using the PVD method. Evaluations were conducted on various image formats, such as BMP, PNG, and TIFF, which showed that the optimal image quality. The mean squared error (MSE) is high, while the peak signal-to-noise ratio (PSNR) is at 40 dB, and the structural similarity index (SSIM) is at 1. These values indicate that the steganography image has a very similar quality to the original image. In addition, steganography images in BMP, PNG, and TIFF formats can be used to extract encrypted text data successfully. However, the extraction process could not be performed successfully in the JPG format, suggesting that this format is not ideal for PVD-based steganography.

The results demonstrate that the PVD steganography scheme combined with the XOR-VLSB cryptographic algorithm effectively conceals text data within images while enhancing data security through encryption. This success confirms the potential of both methods used in the data security process.

As a suggestion for further development, the integration of the PVD scheme with the XOR-VLSB algorithm can be enhanced by replacing the XOR-VLSB cryptographic algorithm with more advanced algorithms, such as AES (Advanced Encryption Standard). The application of the AES algorithm, which has a higher security standard, is expected to provide stronger protection against hidden text data, thereby improving the overall security of the system. This integration will enhance the joint method's resilience against a broader range of complex security threats in the future.

AUTHOR'S CONTRIBUTION

In the study titled "Implementation and Performance Analysis of PVD Method in Concealing Encrypted Data on Images," each team member played a complementary role to ensure the success of this research.

Ardhan Hanif held primary responsibility for data collection and analysis, as well as for ensuring that the methodology applied is under the established research design. He performed in-depth technical and analytical measures to obtain valid and accountable results. In addition, Ardhan was also active in evaluating every stage of method implementation, including data testing and validation.

Nur Rochmah Dyah Puji Astuti played an important role in ensuring that the entire research writing process was carried out systematically, consistently, and aligns with the methodology that had been designed from the beginning. He

ensured that every part of the research, from the formulation of the problem to the conclusion, was structured and logical, thus providing a clear flow and supporting the integrity of the research. Its role also included a final review of the manuscript to verify the suitability of the research content with applicable academic standards, including grammar, writing format, and completeness of references.

As the person in charge of the final preparation process, Nur Rochmah Dyah Puji Astuti ensured that the research results were presented with a high level of clarity and accuracy, so that they were easy to understand by readers and relevant to the research objectives. A detailed review was carried out on each part of the manuscript, starting from an introduction that provides a scientific background, a comprehensive literature review, a transparent methodology, an in-depth analysis, to an accurate conclusion. The attention paid to these details not only ensured cohesion in presentation but also supported the scientific integrity of the research.

Eko Aribowo played an important role in providing valuable input that greatly contributed to the success of the data collection in this study. The input provided was not only limited to technical aspects, but also included a range of strategic considerations, ensuring the data collected was relevant and supported the main objectives of the research. In the process, Eko Aribowo provided guidance related to the most effective and efficient method, helping the research team to choose an approach that suited the needs of the study.

In addition, his contribution to analyzing the proposed method, his role as the person in charge were crucial in ensuring the research remained focused on methods that significantly impacted the expected outcome. His advice and input helped in identifying the right data sources, determining the most suitable method for data collection, and ensuring that the process was carried out in a systematic and structured manner. This not only improved time and resource efficiency but also minimized the risk of collecting data that was less relevant or inconsistent with the research objectives.

Through close collaboration and integrated direction from all team members, this research could be completed. Each member makes a significant contribution under their respective expertise, to produce research that is expected to be able to make a meaningful contribution to the development of science, especially in the field of steganography. The results of this research are not only useful for enriching scientific literature but also have the potential to be applied to various practical needs in the real world.

COMPETING INTERESTS

By the ethics of the publication of this journal, Ardhan Hanif, Nur Rochmah Dyah Puji Astuti and Eko Aribowo as the authors of this journal article, stated that this journal article does not have a conflict of interest (COI) or competing interest (CI).

ACKNOWLEDGMENT

This study was supported by the Directorate of Research, Technology, and Community Service Ministry of Education, Culture, Research and Technology, Indonesia under the Grant No.0609.12/LL5-INT/Al.04/2024 and 044/PFR/LPPM-UAD/VI/2024.

REFERENCES

[1] A. Nikiforova, “Data Security as a Top Priority in the Digital World: Preserve Data Value by Being Proactive and Thinking Security First,” *Springer Proceedings in Complexity*, pp. 3–15, 2023, doi: 10.1007/978-3-031-19560-0_1.

[2] N. Pamungkas, B. V. Indriyono, and I. Setiarso, “Concept of Data Security in Digital Image Media Using Spread Spectrum Steganography and Playfair Cipher Cryptography,” *Explore: Jurnal Sistem Informasi dan Telematika*, vol. 15, no. 1, p. 79, 2024, doi: 10.36448/jsit.v15i1.3517.

[3] V. Himthani, V. S. Dhaka, M. Kaur, G. Rani, M. Oza, and H. N. Lee, “Comparative performance assessment of deep learning based image steganography techniques,” *Sci Rep*, vol. 12, no. 1, pp. 1–16, 2022, doi: 10.1038/s41598-022-17362-1.

[4] C. A. Buckner *et al.*, “We are IntechOpen , the world ’ s leading publisher of Open Access books Built by scientists , for scientists TOP 1 %,” *Intech*, vol. 11, no. tourism, p. 13, 2016.

[5] S. Ghoul, R. Sulaiman, and Z. Shukur, “A Review on Security Techniques in Image Steganography,” *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, pp. 361–385, 2023, doi: 10.14569/IJACSA.2023.0140640.

[6] A. Gustiawan, J. Wahyudi, and E. Suryana, “Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode Pixel Value Differencing,” *JUKI: Jurnal Komputer dan Infromatika*, vol. 5, pp. 151–163, 2023.

[7] D. C. Wu, Z. N. Shih, and J. H. Wu, “Modified Multiway Pixel-Value Differencing Methods Based on General Quantization Ranges for Image Steganography,” *IEEE Access*, vol. 10, pp. 8824–8839, 2022, doi: 10.1109/ACCESS.2021.3138895.

[8] T. Cevik, N. Cevik, J. Rasheed, T. Asuroglu, S. Alsubai, and M. Turan, “Reversible Logic-Based Hexel Value Differencing - A Spatial Domain Steganography Method for Hexagonal Image Processing,” *IEEE Access*, vol. 11, no. October, pp. 118186–118203, 2023, doi: 10.1109/ACCESS.2023.3326857.

[9] C. T. Huang, N. S. Shongwe, and C. Y. Weng, “Enhanced Embedding Capacity for Data Hiding Approach Based on Pixel Value Differencing and Pixel Shifting Technology,” *Electronics (Switzerland)*, vol. 12, no. 5, 2023, doi: 10.3390/electronics12051200.

[10] M. Sahu, N. Padhy, and S. S. Gantayat, “Multi-directional PVD steganography avoiding PDH and boundary issue,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8838–8851, 2022, doi: 10.1016/j.jksuci.2021.10.007.

[11] R. Yadav, "Analysis of Cryptography in Information Technology," *Interantional Journal of Scientific Research in Engineering and Management*, vol. 07, no. 03, pp. 1–6, 2023, doi: 10.55041/ijsrem18379.

[12] A. Ihsan and N. Doğan, "Improved affine encryption algorithm for color images using LFSR and XOR encryption," *Multimed Tools Appl*, vol. 82, no. 5, pp. 7621–7637, 2023, doi: 10.1007/s11042-022-13727-w.

[13] L. Ludyawati, M. Khudzaifah, and E. Herawati, "Penggabungan Metode Vigènere Cipher dan ElGamal Pada Pengamanan Pesan Rahasia," *Jurnal Riset Mahasiswa Matematika*, vol. 2, no. 6, pp. 247–256, 2023, doi: 10.18860/jrmm.v2i6.22041.

[14] Purwanti, S. D. Nurcahya, and D. Nazelliana, "Message Security in Classical Cryptography Using the Vigenere Cipher Method," *International Journal Software Engineering and Computer Science (IJSECS)*, vol. 4, no. 1, pp. 350–357, 2024, doi: 10.35870/ijsecs.v4i1.2263.

[15] I. Riadi, A. Fadlil, and F. A. Tsani, "Vigenère Cipher Algorithm Optimization for Digital Image Security using SHA512," *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, vol. 13, no. 2, p. 84, 2022, doi: 10.24843/lkjiti.2022.v13.i02.p02.

[16] K. Khairani and M. Z. Siambaton, "Pengamanan Data Teks Menggunakan Algoritma Kriptografi Elgamal dan XOR dari Serangan Hacker," *sudo Jurnal Teknik Informatika*, vol. 2, no. 4, pp. 176–187, 2023, doi: 10.56211/sudo.v2i4.401.

[17] S. Alam, N. Shukla, K. Asifuzzaman, and A. Aziz, "CMOS-based Single-Cycle In-Memory XOR / XNOR," pp. 1–12.

[18] M. I. Harahap, S. Suherman, and R. W. Sembiring, "Three Pass Protocol for Key Security Using Affine Cipher Algortima and Exclusive-or (Xor) Combination," *Sinkron*, vol. 8, no. 4, pp. 2602–2614, 2023, doi: 10.33395/sinkron.v8i4.13051.

[19] S. Camtepe *et al.*, "ANS-based compression and encryption with 128-bit security," *Int J Inf Secur*, vol. 21, no. 5, pp. 1051–1067, 2022, doi: 10.1007/s10207-022-00597-4.

[20] D. P. Sabaya, A. A. Semlambo, and J. K. Simon, "Data Security Through Crypto-Stegano Systems," *International Journal of Computational Science, Information Technology and Control Engineering*, vol. 10, no. 1/2/3, pp. 1–23, 2023, doi: 10.5121/ijcsitce.2023.10301.

[21] S. E. Naffouti, A. Kricha, and A. Sakly, "A sophisticated and provably grayscale image watermarking system using DWT-SVD domain," *Visual Computer*, vol. 39, no. 9, pp. 4227–4247, 2023, doi: 10.1007/s00371-022-02587-y.

[22] E. Fragoso-Navarro, F. Garcia-Ugalde, and M. Cedillo-Hernandez, "Protecting the Distribution of Color Images via Inverse Colorization, Visible-Imperceptible Watermarking and Reversible Data Hiding," *IEEE Access*, vol. 11, pp. 61025–61048, 2023, doi: 10.1109/ACCESS.2023.3286865.

[23] G. Miftakhul Fahmi, K. N. Isnaini, and D. Suhartono, "Implementation of Steganography on Digital Image With Modified Vigenere Cipher Algorithm and Least Significant Bit (Lsb) Method," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 2, pp. 333–344, 2023, doi: 10.52436/1.jutif.2023.4.2.340.

[24] R. I. Adam, M. Garno, and M. Roba'i, "Interpolasi Dalam Proses Penyisipan Pesan Dengan Metode Pixel Value Differencing (Pvd)," *JIKO (Jurnal Informatika dan Komputer)*, vol. 6, no. 2, p. 148, 2022, doi: 10.26798/jiko.v6i2.275.

[25] Patrisius Batarius, Alfry Aristo Sinlae, and Elisabeth F. Fahik, "Analysis of the Quality of Natural Dyes in Weaving Exposed to Sunlight Using MSE and PSNR Parameters," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 5, pp. 797–802, 2022, doi: 10.29207/resti.v6i5.4339.

[26] I. M. A., M. M. B., A. A. E., and S. B. O, "An Extensive Survey of Digital Image Steganography: State of the Art," *Journal of Science Technology and Education*, vol. 8, no. 2, pp. 40–54, 2024.

[27] H. Caballero, V. Muñoz, and M. A. Ramos-Corchado, "A comparative study of steganography using watermarking and modifications pixels versus least significant bit," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 6, pp. 6335–6350, 2023, doi: 10.11591/ijece.v13i6.pp6335-6350.

[28] R. F. Faizal, "Steganografi Pengukuran Akurasi Dan Kualitas File Multimedia Menggunakan Algoritma Low Bit Coding," *Technologia : Jurnal Ilmiah*, vol. 15, no. 3, p. 361, 2024, doi: 10.31602/tji.v15i3.14844.

[29] A. P. Purnacandra and S. Subektiningsih, "Anti-Forensics with Steganographic File Embedding in Digital Image Using Genetic Algorithm," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, vol. 8, no. 2, p. 326, 2022, doi: 10.26555/jiteki.v8i2.24208.

[30] M. S. Abuali, C. B. M. Rashidi, R. A. A. Raof, K. N. F. K. Azir, S. S. Hussein, and A. Q. Abd-Alhasan, "Enhancing Security with Multi-level Steganography: A Dynamic Least Significant Bit and Wavelet-Based Approach," *Mathematical Modelling of Engineering Problems*, vol. 11, no. 6, pp. 1403–1416, 2024, doi: 10.18280/mmep.110602.

[31] S. Rahman *et al.*, "Multi Perspectives Steganography Algorithm for Color Images on Multiple-Formats," *Sustainability (Switzerland)*, vol. 15, no. 5, 2023, doi: 10.3390/su15054252.

[32] X. Xue *et al.*, "Modelling and Analysis of Hybrid Transformation for Lossless Big Medical Image Compression," *Bioengineering*, vol. 10, no. 3, 2023, doi: 10.3390/bioengineering10030333.