KOMPUTASI: JURNAL ILMIAH ILMU KOMPUTER DAN MATEMATIKA
VOL. 21 (1) (2024), 21-30 p-ISSN: 693-7554, e-ISSN:2654-3990

Message Encryption in Digital Images using the Zhang LSB Imange Method

Asep Saepulrohman[1], **Agus Ismangi**[2], **Leny Heliawati**[3]

[1,2]Computer Science Study Program, Faculty of Mathematics and Natural Science, Universitas Pakuan, West Java, 16143, Indonesia
[3]Masters in Science Education Study Program, Postgraduate School, Universitas Pakuan, West Java, 16143, Indonesia

Abstract

Message encryption in digital images using the Zhang LSB Image method is a steganography technique that utilizes the Least Significant Bit (LSB) method to hide secret messages in the last bit of the image pixel. This method allows the use of images as a medium to convey hidden messages. The encryption process involves two main stages, namely message encryption and message hiding in an image. Message encryption is carried out using strong cryptographic algorithms to secure the authenticity and confidentiality of messages. Then, the encrypted message is inserted into the last bit of the image pixel using the LSB method. This is done by modifying the last bit value of the pixel so that the change is not visually visible to the human eye. To recover the original message, the message recovery process involves extracting the last bit of the modified image pixel and decrypting the message using the appropriate key. The Zhang LSB Image method is a steganography technique that is relatively simple but effective in hiding messages in digital images.

Keywords: *Zhang; LSB; encryption; Cryptography; steganography*

1. Introduction

Steganography has become an attractive alternative for transmitting secret or sensitive information, especially in the context of restrictions on the strength of cryptographic systems by some governments. In some countries, there are regulations governing the use and distribution of strong cryptographic algorithms, which may limit secure communications capabilities [1]-[4]. Steganography offers a way to hide secret messages in seemingly ordinary media, such as images, audio, or video. By using techniques such as the LSB method on images, messages can be hidden hidden in the bits that represent the pixels of the image. Therefore, even if the message is discovered, it is difficult for unauthorized parties to be aware of the message's existence or understand its contents [5]-[7].

Additionally, businesses are also increasingly realizing the potential of steganography in keeping their trade information or new products confidential. By using steganography, important information can be stored in images or other media, and communication can be carried out through unsuspecting channels, reducing the risk of the information being leaked to unauthorized parties.

*Corresponding author: ***E-mail adress:*** *asepspl@unpak.ac.id*
Received: 04 Dec 2023, Accepted: Accepted: 19 Jan 2024 and available online 30 Jan 2024
DOI: https://doi.org/10.33751/komputasi.v21i1.9314

However, it is important to remember that the use of steganography can also pose risks if used in an unethical or illegal manner. As with any technology, the use of steganography must take security, privacy and legal compliance into account [8].

In this research, we discuss the development of a combined system between cryptography and steganography using the Zhang and MARS methods with uncompressed bitmap image media. The goal is to create an application that can provide higher communication security by combining both techniques. The use of cryptography in communication can raise suspicions that the message sent is a secret message, because the use of encryption methods can be seen by unauthorized parties. Therefore, hiding information in the media such as company picnic photos, which are less suspicious, may be a better alternative. The steganography method used in this research is the Zhang method, which utilizes the last bit of an image pixel to hide the message. However, modifications were also made to Zhang's algorithm to address situations where the leading bit is involved in its internal operations [9]-[10].

Digital images are represented in the form of a 2-dimensional matrix, where each matrix element represents a pixel in the image. In this context, the image used is an uncompressed bitmap image. By combining cryptography and steganography techniques, it is hoped that it can increase the trust of governments, businesses or other parties who want to send secret messages securely. In practice, the application developed can be used to hide messages in digital images using the Zhang method and applying encryption using the MARS algorithm to maintain message confidentiality. This research contributes to the development of a communications security system that combines cryptography and steganography, as well as providing an understanding of digital image representation in the form of a pixel matrix [5]-[6] [11].

In previous research entitled "Invertible secret image sharing with steganography and authentication for AMBTC compressed images" by WuX, et al. in 2019, a secret image sharing (SIS) scheme was developed that combines steganography and authentication. However, the scheme cannot handle compressed images using the Absolute Moment Block Truncation Coding (AMBTC) method. Additionally, if the cover image is of significant size, the resulting stego image may be distorted and it is difficult to restore it to its original form [5]-[7].

In this research, a reversible SIS scheme using steganography and authentication for AMBTC compressed images is proposed. The secret image that has been compressed using the AMBTC method is divided and embedded into the cover image to produce a number of AMBTC compressed stego images. To ensure the integrity of the stego image, parity bits are built and hidden in the stego image. During the secret image disclosure process, the stego image is verified using the parity bits that have been hidden. By using a successfully verified stego image, the secret image can be recovered without distortion, and the original cover image can also be reconstructed [12]-[16].

The results of the experiments conducted in this study are shown to demonstrate the effectiveness and advantages of the proposed scheme. This scheme overcomes the constraints of previous schemes with the ability to resolve AMBTC compressed images and maintain integrity and avoid significant distortion in stego images.

2. Methods

The following is a research method that can be used to analyze message encryption using the MARS method on images using the Zhang LSB image method:

a. Data Preparation:

1. Collect images that will be used as steganography media. Make sure the image is in an uncompressed format, such as a bitmap image.

2. Prepare the message to be encrypted and inserted into the image. The message must be converted into a format suitable for encrypting with the MARS method.

b. Implementation of Zhang LSB Image Method:

1. Apply Zhang's LSB Image method to hide the message in the image. This method involves changing the last bit of an image pixel to store message bits.
2. Carry out the message insertion process sequentially on each image pixel, replacing the last bit with the message bit to be inserted.

c. Message Encryption with MARS Method:

1. Use the MARS encryption algorithm to encrypt messages that have been embedded in the image. MARS is a strong encryption algorithm and can be used to protect the confidentiality of messages.
2. Apply the appropriate encryption key to the messages to be encrypted with MARS. Make sure the encryption key is secure and known only to the intended recipient.

d. Security Analysis:

1. Evaluate the security of the encryption method used. This analysis may involve testing the strength of MARS encryption, such as key strength, resistance to attack, and statistical testing of encrypted messages.
2. Also evaluate the security of the Zhang LSB Image steganography method, including resistance to detection and message hiding power.

e. Trial and Evaluation:

1. Conduct trials on systems that have been implemented using various images and different messages.
2. Evaluate the quality of the resulting stego image, including visual distortions that may occur due to message insertion.
3. Evaluate the success of message decryption and the authenticity of the decrypted message using the MARS method.

f. Conclusion:

1. Make conclusions based on the results of the analysis and evaluation that have been carried out.
2. Discuss the advantages, disadvantages, and potential for further development of the encryption and steganography methods used

The word stegonagraphy comes from the Greek words stegos and graphia, which means stegos is closed and graphia is writing. So steganography is the science and art of hiding the existence of data communications (covered writing). With steganography, secret messages can be inserted into other media which can be images, sound, video, or other forms so that they are not suspicious when sent and without anyone knowing the existence of the message. Stegonography requires two main properties to hide messages, namely the cover media and the secret message. The container media can be images, sound, video, or text, while the hidden message can be anything, be it writing, images, code, programs, sound, video, or other messages. The advantage of stegonography compared to cryptography is that the message sent does not attract attention so it does not leave suspicion for other parties. There are several steganography terms that need to be understood, namely:

a. Message to be hidden (embedded message)

b. Media to hide the message (cover-object), if the cover is an image then it is called cover-image and if it is audio it is called cover-audio, and so on.

c. Message carrier media that already contains a hidden message (stego-object), if it is in the form of an image it is called stego-image and if it is audio it is called stego-audio, and so on

d. The secret key used to insert messages into the cover (stego-key).

Inserting a message into the cover is called embedding and extracting the message from the stego-object is called extraction or extracting where this process requires a secret key (stego-key) so that the authorities can carry out message insertion and message extraction. The observer or enemy (adversary) does not know that there is a message hidden in the stego-object as in Figure 1.

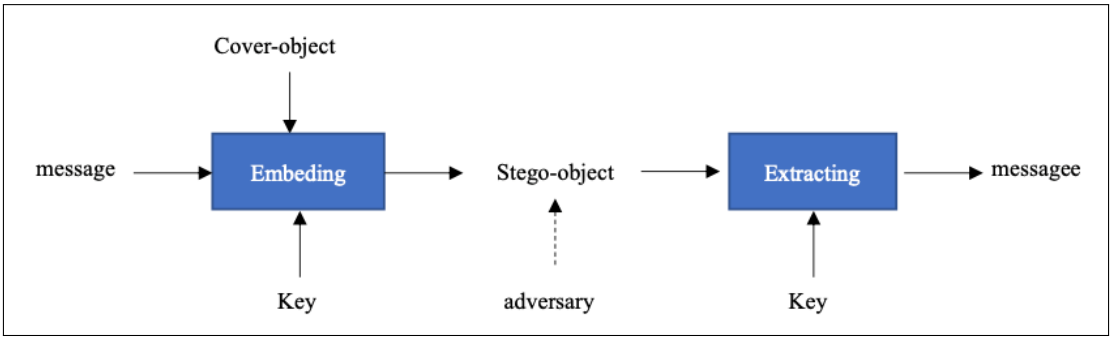


Figure 1. Original image without any digital image alteration

3. Result and Discussion

The results of the Zhang LSB Image steganography method are one of the methods used to hide secret messages in digital images. This method focuses on modifying the last bit of the image pixel to store the message bit. By exploiting human resistance to small changes in image pixels, messages can be inserted invisible to the human eye as follows:

a. Least Significant Bit (LSB)

The LSB (Least Significant Bit) method is one of the simplest and most commonly used steganography methods. This method exploits the inability of the human eye to distinguish small changes in the last bit (LSB) of each image pixel. In the context of digital images, images consist of a collection of pixels that form a grid. Each pixel is represented in the form of an M × N matrix, where M is the number of rows and N is the number of columns. Each pixel in the image has a value that represents color or brightness level, depending on the type of image used.

Binary images (black and white) have 1 bit per pixel, where the value 0 represents black and the value 1 represents white. Grayscale images have 8 bits per pixel, which provides a degree of gray between black and white. Meanwhile, true color images use 24 bits per pixel, which consists of three main color components (RGB), namely red, green and blue. In the LSB method, messages or secret information are inserted by replacing the last bit of the image pixel with the message bits to be inserted. In true color images, for example, the LSB of the RGB component can be used to store messages. Because changes to the last bit are usually invisible to the human eye, messages can be effectively hidden in the image without significantly compromising visual quality.

However, it should be remembered that the LSB method is vulnerable to steganalysis techniques which can detect changes in the LSB bits. Therefore, if security is an important factor, more complex and powerful steganography methods may need to be considered. For example, see the process in Figure 2.

Figure 2. Original image without any digital image alteration

Data image modification:

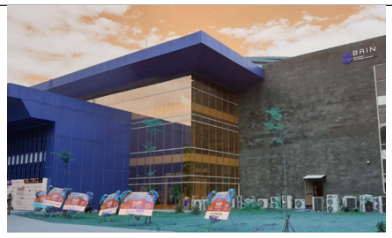
1. brin_abu = cv2.cvtColor(brin,cv2.COLOR_BGR2GRAY)
2. brin_rgb = cv2.cvtColor(brin,cv2.COLOR_BGR2RGB)
3. brin_hsv = cv2.cvtColor(brin,cv2.COLOR_BGR2HSV)

   print(brin_abu.shape)

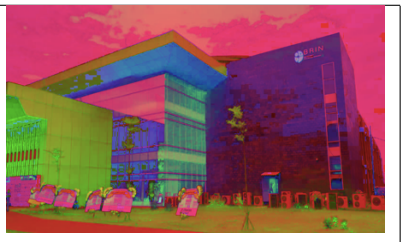
   print("BRIN berwarna abu")

   cv2_imshow(brin_abu)

Grayscale image (8 bit)



True color image (24 bit)



Binary image (1 bit)

Figure 3. Gray, RGB, and HSV digital image conversion

b. Data Insertion with LSB

Byte representation, the bits are arranged from left to right starting from the most significant bit (MSB) to the least significant bit (Least Significant Bit/LSB). In a byte, the bit arrangement is:

$$b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0$$

b_0 is the LSB bit, while b_7 is the MSB bit. For example, in byte 10011010, the first bit 1 is the MSB bit and the last bit 0 is the LSB bit. If you change the LSB bit (from 1 to 0 or vice versa), then the modification only changes the byte one higher or one lower than the previous value and this results in the gray value of each pixel perceiving a certain color in other words small changes that do not change color significantly meaning that the human eye is less sensitive to very small changes in color degradation. This is the basic concept of the LSB modification method by replacing the LSB bits for each pixel with message bits because these changes cannot be distinguished visually.

Calculating the message embedding capacity (in bytes) hidden in the image depends on the size of the cover image. In an 8-bit image measuring 256 x 256 pixels where each pixel is 1 byte so that the message that can be hidden is 65536 bits or 8192 bytes (8 KB). Another example is a 24-bit image measuring 256x256 pixels, one pixel is 3 bytes (1 byte for each R,G,B component) so we can insert a message of 65536 x 3 bits (196,608 bits) or 24,576 bytes (24KB). Calculating image quality after message insertion is by using a metric called PSNR (Peak-signal-tonoise-ratio) which is commonly used to measure image quality in 1.

$$PNSR = 20log_{10}\left(\frac{255}{RMS}\right) \tag{1}$$

The PNSR unit is decibe (dB) which expresses the visibility of noise in the image and the value 255 is the largest signal in the image with 256 degrees of gray and RMS (Root Mean Square) is the standard deviation of two I (image-cover) and (I) (stego-image) which has dimensions M $\times$ N with Equation 2 stating the standard deviation of two images.

$$RMS = \sqrt{\frac{1}{MN}\sum_{i}^{n} i = 1 \sum_{j}^{m}(I_{ij} - \hat{I}_{ij})} \tag{2}$$

From empirical experience, an image is considered to be of good quality if PSNR $\geq$ 30 and if PNSR $<$30 it is said that the image quality has been significantly degraded.

c. The MARS algorithm

The MARS algorithm that you mention in your context actually refers to two different concepts, namely the MARS cryptographic algorithm (MARS cipher) and the MARS nonparametric regression method (MARS nonparametric regression). I will give a brief explanation of both.

1. MARS Cryptographic Algorithm (MARS Cipher): The MARS cryptographic algorithm is a block cipher developed by Burwick et al. in 1998. A block cipher is a cryptographic algorithm that encrypts and decrypts data in blocks of a fixed size, in the case of MARS it is 128 bits. This cipher supports key sizes that vary between 128 bits and 400 bits. The MARS algorithm is categorized as a symmetric cryptographic algorithm, which means the keys used for encryption and decryption are the same. However, it is important to note that the MARS algorithm is not directly related to steganography or LSB conversion which we discussed earlier.

2. MARS Nonparametric Regression Method (MARS Nonparametric Regression): The MARS nonparametric regression method is a regression approach that was first introduced by Friedman in 1991. This method is used to model the relationship between predictor variables and response variables in a regression context. MARS allows flexible regression models without certain assumptions about the form of relationships between variables. This method is suitable for dealing with problems with high-dimensional data, where the number of predictor variables is large and the sample size is large. MARS builds a regression model based on knots and uses the Generalized Cross Validation (GCV) method to select optimal knots. However, it should be noted that the MARS nonparametric regression method is also not directly related to cryptography or LSB alteration.

The following is an example of implementing the MARS cryptographic algorithm using the Python programming language. However, keep in mind that secure and reliable implementation of cryptography requires deep expertise in the field, and using an implementation that has been tested and verified is preferable to relying on your own implementation. The following is the MARS program using Python in Figure 4.

In the example above, we use the mars module which implements the MARS algorithm. This module can contain functions to generate random keys, random plaintext, as well as functions to perform encryption and decryption using the MARS algorithm.

```
import mars

# Generate a random 128-bit key
key = mars.generate_key(128)

# Generate a random 128-bit plaintext
plaintext = mars.generate_plaintext(128)

# Encrypt the plaintext using MARS
ciphertext = mars.encrypt(key, plaintext)

# Decrypt the ciphertext using MARS
decrypted_plaintext = mars.decrypt(key, ciphertext)

# Print the results
print("Key:", key)
print("Plaintext:", plaintext)
print("Ciphertext:", ciphertext)
print("Decrypted Plaintext:", decrypted_plaintext)
```

Figure 4. Original image without any digital image alteration

d. Use Case Realization Analysis Stage

This section contains use case scenarios for software for embedding messages, extracting messages, encrypting messages, decrypting messages, selecting the pixels used as shown in Table 1 in the global analysis class complete with sterotypes for each class.

Table 1. Complete Global Analysis with Sterotype

No	Class name	Stereotype
1	Interface	controller
2	ZHANG	controller
3	MARS	controller
4	LCD	controller
5	LSB Image	Entity
6	Message	Entity

Each class has its own responsibilities and the responsibilities and attributes possessed by each class can be seen in Table 2.

e. Enter Data

One of the techniques used in steganography cryptography is hiding secret messages in images. In this context, secret messages are usually encrypted using cryptographic algorithms such as the MARS cipher before being inserted into the image using steganography techniques. Following are the general steps involved in message encryption and embedding into an image using steganography:

1. Message Encryption: The secret message you want to send must be encrypted using a cryptographic algorithm such as the MARS cipher. In this case, you can use the MARS cipher implementation in Python as explained previously.
2. Select Hiding Image: Select the image that will be used as hiding media. This image must have sufficient capacity to store secret messages without significantly disrupting the visual quality of the image.
3. Message to Bitstream Conversion: Converts an encrypted secret message into a bitstream. Each bit in the message will be inserted into an image pixel.

Table 2. Complete Global Analysis with Sterotype

No	Class Name	Responsibility	Attribute
1	Interface		
		1. Interact with user	
		2. Receive input data to be processed by other classes	
		3. Provide information to users in the form of notifications	
2	ZHANG		
		1. Interact encrypted	
		2. Extract the encrypted message	
3	MARS		
		1. Encrypt the message	
		2. Decrypt the message	
4	LCD		
		1. Encrypt the message	
		2. Decrypt the message	
5	LCD		Pixel LSB: array of m bit
		1. Encrypt the message	
		2. Decrypt the message	
6	Message		Raw message: array of byte Word message: array of word
		1. Convert the message into an array of words	
		2. Converts the message to an array of m bits, a number m based on user input	

4. Insert Message into Image: Insert secret message bits into image pixels. There are several embedding methods that can be used, such as Least Significant Bit (LSB) or other transformation methods. The LSB method is a commonly used method, where the message bits are replaced with the last bit (LSB) of the pixel value in the image.
5. Save Inserted Image: Save the image that has a secret message inserted as a new image. This image will function as a medium for sending secret messages.

f. Output Data

When you insert a message into an image using steganography techniques, the output data involved includes an image that has been modified to store the secret message. The process of inserting a message can produce a new image that is different from the original image. The output

data involved in encrypting a message into an image is usually an image that has a secret message inserted. This image will contain message information hidden in the pixels. The steganography method used will influence how the message is inserted and how the image is modified. If you use the Least Significant Bit (LSB) method to insert a message, the output data will be an image that has changes in the last bit (LSB) of each pixel used to store message bits. In this case, the modified image will appear similar to the original image, but there will be very small changes in the pixels involved in embedding the message.

However, it is important to remember that the output data in the form of modified images does not directly contain hidden secret messages. To read back the secret message from a modified image, you need to perform a steganographic extraction process which involves reprocessing the image and extracting hidden message bits using appropriate algorithms.

4. Conclusion

Analysis of message encryption using the MARS method on images using the Zhang LSB Image method is as follows: MARS Method: MARS is a strong and secure encryption algorithm. In this analysis, the MARS method is used to encrypt messages in images. Zhang LSB Image Method: The Zhang LSB Image method is a steganography technique that uses the Least Significant Bit (LSB) method to insert a message in the image. In this analysis, this method is used to insert encrypted messages using the MARS algorithm. Security: The combination of the MARS method and the Zhang LSB Image method can provide a higher level of security in securing messages hidden in images. The MARS method provides strong encryption security, while the Zhang LSB Image method hides messages invisibly in the image. Encryption strength: The use of MARS method in message encryption provides high encryption strength. MARS has been proven to be secure and resistant to certain cryptanalysis attacks. Thus, messages encrypted using the MARS method will be difficult to decrypt without the right key. Weaknesses: Although the MARS method and the Zhang LSB Image method are able to provide a high level of security, no security system is perfect. Possible weaknesses in this method may occur if the encryption or steganography method is poorly designed or if the encryption or steganography key falls into the wrong hands.

References

[1] A. Saepulrohman and P. Negara, "IMPLEMENTASI ALGORITMA TANDA TANGAN DIGITAL BERBASIS KRIPTOGRAFI KURVA ELIPTIK DIFFIE-HELLMAN," vol. 18, no. 1, pp. 22–28, 2021, [Online]. Available: https://asecuritysite.com/encryption/js08.

[2] A. Saepulrohman and U. Pakuan, "Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA) Agus Ismangil," International Journal of Electronics and Communications System, vol. 1, no. 1, pp. 11–15, 2021, [Online]. Available: http://ejournal.radenintan.ac.id/index.php/IJECS/index://creativecommons.org/licenses/by-sa/4.0/

[3] A. Saepulrohman, A. Denih, and A. Talib Bon, "Elliptic Curve Diffie-Hellman Cryptosystem for Public Exchange Process Sukono." [Online]. Available: https://asecuritysite.com/encryption/js08.

[4] A. Saepulrohman and T. P. Negara, "Implementation of Elliptic Curve Diffie-Hellman (ECDH) for Encoding Messeges Becomes a Point on the GF(í µí2‘í µí2‘) 1*," International Journal of Advanced Science and Technology, vol. 29, no. 6, pp. 3264–3273, 2020, [Online]. Available: http://www.asciitable.com.

[5] D. K. Sarmah and A. J. Kulkarni, "Improved Cohort Intelligence—A high capacity, swift and secure approach on JPEG image steganography," Journal of Information Security and Applications, vol. 45, pp. 90–106, Apr. 2019, doi: 10.1016/j.jisa.2019.01.002.J. Chang, Y. Zhou, M. Tahir, U. Qamar, L. Chen, dan Y. Ding, "Prediction of Protein – Protein Interactions by Evidence Combining Methods," Int. J. Mol. Sci., vol. 17, hal. 1946, 2016.

[6] X. Wu and C. N. Yang, "Invertible secret image sharing with steganography and authentication for AMBTC compressed images," Signal Process Image Commun, vol. 78, pp. 437–447, Oct. 2019, doi: 10.1016/j.image.2019.08.007.

[7] D. Adhar, A. Syahputra, R. A. Sugianto, R. Oktari Batubara, A. Sanjaya, and A. Sabir, "Steganografi Pengamanan Data Teks. . . 211 Fakultas Teknik dan Ilmu Komputer 12345 , Fakultas Psikologi 6 Universitas Potensi Utama 124 Universitas Muhammadiyah Sumtera Utara 3 Universitas Nusa Mandiri 5."

[8] "YOLANDA OKTAVIANI (13150076".

[9] B. Tsaban, "Fast generators for the Diffie-Hellman key agreement protocol and malicious standards," Inf Process Lett, vol. 99, no. 4, pp. 145–148, Aug. 2006, doi: 10.1016/j.ipl.2005.11.025.

[10] O. A. Imran, S. F. Yousif, I. S. Hameed, W. N. Al-Din Abed, and A. T. Hammid, "Implementation of El-Gamal algorithm for speech signals encryption and decryption," in Procedia Computer Science, Elsevier B.V., 2020, pp. 1028–1037. doi: 10.1016/j.procs.2020.03.402.

[11] D. Sartika, "PENGEMBANGAN PERANGKAT LUNAK PENYEMBUNYIAN PESAN TERENKRIPSI MENGGUNAKAN ALGORITMA MARS PADA CITRA DIGITAL DENGAN METODE ADAPTIF," vol. 7, no. 1, 2016.

[12] Y. Yanti and A. Saepulrohman, "Segmentation and Positioning of Lecturers in the Department of Computer Science at Pakuan University Based on Student Assessment," Indonesian Journal of Statistics and Its Applications, vol. 5, no. 1, pp. 92–104, Mar. 2021, doi: 10.29244/ijsa.v5i1p92-104.

[13] A. Saepulrohman and U. Pakuan, "Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA) Agus Ismangil," International Journal of Electronics and Communications System, vol. 1, no. 1, pp. 11–15, 2021, [Online]. Available: http://ejournal.radenintan.ac.id/index.php/IJECS/index://creativecommons.org/licenses/by-sa/4.0/

[14] A. Saepulrohman and P. Negara, "IMPLEMENTASI ALGORITMA TANDA TANGAN DIGITAL BERBASIS KRIPTOGRAFI KURVA ELIPTIK DIFFIE-HELLMAN," vol. 18, no. 1, pp. 22–28, 2021, [Online]. Available: https://asecuritysite.com/encryption/js08.

[15] A. Saepulrohman and U. Pakuan, "Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA) Agus Ismangil," International Journal of Electronics and Communications System, vol. 1, no. 1, pp. 11–15, 2021, [Online]. Available: http://ejournal.radenintan.ac.id/index.php/IJECS/index://creativecommons.org/licenses/by-sa/4.0/

[16] B. Widjanarko Otok, "Pendekatan Multivariate Adaptive Regression Spline (MARS) pada Pengelompokkan Zona Musim Suatu Wilayah," 2010.