Instal : Jurnal Komputer

E-ISSN: 2808-683X
Edisi : Volume xx Nomor xx | Bulan 2024

Available online at https://journalinstal.cattleyadf.org/index.php/Instal/index

WEBSITE SECURITY AND HIDING OF SECRET MESSAGES WITH RC4 METHOD AND ADAPTIVE PATTER

Luthfi Ahmad Rifqi [1], T.M Diansyah [2], Imran Lubis [3]
[1,2,3]Universitas Harapan Medan, Medan, Indonesia

ARTICLE INFO

Article history:

Received :
Revised :
Accepted :

Keywords:

Steganography,
RC4 Method,
Adaptive Pattern,

ABSTRACT

The application of technology in the field of data and information security has been carried out a lot. Threats to information security can occur when the information sent is not addressed to everyone but only to certain people, especially if the information provided is confidential. Currently there have been many crimes in cyberspace, where confidential information can be taken by a hacker without being noticed. This raises concerns for the owner of the confidential information. So the purpose of this thesis research is to create a Website for Security and Concealment of Secret Messages with the RC4 Method and Adaptive Pattern which aims to keep secret or hide hidden information so that it is not spread to other unauthorized parties. In the research that has been done, the messages that have been entrusted do not make significant changes to other digital data. It would not physically attract the attention of a potential attacker or hacker, for example an image that looks harmless or not potentially attackable.

Corresponding Author:
Luthfi Ahmad Rifqi
Universitas Harapan Medan
Email: Luthfiahmadrifqi@gmail.com

INTRODUCTION

The development of information technology in this modern era is very rapid, this is due to the existence of tools (computers) that can be used to process and process data. Now computers have utilized basic technology in processing and presenting information. A company or institution can make the right decision supported by aspects of information technology that are expected to be able to handle problems quickly, accurately and efficiently. The security of information in this global era makes it a vital need in various aspects of life. Information will have a higher value if it includes aspects of business decisions, security, or public interest. Wherever the information is, of course, it will be in great demand by various parties who also have interests in it. For that, one way of security that can be done is to use steganography techniques, which are a technique for hiding information behind cover media such as images so that the actual information or data is not visible and does not have a bad impact on others. Security will be more robust by combining steganography and cryptography techniques, where if the hidden secret information can be detected by irresponsible information parties,

Page : x-x
Doi.

then the secret is still protected by a cryptography method. Through previous research, the two data security techniques will be combined. The case discussed in this study is the security of secret messages using RC4 and adaptive patterns. The media used to store secret messages is a digital image. This is because of the limitations of human sensitivity in terms of visualization systems (Angraini & Utami, 2017). There are a number of main criteria in producing good stego media, namely imperceptible, fidelity and recovery. Imperceptible means that the existence of a secret message cannot be perceived by the senses, in the sense that the stego media containing the message, visually or audio-visually, is difficult to distinguish from the cover media. Fidelity means that the quality of the media does not change much after the message is hidden, and recovery means that the hidden secret message can be reappeared. The recovery aspect in question is that the secret message must be able to be revealed again. Ensuring that the secret data inserted in the digital image can be retrieved intact. The most important criterion of the steganography method is imperceptible (Rihartanto, et al., 2019). To improve the imperceptible nature of the steganography method, a steganography method using adaptive patterns can be applied. Based on the test results, the steganography method with adaptive patterns is able to increase the PSNR value from 52.49 to 57.45 and the SSIM value from 0.9991 to 0.9999. Meanwhile, to increase the level of security, the steganography method can be combined with a cryptography method. One method that can be applied is the RC4 method. The working process is to secure the secret message by using the RC4 method first. Then, the adaptive pattern steganography method is used to hide the encrypted ciphertext into a cover image. Based on the description above, the author is interested in applying the steganography method using adaptive patterns by taking a thesis entitled "Website Security and Hiding Secret Messages with the RC4 and Adaptive Pattern Methods".

METHODS

Process analysis explains how the system works, how the developed application can hide secret messages in images. The main process carried out is divided into two stages, namely: the attachment stage and the extraction stage. Flowchart of the analysis of the process of the website hiding secret messages in images with the RC4 method and steganography using Adaptive Pattern.

Needs Analysis

System requirement analysis is an overall description of how a system works well seen from non-functional analysis and functional analysis consisting of software analysis and hardware analysis as well as analysis of the users involved. Functional requirements are requirements that are reviewed from all entities that interact with the system. Functional requirements will be described in the form of a use case diagram.

Page : x-x
Doi.

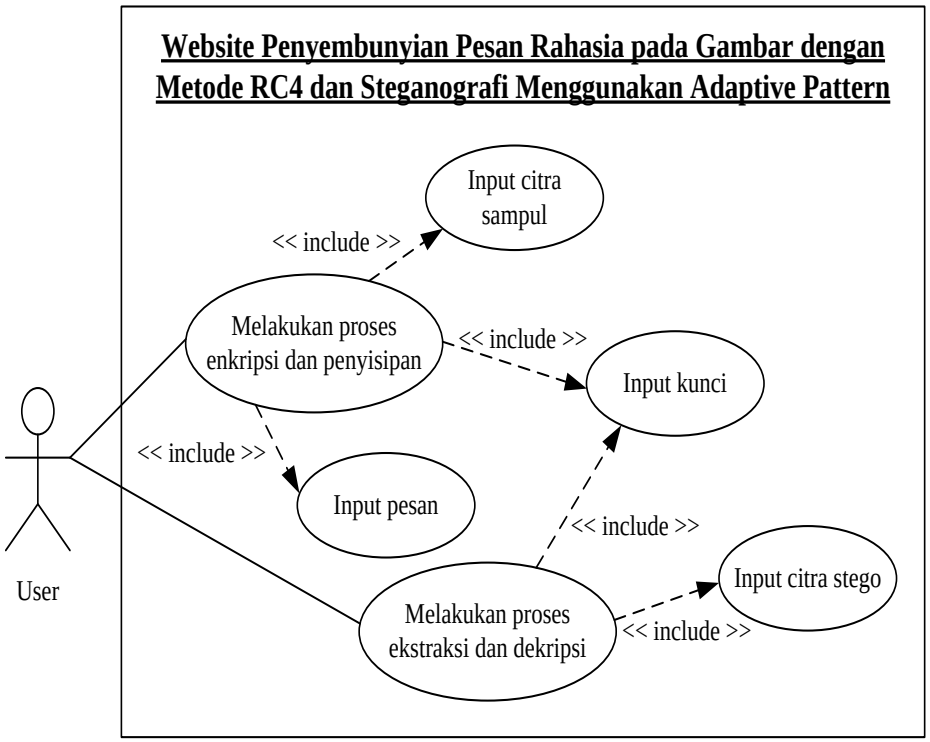

Figure 1. Use Case Website Hiding Secret Messages

RESULTS AND DISCUSSION

o use this software, run the browser by accessing the address "http://localhost/adaptive_pattern/index.php", then the main display of the program will be displayed.

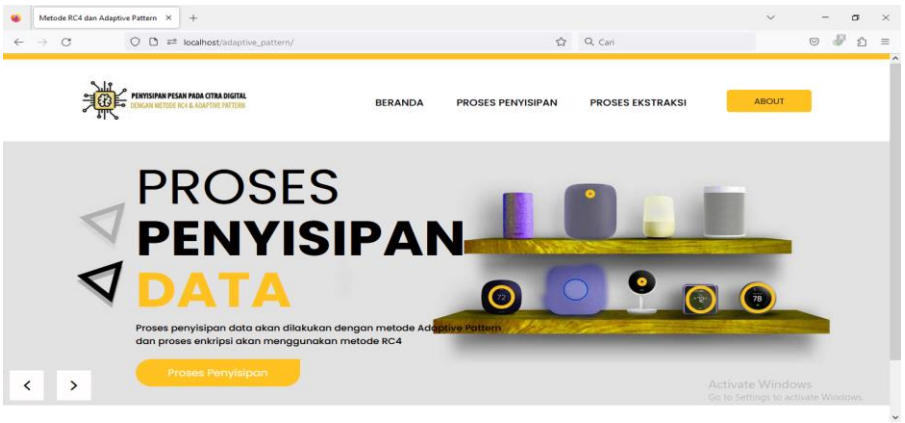

Figure 2. Main View

In this main display there are several menus that function to access the pages contained in the system. The following are details of the links contained in the system:

1. Insertion Process

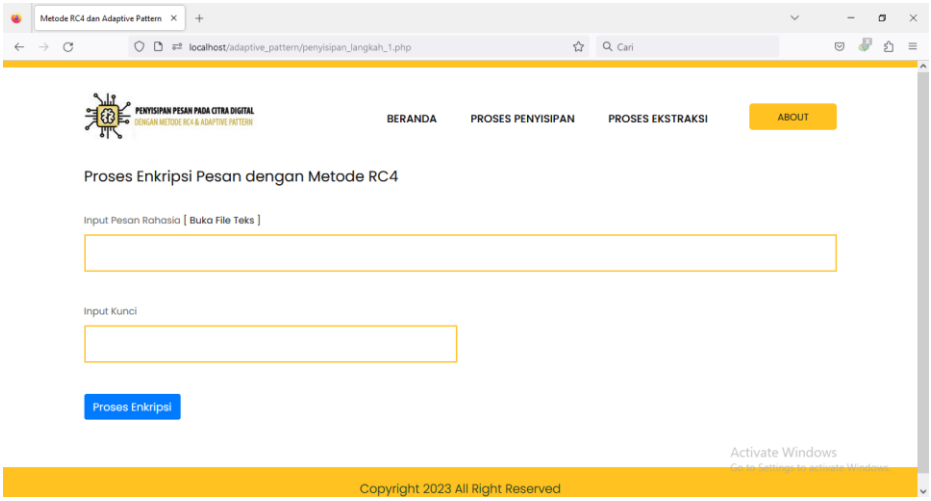

Figure 3. Insertion Process View Step 1

On this page, the user can enter a secret message to be encrypted using the RC4 method. To carry out the encryption process, a secret key is also required. After the user enters the secret message data and key, the user can click the encryption process button to start the encryption process. If the user wants to select a text file, they can click the open text file link, so that the system will display the file browse page.

2. Browse File Page View

Figure 4. Browse File Page View

3. Display Insertion Process Step 1 After Data Filling

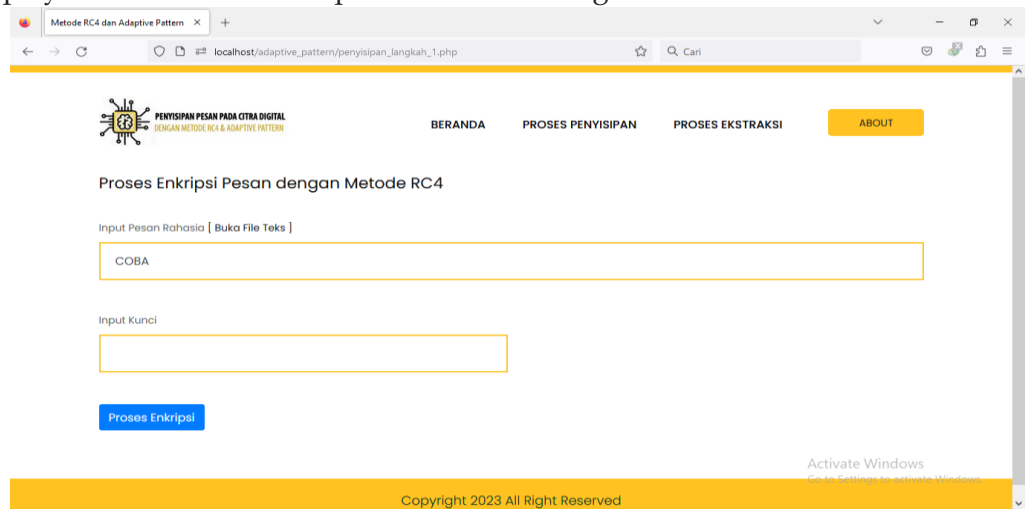

Figure 5. Display Insertion Process Step 1 After Data Filling

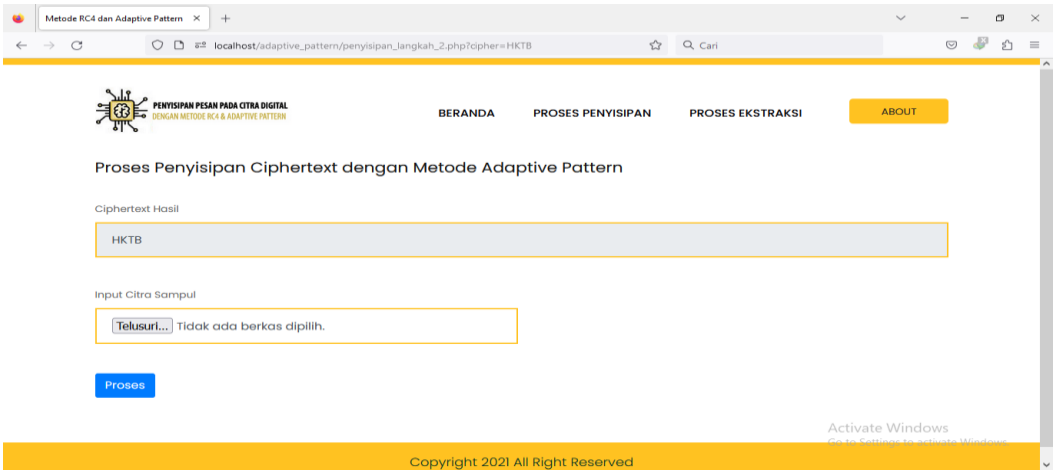

Figure 6. nsertion Process View Step 1

On this step 2 insertion process page, the user can see the ciphertext of the encryption results using the RC4 method. After that, the user can select the cover image file that will be used to accommodate the ciphertext. The way to do this is by clicking the browse button so that the system will display a dialog box.

4. Cover Image Selection Dialog Box Display

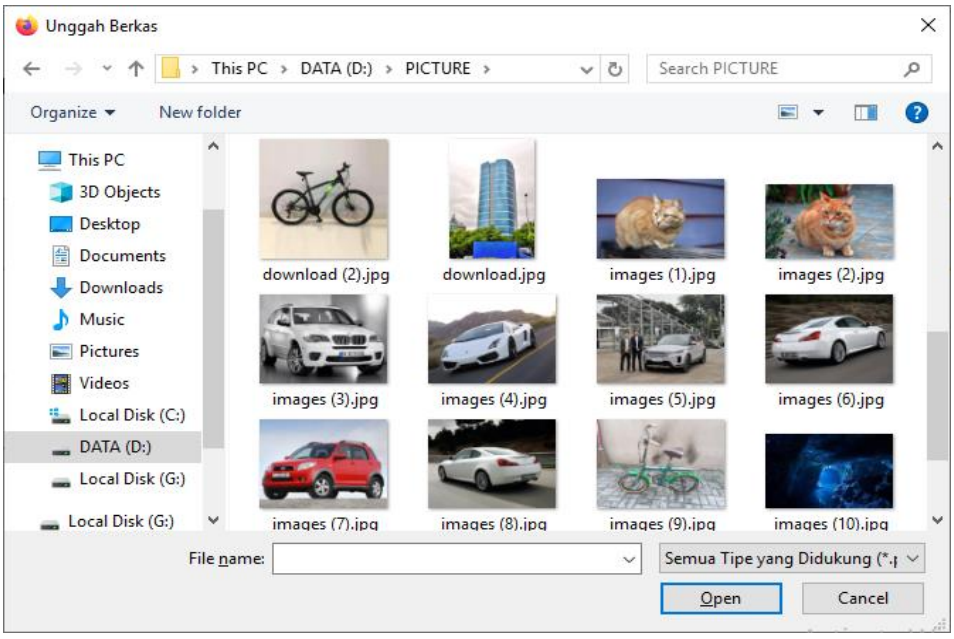

Figure 7. Cover Image Selection Dialog Box Display

Users can select the desired file and click the open button to read the image file. After that, users can click the process button on the insertion process page step 2 so that the system will insert the ciphertext into the cover image using the adaptive Pattern method.

5. Display a Notification Message That the Insertion Process is Complete

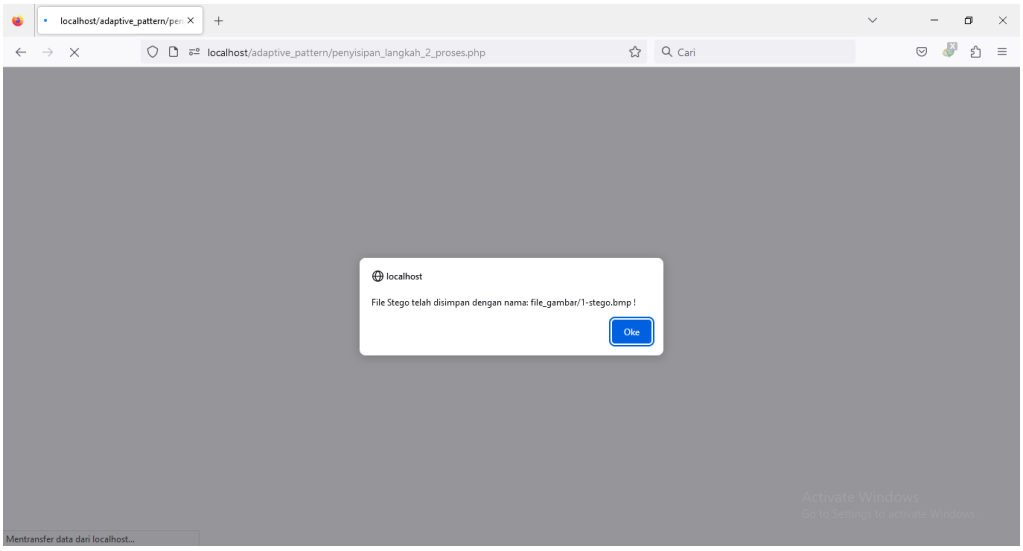

Figure 8. Display a Notification Message That the Insertion Process is Complete

The resulting stego image file along with the original image file will be saved in the image_file folder.

6. indows Explorer View Showing Original Image File and Stego Image File Information

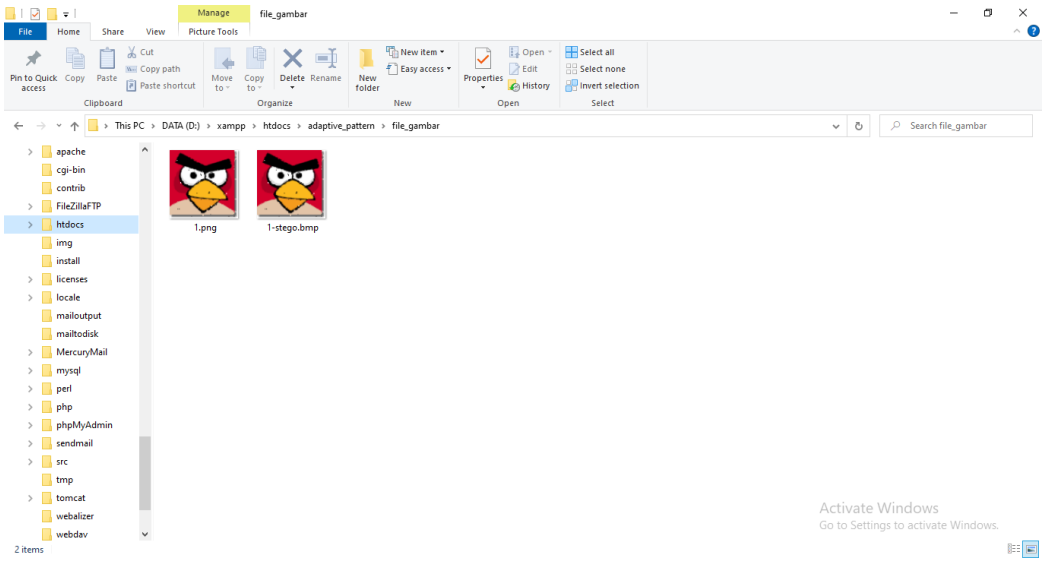

Figure 9. Windows Explorer View

Message Extraction Process

To carry out the message extraction process, you can click on the 'extraction process' menu, so that the system will display the extraction step 1 page. Users can select the stego image file whose ciphertext will be extracted by clicking the Browse button so that the system will display the stego image selection dialog box..

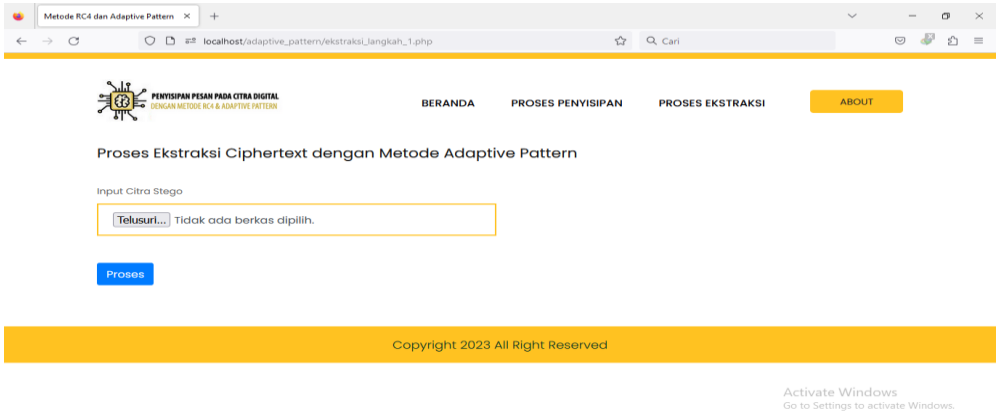

Figure 10. Extraction Process View Step 1

7. tego Image Selection Dialog Box Display

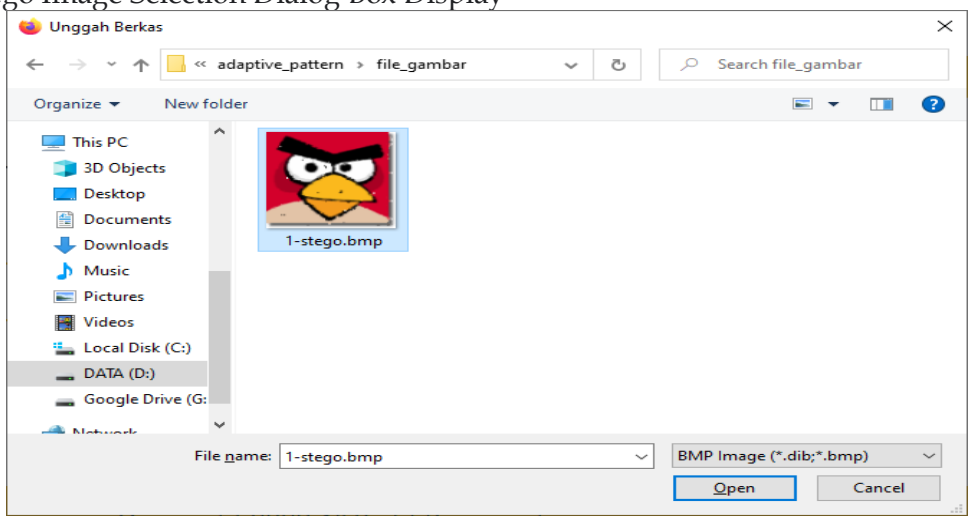

Figure 11. tego Image Selection Dialog Box Display

After that, the user can click the open button to open the selected stego image file. Then, the user can click the process button on the step 1 extraction page, so that the system will extract the ciphertext out of the stego image and display it on the step 2 extraction page.

8. Extraction Page View Step 2

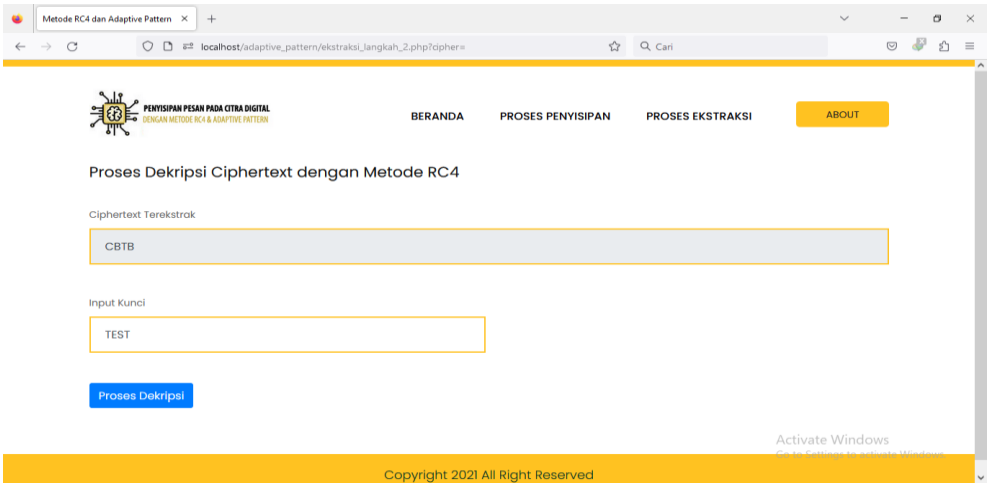

Figure 12. Extraction Page View Step 2

9. Extraction Page View Step 3

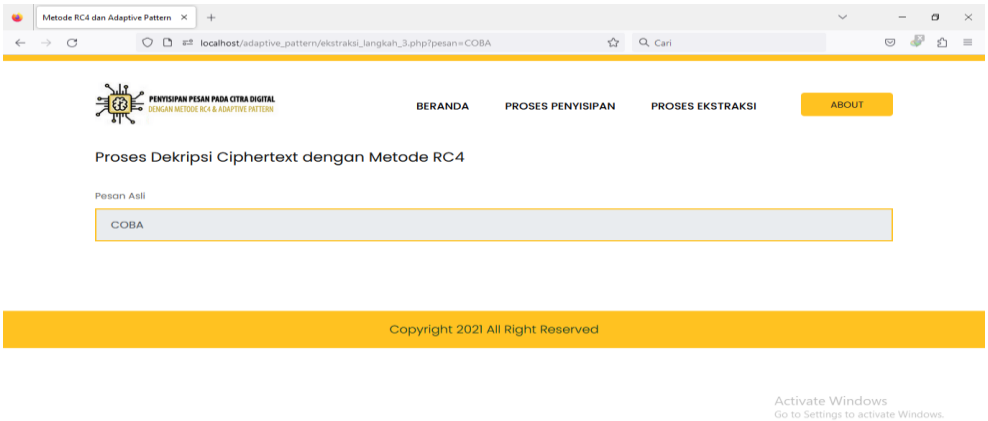

Figure 13. Extraction Page View Step 3

Discussion

The advantages of the program created are: The application can be used to hide secret messages in digital images. The difference in color between the input image and the output image is also not clearly visible. The disadvantages of the program created are: The output of the digital image is only in the form of a BMP format image, because the process of storing data in JPG format will change the color of the digital image pixels so that the inserted information is damaged or lost. The execution process for large images is relatively long.

CONCLUSION

After completing the creation of this software, the author can draw several conclusions as follows: 1. The process of inserting messages into images can be increased in security by using the RC4 encryption method. 2. The process of recovering secret messages that have been hidden in images will start from the process of extracting encrypted data from the stego image, then continued with the decryption process of the encrypted data to obtain the original secret message. 3. The steganography method using adaptive Pattern can be used to hide secret messages in images by inserting secret data into the pixel colors of the inserted image. While the author's suggestions are: The software can be further developed by adding other features such as a tutorial feature that is able to explain the working procedures of the algorithm discussed in detail. The software can be developed by comparing the steganography algorithm discussed with other similar algorithms to determine the advantages and disadvantages of the algorithm created.

REFERENCES

[1] Ardiansyah, A., & Kurniasih, M. (2018). Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganograpi Menggunakan Metode Least Significant Bit. *Jurnal Teknologi Informasi, XIII*(3), 96-101.

[2] Anggraini, Ema Utami. (2017). Analisis Penyisipan Data pada Citra Bitmap

[3] menggunakan Metode Bit Plane Complexity Segmentation, diakses pada tanggal17Februari2017,darihttp://p3m.amikom.ac.id/detail.php?id=62&Analisis-Penyisipan-Data-Pada-Citra-Bitmap-Menggunakan-Metode-Bit-Plane Complexcity-Segmentation.

[4] Ariyanto. (2020). Analisis Implementasi Algoritma Stream Cipher Sosemanuk dan Dicing dalam Proses Enkripsi Data. Seminar Nasional Informatika, 351-357.

[5] Fachri. (2020). Steganografi Citra Ke Dalam Citra Menggunakan Metode Least Significant Bit, Run-Length Encoding dan Linear Congruential Generator Steganography. 1–10.

[6] Furqan, M., Sriani, S., & Siregar, Y. K. (2020). Perbandingan Algoritma Contraharmonic Mean Filter dan Arithmetic Mean Filter untuk Mereduksi Exponential Noise. JISKA (Jurnal Informatika Sunan Kalijaga), 5(2), 107– 115. https://doi.org/10.14421/jiska.2020.52-05

[7] Ginni. (2022). E-filing of Taxes – A Research Paper. International Journal of Enterprise Computing and Business Systems Volume 2, Issue 1, January2012. pp1-8.

[8] Hastanti, R. P., Purnama, B. E., & Wardati, I. U. (2018). Sistem Penjualan Berbasis Web (E-Commerce) Pada Tata Distro Kabupaten Pacitan. *Jurnal Bianglala Informatika, 3*(2).

[9] Hermawati. (2020). Pengolahan Citra Digital, Yogyakarta.

[10] Ichsan. (2018). Perancangan dan Pembuatan Sistem Visual Inspection Sebagai Seleksi Buah Tomat Berdasarkan Kematangan Berbasis Web Camera.

[11] Karim. (2017). *Studi Dan Implementasi Penggabungan Steganografi Dan Kriptografi Metode End Of File (EOF) Dan Advanced Encryption Standard (AES)*, *Skripsi*, Teknik Informatika Dan Matematika, Universitas Bina Nusantara, Jakarta.

[12] Malese, L. P. (2021). Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB). *Jurnal Ilmiah Wahana Pendidikan*, *7*(5), 343-354.

[13] Munir, Rinaldi, 2018. Pengolahan Citra Digital dengan Pendekatan Algoritmik,Informatika Bandung.

[14] Munir. (2017). Pembelajaran Digital. Tersedia pada laman web: http://file.upi.edu/Direktori/FPMIPA/PRODI._ILMU_KOMPUTER/196603252001121-MUNIR/BUKU/Pembelajaran%20Digital.pdf: https://www.google.com/. Diakses Psds 20 Maret 2019.

[15] Nurdin. (2017). Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma Cipher Transposition. Vol.3 No.1. http://http://lppm.unfari.ac.id/assets/file/55-188-1-PB.pdf

[16] Rifai, Santoso, Christyono. (2019). Implementasi Algoritma Kriptografi RivestCode 4, Rivest Shamir Adleman, dan Metode Steganografi Untuk Pengamanan Pesan Rahasia Pada Berkas Teks Digital. TRANSIENT, vol.5(No.1),p. 87.

[17] Rihartanto, Utomo, D. B., & Rizal, A. (2019). IMPLEMENTASI IMAGE TILLING PADA PENYEMBUNYIAN PESAN MENGGUNAKAN LSB. *Proceeding SINTAK 2019*, 186-192.

[18] Rudianto. 2023. “Pemrograman Web Dinamis Menggunakan PHP dan MySQL”. Yogyakarta

[19] Rustad, S., Setiadi, D. I., Syukur, A., & Andono, P. N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. *Journal of King Saud University – Computer and Information Sciences, 34*, 3559-3568.

[20] Santi. (2018). Sistem Informasi Pengarsipan Surat- Surat pada PT SinergiPerkebunan Nusantara. Jurnal Ilmiah Intech : Information Technology Journal of UMUS , 51-60.

[21] Schneier, Wiley. (2019)“Applied Cryptography Second Edition: protocol, algorithm, and source code in C”; John Wiley and Son.

[22] Sebok, Vermat. (2018). Discovering Computer 2018 (Digital Technology, Data, and Device). Boston: Cengage Learning.

[23] Sholeh. (2018). Mengamankan skrip pada bahasa pemprograman PHP denganSulistiyani, (2017). Dipetik dari http://repository.ump.ac.id/4953

[24] Supriadi, Novantar. (2008). Digital Image Processing Third Edition, Pearson Prentice Hall, Upper Saddle River, New Jersey.

[25] Susilowati. (2017), Implementasi Algoritma Kriptografi RSA pada Keamanan Data Transkip Nilai Mahasiswa UNM Jurusan Matematika Menggunakan Bahasa Pemrograman PHP, Skripsi, Prodi Matematika, Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Makassar: Makassar