Journal of Information System and Technology Research

journal homepage: https://journal.aira.or.id/index.php/jistr/

Data Security Techniques Using Vigenere Cipher And Steganography Methods In Inserting Text Messages In Images

[1] Vincent Smith , [2] Maximilian Mendoza, [3]Insaf Ullah

[1]University of Charleston, USA
[2]University College Dublin, Republic Irlandia
[3]University Of Essex , United Kingdom

ARTICLE INFO

Article history:

Received July 1, 2024
Accepted August 28, 2024
Available online Septem 30, 2024

Keywords:

Cryptography
Steganography
Data Security
Vigenere Chipher
Text Message

ABSTRACT

Improving data security has become a top priority in many industries, especially when it comes to sending and receiving private communications. Embedding text into photos using steganography and the Vigenere Cipher Method is one method of protecting text messages. In order to maintain the security of text embedded in images via web-based applications, the main challenge in this research is how to integrate and apply the Vigenere Cipher algorithm and LSB steganography while still paying attention to the size of the image message that has been ciphertexted. insertion and what not. Combining these two techniques aims to increase the level of security when encrypting message text. The message text is encrypted using the Vigenere Cipher to protect it; Encrypted messages are difficult to decipher without the right key. Meanwhile, message text may be hidden visually in photos using steganography. Text messages are efficiently disguised in images and significantly encrypted thanks to the combination of these two techniques. In this research, steganography and Vigenere Cipher techniques are used and tested on various types of images. The combined use of these two techniques effectively improves data security, according to test results. The study also discusses a number of possible defenses, such as image size and quality, that may arise from combining the two approaches. The findings of this research can be applied to improve the security of text messages in various contexts, such as online communications and data storage. Through the integration of steganography and Vigenere Cipher technology, users can guarantee the confidentiality of their communication texts and prevent unapproved access.

Corresponding Author:

Vincent Smith
University of Charleston, USA
Email: Vincentsmith@ccu.edu.tw

1. INTRODUCTION

Current rapid technological advances, especially in the field of communication technology, have resulted in demands for fast access to information. This trend is clearly visible, especially in the field of electronic media, where the internet plays an important role in contributing to this phenomenon. Nowadays, people can use portable electronic devices such as smartphones or tablets or technological gadgets such as PCs (Personal Computers) to connect online[1]. The use of social media and the internet is increasingly widespread, therefore, the need for communication security is increasing. Hiding data before transmission is one tactic used. Information systems must follow strict guidelines to protect data privacy and security[2], [3]. As a reaction to the rapid advances in technology and information, some users of security features in information systems have created new methods. Information owners may experience negative impacts when their information is shared with others[4], [5], [6], [7].

Several terms known in the field of computer science and mathematics related to message or data security involve the concepts of Cryptography and Steganography. By applying Converting communications into ciphertext is the goal of cryptography, which uses encryption methods and secret keys. On the other hand, in Steganography, the message is hidden by another object[8], [9]. The main goal of steganography and cryptography approaches is to prevent unauthorized parties from accessing data. The main difference between the two is that, although encryption in cryptography rewrites the message to protect its contents, the message appears to be written because it is in plain text[10], [11], [12], [13].

One of the techniques that can be used in cryptographic activities is the Vigenere Cipher algorithm. The Vigenere Cipher method uses various Caesar ciphers based on the letters of several keywords to encrypt alphabetic text. This method uses a shift mechanism that involves using Vigenere tables to shift plaintext letters by varying amounts. Then, some algorithms can be implemented using the Vigenere tables suggested by this approach. Steganography, on the other hand, hides messages in digital materials with the aim of making them invisible [14]. In this research, without changing the visual appearance or impression of digital data, such as photos, sound or video, hidden information or messages can be hidden using the LSB (Least Significant Bit) steganography approach. In this way, the message will be inserted into the image. Images that include messages encoded by one of these two methods—cryptography or steganography—or a combination of both can be difficult to decipher.

The Greek terms "cryptos" (which means "secret") and "graphein" (which means "writing") are the sources of the word "cryptography". Therefore, the use of secret messages is one way to understand cryptography. The science and art of maintaining message security is known as cryptography [15]. In the context of terminology, a process referred to as encryption can be used to change or encode cryptographic information so that challenging or possibly unintelligible material. Through cryptography, plaintext can be converted into ciphertext and vice vers [16]. Plaintext refers to original data that can still be read and understood. In contrast, the study of cryptography includes the application of mathematical methods to information security problems, including data integrity, confidentiality, and authentication. The use of the term "art" in this context refers to the historical fact that early in the development of cryptography, each individual had a specific approach to maintaining the confidentiality of messages. Encryption involves the transformation of plaintext into ciphertext, while decryption is the step to return the ciphertext to its original plaintext form [17].

A classic cryptographic algorithm, the Vigenere cipher first appeared in 1986 in the 16th century. French cryptographer and diplomat Blaise de Vigenere discovered this procedure and published the formula in his book, but he made several modifications to it. Giovan Batista Belaso, in 1553, also wrote a book entitled La Cifra del Sig. Giovan Batista Belaso [18]. Vigenere Cipher, a method for encrypting alphabetic text that uses the Caesar cipher sequence depending on keyword letters [19]. Like Vigenere, this conventional cryptographic technique uses various alphabet substitution techniques. The Vigenere key is repeated until it reaches the plaintext length to prevent ciphertext fragmentation. However, problems with the ciphertext and Vigenere algorithms can be overcome by applying the Kasiski frequency analysis method [20].

Steganography is a method that can be used to hide sensitive data by disguising it as regular data. Currently, the term "steganography" usually refers to the technique of hiding files or data in digital image, audio, or video formats [21]. Important requirements that must be met by effective steganography, according to [22], include that the storage container does not experience significant changes after secret data is inserted, the existence of the data remains confidential, the storage container does not affect the existence and quality of the data, and allows data to be returned to its original state. The steganography process embedded in the covering media is described schematically below. Additionally, the science and art of encrypting messages in such a way that people cannot read them is known as steganography [23].

In the past five years, research on cryptography and steganography has continued to advance, focusing on improving the security, efficiency, and practicality of these techniques in the face of evolving digital threats. Research Bagane [24]explored the combination of the Vigenere Cipher with modern cryptographic algorithms to enhance the security of encrypted messages. Their study emphasized the use of hybrid encryption techniques to mitigate the weaknesses of traditional ciphers, such as the Vigenere Cipher, against contemporary cryptanalytic attacks. They demonstrated that by integrating Vigenere with algorithms like AES (Advanced Encryption Standard), the overall encryption process could be made more secure without significantly impacting computational efficiency. According Nagi [25] investigated the application of steganography in digital image processing, focusing on the LSB (Least Significant Bit) technique. Their research highlighted the effectiveness of LSB steganography in embedding hidden messages within images while maintaining high levels of imperceptibility. They proposed an improved LSB method that enhances the robustness of hidden data against steganalysis attacks, ensuring that the embedded messages remain secure even under security.

According Varghese [26] developed a hybrid cryptography-steganography system aimed at securing multimedia data transmission. Their work combined the Vigenere Cipher with LSB steganography to create a dual-layer security system. They conducted experiments to assess the performance of this hybrid approach, showing that it provided a significant improvement in data security while maintaining the quality of the multimedia content. This system was particularly effective in preventing unauthorized access to sensitive data transmitted over public networks. According fadil [20]introduced an enhanced version of the Vigenere Cipher that incorporates dynamic key generation techniques. Their research ad dressed the vulnerability of static keys in traditional Vigenere encryption by proposing a method that generates keys based on real-time data, making the cipher more resistant to brute-force attacks. This dynamic key approach was tested in conjunction with LSB steganography, further increasing the security of hidden messages within digital images. According Mahmod [27] conducted a study on the integration of machine learning with steganography to improve the detection and prevention of steganalysis attacks. They developed a machine learning-based framework that could adaptively select the best steganographic technique for a given digital medium, depending on the characteristics of the data and the potential threats. Their work also explored the use of cryptographic algorithms, like the Vigenere Cipher, in conjunction with this framework to provide a comprehensive security solution.

These recent studies illustrate the ongoing innovation in the fields of cryptography and steganography, with a particular focus on integrating traditional methods like the Vigenere Cipher with modern techniques and technologies. The research from the last five years has significantly contributed to enhancing the security of data in digital communications, making it increasingly difficult for unauthorized parties to access or decipher sensitive information.

Technically an image or picture is a two-dimensional (dwimatra) plane image. From a mathematical point of view, the image can be thought of as a continuous function of light intensity when viewed from one side of the dual matrix viewpoint. The objects in the image are partially reflected from the light source that illuminates them. Both the human eye and electronic instruments, such as cameras, capture this reflected light, while other tools such as scanners are used to record images of an object and are referred to as images [28]. As stated in the journal by [29], grouping pixels that can be processed by a computer produces digital images.

2. RESEARCH METHOD

Explaining research chronological, including research design, research procedure (in the form of algorithms, Pseudocode or other), how to test and data acquisition.

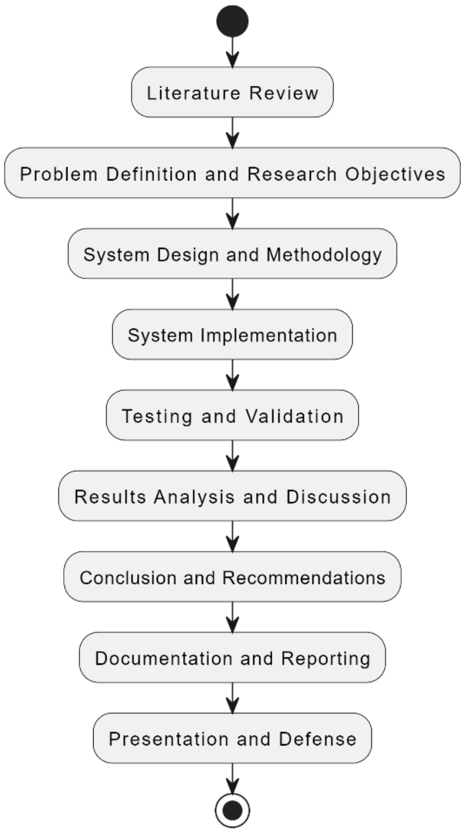
Literature Review
Problem Definition and Research Objectives
System Design and Methodology
System Implementation
Testing and Validation
Results Analysis and Discussion
Conclusion and Recommendations
Documentation and Reporting
Presentation and Defense

Figure 1. Research Stages

1). Literature Review

Objective: Conduct a comprehensive review of existing research on cryptography and steganography, with a specific focus on the Vigenere Cipher and LSB (Least Significant Bit) steganography methods.

Activities:

Collect and review academic papers, books, and articles related to cryptography, steganography, and their applications in data security.

Analyze the strengths and weaknesses of existing techniques.

Identify gaps in the current research that the study aims to address.

2). Problem Definition and Research Objectives

Objective: Clearly define the problem the research intends to solve and establish specific research objectives.

Activities:

Articulate the need for combining the Vigenere Cipher and steganography for text message security.

Define the research questions and hypotheses.
Outline the goals of the research, such as improving data security or enhancing the robustness of existing methods.
3). System Design and Methodology
Objective: Design the system that will implement the Vigenere Cipher and steganography for securing text messages within images.
Activities:
Develop a system architecture that integrates the Vigenere Cipher for encryption and LSB steganography for embedding encrypted text into images.
Design algorithms for the encryption, embedding, and extraction processes.
Specify the tools and programming languages to be used for system development.
Outline the methodology for testing and evaluating the system.
4). System Implementation
Objective: Implement the designed system, integrating the Vigenere Cipher and steganography techniques.
Activities:
Write and compile the code for encrypting text using the Vigenere Cipher.
Implement the LSB steganography method to hide encrypted text in digital images.
Develop the extraction and decryption modules to retrieve and decode the hidden messages.
Ensure the system functions correctly through initial debugging and refinement.
5). Testing and Validation
Objective: Test the system to ensure its reliability, effectiveness, and security.
Activities:
Perform functional testing to verify that the system correctly encrypts, embeds, extracts, and decrypts messages.
Evaluate the system’s security by testing its resistance to cryptanalysis and steganalysis attacks.
Assess the impact of steganography on image quality using metrics such as PSNR (Peak Signal-to-Noise Ratio).
Conduct comparative analysis with existing methods to validate improvements.
6). Results Analysis and Discussion
Objective: Analyze the test results and discuss the findings in the context of the research objectives.
Activities:
Compile and interpret the data collected during testing.
Discuss the effectiveness of the combined Vigenere Cipher and steganography approach in securing data.
Compare the results with those of previous studies to highlight the contributions of the research.
Identify any limitations or areas for further improvement.
7). Conclusion and Recommendations
Objective: Conclude the research by summarizing the findings and proposing recommendations for future work.
Activities:
Summarize the key outcomes of the research, emphasizing the contributions to the field of data security.
Suggest possible improvements to the system or alternative approaches that could be explored.
Provide recommendations for future research based on the limitations encountered and new questions raised during the study.
8). Documentation and Reporting
Objective: Prepare a comprehensive report that documents the entire research process, findings, and conclusions.
Activities:
Compile all research activities, methodologies, results, and discussions into a structured report.
Prepare visual aids (graphs, charts, diagrams) to support the findings.
Write the final research paper, ensuring it meets academic standards and guidelines.
Review and revise the paper based on feedback from peers or advisors.
9). Presentation and Defense
Objective: Present the research findings to an academic audience and defend the methodology and results.
Activities:
Prepare a presentation that summarizes the research objectives, methodology, results, and conclusions.
Address questions and feedback from the audience or review panel.
Finalize any revisions to the research paper based on the defense outcomes.

3. RESULTS AND DISCUSSION

3.1. Requirements for Minimum Hardware and Software Specifications

Researchers will provide an explanation of the system's functions and results in this chapter. Data input is the first step in implementing the Vigenere cipher and Least Significant Bit steganography. Additionally, each feature will be tested by researchers to determine whether it produces the expected results.

The following equipment and software were used during the entire testing procedure:

a. Hardware. The following are the hardware specification requirements needed to create a system for the program being developed:
1) Laptop with Intel Core i3 processor, 4GB RAM and 500GB hard disk.
2) Mouse
b. Software. The following are prerequisite software specifications for building a system in the program:
1) Google Chrome as a browser to run the web on the program.
2) Visual Studio or Sublime Text as a text editor.
3) Xampp as support for running program scripts.

3.2. Manual calculation of vigenere cipher and LSB steganography

Sample case:

M	E	E	T	I	N	G	O	N	M	O	N	D	A	Y	A	T	T	H	E	O	F	F	I	C	I	N
M	E	E	T	I	N	G	M	E	E	T	I	N	G	M	E	E	T	I	N	G	M	E	E	T	I	N

meeting on Monday at the office

Encryption process:
The Vigenere Cipher encryption formula is:
Ci = (Pi + Ki) mod 26
Or Ci = (Pi + Ki) if the sum of Pi and Ki exceeds 26.

Table 1 Encryption Process

Plaintexs	M	E	E	T	I	N	G	O	N
Key	M	E	E	T	I	N	G	M	E
Plaintext value	15	4	17	19	4	12	20	0	13
Key Value	17	0	15	0	19	17	0	15	0
Results	32	4	32	19	23	29	20	15	13
Ciphertext	G	E	G	T	X	D	U	P	N

Table 2 Encryption Process

Plaintexs	M	E	E	T	I
Key	T	R	A	P	A
Plaintext value	17	0	15	0	19
Key Value	19	17	0	15	0
Results	36	17	15	15	19
Ciphertext	K	R	P	P	T

Plaintexs	M	O	N	D
Key	T	R	A	P
Plaintext value	15	0	3	0
Key Value	19	17	0	15
Results	34	17	3	15
Ciphertext	I	R	D	P

Plaintexs	A	T	T	H
Key	A	T	R	A
Plaintext value	7	0	17	8
Key Value	0	19	17	0
Results	7	19	34	8
Ciphertext	H	T	I	I

Plaintexs	O	F	F	I	C
Key	P	A	T	R	A
Plaintext value	18	4	13	8	13
Key Value	15	0	19	17	0
Results	33	4	32	25	13
Ciphertext	H	E	G	Z	N

So the ciphertext for encrypting the message “MEETINGONMONDAYATTHEOFFICE” is “GEGTXDUPN KRPPT IRDP HTII HEGZN”

The process of inserting a message into an image:

c. Convert Color Components to Binary:
R (Red) = 25 converted to binary to 11001
G (Green) = 67 converted to binary to 1000011
B (Blue) = 65 converted to binary to 1000001

d. Binary Message "GEGTXDUPN KRPPT IRDP HTII HEGZN":

G: 1000111 E: 1000101 G: 1000111 T: 1010100 X: 1011000
D: 1000100 U: 1010101 P: 1010000 N: 1001110
K: 1001011 R: 1010010 P: 1010000 P: 1010000 T: 1010100
I: 1001001 R: 1010010 D: 1000100 P: 1010000
H: 1001000 T: 1010100 I: 1001001 I: 1001001
H: 1001000 E: 1000101 G: 1000111 Z: 1011010 N: 1001110

e. Embed Message Bits into LSB Bits:
Replace the LSB bits of each color component with the message bits sequentially. For example, for starting pixels (25,67,65)
R: 0010010 G: 1000011 B: 1000001
Substitute the last bit:
R: 0010011 (G) G: 1000010 (E) B: 1000000 (G)

f. Pixel Results After Embedding:
(27,66,64)

Step Description:
The formula for the Vigenere Cipher description is:
Pi = (Ci - Ki) mod 26
Or Pi = (Ci - Ki) + 26 if the result of subtracting Ci and Ki produces a negative value.

Ciphertext	G	E	G	T	X	D	U	P	N
Key	R	A	P	A	T	R	A	P	A
Ciphertext value	6	4	6	19	23	3	20	15	13
Key Value	17	0	15	0	19	17	0	15	0
Results	15	30	17	45	30	12	46	26	39
Plaintexs	M	E	E	T	I	N	G	O	N

Ciphertext	K	R	P	P	T
Key	T	R	A	P	A
Ciphertext value	10	17	15	15	19
Key Value	19	17	0	15	0
Results	17	26	41	26	45
Plaintexs	M	O	N	D	A

Ciphertext	I	R	D	P
Key	T	R	A	P
Ciphertext value	8	17	3	15
Key Value	19	17	0	15
Results	15	26	29	26
Plaintexs	Y	A	T	T

Ciphertext	H	T	I	I
Key	A	T	R	A
Ciphertext value	7	19	8	8
Key Value	0	19	17	0
Results	33	26	17	34
Plaintexs	H	E	O	F

Ciphertext	H	E	G	Z	N
Key	P	A	T	R	A
Ciphertext value	7	4	6	25	13
Key Value	15	0	19	17	0
Results	18	30	13	34	39
Plaintexs	O	F	F	I	C

So the result of the description of the message "GEGTXDUPN KRPPT IRDP HTII HEGZN" is “MEETING ON MONDAY AT THE OFFICE”.

Message extraction process in images:

a. Convert Color Components to Binary:
R (Red) = 25 converted to binary to 11001
G (Green) = 67 converted to binary to 1000011
B (Blue) = 65 converted to binary to 1000001

b. Take the last bit of each color component:
R: 1 G: 0 B: 0

c. Group the bits into each message character in binary form:
G: 1 E: 0 G: 0 T: 1 X: 0

D: 1 U: 0 P: 0 N: 0
K: 1 R: 0 P: 0 P: 0 T: 1
I: 1 R: 0 D: 1 P: 0
H: 1 T: 0 I: 1 I: 1
H: 1 E: 0 G: 0 Z: 1 N: 0

d. Convert binary to ASCII value:
G: 71 E: 69 G: 71 T: 84 X: 88
D: 68 U: 85 P: 80 N: 78
K: 75 R: 82 P: 80 P: 80 T: 84
I: 73 R: 82 D: 68 P: 80
H: 72 T: 84 I: 73 I: 73
H: 72 E: 69 G: 71 Z: 90 N: 78

Thus, the message extracted from the image is "GEGTXDUPN KRPPT IRDP HTII HEGZN".

3.3. System Display Results

The following is a display of the system that has been successfully created by researchers.

a. Main page display
This display is the main interface of the application, where users are given the option to choose whether they want to carry out the encryption or decryption process.

b. Encryption page display
The visible display is the interface for the encryption process. In it, the user is asked to enter an image file that will be used as a message container, create the plaintext or original data to be conveyed, and include a key. After these steps are carried out, the system will generate a ciphertext from the original data.

c. The display selects the image file you want to encrypt
The display that is visible is the interface for selecting the image file that will be used as a place to insert the message. After the user clicks on this option, the system will direct him to the directory of the device being used.\

d. Encryption results page
The display that is visible is an interface that displays the results of the message encryption process that has been inserted into the image file. To generate ciphertext and insert a message in an image file, the user needs to enter the message to be conveyed and a key in the system interface. After these steps have been successfully carried out, the user only needs to "submit", and the image file and key will be automatically downloaded to the user's device.

Analyzes the effectiveness of combining two security techniques to enhance data confidentiality and concealment. The Vigenere Cipher, a classical encryption method, encrypts the text, which is then hidden within an image using Least Significant Bit (LSB) steganography. This dual-layer approach significantly increases the difficulty for unauthorized parties to detect and decipher the message, making it particularly useful in scenarios requiring both security and stealth. However, the research highlights that the effectiveness of this method depends on careful implementation, including the choice of a strong keyword for the cipher and an appropriate image for steganography. While this combination offers robust protection, it is also vulnerable to advanced cryptanalysis and steganalysis techniques, suggesting the need for further research to improve its resistance and explore alternative cryptographic methods.

4. CONCLUSION

After investigating the implementation of data security using LSB steganography and Vigenere Cipher encryption, the conclusion is that the use of the Vigenere Cipher method and steganography in combination is able to provide a layer of security for messages embedded in images. This makes the message scrambled and can be returned to its original form without changes to the message text. The test results show that the file size after the message insertion process increases compared to the original file size, and this increase in size depends on the number of messages inserted. This research is able to measure the extent to which text messages can be inserted into images without sacrificing the visual quality of the image. Even though the image size is larger than the original file, the visual quality of the image is still maintained. Future work could focus on developing more sophisticated methods to choose keywords dynamically, improving the resistance of the Vigenere Cipher to cryptanalysis, and enhancing the robustness of LSB steganography against steganalysis attacks. Additionally, exploring the use of alternative cryptographic algorithms in conjunction with steganography could further improve security.

REFERENCES

[1] I. Keshta *et al.*, "Blockchain aware proxy re-encryption algorithm-based data sharing scheme," *Phys. Commun.*, vol. 58, 2023, doi: 10.1016/j.phycom.2023.102048.

[2] L. Shen *et al.*, "SPEFL: Efficient Security and Privacy-Enhanced Federated Learning Against Poisoning Attacks," *IEEE Internet Things J.*, vol. 11, no. 8, pp. 13437 – 13451, 2024, doi: 10.1109/JIOT.2023.3339638.

[3] W. M. Wilda and L. Hanum, "Information System Application Alanysis And Design Web-Based Network Complaints Using Php And Bootsrap On Diskominfo," *J. Inf. Syst. Technol. Res.*, vol. 1, no. 2, pp. 68–78, May 2022, doi: 10.55537/jistr.v1i2.131.

[4] W. Bai, J. Blocki, and M. H. Ameri, "Cost-asymmetric memory hard password hashing," *Inf. Comput.*, vol. 297, 2024, doi: 10.1016/j.ic.2023.105134.

[5] M. Ramzan and M. F. Khan, "A Robust Steganographic Algorithm based on Linear Fractional Transformation and Chaotic Maps," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 3, pp. 452 – 461, 2023, doi: 10.14569/IJACSA.2023.0140351.

[6] B. Mennink, "Encryption and Security of Counter Mode," in *Symmetric Cryptography 1: Design and Security Proofs*, 2024. doi: 10.1002/9781394256358.ch11.

[7] M. L. A. S. Lutfil, Samsudin, and Triase, "Application Of The Triple Exponential Smoothing Method In Predicting Electronic Equipment Inventory Based On Customer Demand," *J. Inf. Syst. Technol. Res.*, vol. 2, no. 2, pp. 54–65, 2023, doi: 10.55537/jistr.v2i2.616.

[8] R. Gafni, I. Aviv, and D. Haim, "Multi-Party Secured Collaboration Architecture from Cloud to Edge," *J. Comput. Inf. Syst.*, 2023, doi: 10.1080/08874417.2023.2248921.

[9] M. S. Sumathi, J. Shruthi, V. Jain, G. K. Kumar, and Z. Z. Khan, "Using Artificial Intelligence (AI) and Internet of Things (IoT) for Improving Network Security by Hybrid Cryptography Approach," *Evergreen*, vol. 10, no. 2, pp. 1133 – 1139, 2023, doi: 10.5109/6793674.

[10] A. R. Mido and E. I. H. Ujianto, "Analisis Pengaruh Citra Terhadap Kombinasi Kriptografi RSA dan STEGANOGRAFi LSB," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 9, no. 2, p. 279, 2022, doi: 10.25126/jtiik.2022914852.

[11] A. Ikhwan, R. A. A. Raof, P. Ehkan, Y. Yacob, and M. Syaifuddin, "Data Security Implementation using Data Encryption Standard Method for Student Values at the Faculty of Medicine, University of North Sumatra," *J. Phys. Conf. Ser.*, vol. 1755, no. 1, 2021, doi: 10.1088/1742-6596/1755/1/012022.

[12] A. Patange *et al.*, "Advancements in optical steganography for secure medical data transmission in telehealth systems," *Opt. Quantum Electron.*, vol. 55, no. 9, 2023, doi: 10.1007/s11082-023-05080-5.

[13] A. Durafe and V. Patidar, "Image Steganography Using Fractal Cover and Combined Chaos-DNA Based Encryption," *Ann. Data Sci.*, vol. 11, no. 3, pp. 855 – 885, 2024, doi: 10.1007/s40745-022-00457-x.

[14] Z. Safaa and M. Khaire, "Image steganography using exploiting modification direction for compressed encrypted data," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2951–2963, 2022, doi: 10.1016/j.jksuci.2019.04.008.

[15] Fina Triana, Jon Endri, and Irma Salamah, "Implementation of CAESAR CIPHER Cryptography Techniques for Android Based Information Data Security," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 627–634, Aug. 2020, doi: 10.29207/resti.v4i4.1984.

[16] D. H. Pane, "IMPLEMENTASI KRIPTOGRAFI KEAMANAN DATA RESI PADA PT JNE PERBAUNGAN MENGGUNAKAN METODE MERKLE HELLMAN," *DEVICE J. Inf. Syst. Comput. Sci. Inf. Technol.*, vol. 1, no. 1, Jun. 2020, doi: 10.46576/device.v1i1.695.

[17] A. Z. F. Rangkuti and H. Fahmi, "Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 170–175, 2020, doi: 10.32672/jnkti.v3i2.2384.

[18] J. Karman and A. Nurhasan, "PERANCANGAN SISTEM KEAMANAN DATA INVENTORY BARANG DI TOKO NANDA BERBASIS WEB MENGGUNAKAN METODE KRIPTOGRAFI VIGENERE CIPHER," *J. Teknol. Inf. MURA*, vol. 11, no. 1, pp. 29–36, Jun. 2019, doi: 10.32767/jti.v11i1.451.

[19] Y. Wiharto and A. Irawan, "Sistem Kehadiran Menggunakan Quick Respone Code Dengan Enkripsi Algorithm Message Digest 5 dan Vigenere Cipher Pada SpeedCom IT Consulting," *J. SISKOM-KB (Sistem Komput. dan Kecerdasan Buatan)*, vol. 2, no. 1, pp. 42–56, 2018.

[20] A. Fadlil, I. Riadi, and A. Nugrahantoro, "Kombinasi Sinkronisasi Jaringan Syaraf Tiruan dan Vigenere Cipher untuk Optimasi Keamanan Informasi," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 1, pp. 81–95, May 2020, doi: 10.31849/digitalzone.v11i1.3945.

[21] Minarni and R. Redha, "Implementasi Least Significant Bit (LSB) dan Algoritma Vigenere Cipher Pada Audio Steganografi," *J. Sains dan Teknol. J. Keilmuan dan Apl. Teknol. Ind.*, vol. 20, no. 2, pp. 168–174, 2020.

[22] R. I. Perwira, D. B. Prasetyo, and F. A. J. Haryanto, "STEGANOGRAFI DENGAN AES PADA MEDIA SUARA BERBASIS INTERNET," *Telematika*, vol. 17, no. 1, p. 18, Apr. 2020, doi: 10.31315/telematika.v17i1.3401.

[23] R. N. Pahlawan, R. Y. Dillak, and J. Sine, "APLIKASI KRIPTOGRAFI ALGORITMA RIVEST-SHAMIR-ADLEMAN DAN RIVEST CODE 4 PADA STEGANOGRAFI CITRA METODE LEAST SIGNIFICANT BIT," *J. Ilm. Flash*, vol. 5, no. 1, p. 05, Jun. 2019, doi: 10.32511/flash.v5i1.626.

[24] P. Bagane *et al.*, "Securing Data in Images Using Cryptography and Steganography Algorithms," *Int. J. Intell. Syst.*

Appl. Eng., vol. 12, no. 15s, pp. 17 – 25, 2024, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85187453046&partnerID=40&md5=2d6062d35dbc521a5e6023ddeb031f06

[25] L. Negi and L. Negi, “Image Steganography Using Steg with AES and LSB,” in *7th International Conference on Computing, Engineering and Design, ICCED 2021*, 2021. doi: 10.1109/ICCED53389.2021.9664834.

[26] F. Varghese and P. Sasikala, “Secure Data Transmission Using Optimized Cryptography and Steganography Using Syndrome-Trellis Coding,” *Wirel. Pers. Commun.*, vol. 130, no. 1, pp. 551 – 578, 2023, doi: 10.1007/s11277-023-10298-3.

[27] A. Mehmood, A. Shafique, M. Alawida, and A. N. Khan, “Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques,” *IEEE Access*, vol. 12, pp. 27530 – 27555, 2024, doi: 10.1109/ACCESS.2024.3367232.

[28] A. Aldo and L. Hakim, “IMPLEMENTASI STEGANOGRAFI PADA CITRA DIGITAL DAN KRIPTOGRAFI ALGORITMA HILL CHIPPER UNTUK PENGAMANAN INFORMASI BERUPA TEXT,” *J. Ilm. Teknol. Infomasi Terap.*, vol. 5, no. 1, pp. 6–17, Aug. 2019, doi: 10.33197/jitter.vol5.iss1.2018.247.

[29] E. Pujiastuti, “Penyembunyian Pesan dalam Gambar dengan Teknik Steganografi menggunakan Matlab 7.7. 0,” *J. Tek. Inform.*, vol. 4, no. 1, pp. 51–56, 2018.