TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 22, No. 1, February 2024, pp. 157~163
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v22i1.24029

Least significant bit technology for hiding text data using video steganography

Huda A. Ali[1], Alyaa J. Jalil[1], Marwah K. Hussein[2]
[1]Department of Computer Science, Faculty of Computer Science and Information Technology, University of Basrah, Basrah, Iraq
[2]Department of Computer Information System, Faculty of Computer Science and Information Technology, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received May 15, 2022
Revised Jul 25, 2022
Accepted Oct 26, 2022

Keywords:

Data hiding
Image processing
Least significant bit
Steganography
Voice message

ABSTRACT

Due to the rapid development of information technology, the process of exchanging information over the web has become simple and fast. Nevertheless, the transmission of information will be at risk due to the nature of the internet, as anyone can access and change the data by hacking it. Therefore, it is necessary for protecting any personal information from being accessed by unlawful individuals. It became necessary to use encryption and steganography techniques for protecting data. Steganography is a manner used for covering hidden information in several other media while preserving the form of the original data and leaving no evidence of hidden data, whereas, encryption changes the original information into unclear or ambiguous information, which is called scrambled. The paper presents a method of video steganography as a powerful and effective tool for data steganography. We used a video as a spreading medium and then used it for concealment of an audio message and a document (in a pdf file) in a method that makes the information invisible using the least significant bit (LSB) method.

Corresponding Author:

Huda A. Ali
Department of Computer Science, Faculty of Computer Science and Information Technology
University of Basrah
Basrah, Iraq
Email: huda.ali@uobasrah.edu.iq

1. INTRODUCTION

Information security aims for shielding databases from the undesirable and dangerous clients' activities that are unapproved. Through the internet, a huge amount of secret information is trad since it is public financial cleverness and mostly accessible method [1]. The mechanical improvement has made computerized data especially disabled to block tries at hacking and afterward unapproved usage, moreover, it had worthy negative consequences for the rights holders on the hand and content makers on the other, to protect information on open sources, the efforts in protection should be integrated into information correspondence frameworks via the internet [2]. Steganography ranks as the most hopeful developments for accomplishing the general objective of ensuring the secure conveyance of data from the source to the destination (approved clients). Steganography is defined as a skill (process) involved in conveying a record, picture, or message inside another document, message, or picture. 'Steganography' means "covered writing" as the Greek called it; it signifies the secure expression of information steganography involves altering the computerized media which that the sender and the expected beneficiary only can identify the hidden data sending through it. In another word, steganography analysis is the technique of identifying a hidden data [3], [4]. Thus, breaking

the steganography framework is the objective of steganography analysis, and if a calculation can decide whether a picture has a secret information then the condition is met.

Security should stay invisible, to lessen the attack probability, undetectable. Consequently, the significant information enables to be embedded into interactive media archives in a way that should not be noticed, i.e., the imperceptible extension of data into sound and sight information [5]. Computerized watermarking is a manner that is applied to improve the indistinctness (for example, intangibility) and strength of security. It can be utilized on any advanced picture, sound document, or content record [6]. Advanced watermarking involves embedding a computerized sign or example (indicating the proprietor of the substance) into advanced content. The sign (otherwise, watermark was called) can be utilized to detect the owner of that work, for following illicit duplicates, furthermore to validate the substance of it [7].

Watermarking and steganography vary in various methods including reason and identification/extraction techniques. The crucial distinction is a view to the topic of the correspondence in watermarking which is the source signal with the inserted information giving copyright insurance. In steganography, in the other side, the article to be sent is the inserted message, moreover the spread sign fills in as a harmless mask that is selected subjectively by the client according to its specialized fairness [8]. Also, within the steganography the outsider couldn't recognize that message in the stage media, yet with watermarking, the outsider couldn't remove the message or supplant it. It Fundamentally averts any illicit duplication [9].

2. THE COMPREHENSIVE THEORETICAL BASIS

2.1. Steganography

It involves embedding important information in techniques whereby only the sender and receiver can detect the hidden data, as in the following formula [10]:

$$Cover\ medium\ +\ Hidden\ data\ +\ Stego\ key\ =\ Stego\ medium$$

The steganography technique could be divided into six kinds:

1) Image (JPEG, GIF, BMP)
2) Audio (WAV, MP3)
3) Video (MPEG, MP4, and AVI)
4) Text
5) Protocol
6) Deoxyribonucleic (DNA

Although all media are suitable for steganography, the most widely used are videos and images because they contain a large percentage of repetition, so the embedding data get less disturbed [11].

2.1.1. Video/image steganography

The low sensitivity in the system of human visual, and the weaknesses of any change in the model are the most important reasons for using digital images and videos for steganography [12], [13]. Because of the above, the important data could be embedded in either the images or video as a cover without being seen as shown in Figure 1. A video contains of numbers of frames. An image (frame) is a set of pixels, each pixel has a combination of red, green and blue (RGB) colors, these pixels appear as three layers. The proposed algorithm is the least significant bit least significant bit (LSB), for both encryption and decryption, and along with application, it is given in this section [14].

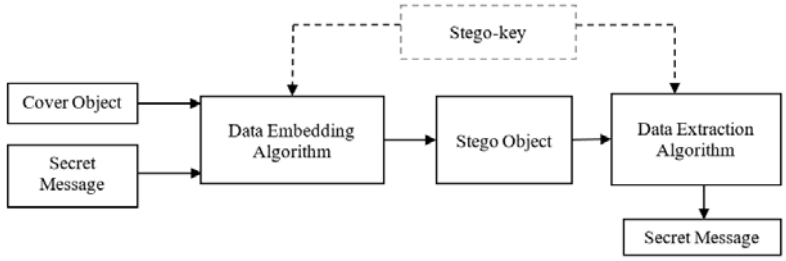


Figure 1. General steganographic model, embedding the process is represented with bold arrows, while extraction process is represented by non-bold arrows

2.1.2. Least significant bit technique

Information is hidden in a video using the LSB algorithm. The main advantages of this technique are a low computational difficulty and a high watermark canal bit rate. That technique changes the secret message bits with the LSB of the covered files. Each bit of the secret image must be hidden in RGB as in the following example, the following bits from the image are given [14], [15]:

00100110-11101000-11001001-00100111-1100111-11001001-11101001-11001000

An American standard code for information interchange (ASCII) value of 98 in decimal for character "b", and its equivalent is 1100010 in binary value. The seven bits are replaced with the least significant bit of every seven bits of covered bytes, as shown in Table 1. As described, there is a tiny difference in the video colors. Therefore, the human eye cannot discern or discover the difference.

Table 1. Hiding character "b" in a part of image using LSB technique

Part of image (cover)	After hiding character "b" in the image
00100110	00100111
11101000	11101001
11001001	11001000
00100111	00100110
11001001	11001000
11101001	11101001
11001000	11001000

2.1.3. Requirements of hiding message in digital object

Several embedding techniques are used to hide information; however, there are some specific requirements to apply steganography methods accurately. The techniques must fulfill the following requirements [16]:

1) Integrity: embedded information must be precise after hidden.
2) Robustness: the concealed information ought to be made due through any preparing activity through which the host signals experiences and ensures its unwaveringness.
3) Increase in data capacity to hide more information.
4) Security.
5) Steganography object should remain unmodified.
6) Finally, we generally assume that the programmer realizes that a hidden information within the stego object. The hiding information in objects is the unexpected thought in comparison to cryptography; however, it utilizes some essential standards of cryptography [4].

2.2. Algorithm of embedding and extracting

In the steganography algorithm, a set of steps are followed on the video in which data is to be hidden. After the video frames are opened, a number of them are selected for the purpose of hiding hidden messages in the lowest bit. After that, the video is assembled for the purpose of sending it. The number of video frames exceeds the size of the entered messages, so a choice is made here. The number of frames in addition to the hiding mechanism itself at the lowest bit location, Figure 2 display the steps of stegano algorithm. On the other hand, the process of obtaining hidden information requires the recipient to know the frames in which it was hidden for the purpose of isolating it from the rest of the frames, processing it, and retrieving the information hidden in it. Figure 3 explainer he extracting algorithm.

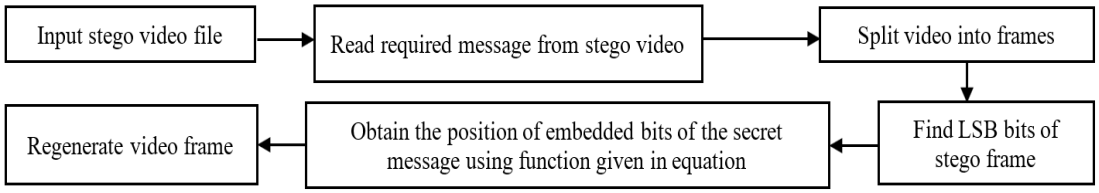


Figure 2. Algorithm of steganography

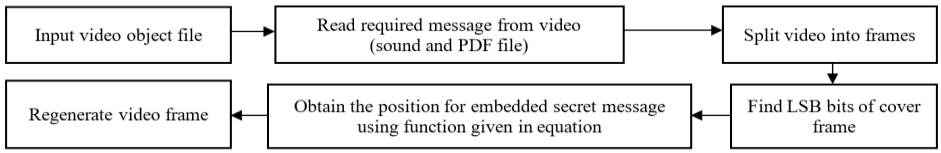
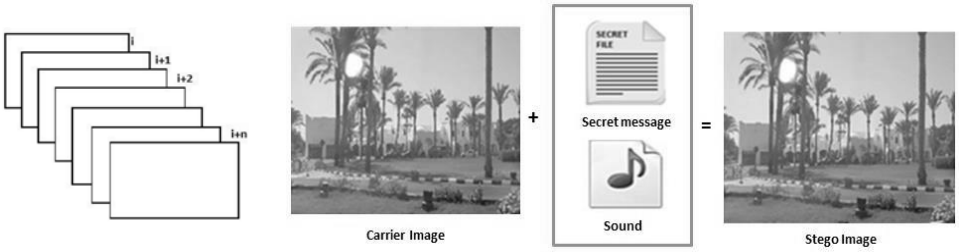


Figure 3. Algorithm of extracting

3. RESEARCH METHOD

The proposed method is based on hiding information in a video clip to hide the message in the frame and recover the hidden message of the video using the least significant bit change method. LSB steganography strategies widely use an image in a steganography rule and consider under several conditions a witness can separate the images (stage, covered). Figure 4 shows that it includes two parts: Figure 4(a) showing the video frames where n refers to the number of video frames, and Figure 4(b) explain that the first is the image carrying the message, and the second is the hidden image, which consists of the hidden message. It is impossible to distinguish between the first video and the Stegano video image.



(a) (b)

Figure 4. Part of video steganography: (a) video frames and (b) steganography using video image

4. RESULTS AND DISCUSSION

4.1. Previous studies

Hanafy *et al*. [17] used a pixel-wise manipulation (PWM) technique to exhibit a stegano graphic model. In his technique, important information is hidden in a bogus random manner using a secret key. He used for a high signal for noise ratio and an average square error to make a comparison between the actual video and the stegano graphic video.

Khan *et al*. [18] used a neural network (NN) to present a steganography algorithm for images. They extracted features from the cover images and hidden secret data, and then used this information as an input to NNs to get the outputs. The main advantage of an NN is that it has the capacity to sacrificial any non-linear functions.

Pan *et al*. [19] proposed a technique to apply steganography. However, this technique is difficult, and its computational complexity means it is slow, in addition to it being highly imperceptible to human eyes. He suggested using codes for linear block and vector in order to hide information into the cover of the media throughout compression.

Hu and Tak U [20] proposed a method of video steganography depending on non-regular rectangular segments. He used two videos; one was secret, and the other was cover. The benefit of this strategy is that it offers a high encoding speed of the image.

Balaji and Naveen [21] presented a new way to protect information; he created an index which was further applied in a frame of the video. Upon the reception, the embedded data are extracted from the frames using the same index. This technique is difficult but less time consuming.

Ghasemi *et al.* [22], Danti and Manjula *et al*. [23] presented steganography strategies using wavelet transform; these algorithms have many advantages when embedding information. Also, several researchers have devised a new steganography system to embed sound files [24]. In order to increase robustness, they used (LSB3) instead of (LSB1) of the cover for embedding, while in 2013, Moon and Raut [25] used (LSB4). The algorithm used computer forensics in a new technique to improve information security. One of the best advantages of this algorithm is that it is very difficult.

Acharya *et al*. [26] presented a technique in video steganography using LSB and chaotic sequence to find an index. This technique gives a better result because videos (actual and the stego) are the same. In the same year, Kelash *et al*. [27] suggested a steganography algorithm depending on a color histogram. This technique had major benefits, such as its ability to embed a large amount of information without error also supplying a great level of authentication for guaranteeing the video integrity. Table 2 gives the details of papers compared with our results; the results are arranged in ascending year order.

Table 2. The researchers with their result and techniques

Year	Author name	Parameter calculated	Technique used
2008	A. A. Hanafy *et al*.	PSNR=51 dB	Pixel wise manipulation
2010	I. Khan *et al*.	PSNR=49.54 dB	Neural network
2010	F. Pan *et al*.	PSNR=43 dB	Motion vector, linear block codes
2011	S. D. Hu and K. Tak U.	PSNR=29.75 dB	Least significant bit
2011	R. Balaji and G. Naveen	Retrieval time is few seconds	Least significant bit insertion method
2011	E. Ghasemi *et al*.	PSNR=39.94 dB	Genetic algorithm, discrete wavelet transforms
2012	A. Danti and G. R. Manjula	MSE=0.000027	Hybrid wavelet transforms
2012	H. A.-K. Younis, A. J. Jalil, and Z. A. Abbood	PSNR=48.9446	3 least significant bit
2013	A. K. Acharya *et al*.	PSNR=31 dB	Least significant bit
2013	H. M. Kelash *et al*.	PSNR=48.91 dB	Histogram
2013	S. K. Moon and R. D. Raut	PSNR=50 dB	4 least significant bit, histogram
2022	Our Work	Correlation=1 Entropy=0.0007 PSNR=69.3 MSE=0.0015 Euclidean=8.0021e-08	Least significant bit

The correlation, entropy, peak signal-to-noise ratio (PSNR), mean-squared error (MSE) and Euclidean distance are the five metrics that help in calculating results, and their equations are shown below:

1) Cross correlation

Cross correlation is a legal technique to link the similarity and batter match between two signals; it is given by [27]. Measure the quality of the stego image. The PSNR is calculated in decibels (dB). A larger value of PSNR indicates a better quality of image. Where PSNR is [28]:

$$Corr = \frac{\sum_m \sum_n (Amn-\bar{A})(Bmn-\bar{B})}{\sqrt{[\sum_m \sum_n (Amn-\bar{A})^2][\sum_m \sum_n (Bmn-\bar{B})^2]}} \quad (1)$$

2) Entropy

Entropy is a scientific notion most often linked with disorder, unpredictability, or uncertainty. The phrase and concept are utilised in a variety of domains, ranging from classical thermodynamics, where it was originally recognised, to statistical physics' microscopic explanation of nature, and to the concepts of information theory and is given by [29]:

$$H(X,Y) = \sum x\mathcal{E}X \sum y\mathcal{E}YP(X,Y)lo\,g(X,Y) \quad (2)$$

3) PSNR

PSNR is an engineering term that refers to the ratio of a signal's maximum achievable power to the power of corrupting noise that affects the fidelity of its representation. PSNR is commonly stated as a logarithmic quantity using the decibel scale because many signals have a very wide dynamic range. The PSNR is calculated to:

$$PSNR = 20\ \log_{10} \frac{MAX}{\sqrt{MSE}} \quad (3)$$

4) MSE

MSE is the difference between the true value and the estimated value MSE, and is given by [23]:

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (4)$$

PSNR is inversely proportional to MSE.

5) Euclidean distance

Euclidean distance between the two images as the following [30]:

$$D(x,y) = \sum_{k=1}^{mn} (x^k - y^k)^2 \quad (5)$$

Where n, m refers to the dimensions of image.

5. CONCLUSION

Different types of steganography strategies are available to conceal information in multimedia using several types of Techniques to ensure the delivery of the information without any online attacks. LSB replacement is the most efficient method that is used to hide the information in multimedia, the previously mentioned approach depends on the intention to conceal a message in video pictures (AVI) that gives a secure and robust method of information transmission. The suggested inserted video steganography includes numerous advantages such as ease of use, simplicity, and effective procedure of installing the hush-hush message with greater security, and the most difficult to discover the position of the secret message on video because of the size of the video (the number of frames).

REFERENCES

[1] P. Gomber, R. J. Kauffman, C. Parker, and B. W. Weber, "On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services," *Journal of Management Information Systems*, vol. 35, no. 1, pp. 220–265, Jan. 2018, doi: 10.1080/07421222.2018.1440766.

[2] R. Palanivelu and P. S. S. Srinivasan, "Safety and security measurement in industrial environment based on smart IOT technology based augmented data recognizing scheme," *Computer Communications*, vol. 150, pp. 777–787, Jan. 2020, doi: 10.1016/j.comcom.2019.12.013.

[3] F. Pasquale and T. A. Ragone, *Protecting health privacy in an era of big data processing and cloud computing*, vol. 17. HeinOnline, 2013. [Online]. Available: https://core.ac.uk/download/pdf/327104569.pdf

[4] M. Dalal and M. Juneja, "A survey on information hiding using video steganography," *Artificial Intelligence Review*, vol. 54, no. 8, pp. 5831–5895, Dec. 2021, doi: 10.1007/s10462-021-09968-0.

[5] M. Andrejevic, *Infoglut: How too much information is changing the way we think and know*. Routledge, 2013, doi: 10.4324/9780203075319.

[6] N. Sharma and A. K. Singh, "Data Hiding Techniques for Consumer Applications," Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh- India, 2017. [Online]. Available: http://www.ir.juit.ac.in:8080/jspui/handle/123456789/5471

[7] G. Dhevanandhini and G. Yamuna, "An effective and secure video watermarking using hybrid technique," *Multimedia Systems*, vol. 27, no. 5, pp. 953–967, Oct. 2021, doi: 10.1007/s00530-021-00765-x.

[8] N. K. Kumar, "Legal Status of Virtual Business in India: Issues and Challenges," vol. 3, no. 2, pp. 243–263, 2016, [Online]. Available: http://ijrra.net/Vol3issue2/IJRRA-03-02-52.pdf

[9] T. Hodgson, "The mechanics of order: An inquiry into the utopian possibilities of the free and open source ecology," Victoria University of Wellington, 2010.

[10] I. E. Salem, H. R. Abdulshaheed, and H. M. Gheni, "A secure telemedicine electronic platform based on lightweight cryptographic approach," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 20, no. 5, p. 988, Oct. 2022, doi: 10.12928/telkomnika.v20i5.22662.

[11] V. Thakur and M. Saikia, "Hiding secret image in video," in *2013 International Conference on Intelligent Systems and Signal Processing (ISSP)*, IEEE, Mar. 2013, pp. 150–153, doi: 10.1109/ISSP.2013.6526892.

[12] M. K. Hussein, K. R. Hassan, and H. M. Al-Mashhadi, "The quality of image encryption techniques by reasoned logic," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 6, p. 2992, Dec. 2020, doi: 10.12928/telkomnika.v18i6.14340.

[13] M. K. Hussein, "The optimum encryption method for image compressed by AES," *Global Journal of Computer Science and Technology*, vol. 8, no. 4, 2020.

[14] E. A. Jameel and S. A. Fadhel, "Hiding health report in X-ray images to protect people privacy," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 20, no. 3, p. 580, Jun. 2022, doi: 10.12928/telkomnika.v20i3.23298.

[15] E. W. Abood, W. A. Khudier, R. H. Jabber, and D. A. Abbas, "Securing Hill encrypted information With Audio steganography: a New Substitution Method," *Journal of Physics: Conference Series*, vol. 1591, no. 1, p. 012021, Jul. 2020, doi: 10.1088/1742-6596/1591/1/012021.

[16] A. Gutub and M. Al-Ghamdi, "Hiding shares by multimedia image steganography for optimized counting-based secret sharing," *Multimedia Tools and Applications*, vol. 79, no. 11–12, pp. 7951–7985, Mar. 2020, doi: 10.1007/s11042-019-08427-x.

[17] A. A. Hanafy, G. I. Salama, and Y. Z. Mohasseb, "A secure covert communication model based on video steganography," in *MILCOM 2008 - 2008 IEEE Military Communications Conference*, IEEE, Nov. 2008, pp. 1–6, doi: 10.1109/MILCOM.2008.4753107.

[18] I. Khan, B. Verma, V. K. Chaudhari, and I. Khan, "Neural network based steganography algorithm for still images," in *INTERACT-2010*, IEEE, Dec. 2010, pp. 46–51, doi: 10.1109/INTERACT.2010.5706192.

[19] F. Pan, L. Xiang, X.-Y. Yang, and Y. Guo, "Video steganography using motion vector and linear block codes," in *2010 IEEE International Conference on Software Engineering and Service Sciences*, IEEE, Jul. 2010, pp. 592–595, doi: 10.1109/ICSESS.2010.5552283.

[20] S. D. Hu and K. Tak U., "A Novel Video Steganography Based on Non-uniform Rectangular Partition," in *2011 14th IEEE International Conference on Computational Science and Engineering*, IEEE, Aug. 2011, pp. 57–61, doi: 10.1109/CSE.2011.24.

[21] R. Balaji and G. Naveen, "Secure data transmission using video Steganography," in *IEEE International Conference on Electro Information Technology*, IEEE, May 2011, pp. 1–5, doi: 10.1109/EIT.2011.5978601.
[22] E. Ghasemi, J. Shanbehzadeh, and B. Zahirazami, "A steganographic method based on Integer Wavelet Transform and Genetic Algorithm," in *ICCSP 2011 - 2011 International Conference on Communications and Signal Processing*, IEEE, Feb. 2011, pp. 42–45, doi: 10.1109/ICCSP.2011.5739395.
[23] A. Danti and G. R. Manjula, "Secured data hiding of invariant sized secrete image based on Discrete and Hybrid Wavelet transform," in *2012 IEEE International Conference on Computational Intelligence and Computing Research*, IEEE, Dec. 2012, pp. 1–6, doi: 10.1109/ICCIC.2012.6510181.
[24] H. A.-K. Younis, A. J. Jalil, and Z. A. Abbood, "Steganography System to Hide a Sound File in a Color Image," *Journal of Thi-Qar Science*, vol. 3, no. 3, 2012.
[25] S. K. Moon and R. D. Raut, "Analysis of secured video steganography using computer forensics technique for enhance data security," in *2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)*, IEEE, Dec. 2013, pp. 660–665, doi: 10.1109/ICIIP.2013.6707677.
[26] A. K. Acharya, R. Paul, S. Batham, and V. K. Yadav, "Hiding large amount of data using a new approach of video steganography," in *Confluence 2013: The Next Generation Information Technology Summit (4th International Conference)*, Institution of Engineering and Technology, 2013, pp. 7.05-7.05, doi: 10.1049/cp.2013.2338.
[27] H. M. Kelash, O. F. Abdel Wahab, O. A. Elshakankiry, and H. S. El-sayed, "Hiding data in video sequences using steganography algorithms," in *2013 International Conference on ICT Convergence (ICTC)*, IEEE, Oct. 2013, pp. 353–358, doi: 10.1109/ICTC.2013.6675372.
[28] V. Sivaraman, S. Grover, A. Kurusingal, A. Dhamdhere, and A. Burdett, "Experimental study of mobility in the soccer field with application to real-time athlete monitoring," in *2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications*, IEEE, Oct. 2010, pp. 337–345, doi: 10.1109/WIMOB.2010.5645046.
[29] M. S. Anower, M. R. Frater, and M. J. Ryan, "Estimation by cross-correlation of the number of nodes in underwater networks," in *2009 Australasian Telecommunication Networks and Applications Conference (ATNAC)*, IEEE, Nov. 2009, pp. 1–6, doi: 10.1109/ATNAC.2009.5464716.
[30] M. K. Hussien, "Encryption of Stereo Images after Compression by Advanced Encryption Standard (AES)," *Al-Mustansiriyah Journal of Science*, vol. 28, no. 2, pp. 156–161, Apr. 2018, doi: 10.23851/mjs.v28i2.511.

BIOGRAPHIES OF AUTHORS

Huda A. Ali was born in Basra, Iraq. She received the bachelor's degree in Computer Science from Basrah University, Basrah, Iraq, and the master's degree in Computer Science from Basrah University too. Her research areas of interest include image processing, security, steganography, NLP, visualization, system analysis, and design. She can be contacted at email: huda.ali@uobasrah.edu.iq.

Alyaa J. Jalil was born in Basra, Iraq. She received the bachelor's degree in Computer Science from Basrah University, Basrah, Iraq, and the master's degree in Computer Science from Basrah University too. Her research areas of interest include sound processing, image processing, security, and steganography. She can be contacted at email: aliaa.jaber@yahoo.com.

Marwah K. Hussein is a lecturer in Computer Information Systems since (2013), University of Basra in Iraq. Her current research interests included information security, video and image processing. She can be contacted at email: marwa.hussein@uobasrah.edu.iq.