World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Steganography based on the B217AN Algorithm for secret messages on flip horizontal and resize image

Muhammad Sony Maulana *, Septian Rheno Widianto and Agung Sasongko

Information System, Universitas Bina Sarana Informatika, Pontianak, Indonesia.

World Journal of Advanced Engineering Technology and Sciences, 2023, 09(01), 017–028

Publication history: Received on 23 March 2023; revised on 29 April 2023; accepted on 02 May 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.9.1.0133

Abstract

The method of storing confidential information in digital images is known as steganography techniques, usually used for security and privacy purposes in various fields including online communication. The concept is to produce a stego image, where the information stored should not change when it is inserted or translated. The application of steganography techniques to digital images does not raise suspicions that an image has secret information or messages embedded. The spread spectrum steganography method is inspired by a communication model that transmits narrowband signals to wideband frequency channels by spreading or spreading, so that through spread spectrum messages embedded in secret information or messages can spread. In order to read the message, the recipient needs an algorithm which is a crypto key and a stego key. The purpose of this research is to test the steganography method by implementing PCMK/B with the Python programming language. The results of steganography testing using the B217AN algorithm can tolerate interference, distortion such as changes in brightness and contrast in JPEG, Gaussian, Poisson, salt and pepper compression, and loss. Tests on horizontal flip and resize stego image data using the B217AN steganography algorithm were successfully carried out, and information or secret messages that have been embedded in the cover image which later became the stego image can be read as it is. in its original condition and not altered or destroyed.

Keyword: Stego image; Steganography; Horizontal flip; Resize stego image; B217AN

1. Introduction

Through the development of digital media which includes: audio, images, text, and video to internet technology, it is very quickly transmitted by internet media. However, data security is the most important challenge when transmitting any form of information through public channels[1][2]. So, it is very necessary to protect the transmitted information from all forms of eavesdropping and from unauthorized or illegal access[3]. Digital images are an intermediary for the process of transmitting hidden information or messages, because they have a high level of redundancy and also low sensitivity from the visual system owned by humans, hidden messages or information can consist of images, videos, text, audio and images[12]. The main challenge faced by steganography applications is that messages or confidential information must be hidden in an image, so that the resulting stego image does not change from the original image, in terms of visuals and statistics[4][5].

Cryptography and steganography are tools that can be used for data security[6]. Cryptography has features such as reliability, confidentiality, and data integrity[7]. For example, data confidentiality resulting from encryption algorithms that encrypt confidential information or messages so that they cannot be read by anyone other than the intended recipient[8][9]. Especially for cryptographic applications, people who are eavesdropping or illegal can find out that there is information or private messages in it and can then decrypt it to read hidden information or secret messages[10].

* Corresponding author: Muhammad Sony Maulana

Steganography ensures that data is safe and is done by hiding secret information or messages so that other people do not know the existence of hidden messages [11].

Steganography can be applied to all types of multimedia files and digital images are often used, because digital images exchange more data over the Internet and are expected to raise suspicions of the confidentiality of the messages entered[13]. The title document of the components consisting of steganography contained in digital image steganography is a digital image[13]. The output of the steganography algorithm is a new image that has a hidden message (stego image)[14]. The sender and receiver are required to have the same stego key[15].

In addition, the recipient must use the stego image to receive the secret message[16]. There are 3 important things that need to be considered in steganography: (1) imperceptibility, is the presence of messages that cannot be understood by human emotions, (2) fidelity, is the quality of steganographic media that does not change much due to the insertion process, and (3) recovery, messages can be taken at any time if needed [17]. There are two systems of steganography, a message storage system and a message retrieval system. This system has six components, including[18]: (1) Secret Message, (2) Cover Document, (3) Stego Document, (4) Stego Key, (5).

Hiding Function f' (M,C,K)→ Z, (6) Detector Function f'(Z,C,K)→M[19]. Spread spectrum in the world of communication is a band signal process which is modulated by a broadband signal which will spread the band signal [20]. In a steganography, narrow band signal is assumed with hidden data to be inserted and wide band signal is assumed to be a digital image that has been decomposed by wavelet or digital media to be inserted hidden data [21].

2. Proposed method/algorithm

The stages carried out in this research are starting from designing the B217AN algorithm, then designing the information insertion process, and finally designing the information extraction process.

2.1. B217AN Algorithm Design

The stages of designing the B217AN Algorithm are:

- For the sender of the message, select the media used with the image and enter the secret message (embedded-image) you want to include.
- The embedding process to penetrate the spread spectrum image. Then it will display, that is, the stego image embedded in the embedded image and the embedded image will be visible.
- The third stage is that the stego-image is tested for reliability in several attacks, the process produces an output that is the attacking stego-image.
- The fourth stage produces an output in the form of a stego-image. The stego image is taken from the recipient to generate a secret message, which is stored in the image on the media.

The flow diagram of the steganographic system in digital images is as shown in Figure 1.

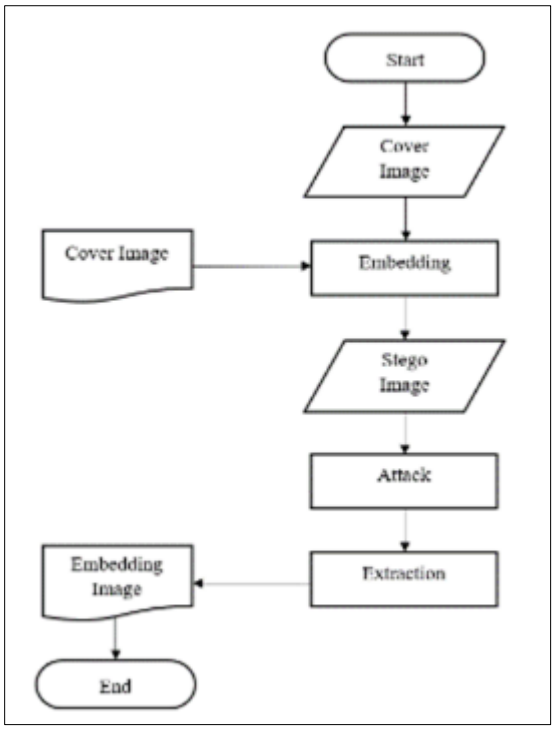

Figure 1 System Flowchart

2.2. Message Insertion Process

The block diagram of the message insertion process in digital images is as shown in Figure 2.

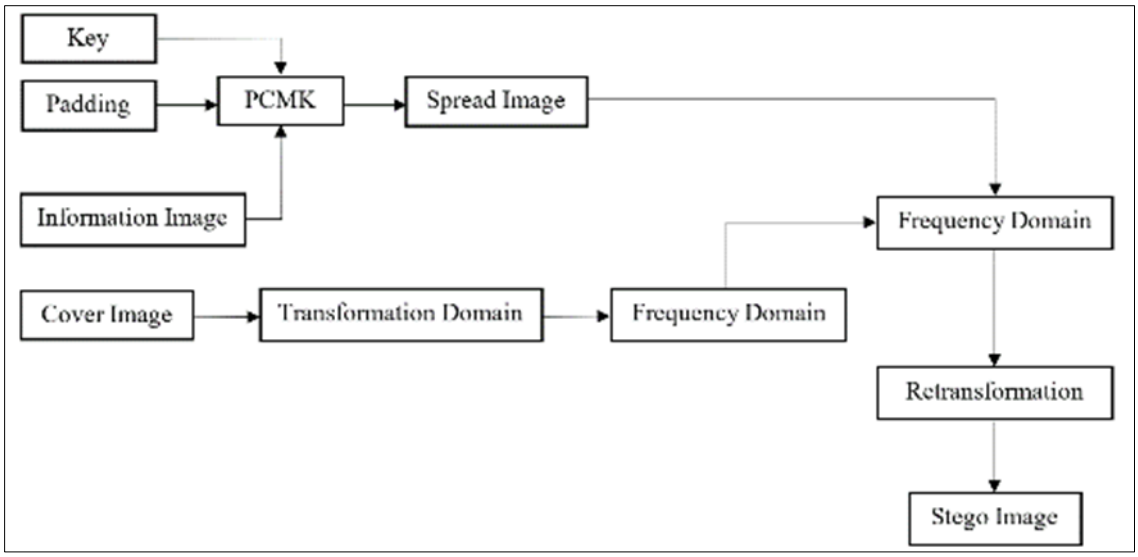

Figure 2 Block Diagram of the Message Insertion Process

The explanation of Figure 2 is as follows:

- To use the key used, the key is combined with the input information and the image and then processed using the PCMK (Shrink Multicycle Chaotic Permutation) method.
- After completing the process, PCMK generates a diffuse image. The results of the images that go into the modulation.
- In the cover frame phase, steps are taken to change the frequency and the results are entered into modulation.

After going through the modulation phase, the next step is to re-transform to create a stego image that is embedded with a key and an information image.

2.3. Message Extraction Process

The block diagram of the message extraction process in digital images is as shown in Figure 3.

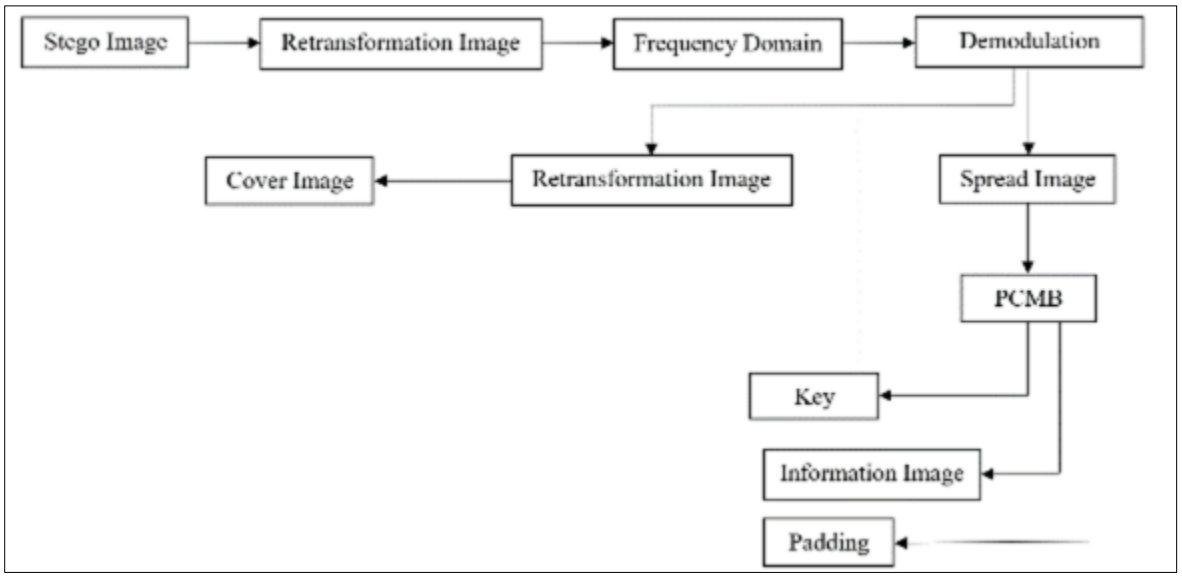

Figure 3 Block Diagram of Message Extraction

The explanation of Figure 3 is as follows:

- The first stage of the message retrieval process from the stego image is generated from the message insertion process, then the image is edited.
- After converting the image, the next step is to convert it into the frequency domain.

The next stage is the demodulation process in the frequency domain.

- After going through the demodulation process, a scatter plot can be made. The distribution image is processed using PCMB (Enlarged Multi-cycle Chaotic Permutation), from the PCMB process it can produce keying, image information and padding. In the end, the filler is not used.

3. Result and discussion

The steganography algorithm produced by B217AN is a steganographic algorithm that can tolerate interference, the interference involved includes interference immunity, such as: changes in brightness and contrast in JPEG, Gaussian, Poisson, salt and pepper compression and data loss[22]. The aim is to create a steganography application based on Multi-loop Chaotic Permutation (PCMK/B) which is created using the Python programming language.

3.1. Testing the B217AN Steganography Algorithm

Tests were carried out using the Kali Linux operating system, WSL Kali Linux on the Windows operating system and the st3g0_noT_001 application which was made using the python3 programming language, and for testing it required a cover image which would be inserted by a secret message which was carried out with the help of the st3g0_nOT_001 tool. More details can be seen in Figure 4.

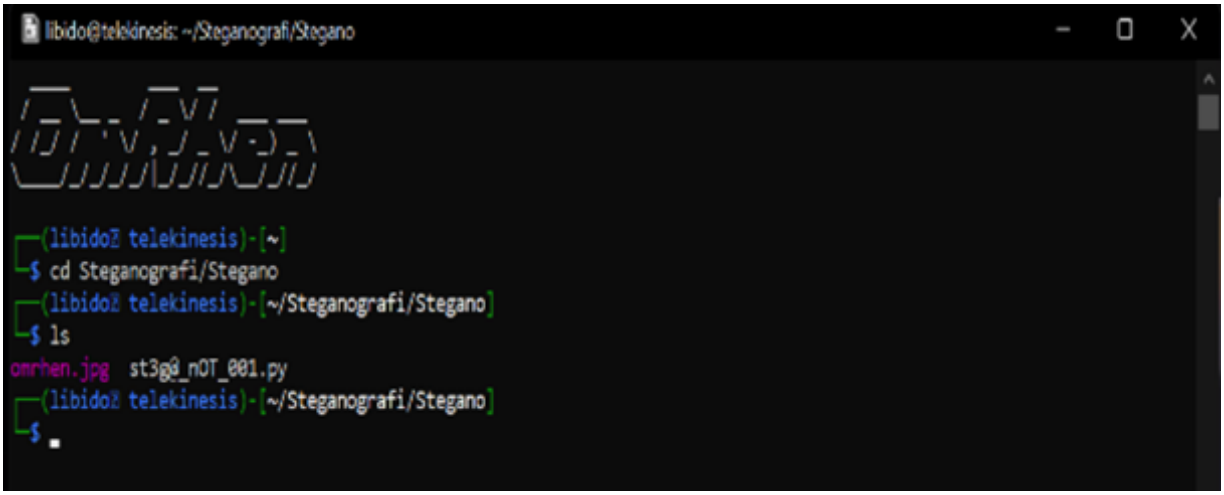

Figure 4 Location of cover image and st3g@_nOT_001

The cover image used has the extension .jpg, .png, .gif or other image extensions, but for testing the st3g@_nOT_001 application, use an image with a .jpg extension. Figure 5 is a Stegano directory containing an image that has been prepared and will be used as a cover image and st3g@_nOT_001 which is an application used to insert confidential information into the image.

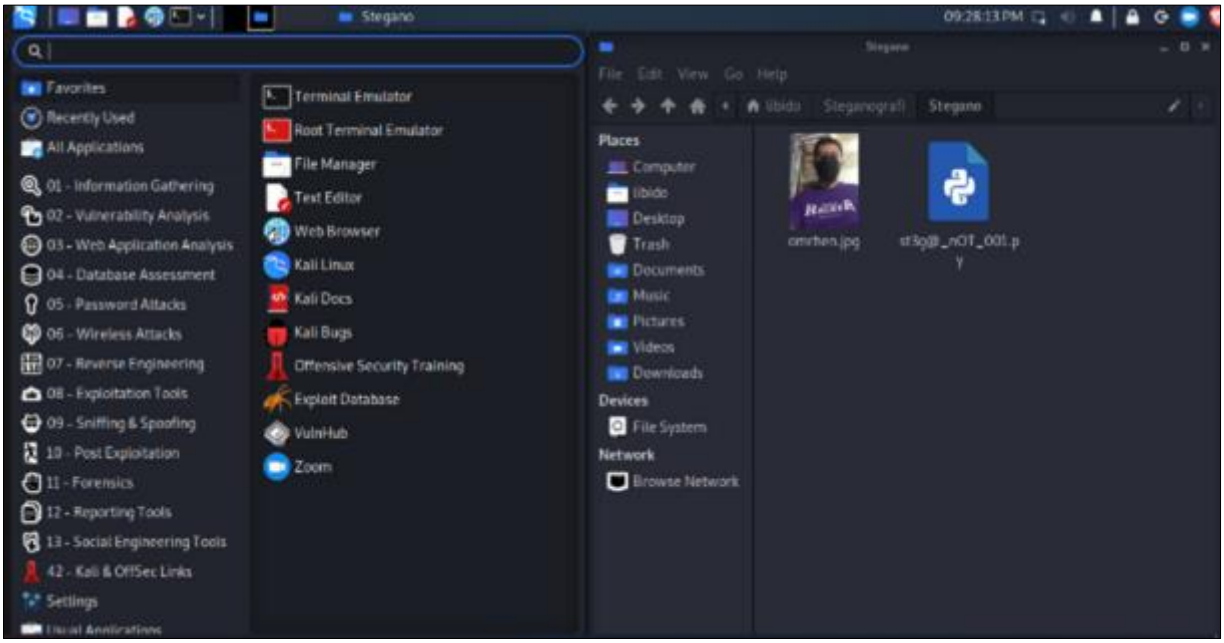

Figure 5 Stegano directory containing cover images and st3g@_nOT_001

The st3g@_nOT_001 steganography application that has been created is run using the kali linux terminal by typing the command python3 st3g@_nOT_001.py, figure 6 is the way to execute the st3g@_nOT_001 application. The st3g@_nOT_001 application has 2 menus, namely Creating Stegano Files and Reading Stegano Files, for the experiment of inserting confidential information into the prepared cover image, it is necessary to select Menu 1 or Create Stegano Files, Figure 6 is the menu display of the st3g@_nOT_001 application. The results of the stego image created by the st3g@_nOT_001 application will be changed, namely horizontal flip and resize image which will be used for testing resistance to horizontal flip interference and resizing the image, so that information or secret messages that have been inserted are not changed or destroyed.

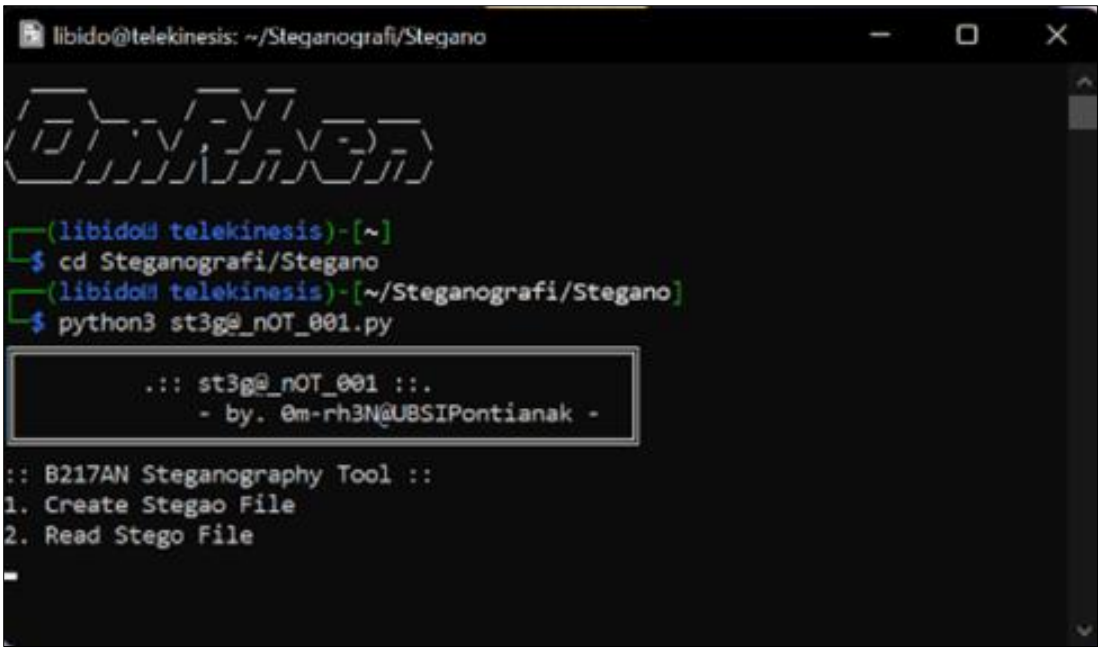

Figure 6 The menu display of the st3g@_nOT_001 application

The next step is to select the menu in the st3g@_nOT_001 application by typing the number 1, and then typing the name of the image that will be used as the cover image. Figure 7 explains how to insert confidential information into an image that is used as a cover image.

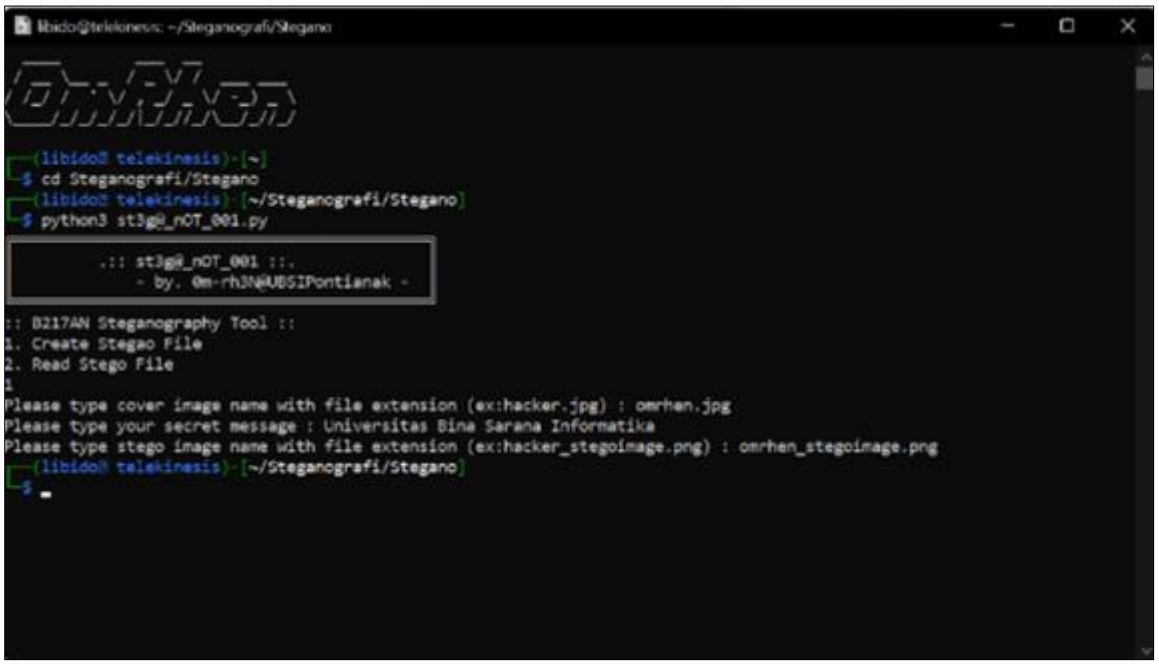

Figure 7 The Process of Inserting Confidential Information

The result of the process carried out by the st3g@_nOT_001 application is to produce a new file in the form of an image that has been inserted a secret message or referred to as a stego image, figure 8 is the result of the message insertion process carried out by the st3g@_nOT_001 application and figure 9 is a display of the stego image file that visible to the human eye there is no change in image quality due to one of the requirements of steganography, namely image quality must not change after inserting confidential information.

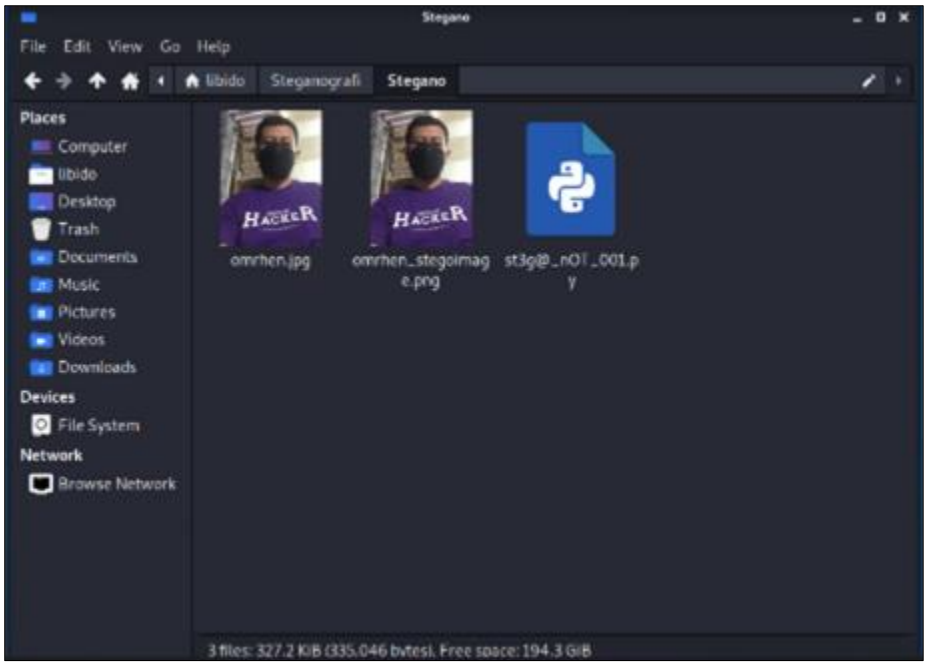

Figure 8 The results of the message insertion process carried out by the st3g@_nOT_001 application

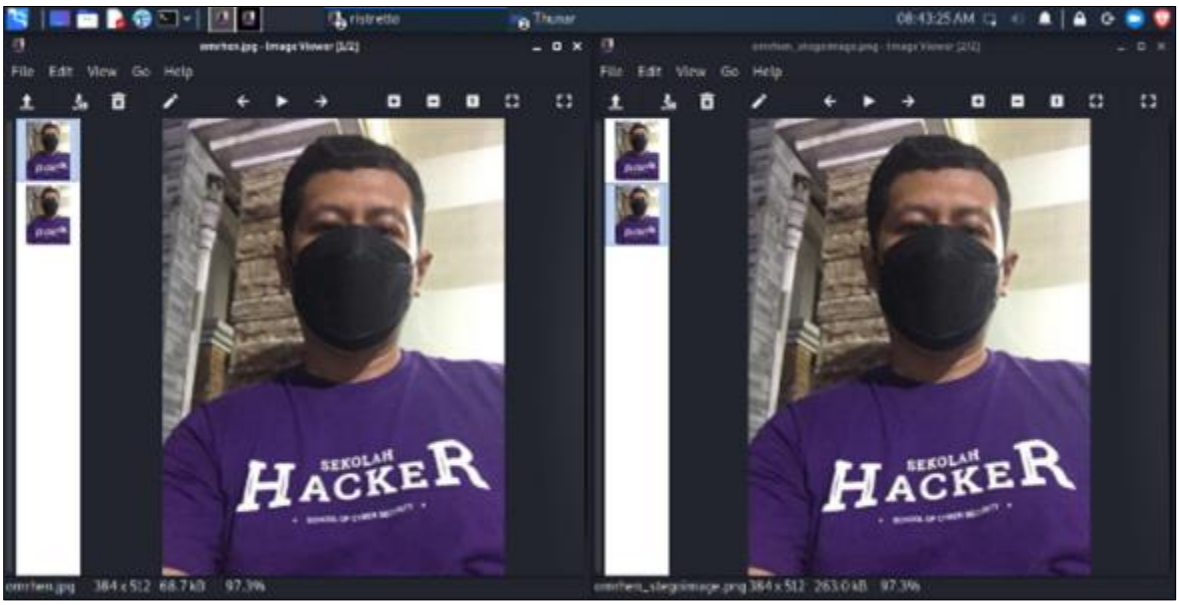

Figure 9 Stego Image File Display

If you look at Figure 9, you don't see a significant change related to image quality, but if you look at the file size it will be clear that there are changes. However, this often deceives other people because other people only see visualizations and rarely pay attention to the details of changes that occur related to the size of the file. The next step after the image file which is also a cover image has successfully inserted confidential information and becomes a stego image using the st3g@_nOT_001 application, then what needs to be done next is to test the cover image that has turned into a stego image and the first test is to test whether the information the secret was successfully inserted into the cover image. Figure 10 is a test to ensure that confidential information is successfully inserted into the cover image and has become a stego image with the file name omrhen_stegoimage.png after inserting the confidential information.

Figure 10 Testing a cover image that has been inserted with confidential information.

3.2. Horizontal Flip Test

The stego image generated from the st3g@_nOT_001 application is also tested with a horizontal flip to ensure that the confidential information that has been inserted into the cover image is not changed, lost or destroyed and ensures that the confidential information will still be readable according to the original information. Figure 11 is a stego image that has been converted into a horizontal flip and will be tested using the st3g@_nOT_001 application to read the confidential information contained in the stego image and Figure 12 is the result of testing the st3g@_nOT_001 application to read the confidential information contained in the stego image and it can be seen that the confidential information is still the same as the original or the first time the confidential information was inserted into the cover image which later became a stego image (omrhen_stegoimage.png).

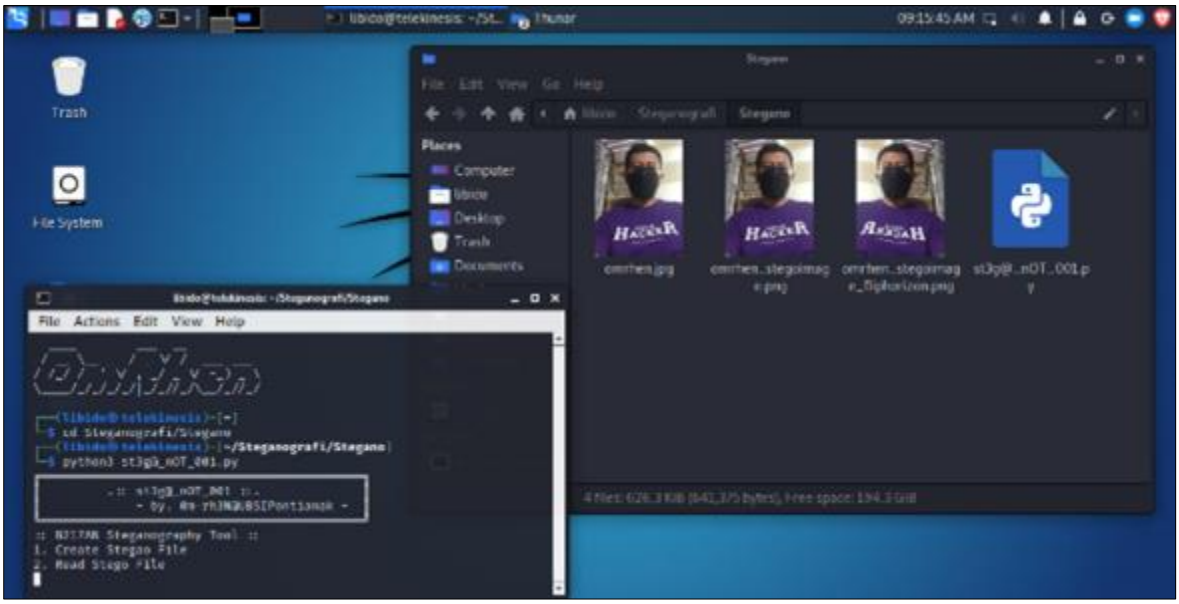

Figure 11 Stego image that has been converted to flip horizontal

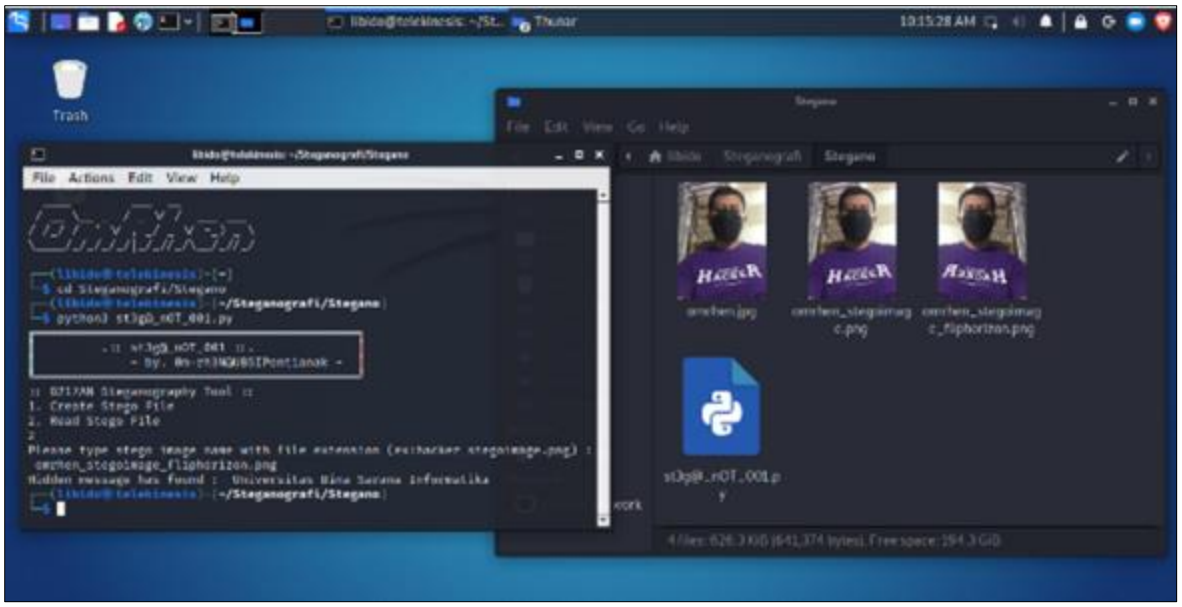

Figure 12 Horizontal flip test results using the st3g@_nOT_001 application**.**

3.3. Resize Image Test

The stego image is tested not only to turn it into a horizontal flip, but also tested by resizing the image which aims to ensure that information or secret messages stored in the stego image are still in their original condition, not changed or destroyed. Figure 13 is a stego image that has been resized image with a size of 80x107 pixels from a stego image file measuring 384x512 pixels and a stego image test will be carried out using the st3g@_nOT_001 application to read information or secret messages contained in the stego image and image 14 is the results of testing the st3g@_nOT_001 application to read confidential information or messages contained in the stego image and it appears that the confidential information is still the same as the original or the first time the confidential information was inserted into the cover image which later became a stego image (omrhen_stegoimage.png).

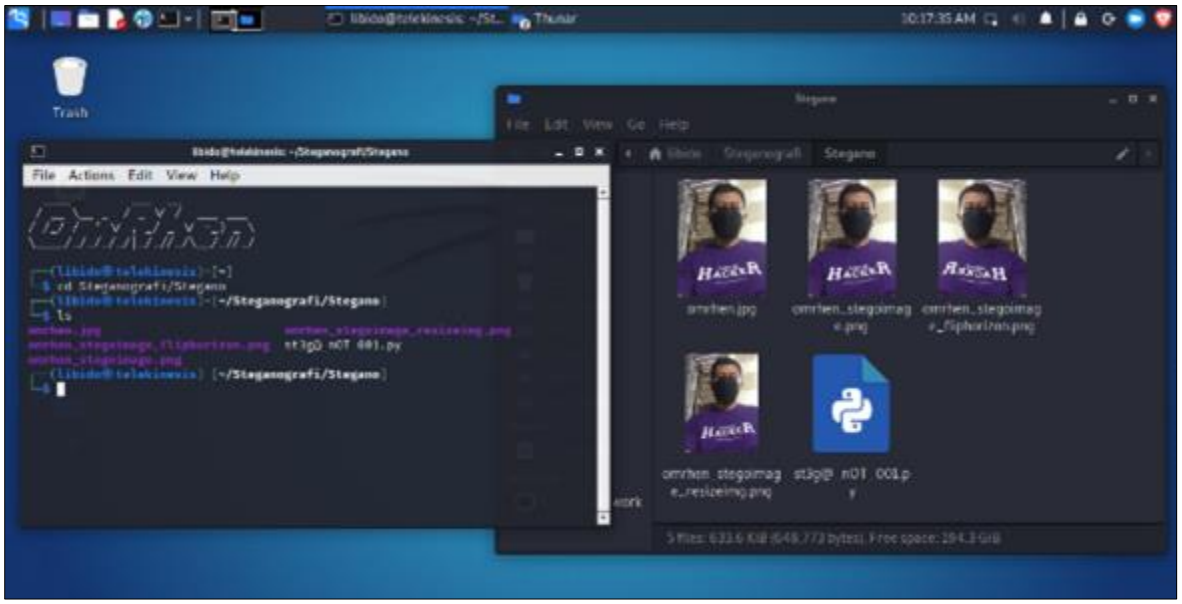

Figure 13 Stego image that has been resized image

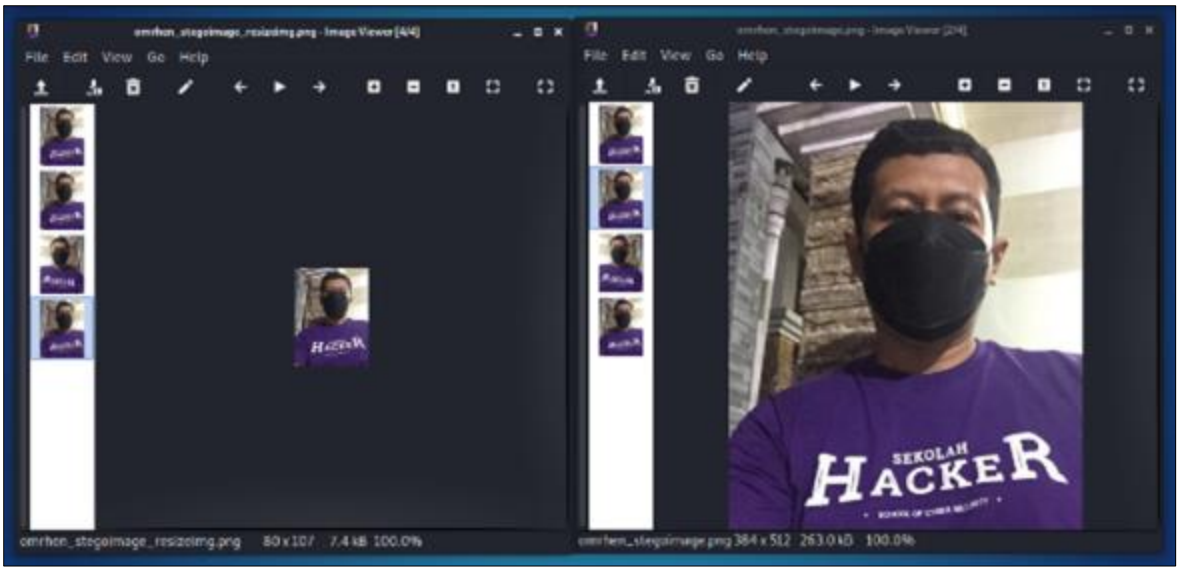

Figure 14 The Result of resized stego image

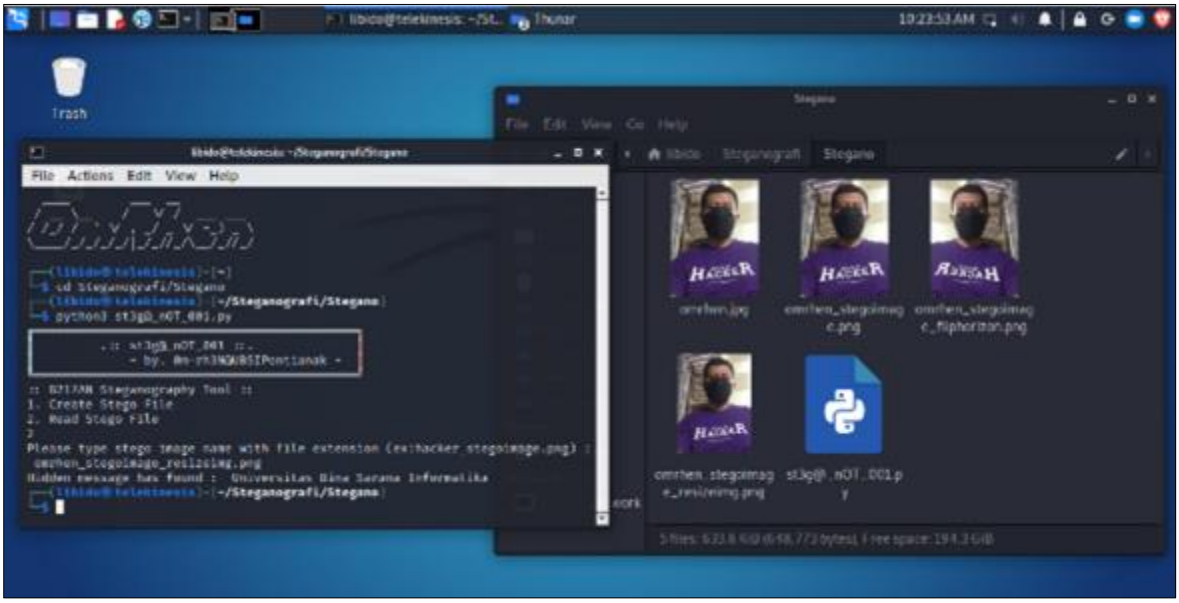

Figure 15 Image resizing test results using the st3g@_nOT_001 application

4. Conclusion

The steganography algorithm combined with the spread spectrum method is used to disseminate information about the embedded image so that the location of the inserted message cannot be determined or the location of the inserted message so that the sender of the message does not know its location. The performance of the resulting steganography algorithm can tolerate differences in brightness and contrast levels caused by JPEG compression, salt and pepper noise, speckle noise, Gaussian noise, and Poisson noise, as well as missing data. To insert a message that uses Chaotic Multicycle Shrink (PCMK) for input, filling, and display of information, a distribution image is generated, which is a randomization of information obtained from previous processes in an image or image. The image change process begins by converting the frequency into a frequency domain and then combining it with the results of the image distribution to convert it back into a stego image. The messaging process starts with a stego image created to change the image, and then the frequency domain is changed automatically, 2 processes result from the modulation process. Images use Enlarged Multicycle Permutation (PCMB), to create keys, image information and insertion of secret information or

messages. The results of the horizontal flip and resize image testing of the stego image using the B217AN steganography algorithm were successfully carried out, and the secret information or message that had been inserted into the cover image which later became a stego image could be read as in its original condition and not changed or destroyed.

Compliance with ethical standards

Acknowledgments

The authors would like to thank University of Bina Sarana Informatika for their assistance with this project and World Journal of Advanced Engineering Technology and Sciences for publishing this article.

Disclosure of conflict of interest

The authors declare that there is no conflict of interest in publishing the paper.

References

[1] Reno, S. (2017). Steganography Algorithm with Spread Spectrum Method Based on PCMK. Multinetics, 3(2), 32. https://doi.org/10.32722/vol3.no2.2017.pp32-37.

[2] Widianto, S. R. (2018). Steganographic Algorithm Design with Spread Spectrum Method Based on PCMK (Shrinking and Enlarging Multi-turn Chaotic Permutation) which is Resistant to Interference. Proceedings of the National Seminar on Science and Technology, pp1–8.

[3] Widianto, S. R. (2018). Design and Analysis of Steganographic Algorithm with Spread Spectrum Method Based on PCMK (Shrinking and Enlarging Multi-turn Chaotic Permutations). Elektra Journal, 3(1), 37–46. https://pei.e-journal.id/jea/article/view/44.

[4] Widianto, S. R., Suryanto, Y. (2020). B217AN Algorithm Using Spread Spectrum Method Based on PCMK/PCMB. Proceedings of the National Seminar on Electrical Engineering, 5(2020), 216–223. http://jurnal.pnj.ac.id/index.php/snte/article/view/40.

[5] Widianto, S. R., Suryanto, Y. (2020). B217AN Algorithm Based on PCMK/PCMB. Gerbang Journal. STMIK Bani Saleh, 10(1). http://jurnal.stmik.banisaleh.ac.id/ojs2/index.php/JIST/article/view/47/47.

[6] Rajesh, D. P., Alam, D. M., Tahernezhadi, D. M., Ravi Kumar, T., & Rajesh, V. P. (2020). Secure communication across the internet by encrypting the data using cryptography and image steganography. International Journal of Advanced Computer Science and Applications, 11(10), 454–458. https://doi.org/10.14569/IJACSA.2020.0111057.

[7] Abel, K. D., Misra, S., Agrawal, A., Maskeliunas, R., & Damasevicius, R. (2022). Data Security Using Cryptography and Steganography Technique on the Cloud. Lecture Notes in Electrical Engineering, 834(6), 475–481. https://doi.org/10.1007/978-981-16-8484-5_46.

[8] Lin, E. T., & Delp, E. J. (1999). A Review of Data Hiding in Digital Images. Society for Imaging Science and Technology: Image Processing, Image Quality, Image Capture, Systems Conference, 274–278.

[9] Wiguna, I. P. H. (2016). Implementation of Blind Watermarking in Digital Image with Haar Wavelet Transform. Journal of Information Technology and Computers, 1(1), 37–42. https://doi.org/10.36002/jutik.v1i1.21.

[10] Cachin, C. (2005). Digital Steganography. Encyclopedia of Cryptography and Security, https://doi.org/10.1007/0-387-23483-7_115, 159-164.

[11] Mutia S, R. (2017). Steganography Algorithm Study and Testing on Steghide Applications. pp1–17. https://docplayer.info/47139166-Studi-dan-pengujian-algoritma-steganografi-pada-aplikasi-steghide.html.

[12] Pranoto, B. (2014). Steganography In Digital Image Using Spread Spectrum Method And Least Significant Bit (LSB) Modification Method.

[13] Soni, T., Baird, R., Lobo, A., & Heydari, V. (2021). Using Least-Significant Bit and Random Pixel Encoding with Encryption for Image Steganography. Advances in Intelligent Systems and Computing, 1271 AISC(September), 139–153. https://doi.org/10.1007/978-3-030-58703-1_9.

[14] Adee, R., & Mouratidis, H. (2022). A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. Sensors, 22(3), 1–23. https://doi.org/10.3390/s22031109.

[15] Hosmani, S., B, H. G. R. B., & Chandrasekaran, K. (2015). Security in Computing and Communications - Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings. 265–276. https://doi.org/10.1007/978-3-319-22915-7.

[16] Albaghdadi, A. F. (2015). A Novel Technique of Image Steganography for sensor information with socket TCP / IP connection. III(7), 7553–7565.

[17] Kan, O. A., Mazhenov, N. A., Kopbalina, K. B., & Turebaeva, G. B. (2021). Issn 2709-3077. 577(07), 72–79.

[18] Swetha, K., Sai Saaketh Sharma, K., Niteesh, A. S., Sumith, O. S., & Kommineni, M. (2019). A Study of Distnict Image Encryption Techniques. Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019, 608–612. https://doi.org/10.1109/I-SMAC47947.2019.9032635.

[19] Gutub, A., & Al-Ghamdi, M. (2020). Hiding shares by multimedia image steganography for optimized counting-based secret sharing. Multimedia Tools and Applications, 79(11–12), 7951–7985. https://doi.org/10.1007/s11042-019-08427-x.

[20] Liao, X., Yin, J., Chen, M., & Qin, Z. (2022). Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features. IEEE Transactions on Dependable and Secure Computing, 19(2), 897–911. https://doi.org/10.1109/TDSC.2020.3004708.

[21] Tao, J., Li, S., Zhang, X., & Wang, Z. (2019). Towards Robust Image Steganography. IEEE Transactions on Circuits and Systems for Video Technology, 29(2), 594–600. https://doi.org/10.1109/TCSVT.2018.2881118.

[22] Zhou, Z., Mu, Y., & Wu, Q. M. J. (2019). Coverless image steganography using partial-duplicate image retrieval. Soft Computing, 23(13), 4927–4938. https://doi.org/10.1007/s00500-018-3151-8.