Borneo International Journal eISSN 2636-9826; Vol. 6 (4); 2023; 60-66
Published by *Majmuah Enterprise*
www.majmuah.com

Information Hiding in Image Using Amplitude Modulation Algorithm

ALAA JABBAR QASIM ALMALIKI[1], ROSHIDI DIN[1], SUNARIYA UTAMA[1]
, SALAM GHANIM NAJEEB[2], JABBAR QASIM ALMALIKI[3]

[1]*School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah Darul Aman, MALAYSIA*
[2]*Department of Medical Laboratories, College of Health and Medical Techniques, Sawa University, Almuthana, Iraq*
[3]*Ashur University, Department of Medical Instrumentation Technique Engineering College, Baghdad, Iraq*

Email :[1]alaa_jabbar@ahsgs.uum.edu.my, [1]roshidi@uum.edu.my, [1]sunariya.utama1@ahsgs.uum.edu.my , [2]Salam.alnajeb@yahoo.com , [3]Jabbar.qassim.f@au.edu.iq
| Tel : | [1]+60184020823 ,[1]+60175981306, [1]+601131548575, [2]+9647813000043, [3]+9647901530655|

Received: December 18, 2023
Accepted: December 21, 2023
Online Published: December 28, 2023

Abstract
With the development of technology, information is now transmitted through digital media. At this point, the concept of information security gains importance. It is the most valuable meta-information today. Many methods have been designed to transmit information in secure ways. While encryption, which is one of these methods, aims to protect the content of the message, steganography aims to hide the message's existence. Greek word meaning "hidden writing" steganography aimed to hide the existence of data. In this study, amplitude modulation, which is one of the steganography algorithms, the algorithm is examined.

Keywords: Steganography; amplitude modulation algorithm; information hiding.

1. Introduction

Steganography is an important method of concealing information (R. Din & Utama, 2023; R. J. B. I. J. e.-. Din, 2023a, 2023b). Information hiding has been used since ancient times. Nowadays, advanced algorithms have replaced primitive methods for information hiding. Currently, steganography applications are conducted on digital objects, and due to advancing technology, they have become frequently used in recent years to protect data. Steganography is divided into two categories: Linguistic Steganography and Technical Steganography. Linguistic steganography is the branch where the carrier data is text. Technical Steganography encompasses various topics. These include invisible ink, secret compartments, microdots, and computer-based methods. The purpose of steganography is to hide the existence of a secret message or information. The intended message is concealed in another seemingly innocent medium, preventing third parties from being aware of the message's existence. Data can be hidden in text, sound, digital images, and video files. These data can be a text file or can involve hiding one image within another. Similarly, a text file can be hidden within an audio file (Alyousuf, Din, Qasim, & Informatics, 2020; Qasim & Alyousuf, 2021; Qasim, Din, Alyousuf, & Informatics, 2020; Utama, Din, & Technology, 2022). In a Stego-system, the medium where information is hidden is called cover data (cover data), and the resulting medium is referred to as Steg text or stego-object [4]. Although steganography and encryption are closely related, they differ in many aspects. Encryption aims to protect information by making it unreadable, while steganography aims to conceal information within a medium so that it is not detected. In this sense, steganography adds an element of security to cryptography. Steganography is divided into three categories based on its application areas. These are text, image, and audio steganography(R. Din, Bakar, et al., 2019; R. Din, Mahmuddin, Qasim, & Technology, 2019; R. Din, Qasim, Abdullah, Elias, & Technology, 2019; R. Din, Qasim, & Informatics, 2019; Razali, Mustapha, Utama, & Din, 2018).

- Text steganography is the field where the medium for hiding information is text. Generally, the text to be hidden can be embedded in another text using various methods such as the meanings or arrangements of words, punctuation, extra space usage, or ASCII encoding.
- Image steganography has become the most used steganography method with the development of digital images. Data can be embedded in the color bits of the pixels in the image. Common methods include data storage in the least significant bit, masking and filtering, algorithms, and transformations.

- Audio steganography is a challenging branch of steganography. Data hiding using low bit coding of audio signals is the most preferred method of audio steganography, along with phase coding, spread spectrum, and echo data hiding among other methods.

In this study, the amplitude modulation algorithm, which is one of the image steganography algorithms, has been examined.

2. Structure of Digital Image

A numeric display is an array of N rows and M columns. Each apple of the array is called a pixel. In the simplest images, the pixel value can be 1 or 0. This type of image is called a binary pattern. Usually, data hiding is done on 24-bit images. This type of image uses 3 bytes per pixel. The color of each pixel; is obtained from three main colors like red (red), green (green), blue (blue). This called RGB value of the pixel(Bosch, Bosch, Bosch, Bosch, & Mathematician, 2006; R. Din, Ghazali, & Qasim, 2017; R. Din, Ghazali, Qasim, & Science, 2018; Westfeld & Pfitzmann, 1999).

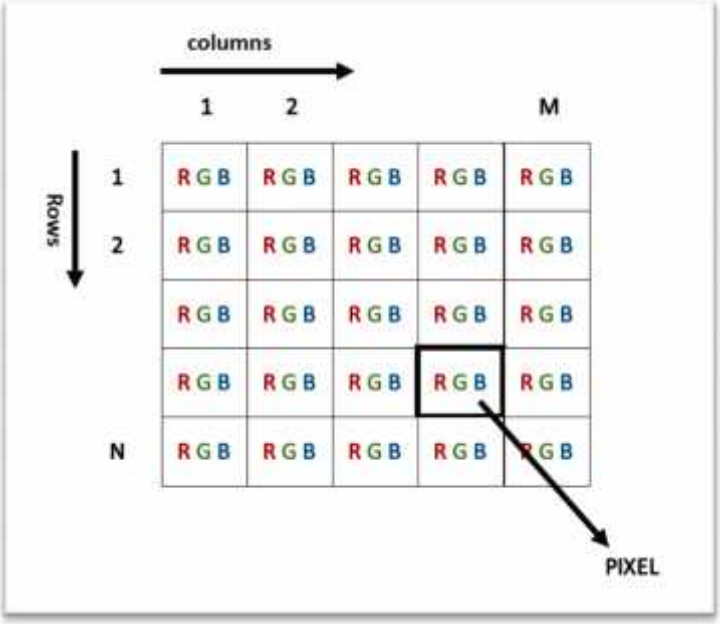


Figure 1: 24-bit image structure

In a 24-bit image, each color is expressed as binary codes that take values between 0 and 255. For example, the RGB code of a turquoise pixel is as follows(Alyousuf et al., 2020; R. Din, Qasim, & Informatics, 2019; Qasim et al., 2020).

R = 48 = 00110000

G = 214 = 11010110

B = 200 = 11001000.

3. Amplitude Modulation

Amplitude modulation is an algorithm that aims to hide data on the blue color channel. In general, the algorithm data will be hidden pixel link is based on increasing or decreasing the blue channel value according to the ratio of the light or the value of the bit. The scheme of the data hiding process according to the amplitude modulation method is shown in figure 2.

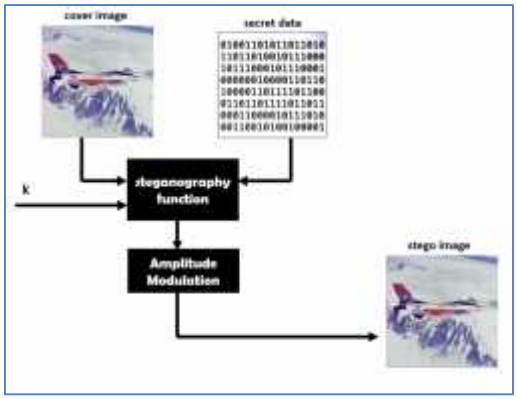


Figure 2: Amplitude Modulation (data hiding)

The human eye can see color values between 400 nm (nanometres) and 700 nm (Figure 3). The blue color is between 400 nm and 500 nm, the first part in the visible area. Therefore, the color in which the change will be noticed the least compared to other colors is blue. If small changes are made on the blue channel to hide the data, the detectability of the secret data will be difficult. The coordinates to be hidden are stored at the points produced by the K key and the random number generator. The data to be stored is placed in the i and j coordinates, which are randomly selected each time(Alwan, Farhan, Mahdi, & Engineering, 2020; Alyousuf et al., 2020).

• B (j,j) indicates the blue hue in the i,j coordinate.

• L (i,j)=0.299R(lj)+0.587G(lj)+0.114B(lj)

• B it (0 or 1) to store the S value

• The q value is a fixed value selected between 0 and 1 to prevent detection of the information to be stored.

With the help of the above formulas and values, the new blue channel color value for the i,j coordinate is calculated according to equation 1.

$$B_{[} = B_{[} + (2s - 1)\, L_{[}\, q$$
(1)

The calculated Bi value is the new blue color channel value of the pixel.

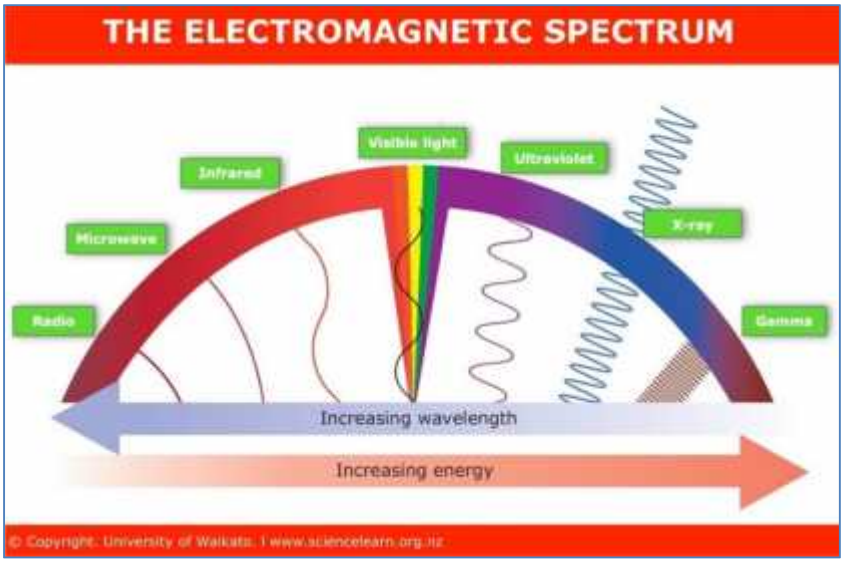


Figure 3: Electromagnetic Spectrum

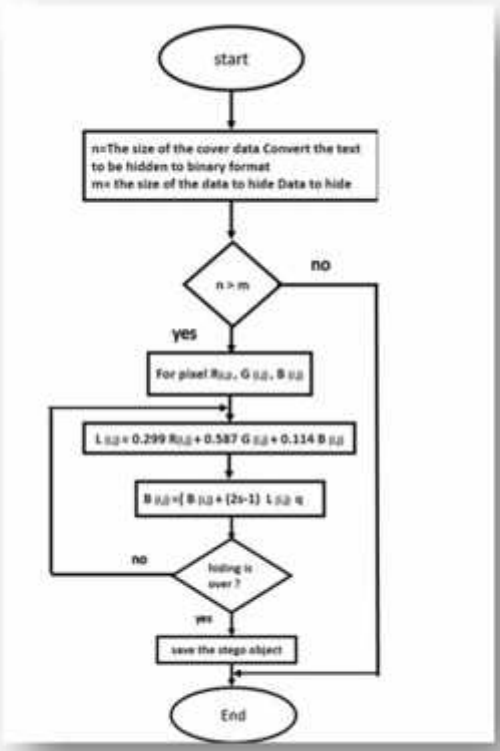


Figure 4: Data hiding algorithm

For example, you want to hide 11000001 data. To hide 1, the first element of the data array to be hidden, the RGB values of the first randomly selected i,j coordinate are 125, 91, 136, respectively.

L = 0.299 * 125 + 0.587 * 91 + 0.114 * 136

= 37.375 + 53.417 + 15.504 = 106.296

B = 136 + (2 * 1 - 1) * 106.296 * 0.5=189.148

According to the calculated values, the new RGB codes of the pixel will be 125, 91, 189, respectively. This change appears to be numerically large, but since the changes made on the blue color channel are perceived less by the eye, the change in the picture is too small to be felt. Similarly, other bits of the data to be hidden are also hidden to the specified coordinates. Flowchart of data hiding algorithm It is shown in Figure 4.

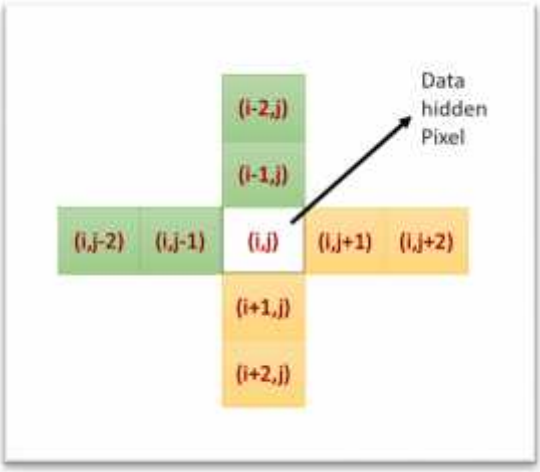


Figure 5: pixel neighbors for c = 2

Borneo International Journal eISSN 2636-9826; Vol. 6 (4); 2023; 60-66
Published by *Majmuah Enterprise*
www.majmuah.com

With the amplitude modulation algorithm, the original blue color values of the cover data need to be estimated to retrieve data from a stego-object whose data is hidden. This prediction is based on the linear combination of the blue channel values of the pixel's neighbors. The best method for estimating the old blue channel color will be to calculate the values of the pixel's neighbors. First of all, to reproduce the data hiding coordinates(Khudher, 2021; Madhi, Shareef, Hashem, Ali, & Sciences, 2021), the locations of the changed pixels are determined with the K key used at the time of hiding. Then, using equation 2, the old blue channel color is estimated by considering the neighbors of the pixel with the data hidden.

$$\hat{B_{i,j}} = \frac{1}{4k}\left(\sum_{k=-c}^{k} B_{i+k,j} + \sum_{k=-c}^{k} B_{i,j+k} - 2B_{i,j}\right)$$

(2)

Control for the c value pixel in Equation 2 is the number of neighbours to be

After estimating the pixel's value, the difference between the estimated blue channel value and the current blue channel value is taken by equation 3. The sign of this difference represents the value of the hidden bit.

$$\delta = \hat{B_{i,j}} - B_{i,j}$$

(3)

Accordingly, the flow chart of the data acquisition processes is expressed in Figure 6. Random coordinates for data hiding or extraction operations in multiple data hiding operations are arranged in a certain order. It needs to be sorted. In these cases, sorting horizontally or vertically plays a role in facilitating attacks(Hanizan Shaker Hussain, 2018; Jiménez-Rodríguez et al., 2018). Instead, making a zig-zag sequence as in Figure 7 will make the attacker's job more difficult(Al-Smadi et al., 2021; Khudher, 2021; Lincy Rachel Mathews 2014; Madhi et al., 2021; Qasim & Alyousuf, 2021; S.Jayasudha, 2013; Vijay, Jayareka, Kirubasri, & Vijay, 2021).

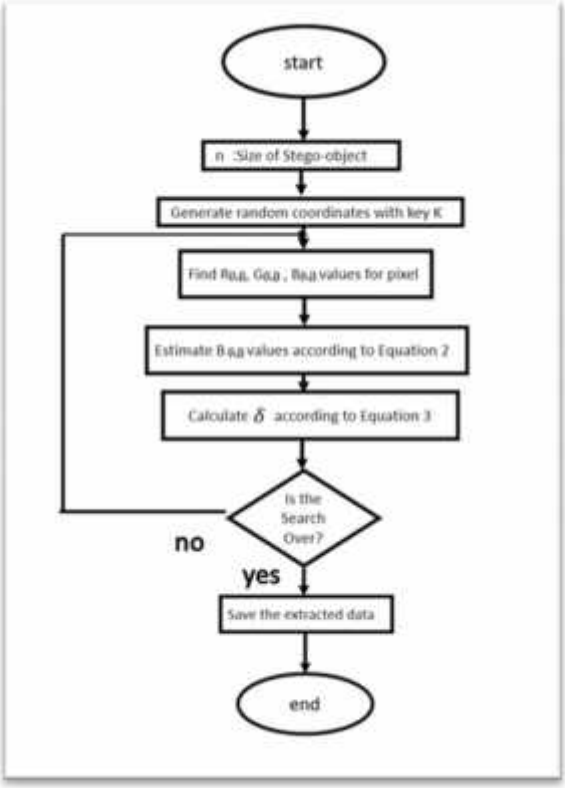


Figure 6: Flow chart of the processes of obtaining confidential data

4. Case Study

A message of 2048 (16384 bit) characters and 304 words were hidden in the 662x529 pixel picture in figure 8(a) belonging to Abidin Dino, and the picture in figure 8(b) was created. The change in Figure 8(b) is invisible to the human eye, but when the figure is examined with the help of a computer, the change in pixels can be seen. The color values of the pixel at i=100, j=252 coordinates in the data When the value one is hidden in this pixel while R:100, G:106, B:118 color values changed as R:100, G:106, B:171.

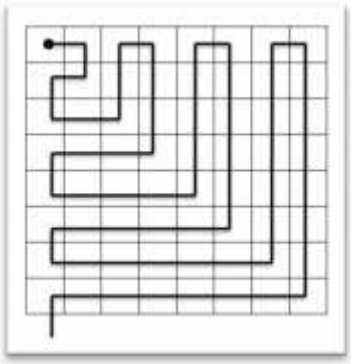
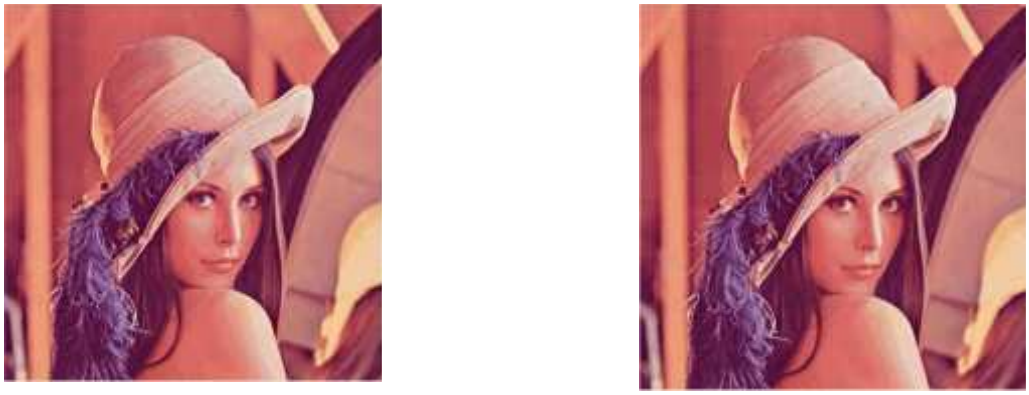


Figure 7: Zigzag data hiding



(a) (b)

Figure 7: Example data hiding

5. Conclusions

The strategy for embedding most steganographic systems of overwriting the least significant bits is at best resistant to apparent attacks. On the one hand, the visual attacks showed that the least significant bits are generally not irrelevant, as is required by today's steganographic applications. On the other hand, it has been shown that irrelevance alone is not enough to prevent attacks. Overwriting the least significant bits leaves traces as statistically independent frequencies are compensated. Statistical attacks are superior to visual attacks because they are not based on the image content of the carrier file. As the embedding rate decreases (in the simplest case by spreading the data to be embedded), the probability of error of the attack increases. Unfortunately, the relative throughput drops and the algorithm works less electively. In the extreme case, we have an application that is completely secure but does not embed anything. Analogous to the development of cryptography, the presented took a step in the iterative process that leads to more secure steganographic systems. Better algorithms should use the operation replace writing with others, e.g. B. by incrementing. Frequencies are then not balanced out, but rather circulate in the range of values. The steganographic changes must also remain limited to the noise maxima of the carrier medium and should not be localized there deterministically. As an alternative to the iterative process (attack defines), non-deterministic phenomena from input devices can be used, such as that of a camera or a scanner. The examination of input devices shows free spaces that allow the embedding of data. If stenographic techniques simulate the peculiarities of a camera, this will be the case do not raise doubts to a potential attacker.

References

Al-Smadi, A. M., Al-Smadi, A., Ali Aloglah, R. M., Abu-Darwish, N., Abugabah, A. J. I. J. o. E., & Engineering, C. (2021). Files cryptography based on one-time pad algorithm. 11.

Alwan, Z. A., Farhan, H. M., Mahdi, S. Q. J. I. J. o. E., & Engineering, C. (2020). Color image steganography in YCbCr space. 10(1).

Alyousuf, F. Q. A., Din, R., Qasim, A. J. J. B. o. E. E., & Informatics. (2020). Analysis review on spatial and transform domain technique in digital steganography. 9(2), 573-581.

Bosch, K., Bosch, K., Bosch, K., Bosch, K., & Mathematician, G. (2006). Elementare Einführung in die Wahrscheinlichkeitsrechnung (Vol. 6): Springer.

Din, R., Bakar, R., Utama, S., Jasmis, J., Elias, S. J. J. B. o. E. E., & Informatics. (2019). The evaluation performance of letter-based technique on text steganography system. 8(1), 291-297.

Din, R., Ghazali, O., & Qasim, A. J. J. I. J. E. E. C. S. (2017). Analytical review on graphical formats used in image steganographic compression. 5(3), 401-408.

Din, R., Ghazali, O., Qasim, A. J. J. I. J. o. E. E., & Science, C. (2018). Analytical review on graphical formats used in image steganographic compression. 12(2), 441-446.

Din, R., Mahmuddin, M., Qasim, A. J. J. I. J. o. E., & Technology. (2019). Review on steganography methods in multi-media domain. 8(1.7), 288-292.

Din, R., Qasim, A. J., Abdullah, S., Elias, S. J. J. I. J. o. E., & Technology. (2019). Analysis Review on Image Compression Domain. 8(1.7), 293-296.

Din, R., Qasim, A. J. J. B. o. E. E., & Informatics. (2019). Steganography analysis techniques applied to audio and image files. 8(4), 1297-1302.

Din, R., & Utama, S. J. B. I. J. e.-. (2023). The Design Review of Feature-based Method in Embedding the Hidden Message in Text as the Implementation of Steganography. 6(3), 88-95.

Din, R. J. B. I. J. e.-. (2023a). Comparative Analysis of Methods for Digital Steganography in Images. 6(3), 119-127.

Din, R. J. B. I. J. e.-. (2023b). Comparison Of Steganographic Techniques of Spatial Domain and Frequency Domain in Digital Images. 6(3), 109-118.

Hanizan Shaker Hussain, R. D., Mohd Hanif Ali, Nor Balqis. (2018). The Embedding Performance of StegSVM Model in Image Steganography. Indonesian Journal of Electrical Engineering and Computer Science, Vol. 12.

Jiménez-Rodríguez, M., Padilla-Leyferman, C. E., Estrada-Gutiérrez, J. C., González-Novoa, M. G., Gómez-Rodríguez, H., & Flores-Siordia, O. J. I. e. i. (2018). Steganography applied in the origin claim of pictures captured by drones based on chaos. 38(2), 61-69.

Khudher, I. M. J. E.-E. J. o. E. T. (2021). LSB Steganography Strengthen Footprint Biometric Template. 1(9), 109.

Lincy Rachel Mathews , A. C. H. V. (2014). Histogram Shifting Based Reversible Data Hiding. nternational Journal of Engineering Trends and Technology (IJETT), 10(10).

Madhi, H. H., Shareef, M. S., Hashem, S. A., Ali, A. W. J. P. o. E., & Sciences, N. (2021). Pixel steganography method for grayscale image steganography on colour images. 9(3), 615-624.

Qasim, A. J., & Alyousuf, F. Q. A. J. Q. Z. J. (2021). History of image digital formats using in information technology. 6(2), 1098-1112.

Qasim, A. J., Din, R., Alyousuf, F. Q. A. J. B. o. E. E., & Informatics. (2020). Review on techniques and file formats of image compression. 9(2), 602-610.

Razali, N., Mustapha, A., Utama, S., & Din, R. (2018). A review on football match outcome prediction using bayesian networks. Paper presented at the Journal of Physics: Conference Series.

S.Jayasudha. (2013). Integer Wavelet Transform Based Steganographic Method Using Opa Algorithm. International Journal Of Engineering And Science, 2(Issn: 2278-4721), Pp 31-35.

Utama, S., Din, R. J. J. o. A. R. i. A. S., & Technology, E. (2022). Performance Review of Feature-Based Method in Implementation Text Steganography Approach. 28(2), 325-333.

Vijay, K., Jayareka, K., Kirubasri, G., & Vijay, P. J. A. o. t. R. S. f. C. B. (2021). Enhancing the Security of Data Using Digital Stemage Technique. 25(6), 9138-9143.

Westfeld, A., & Pfitzmann, A. (1999). Attacks on steganographic systems: Breaking the steganographic utilities EzStego, Jsteg, Steganos, and S-Tools-and some lessons learned. Paper presented at the International workshop on information hiding.