Video steganography using 3D distance calculator based on YCbCr color components

Esraa Jaffar Baker¹, Adil Abbas Majeed², Sundos Abdulameer Alazawi³, Shahreen Kasim⁴, Rohayanti Hassan⁵, Noor Hidayah Zakaria⁶, Tole Sutikno⁷

^{1,3}Computer Sciences Department, College of Science, Mustansiriyah University, Baghdad, Iraq ²Al-Mansour University College, Baghdad, Iraq

^{3,4}Faculty of Computing Science and Information Technology, Universiti Tun Hussein Onn, Johor, Malaysia ^{5,6}School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, Johor, Malaysia ⁷Department of Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Article Info

Article history:

Received May 11, 2021 Revised Oct 5, 2021 Accepted Oct 23, 2021

Keywords:

3D distance calculator Hash function Steganography Video frames YCbCr color components

ABSTRACT

Steganography techniques have taken a major role in the development in the field of transferring multimedia contents and communications. Therefore, field of steganography become interested as the need for security increased significantly. Steganography is a technique to hide information within cover media so that this media does not change significantly. Steganography process in a video is to hide the information from the intruder and prevent him access to that hidden information. This paper presents the algorithm of steganography in the video frames. The proposed algorithm selected the best frames to hide the message in video using 3D distance equation to increasing difficulty onto the intruder to detect and guess the location of the message in the video frames. As well as selected the best frames in this algorithm increased the difficulty and give us the best stego-video quality using structural similarity (SSIM). Also, the hash function was used to generate random positions to hide the message in the lines of video frames. The proposed algorithm evaluated with mean squared error (MSE), peak signalto-noise ratio (PSNR) and SSIM measurement. The results were acceptable and shows that is the difficulty of distinguishing the hidden message in stego-video with the human eye.

This is an open access article under the **CC BY-SA** license.



831

Corresponding Author:

Sundos Abdulameer Alazawi Computer Sciences Department, College of Science, Mustansiriyah University, Baghdad, Iraq Email: ss.aa.cs@uomustansiriyah.edu.iq

1. INTRODUCTION

The process of transferring information became very easy and fast with the development of communication technology. As a result of this development, the world has paid great attention to the information it considers a major revolution that needs safe ways to transmit it. Accordingly, methods of steganography the information became extremely important to prevent the discovery of secret information [1]–[13]. Steganography is a subpart of the information security process that hides confidential information in a digital medium [12]–[19], which makes the attacker difficult to extract information without knowing the algorithm to extract that information that is sent to the intended recipient [2], [20]–[26]. The digital medium includes all known multimedia types such as video, images, text, and others [27]. One of the most important goals of the process of steganography in digital media is to make the secret message that is sent over the internet difficult to access by unauthorized persons [4], [11], [17], [18], [23], [28]–[34]. Also, the hiding process also takes place in a manner that does not attract the doubt of any third party having a secret message

and at the same time, it is difficult to obtain the contents of the hidden message. If the doubt is lifted, the goal of that entire process is not achieved, and the science of steganography becomes useless [4], [11], [12], [16], [19], [23], [25], [33], [35]–[50].

The message hiding process begins with choosing the appropriate medium as a cover, and then include the bits of the secret message in the digital medium. The most traditional methods rely on steganography in images, but recent researches indicate an increased interest in steganography in a video, as the digital video represents a group of visual images that move in the form of digital data. In addition, the video is considered more complicated than the image files, and this increases security against attacks, and this is why the process of steganography the message in the video is an important part of the art of hiding information, which prevents the detection of the hidden message [33], [43], [51], [52]. Most methods of steganography are conducted by including secret messages, with less distortion in the digital medium [4], [8], [41], [53]–[60], [11], [12], [23], [28], [29], [33], [34], [39]. Therefore, to maintain the quality of the digital medium, it provides limited security capability for any limited medium [11], [61], [62], also by considering the use of a method to successfully detect the hidden message in the digital medium by the recipient [4], [11], [12], [23], [39], [41], [63], [64].

For all these and other reasons, this research paper presents a proposed algorithm to embed a secret text in the digital video, which is sent over an untrusted network. And one of the mathematical equations is adopted in the process of calculating the location of concealment of secret text in the digital video. There is selectivity by choosing the frames of digital video suitably which is used to apply the embedding process to get a secret message, that is difficult to sense with the human eye. The aim of this research to provide a secret message using a steganography technique with video cover. This message does not distort the cover of the video and not sense by the human eyes. In addition to this, the proposed algorithm follows an approach to distribute the hidden bits in places, that is difficult for the attacker to guess and access without knowing the extraction algorithm. The algorithm uses the distance equation to this purpose. Also, the appropriate selection of the video frames increases the inability of the attacker to reach the video frames selected. Furthermore, the hash function is used to provide more security in this study.

2. RELATED WORKS

A digital video is a collection of audios and images. Therefore, most steganographic techniques related to audios and images are implemented to video too. Steganography in the video is similar to steganography in the images apart from data is hidden in each frame of the video [1], [18], [47], [48], [54]–[57], [65]–[68], [20], [69]–[77], [22], [23], [33], [34], [43]–[45]. The main advantages of embedding information in a video are the huge amount of information that are hidden inside the covers [4], [11], [17], [22], [40], [45], [48], [51], [57], [78], [79]. Thus, any small distortions might go without noticed by the human eye because of the continuous flow of information. In steganography, the video cover is then broken down into many frames and the message is embedded inside these frames. The size of the information does not issue in video steganography because it is embedded inside multiple frames. Although video steganography bear the large size of the message [1], [18], [48], [54]–[57], [65]–[69], [20], [70]–[77], [22], [23], [33], [34], [44], [45], [47]. But it is necessary the algorithm selects the best bits to embed the information on it [11], [23], [47], [59], [69], [76], [80], [81].

In general, there are two types of steganography in the video, the first one in the spatial domain and the second in the frequency domain [11], [18], [40], [59], [82]. In the spatial domain, this technology directly changes the pixel value of the video cover to obtain the desired improvement. This method is considered one of the most common methods of steganography and is called least significant bit (LSB) [18], [40], [59]. One of the advantages of this method is that it provides a high capacity of data embedding. In this method, the video pixel is selected in advance according to an algorithm, to hide by the LSB so that it cannot be visual by humans. The disadvantage of this method is that it is easy to extract the secret message and thus the third party (the attacker) able to extract the data easily. In order for this method to be more effective, it requires a high number of mathematical operations. In addition to distributing the hidden secret message on the cover video through an algorithm, so that it is difficult for the attacker to fully access the message. The algorithm that is proposed with this research uses this type of method [73], [82].

Some researchers used LSB the spatial domain to embedding many types of message inside video such as [18], [40], [59], [77] that suggested algorithm to embed message randomly inside a video by using LSB with a layer of security to prevent attackers from getting the secret message. It was concluded from the study that the proposed algorithm was efficient and effective with this technique. Also, Narayanan *et al.* [68] and some researchers [18], [23], [83]–[92] proposed a logistic chaos map to choose randomly pixels of video for embedding messages by using 3-2-2 LSB substitution. The results of this algorithm were analyzed with the measuring of steganography and it was getting in line with standard steganography results. Abikoye and

Ogundokun [48] as well Shanthakumari and Malliga [66] suggested an algorithm to hiding message to the video using LSB matching revisited technique (LSBMR). The region of embedding bits in the video frame was selected depending on the size of secret message and difference between two sequence pixels. This algorithm used the sharper edge region to embedding message, this led to lower embedding rate with a larger message data. The result is the higher visual quality stego-video.

Suttichaiya and Sombatkiripaiboon [71] offered an algorithm to hide the information inside cover video using LSB. The algorithm suggested combining a color detection technique to enhance steganography implementation with higher PSNR. Likewise, Ahmad [67] proposed an algorithm of video steganography by providing zero variability for a data message and low computation. The results were compared with other studies and it shows to enhance PSNR values with the existing technique. Deshmukh and Rahangdale [72] suggested an algorithm to hide the message in the video using the hash function encryption method and by using the LSB. The results were acceptable and less distortion. Also, the proposed algorithm provided us with high security through data transfer.

Aswath *et al.* [74] presented a novel algorithm during hiding secret video inside cover video using LSB. The algorithm used Map frame to hide the secret message by an added frame after each video frame that indicated into secret message pixel. The results showed double secure than other algorithms. Kelash *et al.* [93] suggested hiding message in cover video based on color histogram for cover sequences directly. The pixel in each video frame divided into two parts. The right part counted the number of pixels in the left part. This technique succeeds to hide the bigger size of data and extract the data without errors. The previous studies attempted to hide a message in video using many methods without distortions. But there is still a need to suggest new techniques to video steganography using effective embedding and extraction algorithms. Therefore, this study suggests an algorithm to video steganography using 3D distance and hash function coding.

3. RELATED MATERIALS

In this section, some concepts related to this study is discussed. It includes the distance equation and measuring of video steganography. Also, these used concepts in the study are justified.

3.1. 3D distance calculator

In 3D geometry, the length between two points represented as the distance. The line between these two points is the shortest line segment that connect them. Figure 1 shown the 3D space points are represented by their positions (x, y and z) axes and each of them perpendicular to each other.

In this study, the theory of geometry in three dimensions space is used to hide message into the video. The theory presents the distance (d) between the two points in 3D space P1(x1, y1, z1) and P2(x2, y2, z2) is given by (1) is adopted from [95] and [96].

Distance = sqrt
$$((Y_{Lpix1} - Y_{LPix2})^2 + (Cb_{LPix1} - Cb_{LPix2})^2 + (Cr_{LPix1} - Cr_{LPix2})^2)$$
 (1)

The formula of 3D distance is applied to find the distance between two pixels for three components (Y, Cb and Cr). As well, to find the position of the pixel whether saving in even or odd pixel in the proposed algorithm. This formula increases difficulty of the attacker to access the stego-message and discover the information.

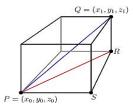


Figure 1. The distance between two points in 3D space [94]

3.2. Performance measures of video steganography

The steganography technique is achieved to hide the secret message inside the cover video and to prevent the attack from accessing the hidden message. Therefore, the quality of the original video is changed, this led to the distortion of the video or some slight changes. In order to measure and evaluate this distortion, to evaluate the distortion of stego-video in the level of acceptable or not, some statistical measurements are utilized to this purpose. In this study, mean square error (MSE), peak signal to noise ratio (PSNR) and the structural similarity (SSIM) index measurements are used, and discussed in the following.

3.2.1. MSE and PSNR measurements

MSE is one of the common measures used to evaluate video steganography distortion. The MSE value of the average of the variation between the cover video without message bits and cover video with message bits [18]. The MSE value is better for the lowest value. The equation of MSE is given by (2).

$$MSE = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} \left(S_{i,j} - C_{i,j} \right)^{2}$$
 (2)

In the (2), Si,j= Stego-video and Yi,j= Cover video. The two parameters X and Y indicated the total numbers of the pixels of video frames for two dimensions [97]. Therefore, MSE is important to measure to evaluate the quality of stego-video and test its modification rate.

Also, PSNR is normally expressed in decibels (dB). PSNR value indicates the level of quality for video after embedding secret message bits. The PSNR formula is in (3).

$$PSNR = 10log_{10} \left(\frac{c^2 Max}{MSE}\right) \tag{3}$$

PSNR is often expressed in decibels (dB). When PSNR value over 30 dB means that is most similar between cover video and stego-video. Besides that, it is difficult for human eyes to detect the modification [98].

3.2.2. **SSIM**

SSIM is a measure recently proposed video fidelity measure that has proved high efficiency for measuring the fidelity of video signals [99]. It is work on high structure nature scene information using HVS for the highly adaptable nature. SSIM provide visual quality between the original video and steg-video because, it has the best capability of perceptual quality [100], [101]. Also, it offers a perfect estimation of perceived video distortion. Therefore, it is used in this study to select the best video frames that has the perceptual quality and at the same time used to measure steg-video. The value acceptable of the SSIM is between the range of (0,1), where is 1 refer to the two frames are identical [102]. SSIM measure is computed by (4).

$$SSIM(x,y) = \frac{(2m_x m_y + C_1)(2\sigma_{XY} + C_2)}{(m_x^2 + m_y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)} \tag{4}$$

 m_x , m_y = mean intensities of cover and stego pixel σ_x , σ_y = mean intensities of cover and stego video block

Where, C_1 =0 and C_2 =0 then SSIM=Q; So, Q becomes a special case of the measure SSIM. Every B blocks of the video's SSIM is calculated and computed the mean SSIM to determine the evaluation of the all video quality [65], [103].

3.3. Hash function

The security is an important attribute of any steganographic algorithm. Any embedding techniques have a high level of security to prevent the attacker from accessing the secret message and obtaining it. In this study hash function technique is used to generate positions random to hide the message bits with original video bits to increase the level of security [75]. The hash function equation represents is in (5).

$$k = p\%n \tag{5}$$

Where k is the position of hiding video frames in LSB; p is the position of each bit in the video frames; and n represents the number of bits for LSB.

The standard variance (STD) video algorithm uses a hash function to generate randomly pixels position and to hide bits message in video frames. The function provides the algorithm with a strong to prevent detection of places and to hide bits in the video by the hacker, which increases the security of the algorithm.

4. METHOD

The research method for this study consists of two parts: embedding algorithm and extraction algorithm.

4.1. Embedding algorithm

Embedding part is the process that the message is hidden inside the video, so that the output is stego-video. The STD video algorithm for this study that is summarized as follows:

Step 1 : To select the frames from cover video.

The idea of this algorithm by selecting the highest amount of color information was selected as the Key frame. In this circumstance, the frames are considered the best visual quality video frames.

- Step 1-1: Transform video to sequence of frames.
- Step 1-2: Convert the RGB color layers of the cover video frame into three different components to Y, Cb and Cr color space by (5) to embed the message.

$$\begin{bmatrix} Y \\ C_b \\ C_T \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.500 \\ 0.500 & -0.419 & -0.081 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$
 (6)

- Step 1-3: Apply SSIM measuring to the frames by (4) which have the largest value is selected to embed the message.
- Step 2 : Find pixels to hide the message by using many steps:
- Step 2-1: Take height (H) and width (W) for the video frame.
- Step 2-2: find summation for first two rows.
- Step 2-3: To start with random pixel by using the equation:

$$Starting = Summation \ mod(int)(0.5 \times (sqrt(Row + Column)))$$

$$If \ Starting < 6 \ then \ Starting = 6 \ (The \ condition \ we \ starting \ from \ sixth \ line \ and \ above)$$

Step 2-4: Calculate the distance (D) between two pixels by (4) for three components (Y, Cb and Cr).

Distance = sqrt
$$((Y_{Lpix1} - Y_{LPix2})^2 + (Cb_{LPix1} - Cb_{LPix2})^2 + (Cr_{LPix1} - Cr_{LPix2})^2)$$
 (7)

- Step 2-5: Find the average (threshold) of summation distances between two components.
- Step 2-6:

 $\begin{cases} distance > average(threshold) then \ hide \ in \ even \ pixel \ in \ less \ line \ bu \ using \ LSB \\ distance < average \ (threshold) then \ hide \ in \ even \ pixel \ in \ greatest \ line \ by \ using \ LSB \\ otherwise = average \ no \ state \end{cases}$

- Step 3 : Embedding process:
- Step 3-1: Calculate the length of text of message steganography and convert to 16 bits.
- Step 3-2: Convert number frame of largest SSIM and convert to 16 bits.
- Step 3-3: Convert Starting value to 16 bits.
- Step 3-4: Store length, starting and number frame 48 bits in LSB of odd bytes of row 4.
- Step 3-5: Repeat step 3-4 with rows (5 and 6) with shift 2 and 4.
- Step 3-6: Convert text of message steganography to bits.
- Step 3-7: In this step, initial store from starting line i.e. (after sixth lines), we take three lines to use first and second lines to find threshold of distance by (4) and third line to save bits of the iteration of steganography text for eleven times by subset LSB method between one bit from text steganography with LSB from (third line).
- Step 3-8: Generate the random position to hide the message by LSB in each line in the video frames; we used hash function technique by (5).

4.2. Extraction algorithm

To extract the original message from the stego-video, the extraction algorithm which is in reverse to the steps of the embedding algorithm is needed. Its inputs were the video of embedding message and its outputs are the original message. The algorithm was applied to many videos and some of them were presented and discuss the results in the next section of this paper. The following summary of the steps of the extraction algorithm:

- Step 1 : Transform video to sequence of frames.
- Step 2 : Restore 48 bits by LSB technique from rows (4, 5, and 6) and take bits of repeat max then convert to length, number frame and starting.
- Step 3: From Starting location, take three lines to calculate the distance between first and second lines depend on distance (4) and take bits by LSB method of third line.
- Step 4 : Using the hash function equation to find the positions of the pixel that used to hide the message in the video frames.
- Step 5 : Extract all text of message steganography bits (eleven frequent).
- Step 6 : Select most frequent bits and convert to text of message steganography.

Step 7 : Display text of message steganography.

5. EXPERIMENT RESULTS AND DISCUSSION

In this section, some experiments were carried on many videos are illustrated. The proposed algorithm tests all frames in videos to select the best frames in each video according to SSIM value to each frame. Figure 2 shown examples to four videos experimented in this study. The SSIM values were used to select the best frames from four videos for this algorithm. It shows that the high bars for each video is represents the highest frames SSIM value and the best value to select. The highest SSIM values of video frames for four videos, these frames are considered the best five frames in each video that used to hide the message in it. Based on [100], the SSIM values for this chart between (0.98-0.88) are acceptable. Figure 2 showed the best video frames were selected with the highest value SSIM. Thus, these frames are the best fidelity and high-quality frames in each video. Furthermore, the cover video in this proposed algorithm converted from RGB to Y, Cb and Cr color space respectively.

Figure 3 shows as one video example from many videos tested in this research, the video frames sequences and converted to Y, Cb and Cr components images to select the best video frames. To evaluate any algorithm, need to use suitable measures. In this study, three measurements are used: MSE, PSNR and SSIM. The results are shown in Table 1. Based on [98] PSNR values in the range (58.7-70.3) are considered acceptable, that means stego-video appear with high-level quality.

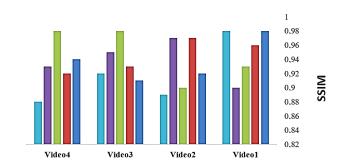


Figure 2. SSIM values for the four video frames

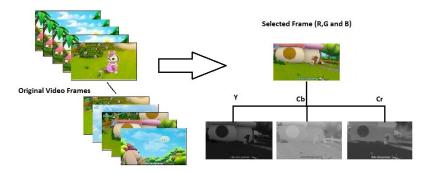


Figure 3. Original video frame RGB to Y, Cb and Cr color space

Figure 4(a) where the chart shows the results of some of the videos used in the experiment, which are found in Table 1 and classify PSNR values. Likewise, the MSE values in the range (0.003-0.016) these indicate poorly distortion and noise for stego-video; as indicated study [98]. Figure 4(b) where the chart displays the results of some of the videos applied in the experiment, which is found in Table 1 and classify PSNR values. Beside that SSIM values appears on the range (0.963-0.995) are acceptable too. This finding is consistent with the studies by Jiang *et al.* [70]. Consequently, stego-video has fidelity and high efficiency, furthermore, shown in Figure 4(c). Also, in Figure 4(d) to compare values between PSNR and SSIM measurements. Which shows the variation between the two measures in measuring the five frames of the four videos.

The Figure 5 shown two video frames, the original video frame before embedding message and stego-video frame after embedding. This means that the intruder is difficult for him to distinguish between the stego-video and the original video, and this is one of the objectives of the proposed algorithm. Therefore, it is concluded from this figure that the stego-video is high visual quality, fidelity and high efficiency.

58.7

0.963

0.016

Despite the difficulty of the proposed algorithm by the intruder to get to steganography message using the distance equation and the best selection of the video frames.

Video Name	Video Frame Size	Text Embedded/Byte	MSE	PSNR	SSIM
Video1	128×128	25	0.003	70.3	0.995
	256×256	55	0.007	68.9	0.991
	512×512	82	0.011	66.7	0.973
Video2	128×128	25	0.006	68.5	0.989
	256×256	55	0.008	65.9	0.985
	512×512	82	0.013	62.6	0.973
Video3	128×128	25	0.003	70.1	0.994
	256×256	55	0.008	68.5	0.990
	512×512	82	0.012	66.5	0.965
Video4	128×128	25	0.008	63.9	0.979
	256×256	55	0.013	61.7	0.971
	Video1 Video2 Video3	Video1 128×128 256×256 512×512 Video2 128×128 256×256 512×512 Video3 128×128 256×256 512×512 Video4 128×128	Video1 128×128 25 256×256 55 512×512 82 Video2 128×128 25 256×256 55 512×512 82 Video3 128×128 25 256×256 55 512×512 82 Video4 128×128 25	Video1 128×128 25 0.003 256×256 55 0.007 512×512 82 0.011 Video2 128×128 25 0.006 256×256 55 0.008 512×512 82 0.013 Video3 128×128 25 0.003 256×256 55 0.008 512×512 82 0.012 Video4 128×128 25 0.008	Videol 128×128 25 0.003 70.3 256×256 55 0.007 68.9 512×512 82 0.011 66.7 Video2 128×128 25 0.006 68.5 256×256 55 0.008 65.9 512×512 82 0.013 62.6 Video3 128×128 25 0.003 70.1 256×256 55 0.008 68.5 512×512 82 0.012 66.5 Video4 128×128 25 0.008 63.9

82

512×512

Table 1. The results for (PSNR, MSE, and SSIM) with different text embedding size

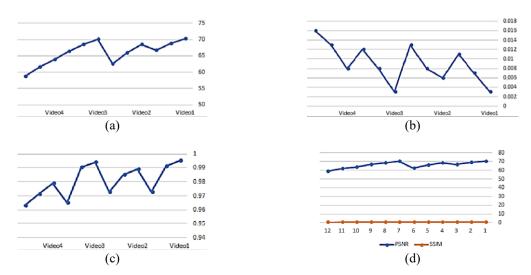


Figure 4. Results of stego-video with (a) PSNR, (b) MSE, (c) SSIM, and (d) compare values between PSNR-SSIM



Figure 5. Applying stego-video frame, (a) original video frame and (b) after steg-video frame

CONCLUSION 6.

This research was proposed the standard variance video algorithm of hiding message bits into a digital video using 3D distance in the space. The proposed algorithm calculates the 3D distance equations and need many steps, provided random location pixels in different videos test. However, the algorithm succeeds to extract the stego-message bits. The technique used the 3D distance equation to increase the strength of the algorithm to resist the intruder to detect and guess the location of the message in the video frames. Likewise, it used the hash function and the iteration of steganography bits for eleven times to increase the level of security. Through the proposed algorithm, the appropriate video frames were selected using a structural similarity (SSIM), which had a role in improving the video quality. Furthermore, was increasing the difficulty of the algorithm on the attacker, that is by selected the different frames in each

video. The proposed algorithm evaluated using the mean square error (MSE) and signal-to-noise ratio (PSNR) measurements, and the results were acceptable. These mean the less distortion between two videos. Also, SSIM used to evaluate the fidelity of stego-video with the original video. The results are stego-video has provided the best capability of perceptual quality. The future work for this study, the proposed algorithm is implemented to another media such as audio. Also, the proposed algorithm is used with frequency domain.

ACKNOWLEDGEMENTS

The authors thank to Mustansiriyah University, Al-Mansour University College, Universiti Tun Hussein Onn and Universitas Ahmad Dahlan for supporting this collaborative research in the present work. Some of this work also was supported by the Malaysian Ministry of Higher Education under Fundamental Research Grant Scheme (FRGS/1/2018/ICT01/UTM/02/4) through Universiti Teknologi Malaysia.

REFERENCES

- [1] H. A. Abdulkadhim and J. N. Shehab, "Audio steganography based on least significant bits algorithm with 4D grid multi-wing hyper-chaotic system," *Int. J. Electr. Comput. Eng.*, vol. 12, no. 1, pp. 320–330, 2022, doi: 10.11591/ijece.v12i1.pp320-330.
- [2] A. R. Khekan, H. M. W. Majeed, and O. F. Ahmed Adeeb, "New text steganography method using the arabic letters dots," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, pp. 1784–1793, 2021, doi: 10.11591/ijeecs.v21.i3.pp1784-1793.
- [3] C. A. Sari, G. Ardiansyah, D. R. I. Moses Setiadi, and E. H. Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 5, pp. 2400–2409, 2019, doi: 10.12928/TELKOMNIKA.v17i5.9570.
- [4] R. Din, O. Ghazali, and A. J. Qasim, "Analytical review on graphical formats used in image steganographic compression," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, no. 2, pp. 441–446, 2018, doi: 10.11591/ijeecs.v12.i2.pp441-446.
- [5] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "A Good Performance OTP encryption image based on DCT-DWT steganography," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 15, no. 4, pp. 1987–1995, 2017, doi: 10.12928/TELKOMNIKA.v15i4.5883.
- [6] R. B. Abduljabbar, O. K. Hamid, and N. J. Alhyani, "Features of genetic algorithm for plain text encryption," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 1, pp. 434–441, 2021, doi: 10.11591/ijece.v11i1.pp434-441.
- [7] L. Sumaryanti, D. H. Kusuma, R. Widijastuti, and M. N. Muzaki, "Improvement security in e-business systems using hybrid algorithm," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 19, no. 5, pp. 1535–1543, 2021, doi: 10.12928/TELKOMNIKA.v19i5.20403.
- [8] M. N. Abdulwahed. and A. k. Ahmed, "Improved anti-noise attack ability of image encryption algorithm using de-noising technique," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 6, pp. 3080–3087, 2020, doi: 10.12928/TELKOMNIKA.v18i6.16384.
- [9] M. Nabil, A. A. M. Khalaf, and S. M. Hassan, "Design and implementation of pipelined and parallel AES encryption systems using FPGA," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 20, no. 1, pp. 287–299, 2020, doi: 10.11591/ijeecs.v20.i1.pp287-299.
- [10] A. I. Salih, A. Alabaich, and A. Y. Tuama, "Enhancing advance encryption standard security based on dual dynamic XOR table and mixcolumns transformation," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 19, no. 3, pp. 1574–1581, 2020, doi: 10.11591/ijeecs.v19.i3.pp%25p.
- [11] T. D. Nguyen and H. D. Le, "A secure image steganography based on JND model," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 2, pp. 2088–2096, 2020, doi: 10.11591/ijece.v10i2.pp2088-2096.
- [12] R. M. Neamah, J. A. Abed, and E. A. Abbood, "Hide text depending on the three channels of pixels in color images using the modified LSB algorithm," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, pp. 809–815, 2020, doi: 10.11591/ijece.v10i1.pp809-815.
- [13] R. Din, R. Bakar, A. Ismail, A. Mustapha, and S. Utama, "Evaluation review of effectiveness and security metrics performance on information technology domain," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 16, no. 2, pp. 1059–1064, 2019, doi: 10.11591/ijeecs.v16.i2.pp1059-1064.
- [14] D. R. I. M. Setiadi, "Improved payload capacity in LSB image steganography uses dilated hybrid edge detection," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 2019, pp. 1–11, Dec. 2019, doi: 10.1016/j.jksuci.2019.12.007.
- [15] V. Sabeti, S. Samavi, M. Mahdavi, and S. Shirani, "Steganalysis and payload estimation of embedding in pixel differences using neural networks," *Pattern Recognit.*, vol. 43, no. 1, pp. 405–415, 2010, doi:

- 10.1016/j.patcog.2009.06.006.
- [16] E. W. Abood, Z. A. Abduljabbar, M. A. Al Sibahee, M. A. Hussain, and Z. A. Hussien, "Securing audio transmission based on encoding and steganography," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 22, no. 3, pp. 1777–1786, 2021, doi: 10.11591/ijeecs.v22.i3.pp1777-1786.
- [17] F. Q. A. Al-Yousuf and R. Din, "Review on secured data capabilities of cryptography, steganography, and watermarking domain," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 17, no. 2, pp. 1053–1059, 2019, doi: 10.11591/ijeecs.v17.i2.pp1053-1058.
- [18] F. Q. A. Alyousuf *et al.*, "Analysis review on spatial and transform domain technique in digital steganography," *Bull. Electr. Eng. Informatics*, vol. 9, no. 2, pp. 573–581, Apr. 2020, doi: 10.11591/eei.v9i2.2068.
- [19] A. Y. Hindi, "A novel method for digital data encoding-decoding," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 5, pp. 2772–2779, 2020, doi: 10.12928/TELKOMNIKA.v18i5.14279.
- [20] K. B. Sudeepa, K. Raju, H. S. Ranjan Kumar, and G. Aithal, "A New Approach for Video Steganography Based on Randomization and Parallelization," *Phys. Procedia*, vol. 78, pp. 483–490, 2016, doi: 10.1016/j.procs.2016.02.092.
- [21] M. O. Dwairi, "A modified symmetric local binary pattern for image features extraction," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 3, pp. 1224–1228, 2020, doi: 10.12928/TELKOMNIKA.v18i3.14256.
- [22] D. Arraziqi and E. S. Haq, "Optimization of video steganography with additional compression and encryption," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 3, pp. 1417–1424, 2019, doi: 10.12928/TELKOMNIKA.V17I3.9513.
- [23] A. Alabaichi, M. A. A. K. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, pp. 935–946, 2020, doi: 10.11591/ijece.v10i1.pp935-946.
- [24] A. A. Sheikh, M. S. Azmi, M. A. Aziz, M. N. Al-Mhiqani, and S. S. Bafjaish, "Diacritic segmentation technique for Arabic handwritten using region-based," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, no. 1, pp. 778–784, 2020, doi: 10.11591/ijeecs.v18.i1.pp478-484.
- [25] N. A. A. Mustafa, "Text hiding in text using invisible character," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 4, pp. 3550–3557, 2020, doi: 10.11591/ijece.v10i4.pp3550-3557.
- [26] Z. N. Al-Kateeb and M. Jader, "Encryption and hiding text using DNA coding and hyperchaotic system," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 19, no. 2, pp. 766–774, 2020, doi: 10.11591/ijeecs.v19.i2.pp766-774.
- [27] A. Albishi *et al.*, "Odd/Even Differential Image Steganography Approach," *21st Saudi Comput. Soc. Natl. Comput. Conf. NCC 2018*, pp. 1–5, 2018, doi: 10.1109/NCG.2018.8593199.
- [28] A. J. Qasim, R. Din, and F. Q. A. Alyousuf, "Review on techniques and file formats of image compression," *Bull. Electr. Eng. Informatics*, vol. 9, no. 2, pp. 602–610, 2020, doi: 10.11591/eei.v9i2.2085.
- [29] N. A. Zebari, D. A. Zebari, D. Q. Zeebaree, and J. N. Saeed, "Significant features for steganography techniques using deoxyribonucleic acid: a review," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 1, pp. 338–347, 2021, doi: 10.11591/ijeecs.v21.i1.pp338-347.
- [30] E. Alrashed and S. S. Alroomi, "Hungarian-puzzled text with dynamic quadratic embedding steganography," *Int. J. Electr. Comput. Eng.*, vol. 7, no. 2, pp. 799–809, 2017, doi: 10.11591/ijece.v7i2.pp799-809.
- [31] S. Fadhel Hamood, M. S. Mohd Rahim, and O. Farook Mohammado, "Chaos image encryption methods: A survey study," *Bull. Electr. Eng. Informatics*, vol. 6, no. 1, pp. 99–104, 2017, doi: 10.11591/eei.v6i1.599.
- [32] M. H. A. Al-Hooti, T. Ahmad, and S. Djanali, "Developing audio data hiding scheme using random sample bits with logical operators," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 13, no. 1, pp. 147–154, 2019, doi: 10.11591/ijeecs.v13.i1.pp147-154.
- [33] S. M. Lokman, A. Mustapha, A. Ismail, and R. Din, "Analysis review on linguistic steganalysis," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 17, no. 2, pp. 950–956, 2019, doi: 10.11591/ijeecs.v17.i2.pp950-956.
- [34] R. Din and A. J. Qasim, "Steganography analysis techniques applied to audio and image files," *Bull. Electr. Eng. Informatics*, vol. 8, no. 4, pp. 1297–1302, 2019, doi: 10.11591/eei.v8i4.1626.
- [35] S. A. Nie, G. Sulong, R. Ali, and A. Abel, "The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 6, pp. 5218–5226, 2019, doi: 10.11591/ijece.v9i6.pp5218-5226.
- [36] G. C. Prasetyadi, R. Refianti, and A. B. Mutiara, "File encryption and hiding application based on AES and append insertion steganography," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 16, no. 1, pp. 361–367, 2018, doi: 10.12928/TELKOMNIKA.v16i1.6409.
- [37] R. S. Sabri, R. Dini, and A. Mustapha, "Analysis review on performance metrics for extraction schemes in

- text steganography," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 2, pp. 761–767, 2018, doi: 10.11591/ijeecs.v11.i2.pp761-767.
- [38] E. A. Abbood, R. M. Neamah, and S. Abdulkadhm, "Text in image hiding using developed LSB and random method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 4, pp. 2091–2097, 2018, doi: 10.11591/ijece.v8i4.pp2091-2097.
- [39] F. Z. Mansor, A. Mustapha, R. Din, A. Abas, and S. Utama, "An Antonym Substitution-based model on linguistic steganography method," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, no. 1, pp. 225–232, 2018, doi: 10.11591/ijeecs.v12.i1.pp225-232.
- [40] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 3, pp. 1168–1175, 2019, doi: 10.12928/TELKOMNIKA.V17I3.12230.
- [41] M. Al-Momin, I. A. Abed, and H. A. Leftah, "A new approach for enhancing LSB steganography using bidirectional coding scheme," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 6, pp. 5286–5294, 2019, doi: 10.11591/ijece.v9i6.pp5286-5294.
- [42] R. Din, R. Bakar, R. S. Sabri, M. Y. Darus, and S. J. Elias, "Performance analysis on secured data method in natural language steganography," *Bull. Electr. Eng. Informatics*, vol. 8, no. 1, pp. 298–304, 2019, doi: 10.11591/eei.v8i1.1441.
- [43] H. K. Tayyeh, M. S. Mahdi, and A. S. A. AL-Jumaili, "Novel steganography scheme using Arabic text features in Holy Quran," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 3, pp. 1910–1918, 2019, doi: 10.11591/ijece.v9i3.pp1910-1918.
- [44] S. Jusoh, A. Mustapha, A. Ismail, and R. Din, "A review of Arabic text steganography: Past and present," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 17, no. 2, pp. 1040–1046, 2020, doi: 10.11591/ijeecs.v17.i2.pp1040-1046.
- [45] M. Fuad and F. Ernawan, "Video steganography based on DCT psychovisual and object motion," *Bull. Electr. Eng. Informatics*, vol. 9, no. 3, pp. 1015–1023, 2020, doi: 10.11591/eei.v9i3.1859.
- [46] M. H. Muhammad, H. S. Hussain, R. Din, H. Samad, and S. Utama, "Review on feature-based method performance in text steganography," *Bull. Electr. Eng. Informatics*, vol. 10, no. 1, pp. 427–433, 2021, doi: 10.11591/eei.v10i1.2508.
- [47] R. Din, R. A. Thabit, N. I. Udzir, and S. Utama, "Traid-bit embedding process on arabic text steganography method," *Bull. Electr. Eng. Informatics*, vol. 10, no. 1, pp. 493–500, 2021, doi: 10.11591/eei.v10i1.2518.
- [48] O. C. Abikoye and R. O. Ogundokun, "Efficiency of LSB steganography on medical information," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 5, pp. 4157–4164, 2021, doi: 10.11591/ijece.v11i5.pp4157-4164.
- [49] B. S. Shashikiran, K. Shaila, and K. R. Venugopal, "Hybrid Domain Steganography for Embedding DES Encrypted QR Code Using Random Bit Binary Search," *Int. J. Innov. Technol. Explor. Eng.(IJITEE)*, vol. 9, no. 2, pp. 310–322, 2021, doi: 10.1007/978-3-030-67101-3 25.
- [50] H. Sajedi and S. Rahbar Yaghobi, "Information hiding methods for E-Healthcare," *Smart Heal.*, vol. 15, p. 100104, Mar. 2020, doi: 10.1016/j.smhl.2019.100104.
- [51] F. L. Malallah, A. A. Jafaar, N. H. Abbas, and M. G. Saeed, "Reversible color video watermarking scheme based on hybrid of integer-to-integer wavelet transform and Arnold transform," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 4, pp. 3519–3527, 2020, doi: 10.11591/ijece.v10i4.pp3519-3527.
- [52] A. R. Hoshi, N. Zainal, M. Ismail, A. R. T. Al Rahem, and S. M. Wadi, "A robust watermark algorithm for copyright protection by using 5-level DWT and two logos," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 22, no. 2, pp. 234–248, 2020, doi: 10.11591/ijeecs.v22.i2.pp234-248.
- [53] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," Comput. Sci. Rev., vol. 13–14, pp. 95–113, Nov. 2014, doi: 10.1016/j.cosrev.2014.09.001.
- [54] P. Shinde and D. T. Rehman, "A Survey: Video Steganography Techniques," *Int. J. Eng. Res. Gen. Sci.*, vol. 3, no. 3, pp. 1457–1464, 2015.
- [55] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC," *IEEE Access*, vol. 5, p. 1, 2017, doi: 10.1109/ACCESS.2017.2691581.
- [56] N. Singh and V. Kumar, "Trends in Digital Video Steganography: A Survey," *Int. J. Comput. Appl.*, vol. 169, no. 7, pp. 6–18, Jul. 2017, doi: 10.5120/ijca2017914786.
- [57] T. Advancements, H. Gupta, R. Gupta, B. Sharma, and S. Gandotra, "Review on Various Techniques of Video Steganography," *Int. J. Sci. Tech. Adv.*, vol. 4, no. 1, pp. 161–164, 2018.
- [58] H. Hamdani *et al.*, "The proposed development of prototype with secret messages model in Whatsapp chat," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3843–3851, 2018, doi: 10.11591/ijece.v8i5.pp3843-3851
- [59] W. A. Shukur and K. K. Jabbar, "Information hiding using LSB technique based on developed PSO

- algorithm," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 2, pp. 1156–1168, 2018, doi: 10.11591/ijece.v8i2.pp1156-1168.
- [60] A. W. A. Qader, I. E. Salem, and H. R. Abdulshaheed, "A new algorithm for implementing message authentication and integrity in software implementations," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 5, pp. 2543–2548, 2020, doi: 10.12928/TELKOMNIKA.V18I5.15276.
- [61] A. Meftouhi, O. Abdelkhalek, A. Allali, A. B. Abdelkader, and T. Toumi, "PV integrated series active filter for sag voltage and harmonic compensation," *Int. J. Power Electron. Drive Syst.*, vol. 10, no. 3, pp. 1255–1262, 2019, doi: 10.11591/ijpeds.v10.i3.1255-1262.
- [62] P. Suresh *et al.*, "Reduction of transients in switches using embedded machine learning," *Int. J. Power Electron. Drive Syst.*, vol. 11, no. 1, pp. 235–241, 2020, doi: 10.11591/ijpeds.v11.i1.pp235-241.
- [63] K. A. Ameen, B. A. Mahmood, and Y. N. Taher, "Secure message transmission scheme in wireless sensor networks," *Bull. Electr. Eng. Informatics*, vol. 10, no. 3, pp. 1514–1523, 2021, doi: 10.11591/eei.v10i3.2856.
- [64] M. J. Alam, T. Chowdhury, S. Hossain, S. Chowdhury, and T. Das, "Child tracking and hidden activities observation system through mobile app," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 22, no. 3, pp. 1659–1666, 2021, doi: 10.11591/ijeecs.v22.i3.pp1659-1666.
- [65] M. M. Hashim, M. S. M. Rahim, F. A. Johi, M. S. Taha, and H. S. Hamad, "Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 3505–3514, 2018.
- [66] R. Shanthakumari and D. Malliga, "Video Steganography Using LSB Matching Revisited Algorithm," *IOSR J. Comput. Eng.*, vol. 16, no. 6, pp. 1–6, 2014, doi: 10.9790/0661-16640106.
- [67] S. Kamil, M. Ayob, S. N. H. Sheikh Abdullah, and Z. Ahmad, "Optimized Data Hiding in Complemented or Non-Complemented Form in Video Steganography," 2018 Cyber Resil. Conf., pp. 1–4, Nov. 2018, doi: 10.1109/CR.2018.8626871.
- [68] G. Narayanan, R. Narayanan, N. Haneef, N. B. Chittaragi, and S. G. Koolagudi, "A Novel Approach to Video Steganography using a 3D Chaotic Map," *TENCON 2019 2019 IEEE Reg. 10 Conf.*, vol. 2019-Octob, pp. 955–959, Oct. 2019, doi: 10.1109/TENCON.2019.8929347.
- [69] M. Yadav and S. Yadav, "Audio and Video based Steganography for Data Hiding-A review," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 6, no. 3, pp. 246–249, 2018, doi: 10.17762/ijritcc.v6i3.1496.
- [70] B. Jiang, G. Yang, and W. Chen, "A CABAC based HEVCc video steganography algorithm without bitrate increase," *J. Comput. Inf. Syst.*, vol. 11, no. 6, pp. 2121–2130, 2015, doi: 10.12733/jcis13774.
- [71] A. Suttichaiya, Y. Sombatkiripaiboon, P. Imtongkhua, C. Poonriboon, and C. So-in, "Video Steganography with LSB Color Detection," *J. Telecommun. Electron. Comput. Eng.*, vol. 9, no. 2, pp. 23–28, 2017.
- [72] P. P. R. Deshmukh and B. Rahangdale, "Hash Based Least Significant Bit Technique For Video Steganography," *Int. J. Eng. Res. Appl.*, vol. 4, no. 1, pp. 44–49, 2014.
- [73] K. U. Singh, "Video Steganography: Text Hiding In Video By LSB Substitution," *Int. J. Eng. Res. Appl.*, vol. 4, no. 5, pp. 105–108, 2014.
- [74] S. Aswath, K. Akshara, P. Pavithra, and D. S. Abinaya, "Implementation of Random Byte Hiding algorithm in Video Steganography," *Int. J. Eng. Res. Technol.*, vol. 5, no. 13, pp. 1–5, 2017, [Online]. Available: https://www.ijert.org/implementation-of-random-byte-hiding-algorithm-in-video-steganography.
- [75] K. Dasgupta, J. K. Mandal, and P. Dutta, "Hash based least significant bit technique for video steganography (HLSB)," *Int. J. Secur. Priv. Trust Manag.*, vol. 1, no. 2, pp. 1–11, 2012.
- [76] V. Swetha, V. Prajith, and V. Kshema, "Data hiding using video steganography-a survey," *Int. J. Sci. Eng. Comput. Technol.*, vol. 5, no. 6, p. 206, 2015.
- [77] A. Basu, G. Kumar, and S. Sarkar, "A Video Steganography Approach using Random Least Significant Bit Algorithm," *Int. J. Sci. Res.*, vol. 3, no. 6, pp. 1811–1816, 2014.
- [78] N. F. Hassan, A. E. Ali, T. W. Aldeen, and A. Al-Adhami, "Video mosaic watermarking using plasma key," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 22, no. 2, pp. 11–20, 2020, doi: 10.11591/ijeecs.v22.i2.pp11-20.
- [79] F. H. MohammedSediq Al-Kadei, "Two-level hiding an encrypted image," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, no. 2, pp. 961–969, 2020, doi: 10.11591/ijeecs.v18.i2.pp961-969.
- [80] J. N. Shehab, H. A. Abdulkadhim, and T. F. H. Al-Tameemi, "Robust large image steganography using lsb algorithm and 5d hyper-chaotic system," *Bull. Electr. Eng. Informatics*, vol. 10, no. 2, pp. 689–698, 2021, doi: 10.11591/eei.v10i2.2747.
- [81] M. Alanezi, I. S. M. Altaay, and S. Y. H. Mallaàloo, "Payload and quality augmentation using steganographic optimization technique based on edge detection," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 23, no. 1, pp. 529–539, 2021, doi: 10.11591/ijeecs.v23.i1.pp529-539.
- [82] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K. H. Jung, "Image steganography in spatial

- domain: A survey," *Signal Process. Image Commun.*, vol. 65, pp. 46–66, 2018, doi: 10.1016/j.image.2018.03.012.
- [83] O. M. Al-Hazaimeh, "A new speech encryption algorithm based on dual shuffling Hénon chaotic map," Int. J. Electr. Comput. Eng., vol. 11, no. 3, pp. 2203–2210, 2021, doi: 10.11591/ijece.v11i3.pp2203-2210.
- [84] H. M. Salih and R. S. Al Mahdawi, "The security of RC4 algorithm using keys generation depending on user's retina," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 24, no. 1, pp. 452–463, 2021, doi: 10.11591/ijeecs.v24.i1.pp452-463.
- [85] N. Krishnaveni and S. Periyasamy, "A novel and innovative approach for image steganography with chaos," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 1, pp. 263–267, 2018, doi: 10.11591/ijeecs.v11.i1.pp263-267.
- [86] O. Omoruyi, C. Okereke, K. Okokpujie, E. Noma-Osaghae, O. Okoyeigbo, and S. John, "Evaluation of the quality of an image encrytion scheme," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 6, pp. 2968–2974, 2019, doi: 10.12928/TELKOMNIKA.v17i6.10488.
- [87] R. A. Mustafa, A. A. Maryoosh, D. N. George, and W. R. Humood, "Iris images encryption based on QR code and chaotic map," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 1, pp. 289–300, 2020, doi: 10.12928/telkomnika.v18i1.13293.
- [88] T. T. Ramanathan, J. Hossen, S. Sayeed, and J. Emerson Raja, "Survey on computational intelligence based image encryption techniques," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 19, no. 3, pp. 1428–1435, 2020, doi: 10.11591/ijeecs.v19.i3.pp1428-1435.
- [89] B. K. Siddartha and G. K. Ravikumar, "An efficient data masking for securing medical data using DNA encoding and chaotic system," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, pp. 6008–6018, 2020, doi: 10.11591/ijece.v10i6.pp6008-6018.
- [90] Y. Alemami, M. A. Mohamed, S. Atiewi, and M. Mamat, "Speech encryption by multiple chaotic maps with fast fourier transform," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, pp. 5658–5664, 2020, doi: 10.11591/ijece.v10i6.pp5658-5664.
- [91] A. H. Khaleel and I. Q. Abduljaleel, "Secure image hiding in speech signal by steganography-mining and encryption," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, pp. 1692–1703, 2021, doi: 10.11591/ijeecs.v21.i3.pp1692-1703.
- [92] H. A. Marzog, M. J. Mohsin, and M. A. Therib, "Chaotic systems with pseudorandom number generate to protect the transmitted data of wireless network," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, pp. 1602–1610, 2021, doi: 10.11591/ijeecs.v21.i3.pp1602-1610.
- [93] H. M. Kelash et. al., "Utilization of Steganographic Techniques in Video Sequences," *Int. J. Comput. Netw. Technol.*, vol. 02, no. 01, pp. 17–24, Jan. 2014, doi: 10.12785/IJCNT/020103.
- [94] S. Schlicker, D. Austin, and M. Boelkins, "Active Calculus Multivariable: 2018 Edition," 2018.
- [95] M. H. Protter and C. B. Morrey, *Intermediate Calculus*. New York, NY: Springer New York, 1985.
- [96] S. K. Stein, *Calculus in the First Three Dimensions*, First Edit. Dover Publications, 2016.
- [97] S. Mungmode, R. R. Sedamkar, and N. Kulkarni, "A Modified High Frequency Adaptive Security Approach using Steganography for Region Selection based on Threshold Value," *Procedia Comput. Sci.*, vol. 79, pp. 912–921, 2016, doi: 10.1016/j.procs.2016.03.114.
- [98] M. H. Shirafkan, E. Akhtarkavan, and J. Vahidi, "A image steganography scheme based on discrete wavelet transform using lattice vector quantization and reed-solomon encoding," in 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Nov. 2015, pp. 177–182, doi: 10.1109/KBEI.2015.7436041.
- [99] P. Ndajah, H. Kikuchi, M. Yukawa, H. Watanabe, and S. Muramatsu, "SSIM image quality metric for denoised images," *Int. Conf. Vis. Imaging Simul. Proc.*, no. August 2015, pp. 53–57, 2010.
- [100] A. Hore and D. Ziou, "Image Quality Metrics: PSNR vs. SSIM," in 2010 20th International Conference on Pattern Recognition, Aug. 2010, pp. 2366–2369, doi: 10.1109/ICPR.2010.579.
- [101] S. Wang, A. Rehman, Z. Wang, S. Ma, and W. Gao, "SSIM-Motivated Rate-Distortion Optimization for Video Coding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 4, pp. 516–529, Apr. 2012, doi: 10.1109/TCSVT.2011.2168269.
- [102] T. Rabie, M. Baziyad, T. Bonny, and R. Fareh, "Toward a Unified Performance Metric for Benchmarking Steganography Systems," *J. Circuits, Syst. Comput.*, vol. 29, no. 03, p. 2050042, Mar. 2020, doi: 10.1142/S0218126620500425.
- [103] A. K. Sahu and G. Swain, "High fidelity based reversible data hiding using modified LSB matching and pixel difference," *J. King Saud Univ. Comput. Inf. Sci.*, Jul. 2019, doi: 10.1016/j.jksuci.2019.07.004.