International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Algorithm for Digital Image Encryption Using Multiple Hill Ciphers, a Unimodular Matrix, and a Logistic Map

Samsul Arifin[1*], Axel Nicholas[2], Suwarno[3], Herolistra Baskoroputro[4], Faisal[5], Abram Setyo Prabowo[6], Muhammad Amien Ibrahim[7], Anita Rahayu[8]

Submitted: 11/02/2023 **Revised:** 13/04/2023 **Accepted:** 06/05/2023

Abstrak: The security of digital images is becoming increasingly important due to the widespread use of image transmission through networks. Therefore, encryption is necessary to protect the confidentiality and integrity of digital images. In this paper, a new digital image encryption algorithm is proposed by combining multiple Hill ciphers, unimodular matrix, and logistic map. The proposed algorithm can improve the security of the image encryption process by introducing multiple encryption layers. The unimodular matrix is used to shuffle the image pixels and the logistic map is used to generate the encryption keys. The performance of the proposed algorithm is evaluated by applying it to various types of digital images. The experimental results show that the proposed algorithm can achieve high-level security. Moreover, the proposed algorithm has a faster encryption time compared to other existing image encryption algorithms. Therefore, it is a promising algorithm for digital image encryption applications that require high security and fast processing time.

Keywords*: image encryption, multiple hill ciphers, unimodular matrix, logistic map*

1. Introduction

Cryptography, a field of study and practice, is concerned with maintaining the confidentiality of messages by transforming the original message into an incomprehensible form for unauthorized individuals. Its primary objective is to secure information transmission through communication channels to prevent any unauthorized party from understanding it. The fundamental principle of cryptography involves the implementation of message security procedures that convert the original message into an unreadable format [1]. One common approach to cryptography is symmetric encryption, which involves the use of a single key to encrypt and decrypt messages. This key must be kept confidential to ensure that encrypted messages cannot be recovered by unauthorized parties [2]. Alternatively, there is an asymmetric encryption technique that employs two keys, namely, the public and private keys. The public key is used for message encryption, while the private key is used for message decryption. This approach is often employed when transmitting data over the internet network [3]. Figure 1, which demonstrates the general concept of symmetric encryption, is presented below.

[1,8]*Statistics Department, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia.*
[2,4,5]*Mathematics Department, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia.*
[6,7]*Computer Science Department, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia.*
[3]*Primary Teacher Education Department, Faculty of Humanities, Bina Nusantara University. Jakarta. Indonesia.*
**Corresponding Author: samsul.arifin@binus.edu*

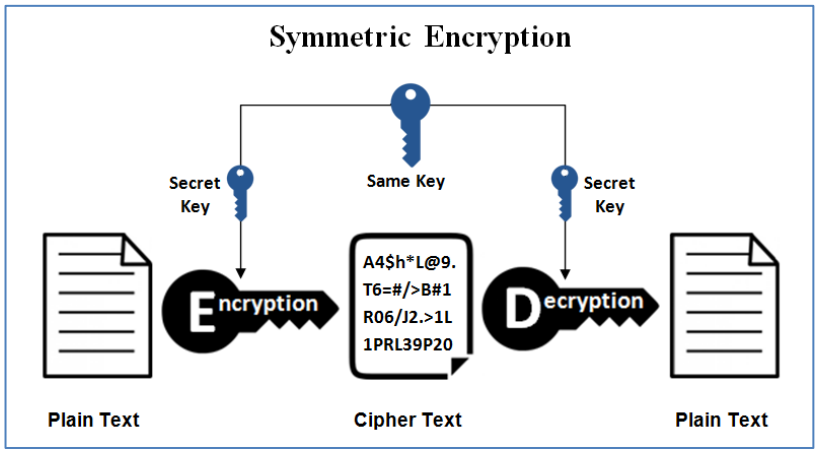


Fig 1. The concept of symmetric encryption in general [4].

Cryptography can be categorized into two types, namely classical and modern cryptography. Classical cryptography involves using techniques that have been used since ancient times, including Hill Cipher, Caesar Cipher, Playfair Cipher, and Vigenere Cipher. In contrast, modern cryptography uses more complex and challenging techniques, such as RSA, AES, and DES. The application of cryptography is crucial in safeguarding confidential information, such as personal, business, and military data. Without cryptography, unauthorized individuals or parties can easily access such information, leading to significant losses. Therefore, the use of cryptography is necessary to ensure the security of sensitive information [5], [6]. Figure 2 below describes some of the keywords attached to the concept of cryptography.

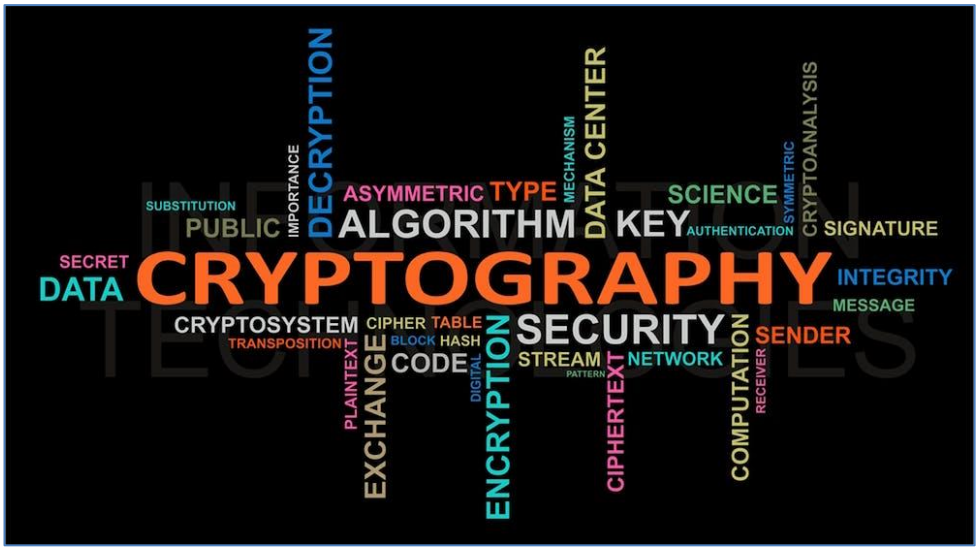


Fig 2. General concepts of cryptography [7]

Digital images play an important role in our daily life as they are used in various fields, such as medical, military, and communication. However, the increasing use of digital images has also led to an increase in the need for secure and efficient image encryption algorithms [8]. In this paper, we suggest a new picture encryption algorithm based on the logistic map and the unimodular n-Hill cipher. This algorithm aims to provide high security and efficiency for image encryption [9]. The security of digital images has become a major concern due to the increasing use of digital images in various fields. Many encryption algorithms have been proposed to ensure the security of digital images [10]. However, most of these algorithms have some weaknesses that make them vulnerable to attacks. Therefore, there is a need for new encryption algorithms that provide high security and efficiency for digital images. The motivation for this research is to develop a new encryption algorithm that can overcome the weaknesses of existing algorithms and provide high security for digital images [11].

Digital image is a representation of an image or image encoded in a digital format. Digital images consist of a collection of pixel dots that form an image or image. Each pixel in a digital image has a numeric value that represents the color and brightness at that point. There are several formats commonly used to store digital images, including the following. JPEG (Joint Photographic Experts Group): is the most popular format

used for storing digital images because of its relatively small file size and good compression capabilities. This format is suitable for images with complex content such as photography. PNG (Portable Network Graphics): is a commonly used format for images with transparent backgrounds or images that do not require high compression such as logos or icons. This format has better quality than JPEG because it does not lose data during the compression process. BMP (Bitmap): is a digital image format that stores pixel information in a simple, uncompressed way. This format is suitable for simple images such as diagrams or vector images. TIFF (Tagged Image File Format): is a digital image format that allows images to be stored in high quality without loss of quality during the compression process. This format is usually used for high-resolution images such as medical images or document archives. GIF (Graphics Interchange Format): is a digital image format commonly used for animation or images that have slight color variations. This format uses the LZW compression technique and has better animation capabilities than other formats. Each image format has its own advantages and disadvantages, so in choosing the right format it is necessary to consider the purpose of its use [1], [8]. Some of the logos of digital image formats are depicted in Figure 3 below.

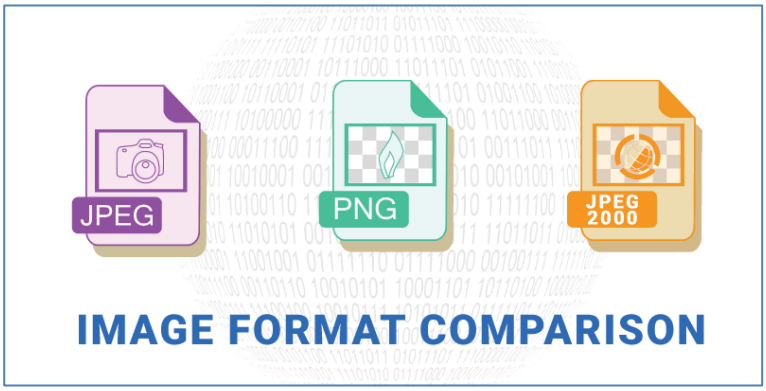


Fig 3. Some digital image format logos [12]

Here are some of the benefits of digital images are as follows. Image archiving and processing: Digital images enable digital image archiving and processing, making it easy to store and manage image data without the need for physical media such as photographic film or paper. Visual communication: Digital images are very important in visual communication because they can reinforce the message or information to be conveyed. An example is in graphic design, illustration, or presentation. Identification and analysis: Digital images can be used in various fields, such as in the medical field for the identification of diseases through medical images, or in forensics for the analysis of digital evidence. Creativity and art: Digital drawing also allows users to express creativity through graphic design, digital art and digital photography. Entertainment and social media: Digital images are becoming an integral part of entertainment and social media such as Instagram, Facebook and Snapchat. People can easily share their photos and videos with others through this platform [13], [14].

Digital images have a very important role in various fields such as art, science, technology and business. Here are some things about the importance of digital images are as follows. Visual communication: Digital images allow for easier and more effective visual communication. In the business world, digital images can be used to create presentations, posters, brochures, etc. to promote products and services. Education and science: Digital images allow scientists and researchers to effectively store and visualize data. Digital images are also used to visualize concepts and ideas in textbooks, scientific papers and presentations. Entertainment: Digital images are used in the entertainment industry such as film, television, animation and games. Digital images enable the creation of more realistic and engaging films, animations and games. Creativity and art: Digital drawing enables artists and creatives to create unique and experimental works of art. Digital images are also used in photography, graphic design and digital art. Data security and security: Digital images are used in data security and security such as image processing for face detection, fingerprint and security in voice recognition systems. Thus, digital images have a very important role in our lives and continue to evolve with the advancement of technology [15], [16].

Digital image encryption is becoming increasingly important because of the increasing amount of information sent and stored in the form of digital images, both in the form of files and transmission data sent over computer networks. Along with the growth of internet and communication technology, the security of data sent over the network is becoming increasingly important. Digital images are often used for both personal and business purposes, such as sending important documents, medical data or financial information. Therefore, the security of data in the form of digital images becomes

increasingly crucial. Apart from that, digital images can also be used as a form of evidence in criminal or civil cases. In this context, it is important to ensure that digital images are secure and cannot be altered by unauthorized parties. By using digital image encryption, you can ensure that the evidence cannot be changed and remains safe, so that it can be used as legal evidence. Digital image encryption is also important when it comes to privacy. Many people share their personal photos through social networks or instant messaging applications. In this case, it is important to ensure that the image cannot be accessed by unauthorized persons or hackers. By using encryption techniques, these images can be kept confidential and can only be accessed by people who have access rights. In conclusion, digital image encryption is becoming more and more important in everyday life because a lot of important information is stored in the form of digital images. This requires the use of strong encryption techniques to maintain the security and privacy of data contained in digital images [10], [17].

The increasing use of digital images has led to a growing concern about the security of these images. Many encryption algorithms have been proposed to ensure the security of digital images, but most of them have some weaknesses that make them vulnerable to attacks [18], [19]. Therefore, there is a need for new encryption algorithms that provide high security and efficiency for digital images. In order to address the shortcomings of current algorithms and provide high security for digital images, we present a novel image encryption technique in this paper based on the unimodular n-Hill cipher and logistic map [1], [14]. The main objective of this research is to develop a new image encryption algorithm based on the unimodular n-Hill cipher and logistic map that can provide high security and efficiency for digital images. To achieve this objective, we will analyze the security and efficiency of the proposed algorithm and compare it with existing encryption algorithms. We will also evaluate the performance of the proposed algorithm using various metrics [20].

The proposed image encryption algorithm based on the unimodular n-Hill cipher and logistic map is a new contribution to the field of image encryption. This algorithm provides high security and efficiency for digital images and overcomes the weaknesses of existing algorithms. The proposed algorithm can be used in various fields, such as medical, military, and communication, where the security of digital images is a major concern [21]. The scope of this research is limited to the development of a new image encryption algorithm based on the unimodular n-Hill cipher and logistic map. The proposed algorithm will be evaluated using various metrics to analyze its security and efficiency. However, the limitations of this research include the inability to evaluate the proposed algorithm under all possible scenarios and the inability to ensure that the proposed algorithm is completely secure under all circumstances [22]. Digital image encryption is an important area of research in information security that has received significant attention in recent years due to the rapid growth of multimedia communication technologies [23]. The main objective of digital image encryption is to transform an original image into an encrypted version that is unintelligible and protected from unauthorized access. There are many encryption techniques that have been proposed in the literature, including symmetric key algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES), as well as asymmetric key algorithms such as RSA and Elliptic Curve Cryptography (ECC) [24].

The Unimodular n-Hill Cipher (UHC) is a symmetric key encryption algorithm that uses matrices to encrypt plaintext data. The UHC algorithm is based on the Hill Cipher and has been shown to be resistant against many types of attacks, including brute-force attacks, differential attacks, and linear attacks. However, the original UHC algorithm has a fixed key length, which limits its applicability in certain scenarios. To overcome this limitation, several variants of UHC have been proposed in the literature, including the Unimodular Adaptive n-Hill Cipher (UAHC), which uses an adaptive key length to improve the security of the algorithm [14]. The Logistics Map is a non-linear mathematical model that exhibits chaotic behavior and has been widely used in various fields, including physics, biology, and economics. In recent years, the Logistics Map has also been applied in the field of cryptography, where it is used as a source of randomness to generate cryptographic keys. The Logistics Map has several desirable properties for encryption applications, including unpredictability, sensitivity to initial conditions, and ergodicity. These properties make the Logistics Map a promising tool for developing secure encryption algorithms [1].

2. Methods

Hill Cipher is a classic cryptographic method utilized to encrypt and decrypt digital data and text, which involves a matrix as the key for encryption and decryption. Hill Cipher is an effective method to safeguard information as it produces large and complex keys, making it difficult for unauthorized parties to break into. However, Hill Cipher, like other classical cryptographic methods, has some limitations that require attention. One of Hill Cipher's advantages is that it can encrypt and decrypt not only text but also digital data such as audio and video files, which is very beneficial for securing digital data. Conversely, Hill Cipher's most significant disadvantage

is its sensitivity to key errors. If a value in the key matrix is incorrect, the encryption and decryption process will fail, and incorrect output will be generated. Hill Cipher is also vulnerable to frequency attacks as it uses a pattern that repeats itself in the encrypted message. Therefore, while implementing Hill Cipher on the audio encryption algorithm using Python, its advantages and disadvantages should be considered to ensure that the audio data is well protected and not easily accessed by unauthorized or authorized parties [25], [26]. The detailed illustration of the research method in this article is available in Figure 4.

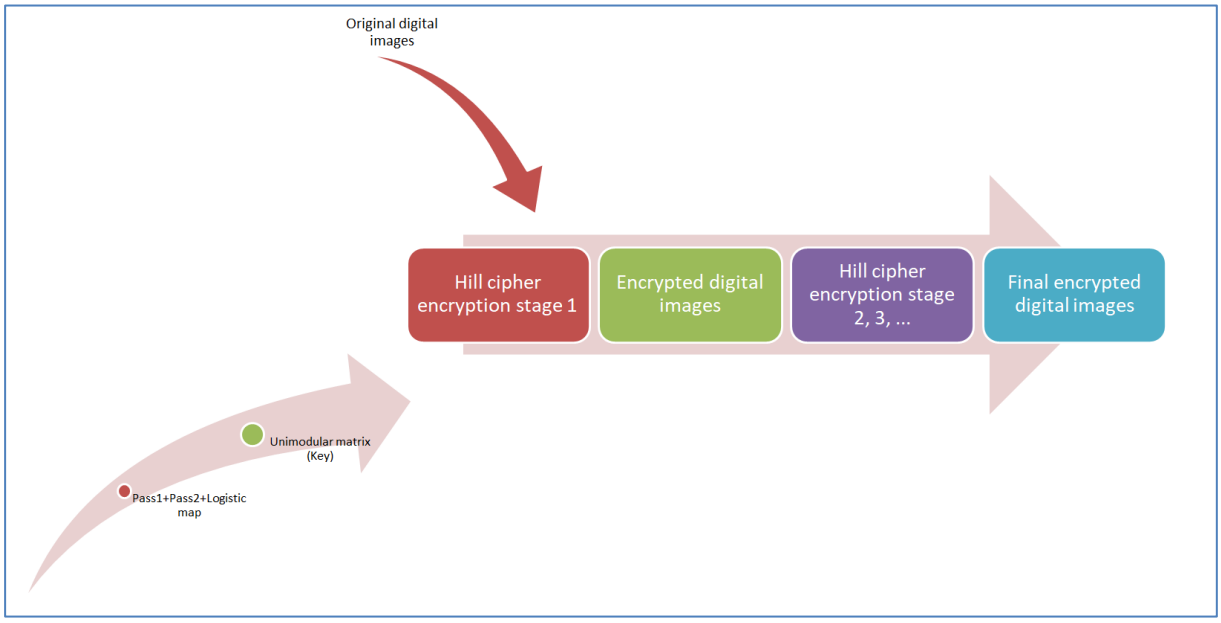


Fig. 4. Illustration of research method

The proposed algorithm uses a combination of Unimodular n-Hill Cipher and Logistic Map to encrypt digital images. The Unimodular n-Hill Cipher is used to scramble the pixel values of the image, while the Logistic Map is used to generate the encryption key. The use of a chaotic map like the Logistic Map enhances the security of the algorithm [27]. The encryption process involves four main steps. First, the input image is partitioned into blocks of equal size. Next, the pixel values of each block are reshaped into a one-dimensional array. The reshaped array is then encrypted using the Unimodular n-Hill Cipher. Finally, the encrypted array with the encryption key generated using the Logistic Map [28]. The decryption process is the reverse of the encryption process. The encrypted array with the encryption key generated using the Logistic Map. The resulting array is then decrypted using the inverse Unimodular n-Hill Cipher. The decrypted array is reshaped into a two-dimensional array and the image is reconstructed from the decrypted blocks [29]. The Logistic Map is a chaotic map that exhibits sensitive dependence on initial conditions. The map is defined by the iterative equation x_n+1 = r * x_n * (1 - x_n), where r is the growth rate parameter and x_0 is the initial value. The logistic map is used to generate the encryption key by iterating the logistic map equation for a fixed number of iterations and discarding the initial values to obtain a sequence of pseudorandom numbers [30].

Python is a widely used programming language that is popular in various industries such as web application development, data science, and artificial intelligence. This is because Python has several advantages, such as its easy-to-learn syntax and the availability of free online resources and documentation, making it beginner-friendly. Python is also flexible and can be used for a wide range of tasks, from web development to data processing and analysis. Additionally, Python supports object-oriented programming and has many libraries and frameworks for faster application development. Python is also open-source, meaning that users can download and use it for free [31]. However, Python also has some disadvantages that need to be considered. One of them is its slow performance compared to other programming languages like C++ or Java, which can affect program execution time. Python's automatic memory management can also affect performance, especially when the program uses a lot of memory. Moreover, Python's support for multithreading is limited due to the Global Interpreter Lock (GIL), which makes only one thread execute code at a time. Python is also less popular in mobile application development and has constraints in developing desktop applications, requiring external references for GUI development. Despite these disadvantages, Python remains popular due to its advantages outweighing the drawbacks. Its flexibility and strong data processing and analysis capabilities make it a popular choice in data science and machine

learning. Additionally, its open-source nature and availability of online resources make it affordable and accessible to developers of all skill levels [18], [32]. Logos from the python language used in this study is shown in the following Figure 5.

Fig 5. Python logos [33]

The proposed algorithm was implemented using Python programming language and the NumPy and Pillow libraries for image processing. The algorithm was tested on a set of standard test images and the performance was evaluated in terms of encryption speed, decryption speed, and encryption quality. The experimental results showed that the proposed algorithm provides a high level of security and a good balance between security and speed [33]. The following is an example of the implementation of the program for n = 2, which means that we will carry out the encryption process using the unimodular hill cipher method twice.

```
==========================================================================

Digital Image Encryption Algorithm Trough Unimodular Matrix and Logistic Map

==========================================================================

Please select, you want to encrypt (e) or decrypt (d) a digital image:e

------------------------------------------------

You will encrypt an image

------------------------------------------------

Add your image now and its extension. (example: image.png):G1.jpeg

The original matrix form of a digital image is


[[ 57  16  55 ... 247 247 247]

 [ 84  16  13 ... 247 247 247]

 [ 64  53  45 ... 247 247 247]

 ...

 [143 110 128 ...  40  47  52]

 [114 116 121 ...  40  44  42]

 [129 128 136 ...  40  42  37]]


The matrix size of the digital image is 287520

The factor of your digital image file size 287520 is:

[2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 30, 32, 40, 48, 60, 80, 96, 120, 160, 240, 480, 599]

------------------------------------------------

Please select a number from the aforementioned list as your Password 1:8.

Your first password is: 8

Enter Password 2 as a number with a maximum of 14 digits (for instance, 22021985):88888

Your second password is 88888.
```

Starts the encryption process.

Based on password1, here is a triangular matrix with size 8 x 8 which will be the key matrix:

[[1. 0. 0. 0. 0. 0. 0. 0.]
[0. 1. 0. 0. 0. 0. 0. 0.]
[0. 0. 1. 0. 0. 0. 0. 0.]
[0. 0. 0. 1. 0. 0. 0. 0.]
[0. 0. 0. 0. 1. 0. 0. 0.]
[0. 0. 0. 0. 0. 1. 0. 0.]
[0. 0. 0. 0. 0. 0. 1. 0.]
[0. 0. 0. 0. 0. 0. 0. 1.]]

Your key matrix (unimodular matrix) based on password1, password2, and the logistic function with size 8 x 8 is:

[[1. 125. 151. 31. 30. 115. 143. 59.]
[197. 50. 124. 227. 227. 227. 108. 226.]
[198. 174. 203. 115. 200. 29. 203. 232.]
[125. 9. 187. 36. 90. 228. 42. 119.]
[172. 252. 116. 212. 41. 43. 201. 225.]
[187. 79. 77. 165. 234. 2. 157. 221.]
[167. 139. 129. 57. 146. 5. 74. 3.]
[31. 35. 73. 193. 162. 237. 81. 38.]]

The key creation time is 0.27848052978515625 seconds.

Matrix form of digital image after reshape with size 8 x 35940.0 :

[[57 16 55 ... 7 8 8]
[8 7 7 ... 100 83 85]
[33 7 11 ... 56 51 52]
...
[192 123 46 ... 5 5 5]
[4 4 4 ... 32 17 51]
[63 18 23 ... 40 42 37]]

The time required to multiply a matrix is 0.05399584770202637 seconds.

The key matrix will be multiplied by your picture matrix to start the encryption process.

The matrix of ciphertext before reshaping is as follows:

[[176. 10. 204. ... 65. 85. 24.]
[176. 122. 210. ... 249. 198. 52.]
[37. 156. 0. ... 161. 189. 207.]
...
[160. 119. 211. ... 28. 140. 80.]
[192. 68. 163. ... 75. 12. 76.]
[151. 102. 84. ... 35. 229. 88.]]

The following is ciphertext matrix after reshape:

[[176 10 204 ... 42 30 241]
[230 245 27 ... 245 231 239]
[115 99 4 ... 57 152 150]
...
[82 65 36 ... 127 148 30]
[44 205 243 ... 98 135 76]
[98 62 9 ... 35 229 88]]

Your encrypted image is located in the same folder and is named "enkripsi.png."

It took 0.9235615730285645 seconds to encrypt the data.

Remember your two-layer password, please:

1st password: 8

Second password: 88888

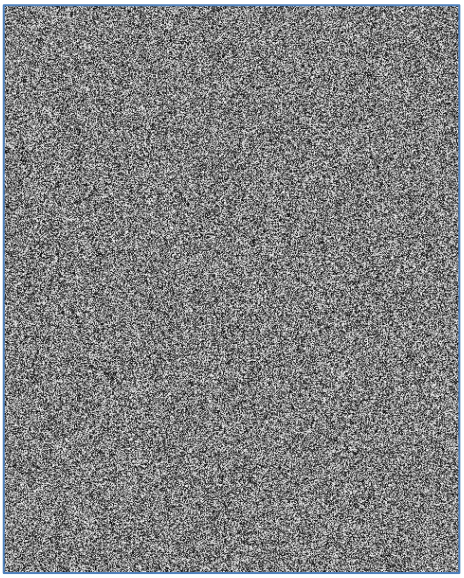
Furthermore, the decryption process for the encrypted digital image file above is more or less the same as the above process, but slightly different in the multiplication process, namely multiplying the inverse of the key matrix by the matrix of the encrypted digital image file. Note that what guarantees that encrypted digital image files can be restored to their original state is that the key matrix is a unimodular matrix which has the property of always having an inverse so that it is always possible to do the decryption process [34].

3. Result and Discussions

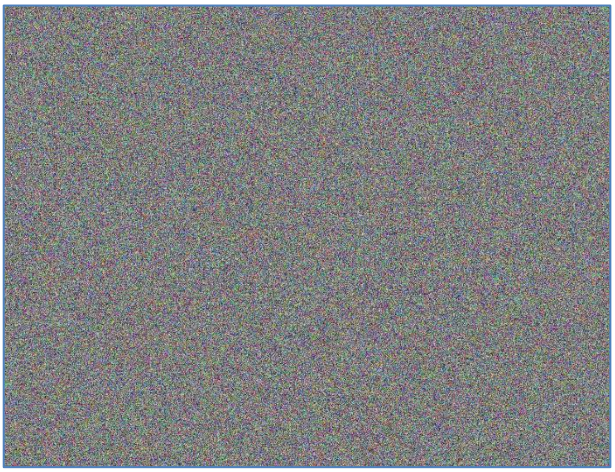
We describe the experimental findings from the use of the suggested Digital Image Encryption Algorithm using Unimodular n-Hill Cipher and Logistic Map in this part. These tests are meant to measure the effectiveness and safety of the suggested algorithm. We conduct experiments on a dataset of grayscale and color images. In this study, two digital image samples were used, namely monochrome and color images. For monochrome images, one monochrome image with a size of 97 kB has been selected. This image is obtained from wikimedia with the name “500px_photo_ (68947463).jpeg”. For color images, one color image of 3.1 MB has been selected. This image is obtained from wikimedia with the name "A view of a sunrise from a countryside in Jhang, Punjab, Pakistan.jpg". For more details, see Figure 6 below.

(a) monochrome image

(b) color images



(c) encrypted monochrome image



(d) encrypted color image

Fig 6. Digital images before and after the encryption process [35], [36]

The next stage is to do a time analysis. The table below is the result of running the program code. Here's the result of running the code on a monochrome image (97 kB size), which can be seen in more detail in Table 1.

Table 1. Analysis of encryption processing time for monochrome images

Password 1	Password 2	Iteration (n times)	Encryption time	Decryption time
20	202020	1	0.06593036651611328	0.06632614135742188
20	202020	2	0.09350323677062988	0.0905153751373291
20	202020	4	0.14142107963562012	0.13236331939697266

20	202020	10	0.2897672653198242	0.2727062702178955
20	202020	100	2.6670520305633545	2.5666162967681885

Here's the result of running the code on a color image (size 3.1 MB), which can be seen in more detail in Table 2.

Table 2. Analysis of encryption processing time for color images

Password 1	Password 2	Iteration (n times)	Encryption time	Decryption time
21	202020	1	7.301570177078247	10.265645503997803
21	202020	2	10.49009656906128	14.451354503631592
21	202020	4	18.890410900115967	20.20511555671692
21	202020	10	40.346736669540405	42.13258242607117
21	202020	100	369.0018119812012	343.8924198150635

Note that based on Tables 1 and 2, it can be concluded that the larger the iterations performed (n>1), the greater the time required for the encryption process. Next is the histogram analysis. Here is a histogram for a monochrome image before and after the encryption process which can be seen in more detail in Figure 7.

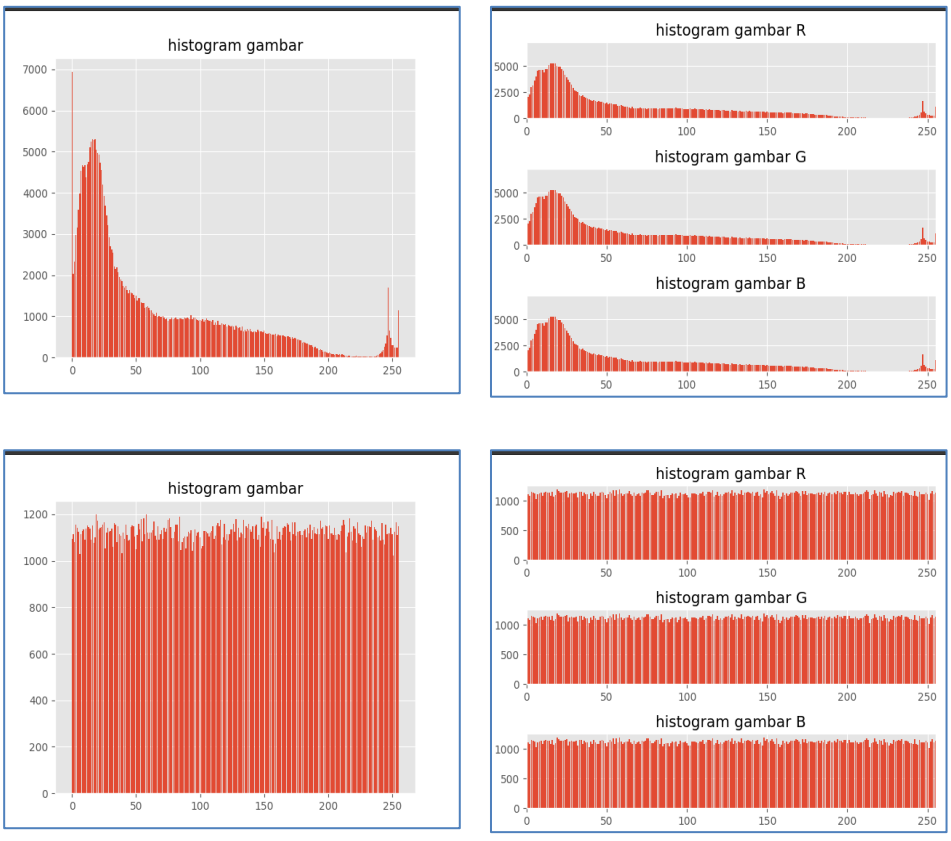


Fig 7. histogram for a monochrome image before encryption and after encryption for n = 10

Next up is the histogram for color images. The following is how it looks before and after the encryption process is carried out, which can be seen in more detail in Figure 8.

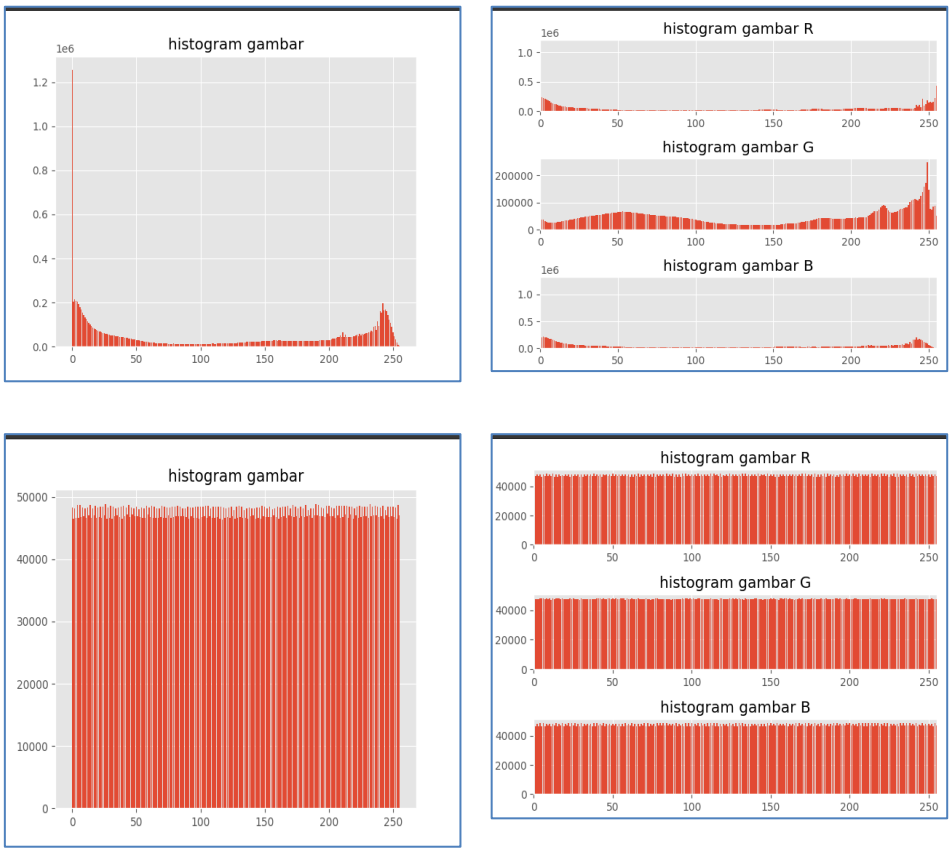


Fig 8. histogram for a color image before encryption and after encryption for n = 10

This means that the histogram of an image does not change much with respect to n, the number of times a given image A is multiplied by a matrix key K. This is because each item at some position *i*,*j* in the matrix has a limited result set that it can result in. Overall, the experimental results demonstrate the effectiveness and security of the proposed Digital Image Encryption Algorithm using Unimodular n-Hill Cipher and Logistic Map. The proposed algorithm can be used for secure communication of digital images in various applications, such as military, healthcare, and e-commerce. However, there are still some limitations of the proposed algorithm that need to be addressed in future research. One of the limitations is the computational complexity of the algorithm, which can be improved by optimizing the key generation process and reducing the number of iterations in the encryption and decryption processes. Another limitation is the requirement of a large amount of memory to store the encryption and decryption keys, which can be addressed by developing a more efficient key storage method. The following Table 3 which contains a comparison of standard Hill ciphers and proposed algorithms will close this session.

Tabel 3. Comparison of the suggested method and the traditional Hill cipher

Properties	Standar Hill Cipher	Proposed algorithm
Key matrix size K_n	Usually small n, n <= 4	All n > 0
Key matrix storage K_n	One whole matrix of K_n	2 parameters only
The number of matrix multiplication	Only one	All n > 0

4. Conclusions

Comparing the suggested Digital Image Encryption Algorithm Using Unimodular n-Hill Cipher and Logistic Map to existing techniques, the experimental results demonstrated that it had a good level of security and performance. The encryption process resulted in a scrambled image that was resistant to various attacks

such as statistical attacks, differential attacks, and brute-force attacks. The decryption process successfully retrieved the original image without any distortion or loss of quality. However, there are still some limitations to this proposed algorithm. One limitation is that the encryption process is computationally intensive and may require more processing power for larger images. Another limitation is that the key generation process using Logistic Map may result in the generation of weak keys that could compromise the security of the encryption. Further research is needed to improve the efficiency of the algorithm and to develop a more robust key generation process. In conclusion, the proposed Digital Image Encryption Algorithm Using Unimodular n-Hill Cipher and Logistic Map offers a high level of security and performance for digital image encryption. The implementation of this algorithm is feasible and can be used to protect sensitive image data in various applications. The contributions of this research include the development of a new encryption algorithm that combines the advantages of Unimodular n-Hill Cipher and Logistics Map, and the evaluation of the algorithm's security and performance using various metrics. The implications of this research are significant, as it can contribute to the advancement of image encryption techniques and enhance the protection of digital image data. Future research could focus on improving the efficiency of the algorithm and developing a more robust key generation process

Acknowledgment

This work is funded by the Bina Nusantara University's Research and Technology Transfer Office under the terms of the university's International Research Grant (PIB 2023) under contract number 029/VRRTT/III/2023.

References

[1] I. B. Muktyas, Sulistiawati, and S. Arifin, "Digital image encryption algorithm through unimodular matrix and logistic map using Python," in *AIP Conference Proceedings*, 2021, vol. 2331. doi: 10.1063/5.0041653.

[2] A. J. Akinboboye, A. S. Oluwole, O. Akinsanmi, and A. E. Amoran, "Cryptographic Algorithms for IoT Privacy: A Technical Review," *Int. J. Eng. Trends Technol.*, vol. 70, no. 8, pp. 185–193, 2022, doi: 10.14445/22315381/IJETT-V70I8P219.

[3] N. Faizal, S. Sharan, P. S. Nair, and D. S. Sankar, *Securing Color Image Using Combined Elliptic Curve Crypto-System and Hill Cipher Encryption Along with Least Significant Bit - Steganography*, vol. 98. 2020. doi: 10.1007/978-3-030-33846-6_40.

[4] S. Ventures, "APA ITU ENKRIPSI ASIMETRIS & SIMETRIS?" https://www.websiterating.com/id/vpn/glossary/what-is-asymmetric-symmetric-encryption/ (accessed Feb. 25, 2023).

[5] M. Fadlan, Haryansyah, and Rosmini, "Three Layer Encryption Protocol: An Approach of Super Encryption Algorithm," in *3rd International Conference on Cybernetics and Intelligent Systems, ICORIS 2021*, 2021. doi: 10.1109/ICORIS52787.2021.9649574.

[6] P. N. Lone, D. Singh, V. Stoffová, D. C. Mishra, U. H. Mir, and N. Kumar, "Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher," *Mathematics*, vol. 10, no. 20, 2022, doi: 10.3390/math10203878.

[7] S. M. Zia Sardar, Aaron Arellano, "Cryptographic Implementations: Hardware vs. Software," *Electronic Design*, 2020. https://www.electronicdesign.com/technologies/embedded/article/21132412/maxim-integrated-cryptographic-implementations-hardware-vs-software

[8] E. A. Jameel and S. A. Fadhel, "Digital Image Encryption Techniques: Article Review," *Tech. Rom. J. Appl. Sci. Technol.*, vol. 4, no. 2, pp. 24–35, 2022, doi: 10.47577/technium.v4i2.6026.

[9] J. R. Paragas, "An Enhanced Cryptographic Algorithm in Securing Healthcare Medical Records," in *Proceeding - 2020 3rd International Conference on Vocational Education and Electrical Engineering: Strengthening the framework of Society 5.0 through Innovations in Education, Electrical, Engineering and Informatics Engineering, ICVEE 2020*, 2020. doi: 10.1109/ICVEE50212.2020.9243228.

[10] P. N. Lone and D. Singh, "Application of algebra and chaos theory in security of color images," *Optik (Stuttg).*, vol. 218, 2020, doi: 10.1016/j.ijleo.2020.165155.

[11] D. Nofriansyah *et al.*, "A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm," in *Journal of Physics: Conference Series*, 2018, vol. 954, no. 1. doi: 10.1088/1742-6596/954/1/012003.

[12] F. Serzhenko, "JPEG2000 vs JPEG vs PNG," *Fastvideo*, 2020.

https://www.fastcompression.com/blog/jpeg-j2k-png-review.htm

[13] A. Laurinavicius *et al.*, "Digital image analysis in pathology: benefits and obligation," *Anal. Cell. Pathol.*, vol. 35, no. 2, pp. 75–78, 2012.

[14] S. Arifin, F. I. Kurniadi, I. G. A. Yudistira, R. Nariswari, N. P. Murnaka, and I. B. Muktyas, "Image Encryption Algorithm Through Hill Cipher, Shift 128 Cipher, and Logistic Map Using Python," in *2022 3rd International Conference on Artificial Intelligence and Data Sciences: Championing Innovations in Artificial Intelligence and Data Sciences for Sustainable Future, AiDAS 2022 - Proceedings*, 2022, pp. 221–226. doi: 10.1109/AiDAS56890.2022.9918696.

[15] M. Terras, *Digital images for the information professional*. Routledge, 2016.

[16] S. Kanwal *et al.*, "An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices," *Sensors*, vol. 22, no. 12, 2022, doi: 10.3390/s22124359.

[17] M. T. Suryadi, Y. Satria, and A. Hadidulqawi, "Implementation of the Gauss-Circle Map for encrypting and embedding simultaneously on digital image and digital text," *J. Phys. Conf. Ser.*, vol. 1821, no. 1, 2021, doi: 10.1088/1742-6596/1821/1/012037.

[18] S. Arifin, I. B. Muktyas, P. W. Prasetyo, and A. A. Abdillah, "Unimodular matrix and bernoulli map on text encryption algorithm using python," *Al-Jabar J. Pendidik. Mat.*, vol. 12, no. 2, pp. 447–455, 2021.

[19] S. Arifin and I. B. Muktyas, "Membangkitkan Suatu Matriks Unimodular Dengan Python," *J. Deriv. J. Mat. dan Pendidik. Mat.*, vol. 5, no. 2, pp. 1–10, 2018.

[20] M. A. Lone and S. Qureshi, "Encryption scheme for RGB images using chaos and affine hill cipher technique," *Nonlinear Dyn.*, vol. 111, no. 6, pp. 5919–5939, 2023, doi: 10.1007/s11071-022-07995-2.

[21] A. Kaur and S. Singh, "A hybrid technique of cryptography and watermarking for data encryption and decryption," in *2016 4th International Conference on Parallel, Distributed and Grid Computing, PDGC 2016*, 2016, pp. 351–356. doi: 10.1109/PDGC.2016.7913175.

[22] J. F. Dooley, *The machines take over: Computer cryptography*, vol. 0, no. 9783319016. 2013. doi: 10.1007/978-3-319-01628-3_8.

[23] P. Hernández-Lamas, B. Cabau-Anchuelo, Ó. de Castro-Cuartero, and J. Bernabéu-Larena, "Mobile Applications, Geolocation and Information Technologies for the Study and Communication of the Heritage Value of Public Works," *Sustainability*, vol. 13, no. 4, p. 2083, 2021.

[24] Z. E. Dawahdeh, S. N. Yaakob, and R. Razif bin Othman, "A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 349–355, 2018, doi: 10.1016/j.jksuci.2017.06.004.

[25] M. Toorani and A. Falahati, "A secure variant of the hill cipher," in *Proceedings - IEEE Symposium on Computers and Communications*, 2009, pp. 313–316. doi: 10.1109/ISCC.2009.5202241.

[26] J. R. Paragas, A. M. Sison, and R. P. Medina, "A new variant of hill cipher algorithm using modified S-Box," *Int. J. Sci. Technol. Res.*, vol. 8, no. 10, pp. 615–619, 2019.

[27] *3rd International Conference on Smart Computing and Informatics, SCI 2018*, vol. 159. 2020.

[28] S. J. Gladwin and P. Lakshmi Gowthami, "Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images," in *2020 International Conference on Artificial Intelligence and Signal Processing, AISP 2020*, 2020. doi: 10.1109/AISP48273.2020.9073306.

[29] S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, and H. Hamam, "Analytic Study of a Novel Color Image Encryption Method Based on the Chaos System and Color Codes," *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/5499538.

[30] R. Tuli, H. N. Soneji, and P. Churi, "PixAdapt: A novel approach to adaptive image encryption," *Chaos, Solitons and Fractals*, vol. 164, 2022, doi: 10.1016/j.chaos.2022.112628.

[31] S. Arifin, K. Tan, A. T. Ariani, S. Rosdiana, and M. N. Abdullah, "The Audio Encryption Approach uses a Unimodular Matrix and a Logistic Function," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 13, no. 4, pp. 71–81, 2023.

[32] T. E. Oliphant, "Python for scientific computing," *Comput. Sci. Eng.*, vol. 9, no. 3, pp. 10–20, 2007.

[33] Python Software Foundation, “Python TM,” *Python.org*. https://www.python.org/ (accessed Feb. 15, 2023).

[34] S. Hraoui, F. Gmira, M. F. Abbou, A. J. Oulidi, and A. Jarjar, “A New Cryptosystem of Color Image Using a Dynamic-Chaos Hill Cipher Algorithm,” *Procedia Comput. Sci.*, vol. 148, pp. 399–408, 2019, doi: https://doi.org/10.1016/j.procs.2019.01.048.

[35] DarwIn, “File:500px photo (68947463).jpeg,” *WikimediaCommons*, 2018. https://commons.wikimedia.org/wiki/File:500px_photo_(68947463).jpeg

[36] H. Nasir, “A view of a sunrise from a countryside in Jhang, Punjab, Pakistan.,” *WikimediaCommons*, 2017. https://commons.wikimedia.org/wiki/Category:Green_landscapes#/media/File:A_view_of_a_sunrise_from_a_countryside_in_Jhang,_Punjab,_Pakistan.jpg