Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2025. Vol. 5. No. 1; e-ISSN: 2808-4519

Steganography Software for Hiding Message in Digital Image by using Five Modulus Method

Nichander Chiunata[1]*, Octara Pribadi[2], Feriani Astuti Tarigan[3]

[1,2] Informatics Engineering, STMIK TIME, Medan
[3]Information System, STMIK TIME, Medan
Nichander.ciu55@gmail.com[1*], octarapribadi@gmail.com[2], Ferianiastutitime@gmail.com[3]

Abstract

Steganography is a technique for concealing information within digital media to prevent unauthorized detection. This research presents the design of a text hiding system using the Five Modulus Method (FMM) applied to digital images. The method utilizes modulus 5 operations on pixel values to embed secret messages discreetly while preserving the visual quality of the image. The developed system includes features for embedding, extracting, and comparing images to evaluate the results. The test results show that the FMM method successfully embeds text messages with minimal changes to the original image, demonstrated by PSNR values exceeding 40 dB in most tests. The extraction process also accurately retrieves the hidden messages as long as the image remains unaltered. However, this method has limitations in data capacity and is vulnerable to lossy compression. This study concludes that the FMM method is effective for hiding small to medium-sized messages and is suitable for lightweight secure communication applications.

Keywords: *Steganography, Five Modulus Method, Text embedding, Digital image, PSNR.*

1. Introduction

In today's world, technological advancements are progressing at an unprecedented pace. Nowadays, sharing information has become incredibly easy through applications developed by humans, which greatly facilitate people's ability to interact with one another without the constraints of time and distance. With the availability of applications that help people send information quickly, the security of information transmission is likely to decrease. Therefore, the author has developed an application using text-based information storage techniques within images to enhance security when sending highly important information[1].
Steganography, or the concealment of information or secrets within digital media to prevent unauthorized detection or access, is a key focus of the author's current research. Some of the objectives of steganography include privacy protection, information security, and confidential communication[2]. With steganography, important information can be sent or stored without being easily detected, making it suitable for use in various applications, such as data security, confidential communication, and digital copyright protection.
The method used in this study to embed important data or text into a message is the 5-modulus method, which involves modifying specific pixels by 5 and utilizing the results to determine
pixel value changes[3]. In addition to the above method, there are several other methods that can be used to store text in digital media, such as the Spectrum Method and the RPE (Redundant Pattern Encoding) Method[4]. By using these methods, users can hide messages by distributing them across the entire frequency spectrum of the host medium, or they can use audio files as a medium for storing text or confidential information[5].
Therefore, the author chose the title using the 5-modulus method to determine whether the data embedded into digital media can function effectively according to the desired results without compromising the intent or information embedded into the digital media.

2. Theoretical Basis

2.1. Steganography

Steganography comes from Greek, namely steganos, which means “hidden” or “protected,” and graphia, which means “writing.” In general, steganography is the science and art of hiding information in other media so that the existence of that information is not detected by other parties. The media used can be text, images, audio, video, or even network protocols.

2.2. Digital Images

A digital image is a rectangular representation of numbers that indicate luminance and color at specific locations within a scene. This image can be viewed as a pixel matrix, where each pixel has three numerical values that are usually associated with color channels. The coordinates of each pixel indicate its spatial position, while its numerical values represent the color intensity at that location. These values depend on the color model used, such as RGB (red, green, blue) or YCC (luminance and two chromaticity components).

2.3. Image File Format

An image file format is a standard or set of rules used to store visual data in digital form. This format determines how image information, such as color, pixels, and metadata, is organized and stored in a file. Each image file format has different compression methods, quality levels, and features that make it suitable for specific purposes, such as web use, printing, or animation.

2.4. Image Resolution

Resolution relates to the ability to distinguish two adjacent pixels as separate entities, so it can be defined that resolution reflects the level of detail that an image can display. This concept is closely related to spatial frequency, which is how fast signal changes occur in space. In the context of spatial frequency, the signal describes variations in brightness with two main values: 0 (minimum brightness) and maximum.

3. Analysis

In systems engineering and software engineering, requirements analysis encompasses various tasks aimed at determining the requirements or conditions that must be met by a new or modified product or project. This process involves analyzing potentially conflicting requirements from various stakeholders, as well as analyzing, documenting, validating, and managing software or system requirements.
Requirements analysis is critical to determining the success or failure of a system or software project. Requirements must be well documented, actionable, measurable, testable, traceable, related to identified business needs or opportunities, and defined in sufficient detail to support the system design process.
Requirement analysis for the proposed system covers two main aspects, namely functional requirement analysis and non-functional requirement analysis.
Functional software analysis can be explained using use cases as illustrated in Figure 3.3 below:

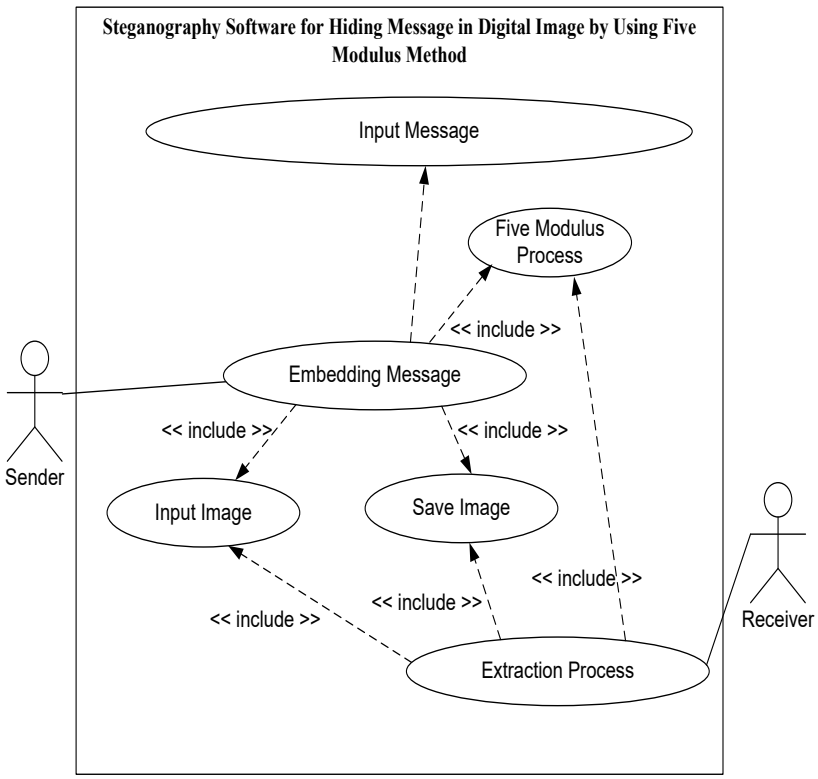

Fig 1: Case Diagram of Using Steganography Software to Hide Messages in Digital Images Using the Five Modulus Method.

4. A Results and Discussion

4.1. Results

The results of the researcher's study are shown in the following explanation

1. Initial Menu Display This form is the main form of the application used to connect other forms in this application. The design of the 'Main' form can be seen in the image below:

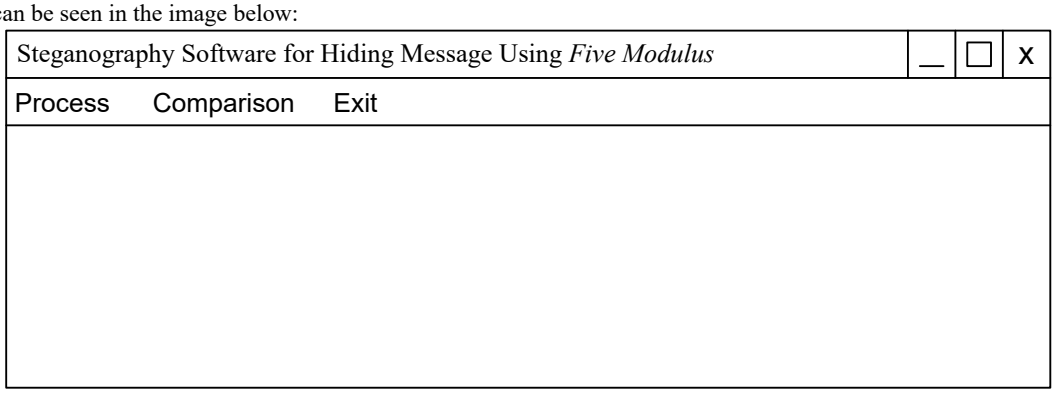

Fig 2: Menu Form Design.

2. Embedding Form Display

This form is used to embed secret messages into cover images. The 'Embedding' form design is as shown in the image below:

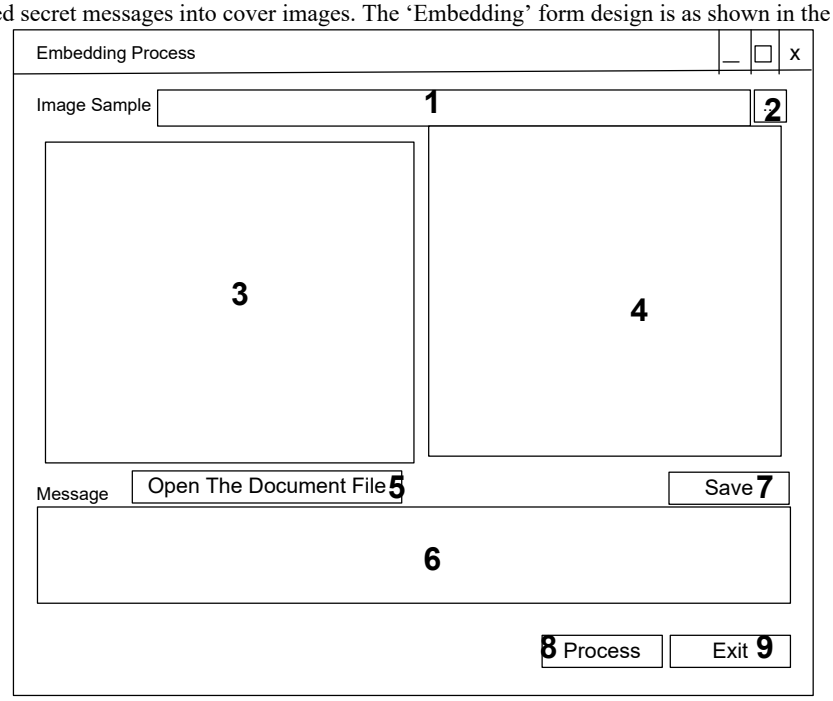

Fig 3: Embedding Form Design Display.

3. Extraction Form

This form is used to extract secret messages from stego images. The design of the 'Extraction' form is shown in the image below:

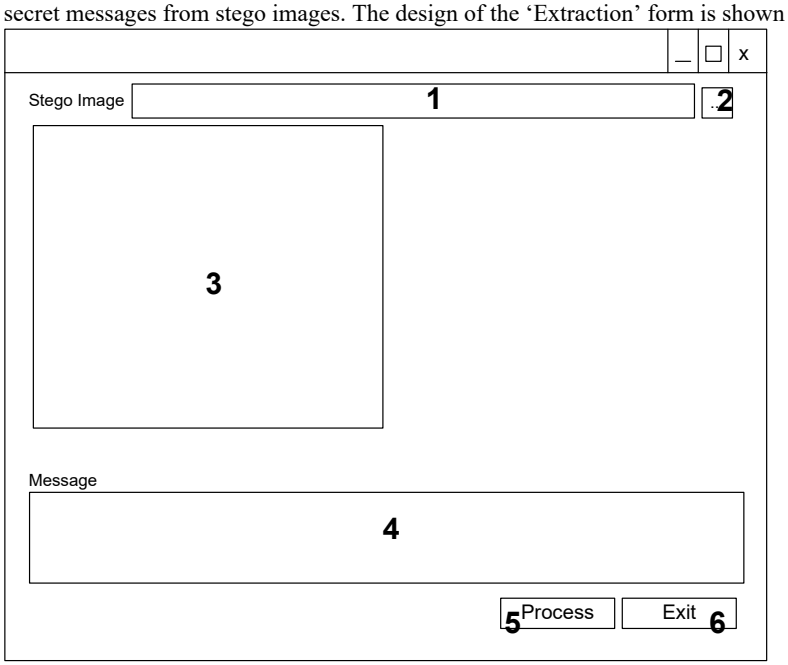

Fig 4: Extraction Embedding Form Design Display.

4. Comparison Form

This form is used to compare the differences between the original image and the stego image. The design of the 'Comparison' form can be shown as in the image below:

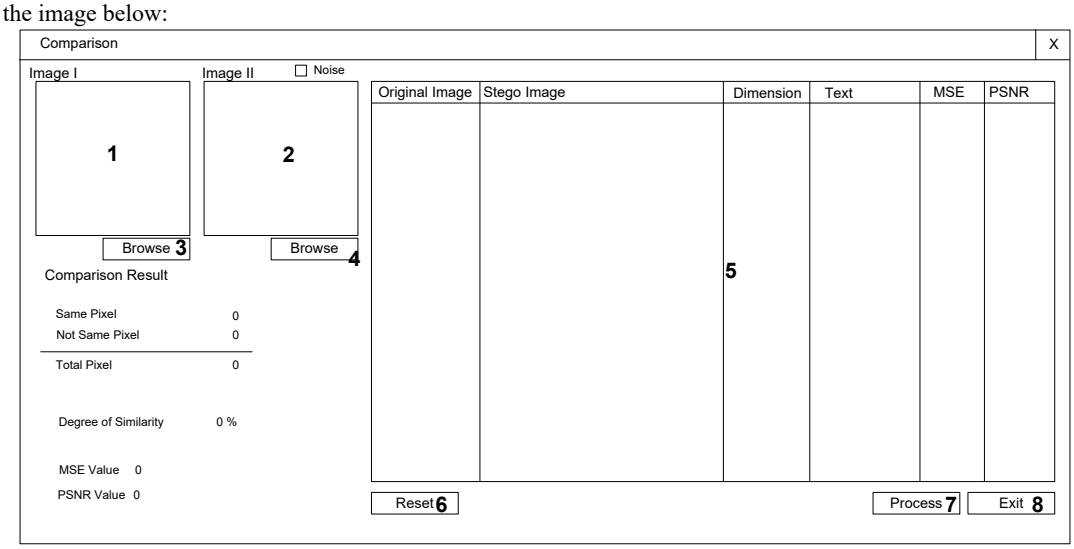

Fig 5: Comparison Form Display.

4.2. Discussion

This discussion provides an analytical explanation of the results of implementing a text storage system in images using the Five Modulus Method (FMM). The main focus is on the effectiveness of the algorithm, the visual quality of the stego image, the insertion capacity, and the reliability of message extraction.

1. Effectiveness of the Insertion Process

The implementation of the FMM algorithm demonstrates that the embedding process can be performed quickly and efficiently. This is because pixel transformation only requires basic mathematical operations (modulus and pixel value adjustment), resulting in relatively low computational load. Experimental results show that the application can embed short to medium-length text messages in less than one second.

2. Visual Quality of Steganographic Images

Based on the PSNR values obtained from testing, the embedded image (stego image) shows no significant visual differences compared to the original image. This indicates that the FMM method effectively preserves image visual quality, as pixel value changes are limited to minor adjustments to make them multiples of five. In many cases, PSNR values exceed 40 dB, which is categorized as high quality.

3. Embedding Capacity

The embedding capacity of the FMM method depends on the number of pixels in the image and the number of pixel positions that are not divisible by five ($\text{mod} \neq 0$). Although this method is relatively safe and does not compromise the visual quality of the image, its embedding capacity is limited, especially when used on small-sized images. This becomes a limitation when attempting to embed a large number of messages.

4. Extraction Reliability

Extraction test results show that text characters can be fully recovered and match the original data, provided the stego image has not been modified or recompressed. This indicates that the FMM method is sufficiently reliable for secret communication as long as the image file is not altered by a third party.

5. Security Analysis

The FMM method is fairly secure against visual detection, but it is not resistant to statistical-based steganalysis techniques or image manipulation such as JPEG compression. This is because the modified pixel structure may undergo changes if lossy compression is applied, leading to extraction failure. Therefore, the system is more suitable for use with lossless image formats such as PNG.

6. Comparison with Other Methods

When compared to the LSB (Least Significant Bit) method, the FMM method is more stable in terms of pixel data structure because the changes made are more controlled. However, LSB still has an advantage in terms of insertion capacity because it can utilize more bits per pixel.

5. Conclusion

Based on the design, development, and implementation stages of the steganography system using the 5 modulus method, a number of conclusions were obtained that summarize the effectiveness and performance of the method used as follows: The Five Modulus method shows efficient performance in terms of processing time, so that the insertion process can be carried out quickly. Increasing the length of the embedded message results in a decrease in the visual quality of the stego image, as the number of modified pixels increases. The message embedding process is performed with minimal changes to pixel values, so there are no significant visual differences between the original image and the stego image. This method is suitable for embedding small to medium-sized messages, but is less optimal for embedding large amounts of data without compromising image quality.

Acknowledgement

Referring to the results of the implementation and evaluation of the performance of the five modulus method, several development steps are recommended to improve the effectiveness and quality of the system in the future, such as:

1. This application can be improved by adding interactive guide or tutorial features to make it easier for users to understand the workflow of the five modulus method.
2. Application development can also be directed toward integrating comparisons between the five-modulus method and other steganography methods, so that the advantages and limitations of each method can be analyzed more objectively.
3. It is recommended to integrate encryption algorithms before the insertion process to better protect the security of confidential messages from unauthorized parties.
4. The application can be further developed by adding a simple steganalysis feature to test how resistant the Five Modulus method is to hidden message detection techniques.
2. It is recommended to add an automatic validation mechanism for the length of the message to be inserted, so that users do not enter a number of characters exceeding the available image capacity.

References

[1.] S. R. G. W. S. Oman Sumantri, “102820,” vol. 67, pp. 1–7, 2015.
[2.] D. Darwis and K. KISWORO, “Teknik Steganografi untuk Penyembunyian Pesan Teks Menggunakan Algoritma End Of File,” Explor. J. Sist. Inf. dan Telemat., vol. 8, no. 2, 2017, doi: 10.36448/jsit.v8i2.950.
[3.] P. Hasan, S. Yunita, and D. Ariyus, “Implementasi Hill Cipher Pada Kode Telepon dan Five Modulus Method dalam Mengamankan Pesan,” Sisfotenika, vol. 10, no. 1, p. 12, 2020, doi: 10.30700/jst.v10i1.521.
[4.] F. C. Venna, “Implementasi Steganografi Audio pada File Wav dengan metode Redundant Pattern Encoding (RPE) Berbasis Sndroid,” Repository.Uinjkt.Ac.Id, 2019, [Online]. Available: http://repository.uinjkt.ac.id/dspace/handle/123456789/47958
[5.] S. Rahma and A. Prapanca, “Analisis Kompresi dan Dekompresi Data Teks dan Audio dengan Algoritma Run Length Encoding (RLE),” J. Informatics Comput. Sci., vol. 2, no. 04, pp. 313–320, 2021, doi: 10.26740/jinacs.v2n04.p313-320.
[6.] A. Saefullah, Himawan, and N. Agani, “Aplikasi Steganografi Untuk Menyembunyikan Teks Dalam Media Image Dengan Menggunakan Metode LSB,” Semin. Nas. Teknol. Inf. Komun. Terap. 2012 (Semantik 2012), vol. 2012, no. Semantik, pp. 151–157, 2012.
[7.] Asiva Noor Rachmayani, “No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title,” p. 6, 2015.
[8.] E. S. Wijaya and Y. Prayudi, “Konsep Hidden Message Menggunakan Teknik,” Media Inform., vol. 2, no. 1, pp. 23–38, 2004.
[9.] M. M. T. Dr. Mars Caroline Wibowo. S.T., Teknologi Gambar Digital. 2021.
[10.] F. N. S. Damanik, A. A. Lubis, B. E. Ezer, and H. W. Siregar, “Perbandingan Kompresi Citra Metode Five-Modulus dan Kuantisasi dengan Perbaikan Citra Histogram-Equalization,” J. SIFO Mikroskil, vol. 18, no. 1, pp. 57–70, 2017, doi: 10.55601/jsm.v18i1.435.
[11.] F. A. Jassim, “A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method,” vol. 72, no. 17, pp. 39–44, 2013, [Online]. Available: http://arxiv.org/abs/1307.0642
[12.] R. K. Ramesh, R. Dodmane, S. Shetty, G. Aithal, M. Sahu, and A. K. Sahu, “A Novel and Secure Fake - Modulus Based Rabin - 3 Cryptosystem,” 2023.
[13.] S. Shah, N. Bhuiyan, N. A. Malek, O. O. Khalifa, F. Diyana, and A. Rahman, “An Improved Image Steganography Algorithm based on PVD,” vol. 10, no. 2, pp. 569–577, 2018, doi: 10.11591/ijeecs.v10.i2.pp569-577.
[14.] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, “applied sciences Image Steganography Using LSB and Hybrid Encryption Algorithms,” 2023.
[15.] A. Durafe and V. Patidar, “Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover,” J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 7, pp. 4483–4498, 2022, doi: 10.1016/j.jksuci.2020.10.008.