International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 23 (2017) pp. 13944-13950

Analysis of JPEG Image Steganography Using Spread Spectrum Method

Jordy Ardian Bagaskara
Department of Computer Engineering,
Telkom University, Bandung-40257, West Java, Indonesia.
Orcid Id: 0000-0002-5977-038X

Tito Waluyo Purboyo
Department of Computer Engineering,
Telkom University, Bandung-40257, West Java, Indonesia.
Orcid Id: 0000-0001-9817-3185

Ratna Astuti Nugrahaeni
Department of Computer Engineering,
Telkom University Bandung-40257, West Java, Indonesia.
Orcid Id: 0000-0002-5471-9593

Abstract

This paper discusses an analysis on Steganography technique performed on JPEG digital images to find out the representation of the image using Spread Spectrum algorithm. Spread Spectrum Algorithm performs the deployment of encoded messages spread to every possible frequency spectrum. The analysis was performed on JPEG format images with RGB and Grayscale type, with the result of comparison between image resolution (pixel) with message size, image resolution with message size (bit), and image size (kb) with steganographic image size (kb).

Keywords: Steganography, JPEG Image, Spread Spectrum Image Steganography.

INTRODUCTION

Information is a message in the form of speech or expression can consist of symbols, or meaning that can be interpreted from a message or a collection of messages. In his use sometime there is special information to be conveyed to others and do not want to be known by people who are not addressed by the owner of the information, there are several ways to maintain the confidentiality of data.

One of them by using cryptography where this method encrypts a data into a random code, so it takes a special technique to read it. Steganography is another technique to hide information on a media. The media can be audio, image, or video.

Changes that occur in the media using steganography technique is not seen conspicuously. This research analysis the use of Spread Spectrum algorithm on steganography to know the difference between the two algorithms, the security level, and the changes that occur in the image based on the use of both algorithms.

STEGANOGRAPHY

Steganography is a technique to hide the information on a cover media, which can be image, audio, or video file [1]. The first recorded uses of steganography can be traced back to 440 BC when Herodotus mentions two examples in his Histories.[2] Histiaeus sent a message to his vassal, Aristagoras, by shaving the head of his most trusted servant, "marking" the message onto his scalp, then sending him on his way once his hair had regrown, with the instruction. “When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon." Additionally, Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces, sometimes used for shorthand. In his work Polygraphiae Johannes Trithemius developed his so-called "*Ave-Maria-Cipher*" that can hide information in a Latin praise of God. "*Auctor Sapientissimus Conseruans Angelica Deferat Nobis Charitas Potentissimi Creatoris*" for example contains the concealed word VICIPEDIA.[3]

In steganography, the existence of information cannot be seen visually and the quality of cover media does not change significantly. Some implementations of steganography that lack a shared secret are forms of security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoffs's principle. [4] The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal. [5]

Currently there are several techniques of steganography that are often used. Here are some commonly used techniques:

1. The substitution technique, by making a certain pixel replacement of the cover image. An example method is LSB.

2. Transform Domain Techniques, by storing confidential information through space transformation. An example of his method is DCT (Discrete Cosine Transform).
3. Spread Spectrum Techniques, this technique the secret information is stored and spread in a certain frequency.
4. Statistical Techniques, the data is encoded with this technique through the conversion of some statistical information from the file container. The file container for the block where each block holds a hidden secret pixel.
5. Distortion Techniques, hidden information based on signal distortion.
6. Cover Generation Techniques, this technique hides confidential information that fits the cover. [6]

The process of steganography can be seen on Figure 1.

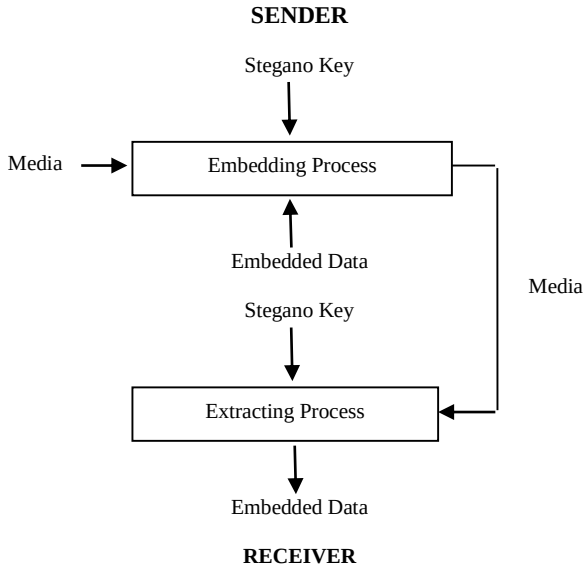

Figure 1: Steganography Process.

JPEG Image

Joint Photographic Experts Group (JPEG) is a standard of lossy compression for digital images, the degree of compression can be adjusted to allowing selectable tradeoff between storage size and image quality. The degree of compression can be adjusted, allowing a selectable tradeoff between storage size and image quality. JPEG typically achieves 10:1 compression with little perceptible loss in image quality. [7] JPEG supports a maximum image size of 65.535 x 65.535 pixels. [8] Hence up to 4 gigapixels for an aspect ratio of 1:1. The standard file format known as "JPEG Interchange Format" (JIF). This file format is rarely used because the difficulty of programming encoders and decoders that fully implement standard.

- Color space definition.
- Component sub-sampling registration.
- Pixel aspect ratio definition.

Spread Spectrum Algorithm

The Spread Spectrum algorithm is a technique that does cover-image as noise and as pseudo noise into the cover-image. A value can be added to the cover-object by transmitting under the added noise value. The process of Spread Spectrum is shown in the Figure 2.

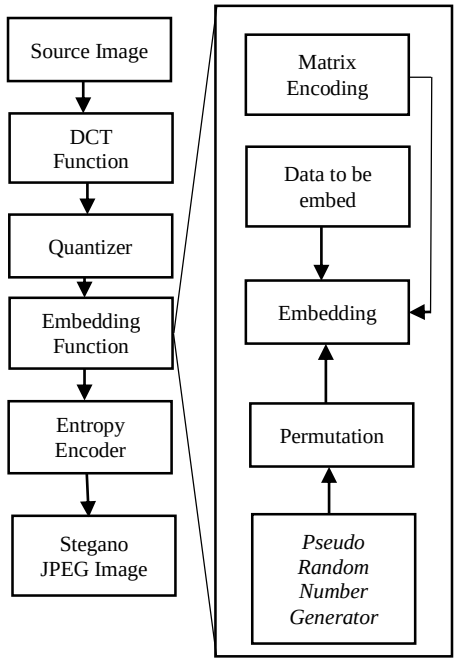

Figure 2: Spread Spectrum Process.

Here are the stages done in the implementation of the algorithm.

1. JPEG image compression process. By taking the 8x8 block on the original image then done the process of DCT transformation and quantization process.
2. Initialize the Pseudo Random Generator Number by using the key of the password used.
3. The permutation process is performed using the PRNG parameter and the sum of the DCT coefficients.
4. Determine the K value of the embedding capacity in the image data and from the message data length.
5. Determine the length of the code word (the array that holds the non-zero coefficients) by the formula $n = 2k - 1$.
6. Perform embedding process to insert message data with $(1, n, k)$ algorithm for matrix encoding.
   a. Charges an array of buffers with non-zero coefficients.
   b. Performs a hashing process on a buffer (to generate hash value with k bit-places).
   c. Adding the next k bits of the message data to the hash value (do in bits per bit with the XOR operator)
   d. If result = 0, then the buffer is not changed. But if the result obtained = 0, then the absolute value of the element in the index should be reduced 1
   e. Checking the changed coefficients is not 0, If the same then the shrinkage process occurs by adding a non-zero

coefficient on the buffer and remove the coefficient value 0

f. If no shrinkage occurs then the contents of the buffer with the next DCT coefficient (starting from the last coefficient index plus 1)

g. Next do JPEG data compression process. [10]

ASCII

ASCII is the traditional name for the encoding system; the Internet Assigned Numbers Authority (IANA) prefers the updated name US-ASCII, which clarifies that this system was developed in the US and based on the typographical symbols predominantly in use there. [11]

ASCII was developed from telegraph code. Its first commercial use was as a seven-bit teleprinter code promoted by Bell data services. Work on the ASCII standard began on October 6, 1960, with the first meeting of the American Standards Association's (ASA) (now the American National Standards Institute or ANSI) X3.2 subcommittee. The first edition of the standard was published in 1963,[12][13] underwent a major revision during 1967,[14][15] and experienced its most recent update during 1986.[16]

Analysis

Implementation is performed on JPEG images in Grayscale and RGB formats, with 5 image sizes start from 4x4, 5x5, 6x6, 7x7, and 8x8. The purpose of the test is to determine the comparison of several factors found in the implementation of steganography using Spread Spectrum algorithm. Then performed a calculation manually to know the comparison and result analysis as follows.

a. Comparison of image resolution (pixel) with message characters.

b. Comparison of image resolution (pixel) with message size (bit).

c. Comparison of image size (kB) with steganographic image size (kB).

The comparison of image resolution with message characters use the following formula.

Greyscale = (length x *width)* ÷ 8

RGB = (length x *width)* x *3* ÷ *8*

The comparison of image resolution with message size use the following formula.

Greyscale = (length x *width)* ÷ *8*

RGB = (length x *width)* x 3 ÷ 8

The comparison of image size with steganographic image size use the following formula:

(stegano image size – normal image size)

Table 1: Data from Greyscale and RGB Image

Resolution	Type	Size
4x4	 Grayscale	8.53 kB
5x5	 Grayscale	8.56 kB
6x6	 Grayscale	8.57 kB
7x7	 Grayscale	8.58 kB
8x8	 Grayscale	8.59 kB
4x4	 RGB	8.08 kB
5x5	 RGB	8.11 kB
6x6	 RGB	8.18 kB
7x7	 RGB	8.19 kB
8x8	 RGB	8.21 kB

RESULT AND DISCUSSION

Analysis on Image Resolution with Message Character

Table 2: Data from Image Resolution with Message Character

Resolution	Grayscale	RGB
4x4	2 Character	6 Character
5x5	3 Character	9 Character
6x6	4 Character	13 Character
7x7	6 Character	18 Character
8x8	8 Character	24 Character

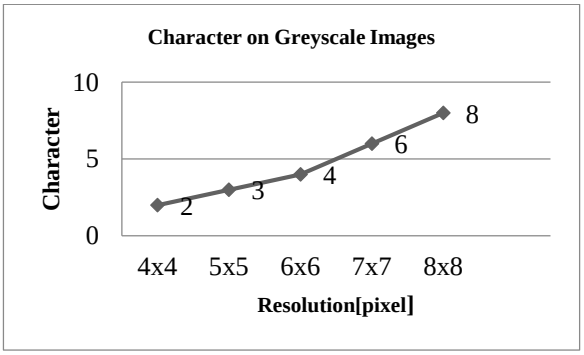

Figure 3: Comparison between Image Resolution and Message Character (Greyscale Image).

Based on the data in Table 2 and Figure 3, image resolution starting from 4x4, 5x5, 6x6, 7x7, 8x8 have an increase in the size of characters that can be inserted starting from 2 - 8 characters in JPEG Grayscale. Thus the larger the pixel size the greater the size of characters that can be inserted.

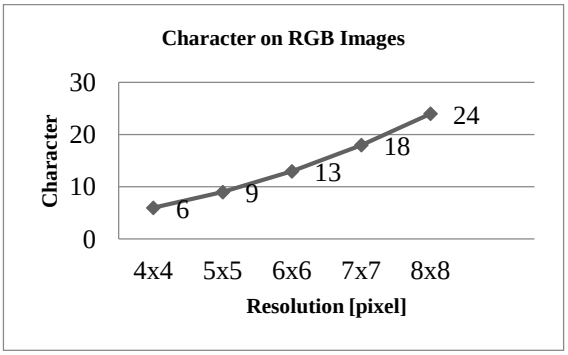

Figure 4: Comparison between Image Resolution and Message Character (RGB Image).

Based on the data in Table 2 and Figure 4, image resolution starting from 4x4, 5x5, 6x6, 7x7, 8x8 have an increase in the size of characters that can be inserted starting from 6 - 24 characters in JPEG RGB.

Thus the larger the resolution size the greater the size of characters that can be inserted. From the two data above shows that the changes that occur in character insertion is directly proportional to the pixel size change used.

Analysis on Image Resolution with Message Size

Table 3: Data from Image Resolution with Message Size

Resolution	Grayscale	RGB
4x4	2 bit	6 bit
5x5	3.125 bit	9.375 bit
6x6	4.5 bit	13.5 bit
7x7	6.125 bit	18.375 bit
8x8	8 bit	24 bit

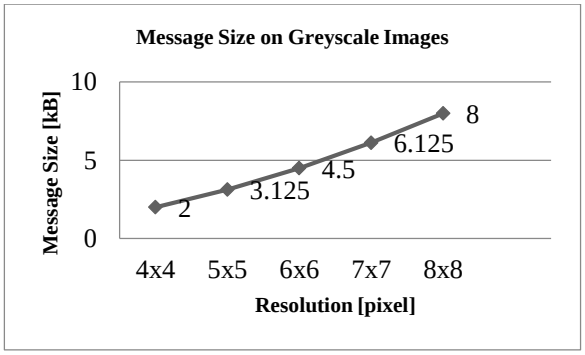

Figure 5: Comparison between Image Resolution and Message Size (Greyscale Image).

Based on the data in Table 3 and Figure 5, image resolutions ranging from 4x4, 5x5, 6x6, 7x7, 8x8 have an increase in the size of messages that can be inserted starting from 2 bit, 3.125 bit, 4.5 bit, 6.125 bit, and 8 bit in JPEG Grayscale. Thus the larger the size of the resolution the greater the size of messages that can be inserted.

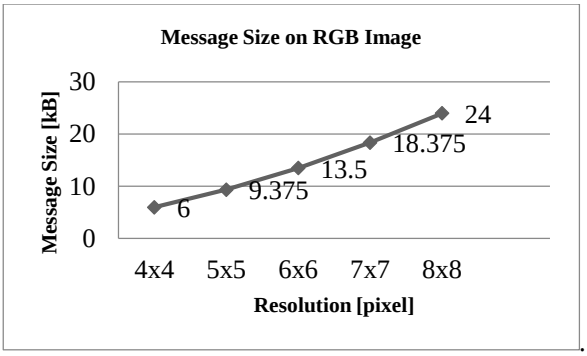

Figure 6: Comparison between Image Resolution with Message Size (RGB Image)

Based on the data in Table 3 and Figure 6, image resolutions ranging from 4x4, 5x5, 6x6, 7x7, 8x8 have an increase in the size of messages that can be entered. characters starting from 6 bit, 9.375 bit, 13.5 bit, 18.375 bit, 24 bit characters on JPEG RGB. Thus the larger the size of the resolution the greater the size of messages that can be inserted. From the two data above shows that the changes that occur on the size of the message is directly proportional to the resolution size changes used.

Analysis on Cover Image Size with Steganographic Image Size

Table 4: Data from Cover Image Size and Steganographic Image Size (Greyscale Image)

Resolution	Cover Image	Stegano Image
4x4	8.53 kB	8.56 kB
5x5	8.56 kB	8.59 kB
6x6	8.57 kB	8.60 kB
7x7	8.58 kB	8.60 kB
8x8	8.59 kB	8.60 kB
Average	0.024 kB	

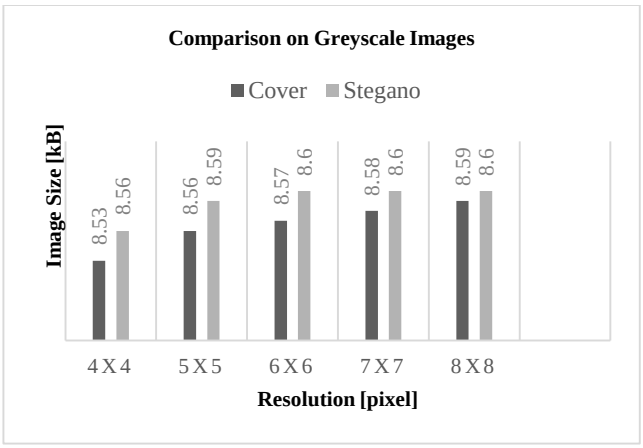

Figure 7: Comparison between Cover Image Size with Steganographic Image Size (Greyscale Image)

Based on the data in Table 4 and Figure 7, data resolutions ranging from 4x4, 5x5, 6x6, 7x7, 8x8 have an average file size increase of 0.024 kB on JPEG Grayscale.

Table 5: Data from Cover Image Size with Steganographic Image Size (RGB)

Resolution	Cover Image	Stegano Image
4x4	8.08 kB	11.28 kB
5x5	8.11 kB	11.31 kB
6x6	8.18 kB	11.37 kB
7x7	8.19 kB	11.38 kB
8x8	8.21 kB	11.40 kB
Average	3.194 kB	

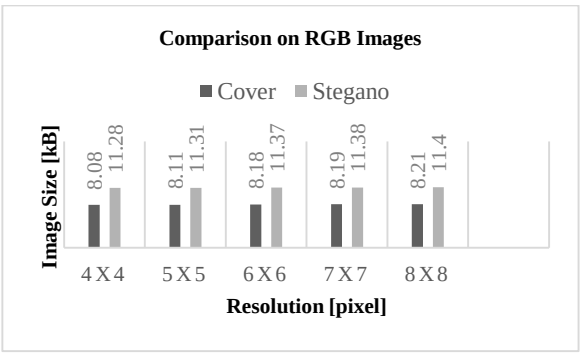

Figure 8: Comparison between Cover Image Size with Steganographic Image Size (RGB Image)

Based on the data in Table 5 and Figure 8, data resolutions ranging from 4x4, 5x5, 6x6, 7x7, 8x8 have an average file size increase of 3.194 kB on JPEG RGB. Thus the size of the steganographic file is greater than the cover file.

Table 6: Size Difference of Cover Image with Steganographic Image (Greyscale)

Resolution	Cover Image	Stegano Image	Difference
4x4	8.53 kB	8.56 kB	0.03 kB
5x5	8.56 kB	8.59 kB	0.03 kB
6x6	8.57 kB	8.60 kB	0.03 kB
7x7	8.58 kB	8.60 kB	0.02 kB
8x8	8.59 kB	8.60 kB	0.02 kB

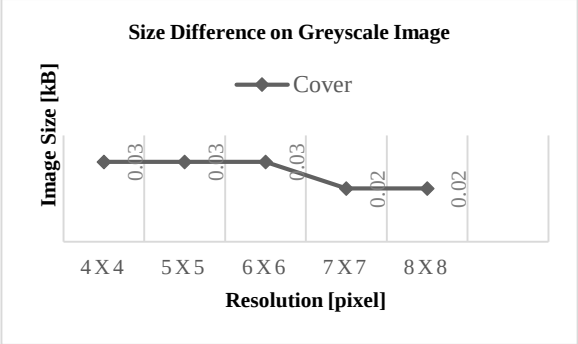

Figure 9: Size Difference of Cover Image with Steganographic Image (Greyscale Image)

Table 7: Size Difference on Cover Image and Steganography Image Size (RGB)

Resolution	Cover Image	Stegano Image	Difference
4x4	8.08 kB	11.28 kB	3.2 kB
5x5	8.11 kB	11.31 kB	3.2 kB
6x6	8.18 kB	11.37 kB	3.19 kB
7x7	8.19 kB	11.38 kB	3.19 kB
8x8	8.21 kB	11.40 kB	3.19 kB

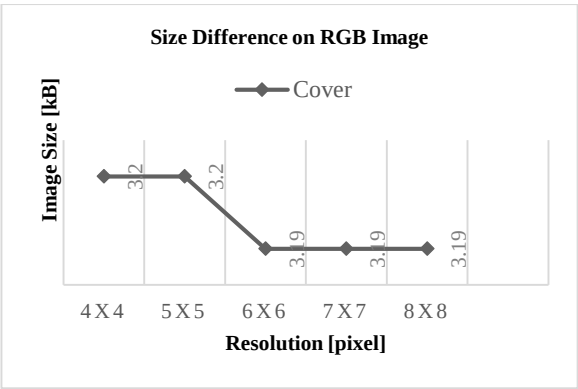

Figure 10: Size Difference of Cover Image Size and Steganography Image (RGB Image)

Table 8: Comparison on Steganography Image Size (Grayscale and RGB Image)

Resolution	Grayscale	RGB
4x4	8.56 kB	11.28 kB
5x5	8.59 kB	11.31 kB
6x6	8.60 kB	11.37 kB
7x7	8.60 kB	11.38 kB
8x8	8.60 kB	11.40 kB

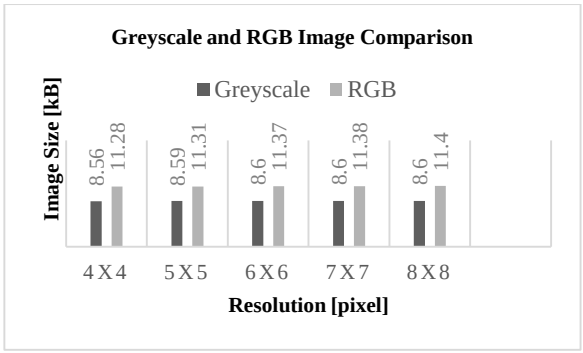

Figure 11: Size Comparison on Steganography Image (Greyscale and RGB Image)

Table 8: Comparison of result on Cover Image Size and Steganography Image Size

Resolution	Grayscale	RGB
4x4	0.03 kB	3.2 kB
5x5	0.03 kB	3.2 kB
6x6	0.03 kB	3.2 kB
7x7	0.02 kB	3.19 kB
8x8	0.02 kB	3.19 kB

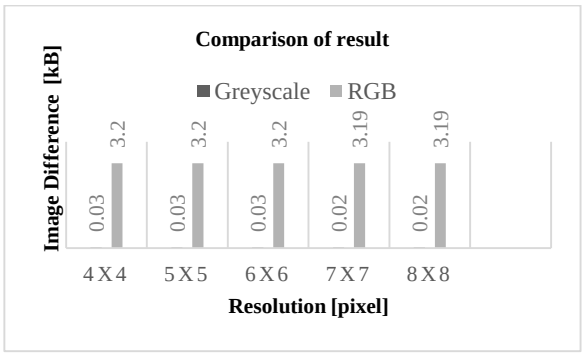

Figure 12: Comparison of result on Greyscale and RGB Steganographic Image Size

CONCLUSION

From the implementation and testing result, the conclusion is as follow:

a. On image resolution starting from 4x4, 5x5, 6x6, 7x7, 8x8, the resolution in the image is directly proportional to the number of characters that can be inserted. Starting from 2, 3, 4, 6, 8 on Grayscale JPEG type and starting from 6, 9, 13, 18, 24 on RGB JPEG type.

b. On image resolution starting from 4x4, 5x5, 6x6, 7x7, 8x8, the resolution in the image is directly proportional to the size of character. Starting from 2 bit, 3.125 bit, 4.5 bit, 6.125 bit, 8 bit on Grayscale JPEG type and starting from 6 bit, 9.375 bit, 13.5 bit, 18.375 bit, 24 bit on RGB JPEG type.

c. On image resolution starting from 4x4, 5x5, 6x6, 7x7, 8x8, the steganographic image sizes will be larger than the size

of the cover image. With difference of 0.024 kB on Grayscale JPEG type and difference of 3.194 kB on RGB JPEG type.

REFERENCES

[1] Cox, Ingenar J., "*Digital Watermarking and Steganography",* Burlington, Morgan Kaufmann Publisher, 2008.

[2] Petitcolas, FAP; Anderson RJ; Kuhn MG (1999). "Information Hiding: A survey" (pdf). Proceedings of the IEEE (special issue). 87 (7): 1062–78. doi:10.1109/5.771065. Retrieved 2008-09-02.

[3] "Polygraphiae (cf. p. 71f)" (in German). Digitale Sammlungen. Retrieved 2015-05-27.

[4] Fridrich, Jessica; M. Goljan; D.Soukai "Seaching for the Stego Key", *Proceedings of SPIE, Electronic Imaging, Security, Steganograohy, and Watermarking of Multimedia Contents VI*. 5306: 70-82, January 23, 2014.

[5] Pahati, OJ (2001-11-29). "Confounding Carnivore: How to Protect Your Online Privacy". AlterNet. Archived from the original on 2007-07-16. Retrieved 2008-09-02.

[6] Hakim, Muhammad, *"Studi dan Implementasi Metode LSB dengan Preprocessing Kompresi Data dan Ekspansi Wadah",* 2016

[7] Haines, Richard F.; Chuang, Sherry L. (1 July 1992). *The effects of video compression on acceptability of images for monitoring life sciences experiments* (Technical report). NASA. NASA-TP-3239, A-92040, NAS 1.60:3239. Retrieved 13 March 2016. The JPEG still-image-compression levels, even with the large range of 5:1 to 120:1 in this study, yielded equally high levels of acceptability.

[8] Hamilton, Eric "*JPEG File Interchange Format*" *Version 1.02* C-Cube Microsystems 1778 McCarthy Blvd. September 1,1992

[9] Simsek, B. 2004 *"Steganography in JPEG Images".* Dokuz Eykuk University.

[10] Piarsa, Nyoman. 2011 *"Steganografi Pada Citra JPEG Dengan Metode Squential dan Spreading"* Faculty of Engineering, Udayana University.

[11] Internet Assigned Numbers Authority (IANA) (May 14, 2017) *"Character Sets"* Accessed 2017-09-17

[12] Brandel, Mary (July 6, 1999). "1963: The Debut of ASCII". CNN. Retrieved 2008-04-14.

[13] "American Standard Code for Information Interchange, ASA X3.4-1963". American Standards Association (ASA). 1963-06-17. Archived from the original on 2016-05-26. Retrieved 2014-05-23.

[14] "USA Standard Code for Information Interchange, USAS X3.4-1967". United States of America Standards Institute (USASI). July 7, 1967.

[15] Jennings, Thomas Daniel (2016-04-20) [1999]. "An annotated history of some character codes or ASCII: American Standard Code for Information Infiltration". World Power Systems (WPS). Archived from the original on 2016-05-22. Retrieved 2016-05-22.

[16] "American National Standard for Information Systems — Coded Character Sets — 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII), ANSI X3.4-1986". American National Standards Institute (ANSI). March 26, 1986.