Aceh Int. J. Sci. Technol., 10(3) 153- 160
December, 2021
doi: 10.13170/aijst.10.3.21079

Aceh International Journal of Science and Technology
ISSN: p-2088-9860; e-2503-2398
Journal homepage: http://jurnal.unsyiah.ac.id/aijst

Storage of Text Messages on e-Book Files using Least Significant Bit and Haar Wavelet Method

Muhaimin Hasanudin[1], Deni Kuswoyo[2*]
[1] Department of Informatics Engineering, Universitas Mercu Buana, Indonesia;
[2] Department of Graphic Design, Politeknik Negeri Media Kreatif, Indonesia;
*Corresponding author email: deni.kuswoyo@polimedia.ac.id

Received : May 18, 2021
Accepted : December 18, 2021
Online : December 30, 2021

Abstract – This study uses the technique of incognito data and information into a container in the form of images combined with the addition of the password by using the method of Least Significant Bit (LSB) and the technique of Haar Wavelet. Testing the system by sending a message in the form of a text file and an image file with the process of the original image are transformed to wear haar wavelet divided into four zones of frequency, namely LL, LH, HL, and HH. Where Bit-bit Readings are planted in a zone LL and attempted insertion of the bit of the file reading into the last bit in each byte of the image file and can show you back the results of the message. The research results, i.e., images processed by the LSB and Haar Wavelet method, do not change the file size, resolution, dpi, and physical form image. The advantage of this method is very simple computing, oriented computers, which need less space to store and are time-efficient.

Keywords: Steganography, Image, Haar Wavelet Method, LSB Method, Text file

Introduction

Steganography comes from the ancient Greek word *steganos*, and the translation is to disguise writing. The stenographic technique provides access or allows one party to communicate information to another party without intermediary third parties, even though the incident is happening. Hamid et al. (2012), Oo and Aung (2020) introduced a procedure for varied and varied secret messages. An important difference can be made between cryptography and the science of disguising information or messages in an object or container (Steganography). Cryptography changes the message even if it is read anywhere is an important difference that can be made between cryptography and the science of disguising information or messages in an object or container (Steganography). Ahmmed et al. (2021), Al-Hussein t al. (2021) believes that Cryptography changes the message even though it is read and detected by a third party, the message cannot be understood.

Meanwhile, Several studies such as Oo and Aung (2020), Fu and Chang (2020) reveal that Steganography involves hidden messages so that third parties or reviewers are unable to detect and find out the information. Steganography is a good choice in priority situations for securing and hiding communication in the form of information such as detailed data or text. Steganography is often combined with cryptography to provide an additional layer of security, as done by Thangadurai and Devi(2014), Oo and Aung (2020).

Roshini and Meena (2020) explored Steganography is used by copyright owners who want to put a password or hidden message in their works to avoid theft and piracy of the copyrights they have created. A password or message can be in text and a logo that identifies the company's property rights or individuals.

Today's technology has progressed rapidly; communication has become something basic and mandatory. Anyone and anywhere must communicate in oral and written ways, as opinions from Hasanudin and Yuliadi (2021), some useful tools such as telephones, cellular phones, computers (intranet and internet). However, these technological developments have not been matched by information security guaranteed confidentiality. Information conveyed via landlines, and cellular phones can still be tapped or recorded. Then the information can be leaked, as well as computer media, data, or information that is confidential in cyberspace can also be taken and misused, such as data and information in electronic mail, sending data via FTP (File Transfer Protocol), or data and information that is stored safely even though an intranet server can be retrieved unilaterally and without the knowledge of the owner. Even speaking verbally about secret matters can be recorded from a certain distance without the person's knowledge, by determining the coordinates of the person's position, all spoken information will be recorded, this tool is commonly used to record player conversations in a field full of audience voices on broadcast live in sports matches.

Confidentiality and privacy for data and information are no longer safe, and it is necessary to find a solution for this, then by disguising data and information into a container in the form of an image that has nothing to do with disguised data or information as opinions from Oo and Aung (2020). This is not considered secure enough, then combined with the coding technique to better disguise confidential data. In Steganography, hidden information or messages that cannot be seen are text data, images, or even sound waves. By pasting the data with visible data images that have nothing to do with the information hidden therein as opinions from Abbas et al. (2021).

Materials and Methods

Steganography

The word Steganography comes from the Greek steganos (στεγανός), which means "to be covered or protected," and graphein (γϱάυειν), which means "to write." The origin of the word Steganography means "hidden writing." Steganography is the art and science of writing an obscure data file so that no single except the intended transmitter and receiver are aware of the information's creation (Pandey). The information will generally appear in another form: a photo, article, shopping list, or some other cover text. Classically, information is hidden using invisible ink between visible lines in a private letter.

Steganography also involves the insertion of information in computer files. In virtual Steganography, a digital verbal exchange can consist of stenographic coding inside the shipping layer, including file documents, photo documents, programs, or protocols, as opinions by Abbas et al. (2021), Al-Huwais et al. (2020). Media documents are best for stenographic transmission due to their massive size. As a simple example, the sender might start with a less complex image file and match the color of every 100 pixels with the letters in the alphabet. Because the changes are so subtle, someone explicitly looking for them can't see the inserted information as opinions from Fu and Cheng (2020). The criteria that must be considered in hiding data using stenographic techniques are as follows:

- Imperceptibility: The presence of the message in the container medium cannot be detected.
- Fidelity: The quality of the container media after adding the secret message is not much different from the quality of the container media before adding the message.
- Recovery: The secret message that has been inserted in the container media must be revealed again.
- Robustness: The hidden message must resist various manipulation operations performed on the container media.

The characteristics of good Steganography are high imperceptibility, high fidelity, maximum recovery, and high robustness has been done by Al-Huwais et al. (2020).

Least Significant Bit

Several studies such as Abbas et al. (2021), Gunawan (2019), Sudrajat (2020). the method used to hide messages on digital media. For example, the message image file can be hidden by inserting it in the low bit or the far right bit (LSB) in the pixel data that compose the file. As is known for 24-bit bitmap files, each point (pixel) in the image consists of a three-color arrangement of red, green, and blue (RGB), each composed of 8-bit numbers, bytes from 0 to 255 or with binary format 00000000 to 11111111 Thus, at each pixel of the 24-bit bitmap file we can insert data bits as opinions from Pandey et al. (2021).

The LSB method has been proven to have good imperceptibility (something that is not known); the data capacity is quite small because it can only store each pixel's LSB in each color (Thangadurai,2014 Pandey). So that the third party is not aware of the secret message stored in the *stego*. The basic concept of LSB is to attach the secret data to the rightmost bit (the bit with the smallest weight) so that the data entry procedure does not affect the original pixel value. The mathematics that presents the LSB method are:

$$X_i^{'} = X_i - X_i \bmod 2^k + m_i \tag{1}$$

In the above equation $X_i^{'}$ represents i value of the stego image pixel, X_i represents the actual image (Cover Image), and m_i is the decimal value of the order-i block in(https://www.semanticscholar.org/paper/A-DWT-Based-Approach-for-Image-Steganography-Chen-Lin/1a7b404bdd21a45bccf86034a01e555f3762dee5)

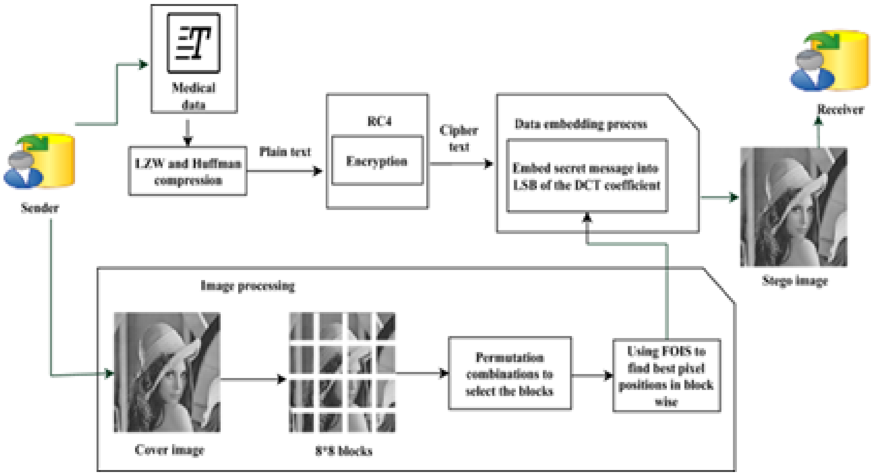

Medical data
Sender
LZW and Huffman compression
Plain text
RC4
Encryption
Cipher text
Data embedding process
Embed secret message into LSB of the DCT coefficient
Receiver
Stego image
Image processing
Cover image
8*8 blocks
Permutation combinations to select the blocks
Using FOIS to find best pixel positions in block wise

Figure 1. LSB Model Data Structure (Roselin et al. 2021)

Haar Wavelet Transformation

Wavelets are a mathematical utility used in signal processing and photo compression, originally applied in geophysics to reflect layers of surface bedrock used in oil and mineral exploration. One of the famous wavelet families is the Haar wavelet; this is the oldest wavelet introduced by Hungarian mathematician Alfred Haar in 1909 and wavelet theory that started a lot in the 1980s. This is a well-known topic in various fields of method and science, the Haar wavelet is also considered a very simple wavelet known first because it consists of the use of a partial constant, which only takes three values of 0, 1, and 1. In the last two decades, the subject of wavelet theory has played a role. Position means a position in many computational mathematical scientists, most notably in time-frequency analysis, signal analysis, and numerical analysis. The wavelet method allows us to decompose various complex uses into a summation of primary uses, and each basic use can result from resolving and translating for the mother wavelet. In effect, wavelet analysis is more accurate than Fourier's analysis. Much research has focused on the orthogonal procedure of polynomials and their roles in obtaining efficient algorithms suitable for digital PCs. A kind of numerical ordinance with eliminating discretization as opinions from Abbas et al. (2021), use of Haar wavelets as opinions from Shah (2019), Abdeljawad et al. (2020), Amin et al. (2020), Gul et al. (2020), Chen and Hsiao (1997), which is defined as:

$$\varphi(t)\begin{cases}1 & 0 \le t < 1/2, \\ -1 & \quad 1/2 \le t1, \\ \;2 & ,x\ another\end{cases} \tag{2}$$

- Image: Steganography is one of the techniques of information hiding; another technique is digital watermarking. Govindasamy et al. (2020) explored the steganography technique with the LSB method as the most frequently used technique, the information that will be hidden is ASCII data, converted and taken to its binary values and then inserted into the LSB a series of bytes in the stego image

- Secret data: The number of LSBs to be replaced is denoted ask. The extraction procedure is to duplicate the rightmost k-bit directly. Mathematically the extracted message is represented as:

Figure 1 shows the basic structure of Steganography with the LSB method, the process that is carried out is encryption of text messages and cover images, then the decryption process is on the stego image.

$$\emptyset(t) = \begin{cases} 1 & 0 \leq t << 1, \\ 0\,, & x\ another \end{cases} \tag{3}$$

In the Haar Wavelet transformation on an image, it is carried out using a low pass filter (LPF) and a high pass filter (HPF) to obtain a wavelet coefficient, as opinions from Govindasamy et al. (2020), Abbas et al. (2021). Algorithm:

- Input: normalized image
- For horizontal and vertical decomposition, find the coefficients of LPF and HPF.

$$\mathrm{f}'_{\mathrm{k}} = \frac{1}{\sqrt{2}}\left(\mathrm{f}_{2\mathrm{k}} + \mathrm{f}_{2\mathrm{k}-1}\right) \tag{4}$$

The LPF coefficient is:

$$\mathrm{f}^{*}_{\mathrm{k}} = \frac{1}{\sqrt{2}}\left(\mathrm{f}_{2\mathrm{k}} - \mathrm{f}_{2\mathrm{k}-1}\right) \tag{5}$$

- Do it repeatedly on the approximation coefficient obtained previously until the desired level

The table below describes the data structure for the steganography system, including the data structure of text files and BMP image files

Table 1. Steganography System Data Structure

No	Files	Data Structure
1	Text files	• Flat text, which is created from a word processing application. • Taken from storage media. • text files are in .txt format • ASCII and UTF-8 • Type is text • Text file size.
2	Images files	• Object data type. • Image file size (width x height x n / 8 bits). • Supports up to 24 bpp. • Supports grayscale, indexed color, and RGB color • The image file format is a BMP extension. • Image files are retrieved from storage media.

Results

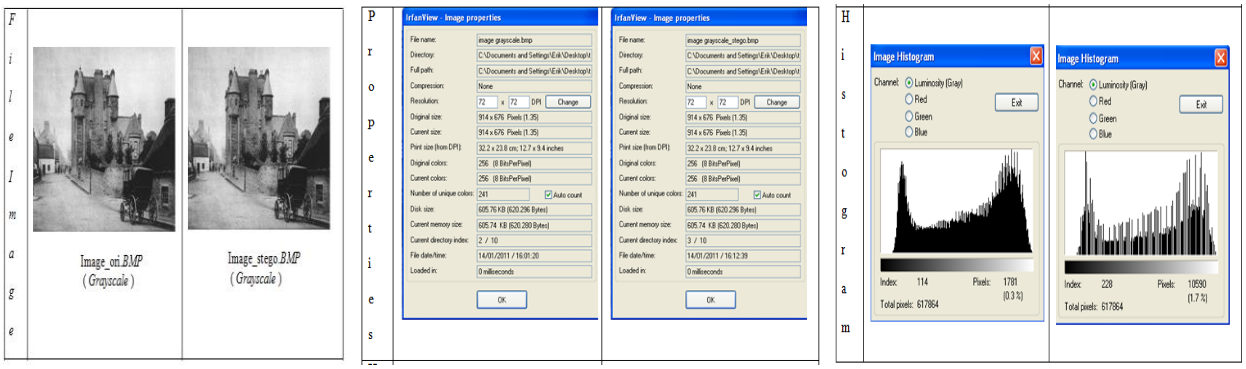
Steganography system testing includes system testing, system testing on black and white images, system testing on color images, testing for stego images used as cover images and stego images. The table below shows the system testing based on the functions of the steganography system menu, based on the appearance and performance of the system. The objects tested include testing the function of the text file input button, the function of the password input menu, the function of the BMP input button, the function of the encode process button, and the decoding process button.

Table 2. Testing on the steganography system

No	Object	Testing
1	Text file input	Input conditions: text can be inputted in .txt form. Special exception: only text files without formatting and support ASCII characters.
2	Enter the password	Input conditions. Value - 6 character strings (condition: in the form of alphanumeric and recognizes capital and non-capital letters).
3	BMP file input	Input conditions. Value - BMP file [file size]. A special exception: only image files with BMP format.
4	Encode	Input conditions. Contains process encode commands. (hiding text file into cover image). Special requirements: input of text file and password, and input of BMP image. Special exception: the process will run if the cover image size is larger than the text file size.
5	Decode	Input conditions. Set - contains the decoded command (returns the hidden message in the stego image). Special requirement: hidden secret messages can be seen and read again by inputting the correct password.

Testing With a Black and White Cover Image

In Figure 2, the steganography application system used is an image with a grayscale format (256 colors - 8 bpp) with a grayscale.bmp image file and a grayscale_stego.bmp image as input data. The resolution and dpi in each file processing result of the two images did not change, but the graphic color change is shown on the histogram graph. In plain view, you will not be able to distinguish an image that has undergone text insertion from the original image.



File name: image grayscale.bmp
Directory: C:\Documents and Settings\Erik\Desktop\t
Full path: C:\Documents and Settings\Erik\Desktop\t
Compression: None
Resolution: 72 x 72 DPI
Original size: 914 x 676 Pixels (1.35)
Current size: 914 x 676 Pixels (1.35)
Print size (from DPI): 32.2 x 23.8 cm; 12.7 x 9.4 inches
Original colors: 256 (8 BitsPerPixel)
Current colors: 256 (8 BitsPerPixel)
Number of unique colors: 241 ☑ Auto count
Disk size: 605.76 KB (620.296 Bytes)
Current memory size: 605.74 KB (620.280 Bytes)
Current directory index: 2 / 10
File date/time: 14/01/2011 / 16:01:20
Loaded in: 0 milliseconds

File name: image grayscale_stego.bmp
Directory: C:\Documents and Settings\Erik\Desktop\t
Full path: C:\Documents and Settings\Erik\Desktop\t
Compression: None
Resolution: 72 x 72 DPI
Original size: 914 x 676 Pixels (1.35)
Current size: 914 x 676 Pixels (1.35)
Print size (from DPI): 32.2 x 23.8 cm; 12.7 x 9.4 inches
Original colors: 256 (8 BitsPerPixel)
Current colors: 256 (8 BitsPerPixel)
Number of unique colors: 241 ☑ Auto count
Disk size: 605.76 KB (620.296 Bytes)
Current memory size: 605.74 KB (620.280 Bytes)
Current directory index: 3 / 10
File date/time: 14/01/2011 / 16:12:39
Loaded in: 0 milliseconds

Channel: ● Luminosity (Gray) ○ Red ○ Green ○ Blue
Index: 114 Pixels: 1781 (0.3 %)
Total pixels: 617864

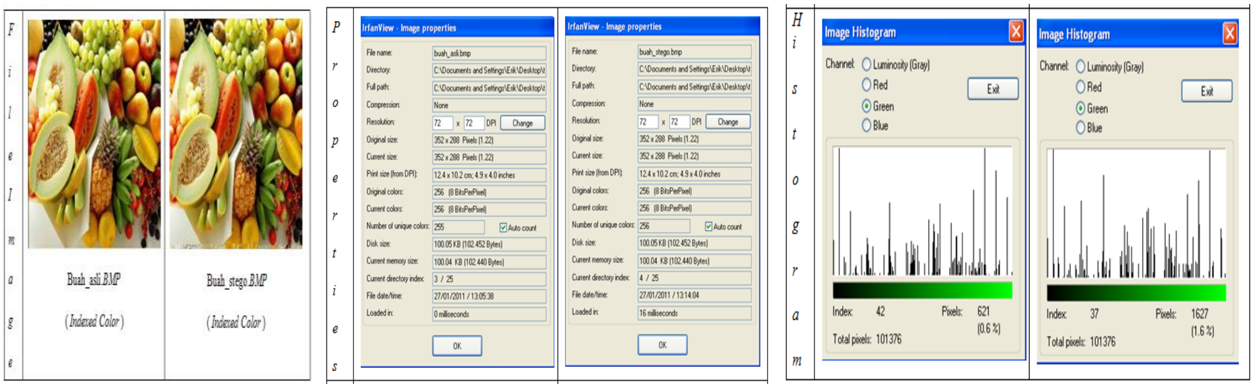
Channel: ● Luminosity (Gray) ○ Red ○ Green ○ Blue
Index: 228 Pixels: 10590 (1.7 %)
Total pixels: 617864

a) Input b) Process c) Output

Figure 2. Testing With Cover Image for Black and White

Testing With Color Indexed Color Cover Image

In Figure 3 in the second test, the cover image test was carried out with the type indexed color (256 colors - 8 bpp) with a Buah_asli.bmp image file and a Buah_stego.bmp image as input data. The size of the resolution, dpi, and size of the cover image does not change, but changes occur in the histogram graphic, and there is slight damage to the image at the bottom of the image.



IrfanView - Image properties

File name: buah_asli.bmp
Directory: C:\Documents and Settings\Erik\Desktop\t
Full path: C:\Documents and Settings\Erik\Desktop\t
Compression: None
Resolution: 72 x 72 DPI Change
Original size: 352 x 288 Pixels (1.22)
Current size: 352 x 288 Pixels (1.22)
Print size (from DPI): 12.4 x 10.2 cm; 4.9 x 4.0 inches
Original colors: 256 (8 BitsPerPixel)
Current colors: 256 (8 BitsPerPixel)
Number of unique colors: 255 ☑ Auto count
Disk size: 100.05 KB (102.452 Bytes)
Current memory size: 100.04 KB (102.440 Bytes)
Current directory index: 3 / 25
File date/time: 27/01/2011 / 13:05:38
Loaded in: 0 milliseconds
OK

IrfanView - Image properties

File name: buah_stego.bmp
Directory: C:\Documents and Settings\Erik\Desktop\t
Full path: C:\Documents and Settings\Erik\Desktop\t
Compression: None
Resolution: 72 x 72 DPI Change
Original size: 352 x 288 Pixels (1.22)
Current size: 352 x 288 Pixels (1.22)
Print size (from DPI): 12.4 x 10.2 cm; 4.9 x 4.0 inches
Original colors: 256 (8 BitsPerPixel)
Current colors: 256 (8 BitsPerPixel)
Number of unique colors: 256 ☑ Auto count
Disk size: 100.05 KB (102.452 Bytes)
Current memory size: 100.04 KB (102.440 Bytes)
Current directory index: 4 / 25
File date/time: 27/01/2011 / 13:14:04
Loaded in: 16 milliseconds
OK

Index: 42 Pixels: 621 (0.6 %)
Total pixels: 101376

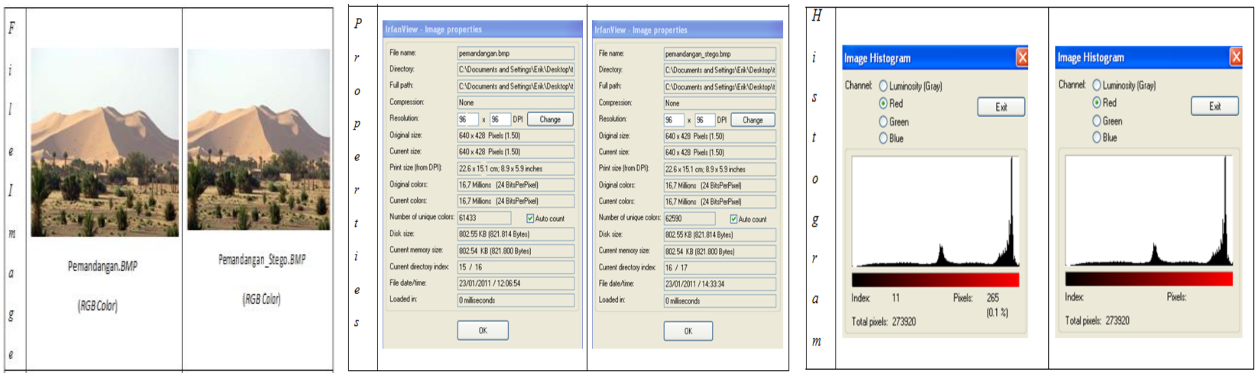
Index: 37 Pixels: 1627 (1.6 %)
Total pixels: 101376

a) Input b) Process c) Output

Figure 3. Testing with Colored Cover Image Type Indexed Color

Testing System With Color Cover Image Type RGB Color

From the results of Figure 4, it can be concluded that the results of input (pemandangan.bmp and pemandangan_stego.bmp) and output do not change in terms of resolution, dpi, and cover image size. In the grayscale image format (256 colors - 8bpp), there is only a change in the histogram graphic, and the indexed color format (256 colors - 24bpp) has a little damage to the stego image, while the image in the RGB color format (16.7 million colors - 24bpp) occurs unique color change. The indexed color format only supports 8 bits per pixel, and the image type is in RGB format. The third steganography application system's third test is the cover image of the RGB color type (16.7 million colors - 24bpp). Where the resolution, dpi and size of the cover image, histogram and stego image do not change visually, the unique color is clearly visible.



IrfanView - Image properties

File name: pemandangan.bmp
Directory: C:\Documents and Settings\Erik\Desktop\t
Full path: C:\Documents and Settings\Erik\Desktop\t
Compression: None
Resolution: 96 x 96 DPI Change
Original size: 640 x 428 Pixels (1.50)
Current size: 640 x 428 Pixels (1.50)
Print size (from DPI): 22.6 x 15.1 cm; 8.9 x 5.9 inches
Original colors: 16,7 Millions (24 BitsPerPixel)
Current colors: 16,7 Millions (24 BitsPerPixel)
Number of unique colors: 61433 ☑ Auto count
Disk size: 802.55 KB (821.814 Bytes)
Current memory size: 802.54 KB (821.800 Bytes)
Current directory index: 15 / 16
File date/time: 23/01/2011 / 12:06:54
Loaded in: 0 milliseconds
OK

IrfanView - Image properties

File name: pemandangan_stego.bmp
Directory: C:\Documents and Settings\Erik\Desktop\t
Full path: C:\Documents and Settings\Erik\Desktop\t
Compression: None
Resolution: 96 x 96 DPI Change
Original size: 640 x 428 Pixels (1.50)
Current size: 640 x 428 Pixels (1.50)
Print size (from DPI): 22.6 x 15.1 cm; 8.9 x 5.9 inches
Original colors: 16,7 Millions (24 BitsPerPixel)
Current colors: 16,7 Millions (24 BitsPerPixel)
Number of unique colors: 62590 ☑ Auto count
Disk size: 802.55 KB (821.814 Bytes)
Current memory size: 802.54 KB (821.800 Bytes)
Current directory index: 16 / 17
File date/time: 23/01/2011 / 14:33:34
Loaded in: 0 milliseconds
OK

Index: 11 Pixels: 265 (0.1 %)
Total pixels: 273920

Index: Pixels:
Total pixels: 273920

a) Input b) Process c) Output

Figure 4 Testing With Color Cover Image Type RGB Color

Table 3. Test Result Data

No	Cover Image			Stego Image			MSE	PSNR	Time
	Name	Size Image	Size Teks	Name	Size Image	Size Teks			
1	image grayscale.bmp	605,8 kb	790 byte	Image grayscale _stego.bmp	605,8 kb	790 byte	0,305	53,289	0 ms
2	Buah_asli.bmp	100,1 kb	790 byte	Buah_stego.bmp	100,1 kb	790 byte	0,086	58,827	16 ms
3	Pemandangan.bmp	802 kb	790 byte	Pemandangan_steg o.bmp	802 kb	790 byte	0,051	61,064	0 ms

Color supports 24bit / pixel; the more bits used, the more color displays and the sharper image results, causing hidden files to be more invisible to the naked eye. The test results mean square errors (MSE), the program's success is 100% - 1.75% = 98.25%, and from the Peak Signal to Noise Ratio (PSNR). In total, the program success is at 55.2db, or the image is of good quality.

Analysis of the results of testing the steganography application system from the tests that have been carried out:

a. a Cover image that has undergone an encoding process on the system compared to the original cover image does not experience changes in file size and resolution size. Because the steganography system only performs the insertion process in the LSB of the cover image structure and does not change the size and resolution structure of the cover image.
b. Cover image with grayscale 8-bit format supports the process in the steganography system, where the file size, dpi, and resolution do not change; changes occur only in the histogram graphic. However, the indexed color format does not support Steganography because there is still a little damage to the image, and there is a change in the histogram. The file size, dpi, and resolution have not changed. Whereas in the 24-bit RGB Color format, it is very supportive for processes in the steganography system, where the file size, dpi, histogram, and resolution do not change; changes occur only in unique colors.
c. Image file must always be larger than the size of the text file because an image file is a container for inserting the text file. Suppose the size of the text message exceeds the size capacity on the cover image. In that case, the encoding process cannot be executed, so when the decoding process is executed, it will fail, and an error message will appear.
d. Program success rate by means of square errors (MSE) is 98.25%, and the Peak Signal to Noise Ratio (PSNR) image quality is at 55.2db or good image quality.
e. The results of the execution time to complete encryption and decryption on the results of Testing With Cover Image for Black & White and Cover Image Type RGB Color are 0 ms, while the results of Testing with Colored Cover Image Type Indexed Color is 16 ms

Conclusion

The results of system analysis and testing are image files that have been processed with the LSB and Haar Wavelet methods that do not change the file size, resolution, dpi, and physical form of the image, as well as text files that are in accordance with the ASCII character format, can be easily converted into binary. With the 8-bit grayscale format and 24-bit RGB color format, stego images can be produced unchanged in file size, resolution, dots per inch (dpi), and the physical form of the image so that the LSB method used in the steganography application system can be applied.

References

Abbas, A. L., Radhi, S. K., & Hussain, A. K. 2021. Haar wavelet method for solving coupled system of fractional order partial differential equations. Indonesian Journal of Electrical Engineering and Computer Science, 21(3), 1444-1454.

Abdeljawad, T., Amin, R., Shah, K. Al-Mdallal, Q. and Jarad. F. 2020. Efficient sustainable algorithm for numerical solutions of systems of fractional order differential equations by Haar wavelet collocation method. Aleexandaria Engineering Journal.

Ahmmed, T., Raha, I.T. Safwat, F. and Turzo, N.A. 2021. Impact of Message Size on Least Significant Bit and Chaotic Logistic Mapping Steganographic Technique.

Al-Hussein, A.I., Alfaras, M.S. and Kadhim, T.A. 2021. Text hiding in an image using least significant bit and ant colony optimization. Materials Today: Proceedings.

Al-Huwais, N.H., Atiyah, Y.A., Parvin, S. and Gawanmeh, A. 2020. An Improved Least Significant Bit Image Steganography Method. In 2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA). IEEE. pp. 90-96

Amin, R., Shah, K. Asif, M. Khan, I. and Ullah, F. 2020. An efficient algorithm for numerical solution of fractional integro-differential equations via Haar wavelet. Journal of Computational and Mathematics, 1: 113028.

Chen, C.F. and Hsiao, C.H. 1997. Haar wavelet method for solving lumped and distributed-parameter systems. IEEE Proc. Control Theory Appl, 144(1): 87-94.

Fu, Z., Wang, F., and Cheng, X. 2020. The secure Steganography for hiding images via GAN. EURASIP Journal on Image and Video Processing, (1): 1-18.

Govindasamy, V., Sharma, A. and Thanikaiselvan, V. 2020. Coverless Image Steganography using Haar Integer Wavelet Transform. In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC). IEEE. pp. 885-890

Gul, H., Alrabaiah, H. Ali, S. Shah, K. and Muhammed, S. 2020. Computation of Solution to Fractional Order Partial Reaction Diffusion Equations. Journal of Advanced Research, 15: 1-8.

Gunawan, W. 2019. Haar Like Feature Algorithm in the Questionnaire Application with Face Recognition and LBS Methods. International Journal of Computer Science and Information Security (IJCSIS), 17(11)

Hamid, N., Yahya, A. Ahmad, R.B., and Al-Qershi, O.M. 2012. Image steganography techniques: an overview. International Journal of Computer Science and Security, 6(3), 168-187.

Hasanudin, M. and Yuliadi, B. 2020. Lifi: Light Fidelity In The School Library. International Journal of Information System and Computer Science, 5(2): 70-76.

https://www.semanticscholar.org/paper/A-DWT-Based-Approach-for-Image-Steganography-Chen-Lin/1a7b404bdd21a45bccf86034a01e555f3762dee5, accessed December 2020

Oo, B.B. and Aung, M.T. 2020. Enhancing Secure Digital Communication Media Using Cryptographic Steganography Techniques. In 2020 International Conference on Advanced Information Technologies (ICAIT) IEEE. pp. 1-6.

Pandey, J., Joshi, K. Sain, M. Singh, G. and Jangra, M. 2021. Steganographic Method Based on Interpolation and Cyclic LSB Substitution of Digital Images. In Advances in Communication and Computational Technology, Springer, Singapore. pp. 731-744.

Roshini, R. and Meena, C. 2020. Review on Steganography for hiding images and security issues.

Shah. K. 2019. Using a numerical method by omitting discretization of data to study numerical solution for for boundary value problems of fractional order differential equations," Mathematical Methods in the Applied Sciences. 42(8): 6944-6959.

Sudrajat, T. 2020. Implementasi metode haar cascade classifier untuk pendeteksian wajah pada aplikasi smart bus menggunakan raspberry pi (Doctoral dissertation, Universitas Mercu Buana Jakarta)

Thangadurai, K. and Devi, G.S. 2014. An analysis of LSB based image steganography techniques. In 2014 International Conference on Computer Communication and Informatics. IEEE. pp 1-4