Zeyad Safaa Younus* and Ghada Thanoon Younus

Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data

https://doi.org/10.1515/jisys-2018-0225
Received May 12, 2018; previously published online February 7, 2019.

Abstract: This paper aims to propose a method for data hiding in video by utilizing the least significant bit (LSB) method and improving it by utilizing the knight tour algorithm for concealing the data inside the AVI video file and using a key function encryption method for encrypting the secret message. First, the secret message is encrypted by utilizing a mathematical equation. The key used in the equation is a set of random numbers. These numbers differ in each implementation to warrant the safety of the hidden message and to increase the security of the secret message. Then, the cover video was converted from a set of frames into separated images to take the advantage of the large size of video file. Afterward, the knight tour algorithm is utilized for random selecting of the pixels inside the frame utilized for embedding the secret message inside it to overcome the shortcoming of the conventional LSB method that utilized the serial selection of pixel and to increase the robustness and security of the proposed method. Afterward, the encrypted secret message is embedded inside the selected pixels by utilizing the LSB method in bits (7 and 8). The observational results have drawn that the proposed method has a superior performance compared to the previous steganography method in terms of quality by a high PSNR of 67.3638 dB and the lowest MSE of 0.2578. Furthermore, this method preserves the security where the secret message cannot be drawn out without knowing the decoding rules.

Keywords: Data hiding, steganography, encryption, LSB, knight tour.

1 Introduction

The protection of digital media on the Internet has become an essential issue because of the vast improvement of personal computers and data innovation and the huge increment in the utilization of Internet networks in the transmission and reception of data and information. Consequently, the researchers concentrated on building methods to protect the information and data and make it more private to prevent intruders and hackers from access to it [3, 18]. Cryptography is a technique used to secure information by utilizing encryption in a way that anybody cannot comprehend and read it except the trusted individual who has the secret key [4, 14]. There are numerous methods utilized to encrypt and decrypt data, but all became ineffective after the emergence of the Internet, so it became necessary to search for other techniques in the data concealment. As a result, the concept of steganography was invented [11, 15, 31]. Steganography is the art of concealing data or concealing the correspondence between the sender and the recipient of the secret information that uses the host media as a cover, for example (text, images, audio, or video) [5, 12, 17, 23]. The distinction among cryptography and steganography is the first term is utilized for rearranging the content of the message in a way that only the sender and the recipient of the message comprehend, while the second term is utilized to hide information within cover without any changing in the content. The merging between the steganography and cryptography methods is more effective to achieve the confidence and protection of

***Corresponding author: Zeyad Safaa Younus,** Assistant Lecturer, Faculty of Computer Sciences and Mathematics, Software Engineering, University of Mosul, Mosul, Iraq, e-mail: ziead_1979@yahoo.com; zeyad.saffawi@uomosul.edu.iq. https://orcid.org/0000-0002-6818-1392
Ghada Thanoon Younus: Lecturer, Faculty of Computer Sciences and Mathematics, Computer Science, University of Mosul, Mosul, Iraq

data [21]. The fundamental challenge in the data concealing process is to embed the information by keeping the quality of cover object, which require extraordinary methods that hide a huge amount of payload and robustness of these techniques against the aggressors. Video steganography comprises two procedures which are the embedder and detector. The embedder has two data sources, which are payload implying the amount of secret message inserted inside a cover, and the cover video is utilized as a cover that contains the message inside it. Most methods of steganography implement the hiding operation on the cover without selecting better pixels. The correct selecting of pixels for hiding data achieves a high quality and robustness [7, 20]. Steganography has many techniques to hide the information. One of them is the least significant bit (LSB) method. The main disadvantages of this technique are the serial selection of pixels within the frame that is used for embedding the information inside it and the weakness against electronic attacks. For this reason, the knight tour algorithm was utilized for random selection of pixels and also a key function encryption method used to encrypt a secret message to increase the security and the robustness for the proposed method. After that, the stego video is made as an outcome of the embedding process and will be sent to the recipient. The detector represents the second procedure where the stego video represents the input to this procedure, and the detector can find the secret message by utilizing an extraction procedure [6, 10, 22].

2 Related Works

There are numerous methods and techniques that were proposed from the scientists in the field of video steganography. The real objective of these methods and techniques is to get exact outcomes. As of late, the researchers concentrated on enhancing the execution of video steganography by utilizing diverse strategies.

Abbas et al. presented a technique in video steganography by utilizing the Cuckoo search algorithm in 2015 [1]. In this technique, the secret message was separated into byte by byte then five different types utilized for showing the bits of each byte. Subsequently, the Euclidian distance was utilized for selecting a better pixel by calculating the similarity between the pixels and diverse byte type. Afterward, the Levy flight random walk is utilized to transfer from one pixel to another randomly, then, the LSB method was utilized for embedding the secret message inside the video frame.

In 2015, Sahu and Mitra introduced a method in video steganography using the LSB method and advanced encryption standard (AES) method [25]. In this method, the secret data was encrypted using the AES method. Then, the frames used for embedding the data was selected randomly, and the pixel swapping algorithm was used to enhance the security. After that, the LSB method was used to embed the secret data within the selected video frame.

Sudeepa et al. proposed a method in video steganography in 2016 [30]. In this method, the secret message is encoded utilizing a key and a feedback shift register (FSR) used for choosing the frame arbitrarily to avoid redundancy. Subsequently, the secret message was inserted inside a video utilizing the LSB method.

In 2016, Sethi and Kapoor presented a method in video steganography by utilizing the AES cryptographic algorithm and the genetic algorithm [27]. In this method, the secret message was compressed to reduce the size. Afterward, the AES algorithm was utilized to transfer the compressed message into the cipher text, and then, the encoded message was embedded in the image by utilizing a genetic algorithm and the LSB method, where the genetic algorithm is utilized for selecting the pixel utilized for embedding the data by utilizing the LSB method.

In 2016, Saleema and Amarunnishad introduced a technique in image steganography by utilizing an arbitrary selection of image pixel utilized for embedding the secret message inside it and by utilizing the LSB method for embedding the data inside the image and by utilizing hybrid Fuzzy Neural Networks for improving the image quality after the embedding process [26]. In 2016, Alsaffawi proposed a method by utilizing LZW to minimize the size of secret message and by utilizing EMD and knight tour algorithm to embed the secret message inside the image [3]. In 2016, Solichin and Painem introduced a method in video steganography called the less significant frame (LSF) method [29]. In this method, the selection of the frame that had the secret message depended on the movement of the frame using the features of optical stream. In 2016, Rezagholipour and Eshghi presented a method in video steganography based on the movement of the frame where the secret message was inserted in the movement vectors of the moving frames [24]. In 2017, Putu

et al. introduced a technique in video steganography, by utilizing an AES-128 bit method for encoding the image. After that, the LSB method was utilized for embedding the encoded image inside the video [21]. In 2017, Mumthas and Lijiya presented a new method in video steganography by utilizing RSA and random DNA for encrypting the secret message, and after that, the encoded message is compressed utilizing the Huffman encoding. After that, the 2D DCT is utilized for embedding the secret data to increase the protection of the system [19]. In this study, the video steganography method was proposed using a proposed encrypted key function for encrypting a secret message to increase the security and using the LSB method for embedding the information within the video and improving it using the knight tour algorithm to increase the robustness and security during the selecting of the pixels used to embed the secret digit inside it as well as to keep the stego video quality and make it like the cover video.

3 Proposed Method

The primary objective of this method is to hide a lot of data with a high quality of stego video and accomplish a high security for the information hiding inside the cover video.

3.1 Preparing the Secret Message

First, the secret message is written with the English alphabetic. After that, the secret message is encoded to increase the security. In this process, the secret message is encrypted utilizing a key that is ascertained by Eq. (1):

$$\text{key} = \text{round}(\text{sum}(u))^2 \tag{1}$$

where u means a set of random values calculated using Eq. (2):

$$u = \text{rand}(1, 5) \tag{2}$$

Here, the function key generates a set of random values, which gives a high degree of security for the secret message. In each stage of implementation, the value of the key will vary according to random values that will be generated, and by applying Eq. (3), the secret message will be encrypted:

$$E = sm + \text{key} \tag{3}$$

where, E represents the values of the encrypted secret message, and sm represents the values of the secret message.

The steps of preparing the secret message can be reviewed as:

Input: secret message.
Output: encrypted secret message.
Step 1: read a secret message.
Step 2: generate a set of random values (u) using Eq. (2).
Step 3: calculate the key by applying Eq. (1).
Step 4: encrypt the secret message using additive method according to Eq. (3).
Step 5: Convert the encrypted secret message into binary.

The flow chart of preparing the secret message is shown in Figure 1.

3.2 Embedding Process

During this stage, the encoded secret message is embedded inside video frames by utilizing the knight tour algorithm and the LSB method. Here, the video is split into frames and converted into a set of images. After

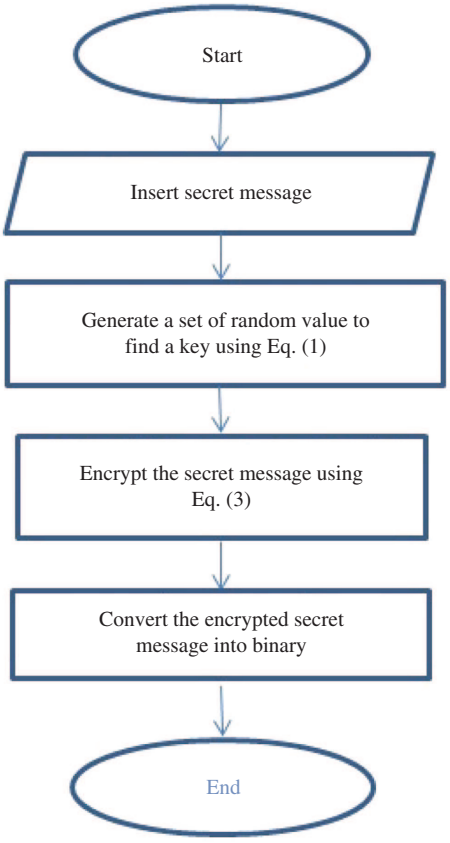

Figure 1: The Flow Chart of Encrypted Secret Message Process.

that, the frames utilized as a cover are chosen randomly. Afterward, the pixels inside the chosen frame utilized for hiding the data inside it is chosen randomly utilizing a knight tour algorithm. Then, the LSB method is utilized to hide the encrypted secret message inside the chosen pixels. Later, this process was applied on the set of images until the encrypted secret message was done. Then, the set of images was converted to the frames. At last, the video frames are merged to get the stego video.

3.2.1 Preparing the Cover Video

This process represents the configuring process for the cover video to embed the information inside it. Here, audio video interleave (AVI) is utilized as a cover for hiding the secret information. AVI is a kind of video file comprised of a gathering of images and sounds and called frames. AVI has a major size, and the principal advantage of utilizing it is hiding the enormous measure of information that can be embedded inside it. Also, it can be transmitted from sender to recipient over the network after the embedding process [2, 13]. Initially, the video is segmented into frames. After that, the frame used for embedding is randomly selected. Then, the knight tour algorithm is utilized to choose a specific pixel of the chosen frame to embed the data utilizing the LSB method.

3.2.2 Knight Tour Algorithm

One of the shortcomings of the LSB method is the serial selection of the pixels. For that reason, it is important to find methods that use a random selection. One of these methods is the knight tour algorithm. It is a succession of moves of a knight on a chessboard to such an extent that the knight visits each square just one time. Subsequent to separating a video into frames, according to this method, the chosen frame is represented as

a chessboard and according to the movement of the knight on the chessboard, which is one row and two columns or two rows and one column in random ways like the letter (L) in English [3, 8], to choose the pixels utilized for embedding the data. This process is utilized to increase the robustness of the proposed method and to beat the detriment of the LSB method that applies the serial choice of the pixels and the shortcoming against the electronic assaults.

3.2.3 Least Significant Bit (LSB) Method

After the process of choosing pixels of frame by utilizing the knight tour algorithm, the LSB method is utilized for the purpose of embedding an encrypted secret message within it. The LSB method is considered a famous and easy method in steganography [28]. In this method, a video frame dealing is finished by changing the least significant bits 7 and 8 to embed the secret data to make the process of change in the video frame hard to recognize by the human eye. Eq. (4) is utilized to compute the pixel value after the embedding process [28]:

$$a_i' = a_i - a_i \bmod 2^n + E_i \tag{4}$$

where the value of a pixel before and after embedding is a_i and a_i', n indicates the quantity of bits that will be embedded, and E_i refers to the encrypted secret message value. Afterward, the video frames are merged to accomplish a stego video that has a secret message.

The steps of embedding process are:

Input: cover video.
Output: stego video.
Step 1: split the video files (.AVI) into frames.
Step 2: convert the video frames into images.
Step 3: select the images used as a cover randomly.
Step4: determine the chosen pixels inside the video frame used for embedding the secret message randomly using knight tour algorithm.
Step 5: LSB method is used to hide an encrypted secret message inside bits (7 and 8).
Step 6: convert the image into the frame.
Step 7: merge the video frames.
Step 8: stego video.

The flowchart of embedding process is shown in Figure 2.

3.3 Extraction Process

In this stage, after the embedding process is completed, the sender sends the stego video into the recipient. The stego video is arranged by dividing the video into frames. Subsequently, the pixels that have the data inside it are determined by utilizing the knight tour algorithm and applying similar steps that are utilized as a part of the embedding process. After that, the LSB method is utilized to extract the encoded secret message from the LSB (7 and 8) of the video frame by utilizing Eq. (5) [28].

$$E_i = a_i' \bmod 2^n \tag{5}$$

where E_i represents the encoded secret message values, and a_i' represents the value of the pixel of the stego image. Later, the encoded secret message will be decoded to get the secret message by utilizing Eq. (6):

$$sm = E - \text{key} \tag{6}$$

where sm represents the secret message values.

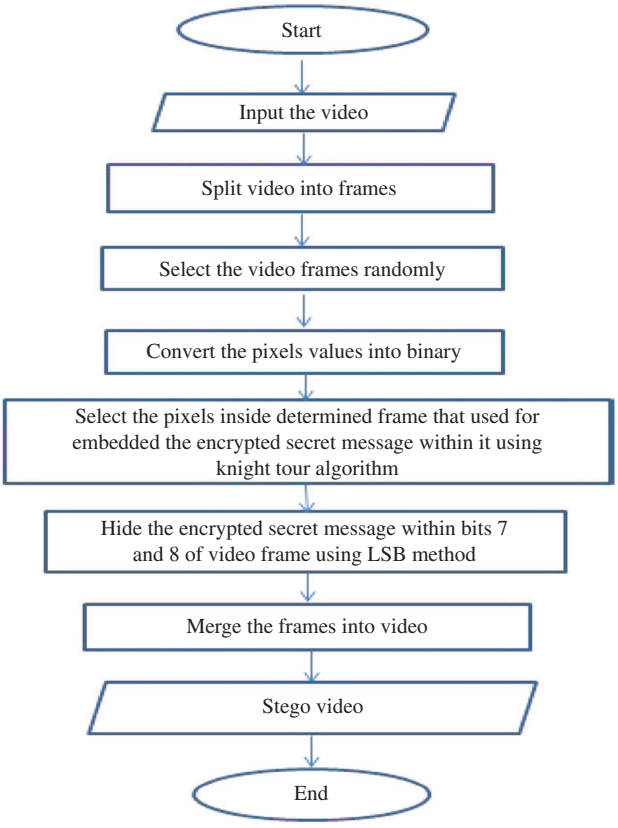

Figure 2: The Flow Chart of Embedding Process.

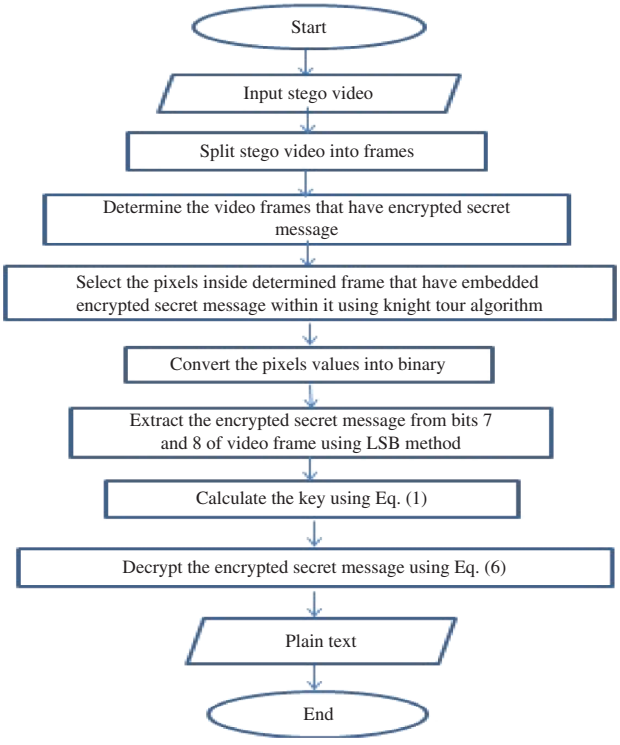

Figure 3: The Flow Chart of Extraction Process.

The steps of the extraction process are:

Input: stego video.
Output: secret message.
Step 1: open the stego video and split it into frames.
Step 2: convert the video frames into images.
Step 3: determine the chosen images used as a cover.
Step 4: determine pixels used for embedding the secret message using knight tour algorithm.
Step 5: LSB method used to recover an encrypted secret message from bits (7 and 8).
Step 6: decrypt the secret message using subtraction method according to Eq. (6).
Step 7: secret message.

Figure 3 explains the flowchart used for the extraction process.

4 Results

The primary objective of this paper is to hide a huge amount of data with high secrecy and saving the quality of video in the meantime. This method is assessed by utilizing numerous components, for example, quality, payload, and robustness. The proposed technique utilizes videos in various sizes as a dataset for assessment as clarified in Figure 4 below.

The peak signal-to-noise ratio (PSNR) is used to assess the quality of the video after the embedding process. If the result of the PSNR is equal or more than 30 dB, it means that the secret data is imperceptible to human vision [9, 16]. The PSNR is used to evaluate the quality using Eq. (7)

$$\mathrm{PSNR} = 10 \log_{10} \frac{\max^2}{\mathrm{MSE}} \tag{7}$$

where, max represents the greatest estimation of pixels in the frame, and MSE (mean square error) is utilized to determine the distortion between the cover video and the stego video and is ascertained utilizing Eq. (8):

$$\mathrm{MSE} = \sum_{i=1}^{\mathrm{M}*\mathrm{N}} (p_i - p_i')^2 / (\mathrm{M}*\mathrm{N}) \tag{8}$$

where, M∗N represent the size of the video frame, while, p_i and p_i' represent the estimation of the pixel before and after the information embedding inside the video frame.


Newsreader.avi


Coastguard.avi


Rhino.avi

Figure 4: The Videos Dataset Used for Evaluating the Proposed Method.

Correlation is utilized to quantify the similarity between the stego videos and cover videos if the value is closer to one, which implies that the stego video is closer to the cover video. Eq. (9) is utilized to compute the correlation as:

$$\mathrm{CR} = \mathrm{cov}(p, p')/\sigma p \sigma p' \tag{9}$$

where CR represents a correlation, cov(p, p') represents the covariation, and $\sigma p \sigma p'$ represents the standard deviation.

Table 1 demonstrates the results of embedding a different size of secret message in the different sizes of cover videos used to assess the proposed method.

From Table 1, observe that the estimation of the PSNR is high, while the estimation of the MSE is low when embedding 24,000 characters inside videos with a size of frame 512∗512. The estimation of the MSE is increasing, and the estimation of the PSNR is decreased when the payloads are increasing to 60,000 and 96,000 characters inside a video, which implies that the quality of the video is decreased when the payload of characters is increased. Also, notice that although the estimation of PSNR is decreased and the estimation of MSE is increased when the size of video frames is decreased to 256∗256 using the same payloads of characters which is used in frame size 512∗512. The results of PSNR are still high, as well the value of the MSE is still low, which means that the stego videos are closer to the original videos. In addition, the values of the correlation are near to 1, and this means that the stego videos are closer to the cover videos.

For the purpose of evaluating or testing the proposed method and the old method, namely, the Sahu and Mitra method [25], the same size of video frame and number of characters are used.

Table 2 represents the comparison between the proposed method and the Sahu and Mitra method [25] using a 256∗256 size of video frames and the payload of 3000 characters that was used for embedding inside the video. The experimental results show that the values of the PSNR and MSE for the proposed method is better than the previous method in all videos used for comparison.

Table 1: The Experimental Results of the Proposed Method.

Video dataset	Size of frame in video	Payload	MSE per frame	PSNR per frame	Correlation per frame
Newsreader.avi	256∗256	24,000	0.2843	66.5255	0.9567
		60,000	0.2891	62.4480	0.9321
		96,000	0.2898	59.9047	0.9012
Newsreader.avi	512∗512	24,000	0.1624	70.9535	0.9856
		60,000	0.1720	66.9081	0.9645
		96,000	0.1794	62.8188	0.9598
Coastguard.avi	256∗256	24,000	0.2753	67.4661	0.9543
		60,000	0.2772	64.1999	0.9335
		96,000	0.2790	61.9156	0.9122
Coastguard.avi	512∗512	24,000	0.1150	68.5684	0.9871
		60,000	0.1164	65.6880	0.9665
		96,000	0.1272	62.9015	0.9610
Rhino.avi	256∗256	24,000	0.2140	68.0999	0.9558
		60,000	0.2152	64.2742	0.9325
		96,000	0.2271	62.8199	0.9082
Rhino.avi	512∗512	24,000	0.1132	70.1098	0.9869
		60,000	0.1251	65.9659	0.9653
		96,000	0.1585	64.4809	0.9599

Table 2: The Experimental Results of the Proposed Method.

Methods	Video dataset	Size of frame in video	No. of characters	MSE per frame	PSNR per frame
Proposed method	Newsreader.avi	256∗256	3000 char	0.2843	66.5255
Sahu and Mitra Method [27]			3000 char	0.6991	63.1972
Proposed method	Coastguard.avi	256∗256	3000 char	0.2753	67.4661
Sahu and Mitra Method [27]			3000 char	0.6371	63.2714
Proposed method	Rhino.avi	256∗256	3000 char	0.2140	68.0999
Sahu and Mitra Method [27]			3000 char	0.5428	65.4914
Average of PSNR and MSE of the proposed method				0.2578	67.3638
Average of PSNR and MSE of the Sahu and Mitra method [27]				0.6263	63.9866

5 Conclusion

In this paper, a novel method for video steganography is proposed by utilizing a proposed key function method to encode a secret message to increase the security. Furthermore, it utilizes a key function for encryption that has an arrangement of arbitrary values that are changed in each process to increase the efficiency and robustness for the proposed method. Also, the knight tour is utilized to enhance the LSB method for embedding the data inside the video frame by randomly selecting the pixels that were utilized for embedding rather than serial selection in the traditional LSB to increase the security and to prevent the hackers from discovering the pixels that have the secret data. The experimental results depict that the proposed method is more reliable in terms of the PSNR, MSE, and security. In future works, it can utilize a key, which represents a set of arbitrary values for selecting frames and embedded image or audio file within a video, and it can used as other methods to select pixels like the PMM and GLV methods.

Bibliography

[1] S. A. Abbas, T. I. El Arif, F. F. Ghaleb and S. M. Khamis, Optimized video steganography using Cuckoo search algorithm, in: *IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS'15)*, 2015, doi: 10.1109/IntelCIS.2015.7397279.

[2] S. A. Alhaj, A. M. Shaheen and T. M. Al-Kharoubi, Multi-layers video steganography, *A Novel Technique for Image Hiding* **4** (2016), 43–52.

[3] Z. S. Y. Alsaffawi, Image steganography by using exploiting modification direction and knight tour algorithm, *J. Al-Qadisiyah Comput. Sci. Math. (QJCM)* **8** (2016), 1–11.

[4] S. Bahrami and M. Naderi, Encryption of video main frames in the field of DCT transform using A5/1 and W7 stream encryption algorithms, *Arab. J. Sci. Eng.* **39** (2014), 4077–4088.

[5] D. Bharti and A. Kumar, Enhanced steganography algorithm to improve security by using vigenere encryption and first component alteration technique, *Int. J. Eng. Trends Technol. (IJETT)* **13** (2014), 242–246.

[6] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, *Digital and Watermarking*, 2nd ed. Elsevier, USA, 2006.

[7] Z. Elzbieta, M. Wojciech and S. Krzysztof, Trends in steganography, *Commun. ACM* **57** (2014), 86–95.

[8] S. Ganzfried, *A New Algorithm for Knight's Tours*, REU Program in Mathematics at Oregon State University, Corvallis, OR, USA, 2004.

[9] K. Jung, and K. Yoo, Improved exploiting modification direction method by modulus operation, *Int. J. Signal Process. Image Process. Pattern Recognit.* **2** (2009), 79–87.

[10] M. Kalra and P. Singh, EMD techniques of image steganography a comparative study, *International Journal of Technological Exploration and Learning (IJTEL)* **3** (2014), 385–390.

[11] M. Kasapbas and W. Elmasry, New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check, *Indian Acad. Sci.* **43** (2018), 1–14.

[12] S. Katzenbeisser and F. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Vol. 28, Artech House, Inc., Norwood, MA, USA, 2000.

[13] M. Kaur and K. Dhindsa, Enhancement of data security using video steganography, *Int. J. Comput. Appl.* **181** (2018), 34–38.

[14] H. Khanzadi, M. Eshghi and S. E. Borujeni, Image encryption using random bit sequence based on chaotic maps, *Arab. J. Sci. Eng.* **39** (2014), 1039–1047.

[15] V. Kumar and D. Kumar, Performance evaluation of modified color image steganography using discrete wavelet transform, *J. Intell. Syst.* (2017), doi:10.1515/jisys-2017-0134.
[16] B. Michael and C. Cachin, Public-key steganography with active attacks, *IBM Res.* **3378** (2004), 1–16.
[17] M. H. Mohammed, M. R. Mohd Shafry and A. A. Ali, A review and open issues of multifarious image steganography techniques in spatial domain, *J. Theor. Appl. Inform. Technol.* **96** (2018), 956–977.
[18] Z. F. Muhsin, A. Rehman, A. Altameem, T. Saba and M. Uddin, Improved quad tree image segmentation approach to region information, *Imaging Sci. J.* **62** (2014), 56–62.
[19] S. Mumthas and A. Lijiya, Transform domain video steganography using RSA, random DNA encryption and Huffman encoding, in: *7th International Conference on Advances in Computing and Communications ICACC-2017*, 115, pp. 660–666, 2017.
[20] S. I. Nipanikar and V. Hima Deepthi, A multiple criteria-based cost function using wavelet and edge transformation for medical image steganography, *J. Intell. Syst.* **27** (2016), doi:10.1515/jisys-2016-0095.
[21] A. Putu, M. Gusti and M. Ni, A MP4 video steganography using least significant bit (LSB) substitution and advanced encryption standard (AES), *J. Theor. Appl. Inform. Technol.* **95** (2017), 5805–5814.
[22] K. Rajalakshmi and K. Mahesh, Video steganography based on embedding the video using PCF technique, in: *IEEE 2017 International Conference on Information communication and Embedded Systems(ICICES)*, pp. 1–4, 2017.
[23] J. J. Ranjani, Data hiding using pseudo magic squares for embedding high payload in digital images, *Multimed. Tools Appl.* **76** (2017), 3715–3729.
[24] K. Rezagholipour and M. Eshghi, Video steganography algorithm based on motion vector of moving object, in: *IEEE Eighth International Conference on Information and Knowledge Technology (IKT)*, 2016, doi: 10.1109/IKT.2016.7777764.
[25] U. Sahu and S. Mitra, A secure data hiding technique using video steganography, *Int. J. Comput. Sci. Commun. Netw.* **5** (2015), 348–357.
[26] A. Saleema and T. Amarunnishad, A new steganography algorithm using hybrid fuzzy neural networks, in: *International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST-2015)*, 24, pp. 1566–1574, 2016.
[27] P. Sethi and V. Kapoor, A proposed novel architecture for information hiding in image steganography by using genetic algorithm and cryptography, *Int. Conf. Comput. Sci.* **87** (2016), 61–66.
[28] A. Shjul and U. Kulkarni, A secure skin tone based steganography using wavelet transform, *IJCTE* **3** (2011), 16–22.
[29] A. Solichin and Painem, Motion-based less significant frame for improving lsb-based video steganography, in: *IEEE International Seminar on Application for Technology of Information and Communication (ISemantic)*, 2016, doi: 10.1109/ISEMANTIC.2016.7873834.
[30] K. Sudeepa, K. Raju, K. Ranjan and A. Ghanesh, A new approach for video steganography based on randomization and parallelization, in: *International Conference on Information Security and Privacy*, 78, pp. 483–490, 2016.
[31] V. Thanikaiselvan, P. Arulmozhivarman, A. Rengarajan, B. John and R. Balaguru, Horse riding and hiding in image for data guarding, in: *International Conference on Communication Technology and System Design 2011, Procedia Engineering 30th 2012*, 2012, pp. 36–44, 2012.