International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 11, November 2020, pg.70 – 76

Using Logical Operations to Secure LSB2 Data Steganography

Dr. Mohammad S. Khrisat; Prof. Ziad A. Alqadi

Albalqa Applied University
Faculty of Engineering Technology
Jordan – Amman

DOI: 10.47760/ijcsmc.2020.v09i11.007

Abstract: Color image steganography is an important task used to secure data and secrete messages, LSB2 method is one of the most popular methods used to secure data transmission by hiding a secrete data into color image. LSB2 method is very simple, efficient and has good quality factors (MSE and PSNR), but it is not secure. In this research paper we will introduce a sequence of logical operation to be implemented with LSB2 to increase the security level of LSB2. This sequence will not negatively affect LSB2 efficiency, and MSE and PSNR values will remain without any changes.

Keywords: Steganography, carrier image, stego_image, LSB2, LBP, LBP_image.

1- Introduction

Image steganography [10] is the process of hiding a secret data (message) within a carrier color image (see figure 1) in such a way that someone cannot know the presence or contents of the hidden message. The purpose of Steganography is to maintain secret communication between two parties, the sender and receiver [8], [9].

Figure 1: Image steganography

Digital color images are recommended to be used to hide secret data for the following reasons:

- ✓ Digital images are very popular and easily obtainable [1], [2], [3].
- ✓ The digital color image is represented by a three-dimensional matrix [11], [12], which facilitates logical and mathematical processing [4], [5].
- ✓ These digital images now have high resolution, which in turn provides a large volume that can be used to hide large blind data [6], [7].

The process of steganography must not add noticeable updates to the stego_image, thus the changes in the stego_image must not be noticed by human eyes.

Stego_method must provide the following features [21], [22]:

- Simplicity, easy to implement.
- Secrecy, difficult to hack.
- High quality factors, minimizing mean square error (MSE) [12], [13], [14], and maximizing peak signal to noise ratio (PSNR) [15], [16] between the carrier image and the stego_image.
- Efficiency, by providing small time for the processes of data hiding and data extraction [17], [18].

2- Steganography Methods

Many methods are used for data steganography [17], [18]] many of them such as LSB2 are based of least significant bit (LSB) methods [19], [20].

LSB2 method provides a higher capacity than LSB method, because it reserves 4 bytes from the carrier image to hide one character from the secrete message, as shown in figure 2 the least two significant bits from the carrier byte are used to hide two bits from the message character [21].

LSB2 method is very simple in handling hiding process (see figure 3) and handling extraction process (see figure 4), it requires a small times to implement these processes, also it provides a good quality parameters by minimizing the values of MSE and maximizing the values of PSNR [22].

LBS2 suffers from the low level of security, and it is easy for third party (hacker) to extract the hidden message, knowing that the used method of data hiding was LSB2.

Figure 2: LSB2 example

Figure 3: LSB2 hiding process

Figure 4: LSB2 extraction process

3- Local Binary Pattern

The first phase of the proposed logical operations to improve LSB2 security is using LBP_image [23], [24]. Local binary pattern (LBP) operator can be calculated for each byte in the carrier color image by using the 8_neighbors as shown in figure 5, the obtained image can be used in various applications[25], [26], but here we will use it as an input image to perform the logical sequence to secure LSB2 method.

Figure 5: Calculating LBP operators to form LBP_image

4- The proposed sequence of logical operation

The proposed sequence of logical operation we recommend to improve LSB2 security is based on the operations shown in figure 6, Where A is the carrier image, B is the LBP_image.

$$\begin{aligned}
 &((A \cdot B \oplus A)) + A = \\
 &\bar{A}\bar{B} \cdot A + AB\bar{A} + A = \\
 &(\bar{A} + \bar{B}) \cdot A + A = \\
 &A \cdot \bar{B} + A = \\
 &A
 \end{aligned}$$

Figure 6: Logical operations sequences.

To increase the security of LSB2 method of data steganography we can apply the following sequence of operations (see figure 7):

- Get the message and the carrier color image (A).
- Calculate the LBP_image (B).
- Calculate the image t1 by anding A and B.
- Calculate the image t2 by xoring t1 and A.
- Use image t2 to hide the message applying LSB2 method.
- Get the stego_image by oring the images t2 and A.

Figure 7: Proposed hiding process

Here we have to notice that the image to be used for data hiding is image t2, and this image must be used for data extraction, if we use directly the original image A for data extraction we will receive rubbish and not the required image, and this was experimentally proved.

5- Implementation and Experimental Results

The proposed sequence was implemented using various images, it was obtained that the calculated output image always the same as the input color image, as shown in figures 8 thru 12.

Figure 8: Original image A

Figure 9: LBP_image B

Figure 10: Image t1

Figure 11: Carrier image t2

Figure 12: Stego_image (the same as original)

The proposed sequence does not negatively affect LSB2 efficiency and quality, 12 images with average 1609800 bytes were taken as a carrier images, a message of 50 characters was hidden in each image and the obtained average value for MSE was 0.0017, PSNR average was equal 182.6865, the hiding time was equal 0.0030 seconds, and extraction time was equal 0.0022 seconds, which are almost closed the value of LSB2 method. It was also obtained that using the original image for message extraction will give a rubbish and not the required message.

6- Conclusion

A simple sequence of logical operations was proposed and implemented to increase the security level of LSB2 method of data steganography, the carrier image used for data hiding is one of the images obtained by implementing the logical sequence instead of using the original image as a carrier image. The proposed sequence keeps LBS2 efficient and the quality factors remain the same as for LSB2 method.

References

- [1]. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, VALUABLE WAVELET PACKET INFORMATION TO ANALYZE COLOR IMAGES FEATURES, International Journal of Current Advanced Research, vol. 9, issue 2, pp. 2319,2020.
- [2]. Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Analysis of Procedures used to build an Optimal Fingerprint Recognition System, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 21 – 37, 2020.
- [3]. Aws AlQaisi, Mokhled AlTarawneh, Ziad A. Alqadi, Ahmad A. Sharadqah, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, pp. 1220-1225, 2019.
- [4]. Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETE TEXT IN WAVE FILE, International Journal of Computer Applications, vol. 151, issue 4, pp. 1-4, 2016.
- [5]. Musbah Aqel, Ziad Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences Journal, vol. 6, issue 1, pp. 45-52, 2009.
- [6]. AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, 2018.

- [7]. Jamil Al-Azzeh, Ziad Alqadi, Mohammed Abuzalata, Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving, international Journal of Computer Science and Mobile computing, vol. 8, issue 2, pp. 20-33, 2019.
- [8]. J Al-Azzeh M Abuzalata, Ziad Alqadi, Modified Inverse LSB Method for Highly Secure Message Hiding, International Journal of Computer Science and Mobile Computing, vol. 8, issue 2, pp. 93-103, 2019.
- [9]. Ziad alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.
- [10]. Amjad Y Hindi, Majed O Dwairi, Ziad A AlQadi, A Novel Technique for Data Steganography, Engineering, Technology & Applied Science Research, vol. 9, issue 6, pp. 4942-4945, 2019.
- [11]. Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, Optimized true-color image processing, World Applied Sciences Journal, vol. 8, issue 10, pp. 1175-1182, 2010.
- [12]. Jamil Al Azzeh, Hussein Alhatamleh, Ziad A Alqadi, Mohammad Khalil Abuzalata, Creating a Color Map to be used to Convert a Gray Image to Color Image, International Journal of Computer Applications, vol. 153, issue 2, pp. 31-34, 2016.
- [13]. Majed O Al-Dwairi, A Hendi, Z AlQadi, An efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology & Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.
- [14]. Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, A novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp. 232-238, 2019.
- [15]. Ziad Alqad, Majid Oraiqat, Hisham Almujafer, Salah Al-Saleh, Hind Al Husban, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 9, pp. 30-48, 2019.
- [16]. amil Al-Azzeh, Ziad Alqadi, Qazem Jaber, A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images, JOIV: International Journal on Informatics Visualization, vol. 3, issue 3, pp. 262-265, 2019.
- [17]. Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Enhancing the Capacity of LSB Method by Introducing LSB2Z Method, International Journal of Computer Science and Mobile Computing, vol. 18, issue 3, pp. 76-90, 2019.
- [18]. Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2019.
- [19]. Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Ahmad Sharadqh, Proposed Implementation Method to Improve LSB Efficiency, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 306-319, 2019.
- [20]. Rushdi Abu Zneit, Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Using Color Image as a Stego-Media to Hide Short Secret Messages, International Journal of Computer Science and Mobile Computing, vol. 8, issue 6, pp. 106-123, 2019.
- [21]. Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Improving the security of LSB image steganography, JOIV: International Journal on Informatics Visualization, vol. 3, issue 4, pp. 384-387, 2019.
- [22]. Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, Rushdi Abu zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 3, pp. 748-754, 2019.
- [23]. ZIAD ALQADI, A MODIFIED LBP METHOD TO EXTRACT FEATURES FROM COLOR IMAGES, Journal of Theoretical and Applied Information Technology, vol. 96, issue 10, pp. 3014-3024, 2018.
- [24]. Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqh, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8, issue 5, pp. 2780-2787, 2018.
- [25]. Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, pp. 50-56, 2019.
- [26]. Jihad Nader Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, vol. 1, issue 4, pp. 49-55, 2019.