IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 11, No. 9, September, 2024, pp. 2587-2593
Journal homepage: http://iieta.org/journals/mmep

Secure Data Hiding Technique for Video Steganography

Sheimaa Hadi*, Suhad A. Ali, Majid Jabbar Jawad

Department of Computer Science, College of Science for Women, University of Babylon, Babylon 51001, Iraq

Corresponding Author Email: wsci.sheimaa.hadi@uobabylon.edu.iq

https://doi.org/10.18280/mmep.110930

Received: 27 August 2023
Revised: 19 November 2023
Accepted: 30 November 2023
Available online: 29 September 2024

Keywords:
steganography, tent map, integer wavelet transform, LSB, odd and even parity method

ABSTRACT

Multimedia material, such as digital video, is utilized to conceal a secret message. Given the features of digital video, which has a large storage capacity, confidential data may be inserted. Three requirements must satisfy to grantee secure steganography system. These requirements include security, robustness, and imperceptibility. This paper proposes a steganography scheme to enhance the security of video steganography and attempt to meet the three requirements mentioned above. The security requirement is accomplished through two levels. In the first level, the secret message is encrypted before the embedding process using proposed encryption method based on a combination of chaotic and Arnold's map. In the second level, the secret message is embedded in the selected frames of the video. Instead of traditional LSB technique, we will use a modified LSB technique to meet the robustness requirement. A modified LSB technique is satisfied by embedding the secret message in the LSB of cover video in frequency domain after applying the integer wavelet transform (IWT). According to the experimental results, the stego video quality is like the original video where the obtained PSNR value was 61.922, so the third requirement, imperceptibility, was satisfied.

1. INTRODUCTION

Information security is the protection of important data from unauthorized users and eavesdroppers. This science is divided into two types: encryption, which means converting confidential data into an incomprehensible form [1]. The other type is steganography, which depends on concealing the same secret message from others [2]. This means that its main difference from encryption is that encryption knows by the intruder but does not understand it, while in steganography, the intrusive does not know the existence of a message at all [3]. With time, digital data has become very massive, and attackers have increased the threat to this data. Therefore, the necessity of finding better ways to protect this data has increased [4].

In any security system, a set of essential characteristics must be considered. One of these characteristics is perceptual transparency [5], which means that the visual design of humans cannot notice any change in the message host. The second characteristic is capacity, which refers to the volume of security information concealed within the host without noticeable distortion [6]. Finally, Tamper resistance. It is noted that in any masking system, there must be a trade-off between these characteristics. The large capacity of the data to be hidden can lead to distortion in the host and vice versa [7]. The higher the perceptual transparency, the lower the tampering resistance [8]. This paper suggests the IWT-based information masking method and the combination of LSB and odd-even methods.

The goal of this paper is to make the steganography system more secure. This is can be accomplished by hiding the secret message in a video frame so that it is difficult to identify which video frame was used for the hiding operation. This method contributed to combining the characteristics of the spatial domain, which is represented by using LSB method to increase storage capacity, and the characteristics of the frequency domain, which is characterized by the robustness of hiding messages.

This paper, suggests a steganography technique combined with encryption technique to ensure imperceptibility, security, and robustness of the video steganography. The second section of the research structure briefly refers to the techniques that were used in this paper. The third section presents and discusses the results that have been reached, and the last section shows conclusions and some proposals that could be implemented in the future.

2. PREVIOUS WORKS

The scientists who study video steganography have offered a wide range of methodologies and strategies. Getting precise results is the primary goal of these strategies and tactics. Recently, researchers have focused on using various techniques to improve the execution of video steganography.

Rajkumar and Malemath [9] suggested video steganography, in which data is concealed beneath video frames. Data is encrypted using a cryptographic technique before being incorporated into video frames. To increase the capacity of hiding technique, LSB coding is the method used to conceal

the data. This work does not take into consideration the robustness of the proposed method against different attacks.

Younus and Younus [10] suggested a way to hide the data after converting the selected frame to the frequency domain using IWT and DWT. Then the LSB method was used in the embedding process. MSE and PSNR measures were utilized to gauge the effectiveness of the suggested approach.

Mstafa et al. [11] has introduced two levels of safety. Firstly, was encodes the secret data using Arnold's method, and at the second level, the shi - Tomasi method was used to discover the corner regions in the video frame selected for the embedding process. Then, the LSB algorithm is applied to hide inside corner points. The results of this work were tested, and the PSNR value was 60.7 dB PSNR.

Hussien et al. [12] presented two methods for data protection. The first method uses public key technology to encrypt data using the Menezes-Vanstone elliptic curve ciphering algorithm. Afterward, based on the seed chosen, the encoded information is randomly added into the frame. The experiment's findings utilized an average PSNR of 65 and an average MSE of 85. Samiappan and Bhubaneswar [13] proposed a way to hide information after encoding it in a video where the AES method was used to encrypt secret information to raise security. The Least Significant Bit (LSB) method was used to hide information using FPGA technology. The frames were chosen randomly to hide and scatter the data between frames. The results of this work were tested, and the PSNR value was 57.1 dB PSNR. Shaik and Thanikaiselvan [14] suggested a video steganography technique based on object motion and DCT-psychosexual. The embedding regions are determined via motion analysis. The pro-posed method selects six DCT coefficients in the middle frequency by using the DCT effect. The suggested approach modifies middle DCT coefficients and embeds a message.

In this study, the video steganography method was proposed using two maps (Arnold and Al-tent chaotic) to encrypt a secret message and increase security. The information was embedded within the video using the LSB method, which was further enhanced by the integer wavelet transform to increase security and robustness when choosing the frame to embed the secret image inside the video while maintaining the quality of the stego video and making it look like the cover video.

3. PRELIMINARIES

3.1 Integer wavelet transform

Many signal patterns encountered in real-world applications are converted to integers, such as analog-to-digital (A/D) signal conversion and color intensity in digital images [15]. IWT is a reversible method for converting an integer to an integer from Wavelet analysis. IWT is used in applications whose purpose is to output integer operands IWT is ideal for lossless data compression applications and is computationally faster and more memory-efficient [16]. It allows the entire integer signal to be reconstructed from integer coefficients [8].

As seen in the following Figure 1, the IWT algorithm has three stages: split, predict, and update. In first stage even and odd set samples are extracted from the input image, then the even sequence samples are used to forecast the odd sequence samples, these done at second stage (predict), finally implemented low-pass filtering process where represent the update stage [17].

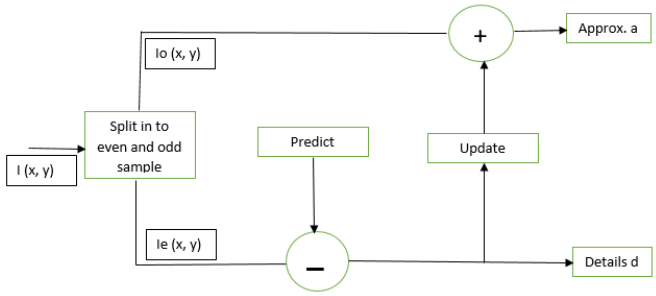

Figure 1. Lifting wavelet forward transform [17]

3.2 Tent chaotic map

A regular, continuous map with a single fixed point is called a chaotic tent map. Following band splitting transitions within the chaotic zone that converge at the transfer stage into the no chaotic field occur once the goal height is reached. In particular, the time-correlation function and power distribution of no periodic orbits were calculated at the band-splitting spots and in the vicinity of other locations.

A tent map (TM) is defined as the following Eq. (1):

$$x_n = \begin{cases} ux_n & x_n < 0.5 \\ u(1-x_n) & 0.5 \leq x_n \end{cases} \quad (1)$$

where, x_n is the initial condition, and $u \in [0, 2]$ represents the control parameter [18]. This map generates random numbers used later as a mask to implement an encrypted process [10].

3.3 Arnold map

To strengthen and secure the steganography technique, the secret message is scrambled by using Arnold's chaotic map depending on the following Eq. (2) [19]:

$$\begin{bmatrix} \bar{q}` \\ p` \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} q \\ p \end{bmatrix} (\text{mod N}) \quad (2)$$

where, $q`$ and $p`$ represent the transformed location, q, and p are the sample's position in the matrix with size (N×N), n={1, 2, 3, …, N-1}.

The Inverse Arnold map is illustrated in the following Eq. (3) [20]:

$$\begin{bmatrix} q \\ p \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \times \begin{bmatrix} \bar{q}` \\ p` \end{bmatrix} (\text{mod N}) \quad (3)$$

4. THE PROPOSED METHOD

Figure 2 illustrates the general block diagram of the proposed video steganography method. The method consists of several procedures. These procedures can be listed as follows:

4.1 Sender side

On this side, two procedures are being done:

4.1.1 Secret image encryption procedure

This subsection explains the proposed encryption method. The encryption procedure is implemented with several steps:

Step 1: Scrambling the secret image using Eq. (2).

Step 2: Generating a mask, a series of numbers, using Eq. (1). The mask's length and the secret image's length must match.

Step 3: Converting the generated mask into binary numbers depending on the following Eq. (4):

$$Mask(i) = \begin{cases} 1 & if \quad Mask(i) \geq Thr \\ 0 & otherwise \end{cases} \tag{4}$$

where, *Thr* is the threshold, the value of the threshold in the proposed steganography method is equal to the average of the generated chaotic sequence in step 2.

Step 4: Encrypt the secret image by performing an XOR operation on the secret image and the mask.

When using XOR encryption, data is encrypted using a technique that is difficult to decrypt using a brute-force approach, which involves creating random encryption keys and matching them with the right one.

The following Figure 2 illustrates example of encryption method where the value of (Thr) is 0.4.

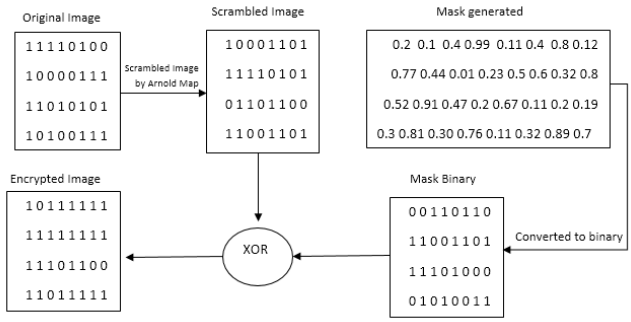

Figure 2. Example of encryption method

4.1.2 Embedding procedure

This subsection explains the proposed embedding operation, as illustrated in Figure 3, along the method for selecting frame (frames) for embedding.

Video frames selecting: In this stage, a frame is selected for embedding. At first, the video is separating into frames. Then, using the Eq. (5) to choose a frame as an embedding place for the hidden image.

$$SF\ no = (Of\ no * Key)\ mod\ NF + 1 \tag{5}$$

where,

Key is a prime number and key ∈ Z–{factors of NF}.

SF no is the number of selected frame.

Of no is the number of original frame.

NF is the total number of video frames.

For example, we have a video which have 20 frames. Suppose the (*Key*) value is (27) and (OFno) value (2) then the selected frame number (SFno) for embedding which is computed according to Eq. (5) is (15).

Embedding operation: The embedding operation is implemented with several steps:

Step 1: Separating the video into frames.

Step2: Using the Eq. (5). to choose a frame as an embedding place for the hidden image.

Step 3: Applying one level of IWT on one band of the selected frame, such as Red, Green, and Blue.

Step 4: Dividing the coefficient of the transformed band into non-overlapping blocks of size 8×8 coefficients.

Step 5: Selecting the four middle coefficients for the block to embed bits of the secret image.

Step 6: Counting ones (*One_bit*) for each coefficient within the middle of blocks according to the following Eq. (6).

$$One\_bit = \sum_{i=1}^{n} b_i \tag{6}$$

where, *One_bit*, *i*, *n*, and *b* are the number of ones, the first bit is the last and bit value, respectively.

Step 7: Checking whether the number of ones is odd. If so, If the bit of a secret message is zero, reverse the LSB bit.

Step 8: Checking whether the number of ones is even. If so, If the bit of a secret message is one, reverse the LSB bit.

Step 9: Repeating Step 5, Step 6, Step 7, and Step 8 until all bits of the secret message are embedded.

Step 10: Implementing inverse of IWT on-stage band.

Step 11: Reconstruct the stego fame with other frames of video.

Step 12: Getting the stego video.

Figure 4 illustrates an example on embedding method.

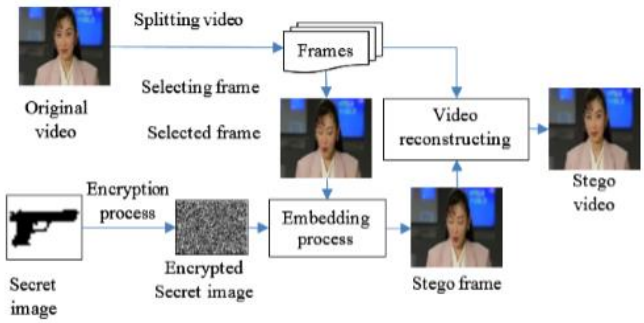

Figure 3. Encryption and embedding procedures

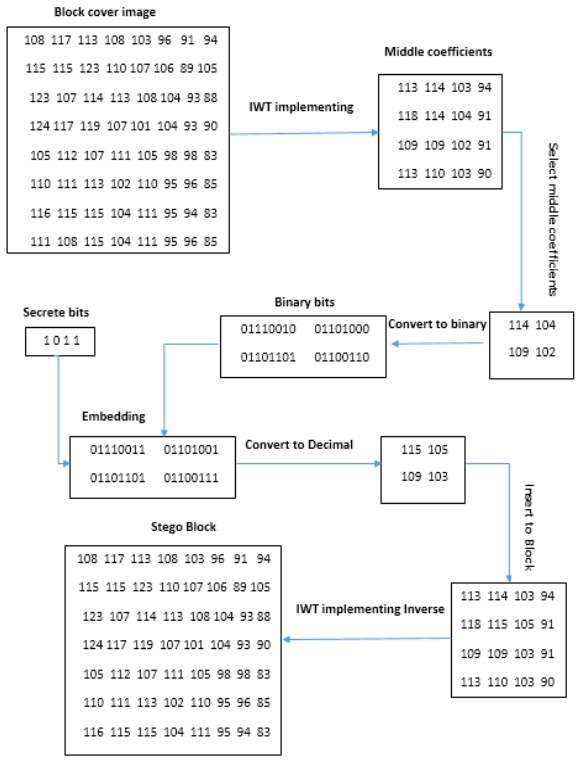

Figure 4. Example of embedding method

Hiding capacity computation: The suggested approach can store non-specific bits of information length in each frame depending on the size of the frame. For a frame of size ($M \times N$) that divides into a block of size (8×8), the capacity (C) can be calculated as follows:

$$C = \frac{M}{8} \times \frac{N}{8} \times 4 \quad (7)$$

However, each block can store (4 bits) of data when the frame size is 256×256 pixels and the size of each block is 8×8 pixels. Therefore, the hiding capacity is 1024×4=4096 bits per cover frame and when increasing the frame size increases the number of blocks; thus, embedding capacity also increases.

4.2 Receiver side

On this side, two procedures are being done:

4.2.1 Extracting the secret image procedure

This subsection explains the proposed extracting method, as illustrated in Figure 5. The extracting procedure is implemented with several steps:

Step 1: Separating the video into frames.

Step 2: Choosing a stego frame as a cover for extracting the secret image using Eq. (5).

Step 3: Applying one level of the IWT frame.

Step 4: Dividing the coefficients transformed the band into non-overlapping blocks of size n*n coefficients.

Step 5: Select the four middle coefficients for the block.

Step 6: Counting ones (One_bit) for each coefficient within the middle of the block according to Eq. (6).

Step 7: Checking whether One_bit is odd. If so, extract 1 from the Stego coefficient.

Step 8: Checking whether One_bit is even. If so, extract 0 from the Stego coefficient.

Step 9: Repeating Step 5, Step 6, Step 7, and Step 8 until all bits of scrambled secret messages are extracted.

The Figure 6 illustrates an example of Decryption method.

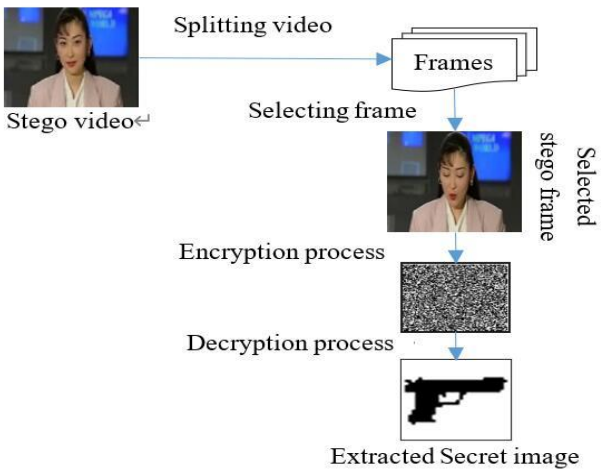

Figure 5. Extracting and decryption procedures

4.2.2 Secret image decryption procedure

This subsection explains the proposed decryption method. The decryption procedure is implemented with several steps:

Step 1: Generating a mask, a series of numbers, using Eq. (1). The length of the mask must be equal to the length of the secret image.

Step 2: Converting the generated mask into binary numbers depending on Eq. (4).

Step 3: Decrypting the secret image by applying the XOR operation between the mask and the scrambled secret image.

Step 4: Descrambling the scrambled secret image using Eq. (3).

The Figure 7 illustrates an example of Decryption method.

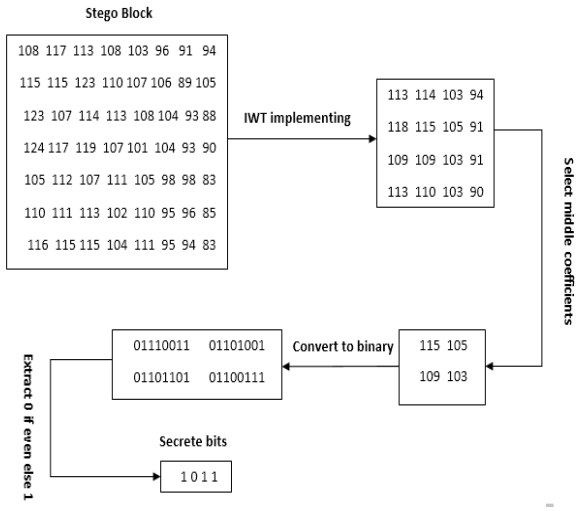

Figure 6. Example of extracting procedures

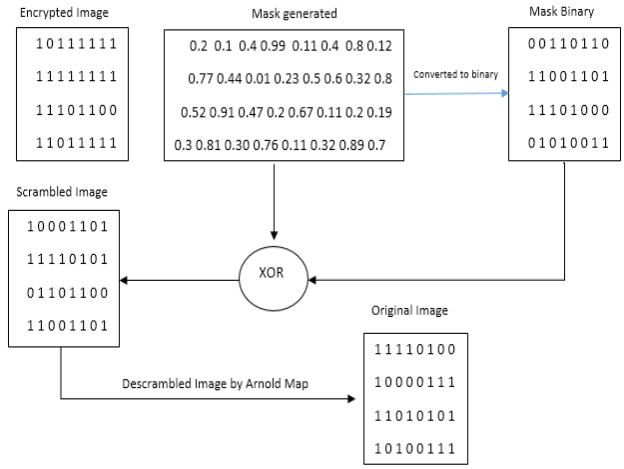

Figure 7. Example of decryption procedures

5. EXPERIMENTAL RESULT

The main goal of this research is to secretly store a significant quantity of data while maintaining video quality. This approach is evaluated using a variety of factors, including quality, payload, and robustness. The following section shows the results obtained by the proposed method.

5.1 Data set

Figures 8 and 9 display the dataset used with the suggested method. The first dataset is AVI videos which will be used as a cover for inserting a secret image. The second dataset is binary images which be used as a secret image.

Men News Boy

Figure 8. Sample of AVI videos to be as covers

Secret1 Secret2 Secret3

Figure 9. Sample of secret images

5.2 Image encryption performance

The security of the proposed method is verified by testing the proposed encryption method based on several criteria adopted to reveal the efficiency of the proposed encryption system.

5.2.1 Entropy

It is one of the essential measures to measure the efficiency of the encrypted image because it indicates the extent of the randomness of the data in the encrypted image. Eq. (8) is used to compute the entropy value [21].

$$Entropy = -\sum_{i=1}^{m} P_i \ log_2(P_i) \tag{8}$$

where, P_i= probability of grayscale (i), and m=number of gray scale of the image.

5.2.2 Correlation coefficient

It is a measure that expresses the degree of relationship between adjacent pixels in an encoded image. The goal of this metric is to conserve the amount of excess information available in the encoded image as low as possible. If the correlation coefficient value is close to zero, the original and the encoded images are wholly dissimilar [22].

$$CC = \frac{\sum_i \sum_j (P_{ij} - \bar{P})(Q_{ij} - \bar{Q})}{\sqrt{(\sum_i \sum_j (P_{ij} - \bar{P})^2 ((\sum_i \sum_j (Q_{ij} - \bar{Q})^2))}} \tag{9}$$

where, P is an original image, Q is an encrypted image, $\bar{P}$ is the mean of P, and $\bar{Q}$ is the mean of Q.

5.2.3 Differential attacks (NPCR and UACI)

Each NPCR and UACI is employed to measure the resistance of the suggested coding system by measuring the change in pixels and the extent to which it affects them. It is a measure related to differential attacks. The value of NPCR can be calculated using Eq. (9) [23].

$$NPCR = \frac{A(i,j)}{m*n} * 100\% \tag{10}$$

where, m is the row, n is the column for the image, and A is computing on the Eq. (11).

$$A(i,j) = \begin{cases} 1 & \text{if } \text{oreginal}_{\text{image}(i,j)} = \text{decryption}_{\text{image}} \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

The value of UACI is calculated using Eq. (12).

$$UACI = \frac{1}{m*n}[\sum_{i,j} \frac{A(i,j) - A'(i,j)}{2^L - 1}]*100\% \tag{12}$$

where, L, A, A' equals the number of gray levels, the original and encrypted images, respectively. Table 1 shows the experimental results after implementing the proposed encryption method.

Table 1. The value of experimental results

Secrets Image	Entropy	Correlation Coefficient	NPCR	UACI
Secret 1	0.9931	0.0011	52.4536	52. 4536
Secret 2	0.9945	0.0149	51.2817	51.2817
Secret 3	0.9915	0.0106	52.1362	52.1362

Table 2. The PSNR and the MSE values after applying the proposed steganography method

Secretes Image	Frame No.	Original Image	Stego_Image	PSNR	MSE
	1			61.922	0.047
	19			61.907	0.049
	37				
	119			61.931	0.047
	231			61.877	0.042
	Averare			61.910	0.0418

5.3 Image steganography performance

This section explains the experiment results after applying the video steganography method (Table 2).

5.3.1 Transparency measuring

To measure the efficiency of the stego-image in terms of transparency, we used the PS N R scale to compare the original frame and the frame after the embedding process, according to the Eq. (13) [24].

$$PSNR = 10\,log\frac{(2^K)^2}{MSE} \tag{13}$$

K is the maximum number of bits required to encode an image's pixel information. *MSE* represents the mean square error, and Eq. (14) represents it.

$$MSE = \frac{1}{N \times M}\sum_{i=1}^{N}\sum_{j=1}^{M}(F_{ij} - S_{ij})^2 \tag{14}$$

S points to the stego frame, *F* points to the original frame, and *N*×*M* points to the frame dimensions.

5.3.2 Robustness measuring

A normal correlation is an essential metric for assessing the robustness of the suggested system. Eq. (15) is used to calculate the normal correlation value [25].

$$NC = \frac{\sum_{p=1}^{x}\sum_{q=1}^{y} SI(p,q)SI'(p,q)}{\sqrt{\sum_{p=1}^{x}\sum_{q=1}^{y} SI(p,q)^2}} \tag{15}$$

SI points to the secret image before hiding, and SI' points to the secret image after retrieval. The value of the normal correlation was equal to (NC=1) for all secret binary images and all the frames tested for hiding. It should be noted that the stego frame was tested against various attacks to ensure its robustness. The results of NC after subjecting the attacks are shown in Table 3.

Table 3. The NC values

Type of Attacks	NC
No attack	1
Salt & pepper (0.001)	0.9984
Salt & pepper (0.01)	0.9865
Salt & pepper (0.03)	0.9627
Cropping 25%	0.9810
Cropping 50%	0.9241
Rotation & cropping 10 degree	1
Rotation & cropping 180 degree	1
Gaussian filter	1
Resize	1

6. CONCLUSIONS

In order to improve security, a new video steganography technique is presented in this research that encrypts a secret image using a suggested encryption mechanism. To further improve the effectiveness and robustness of the suggested approach, the frame selecting method is used to improve the LSB method of embedding data inside the video frame. Rather than using serial selection as in the traditional LSB, random selection of the frame used for embedding increases security and keeps hackers from finding the frame containing the secret data. According to the experimental findings, the suggested approach is more dependable in terms of PSNR, MSE measures. In future works, the following is a list of the proposed:

- 1. Studying the possibility of using the suggested strategy with delicate images like those in the medical and military fields.
- 2. Studying the possibility of applying the proposed method to other media such as text or voice.

ACKNOWLEDGMENT

The Department of Computer Science, College of Science for Women, Babylon University, Babylon, Iraq, supported this work.

REFERENCES

[1] Joshi, J., Choudhary, M., Tiwari, V., Bhagasara, S. (2015). A review on data security using video steganography. International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering, 4(5): 3892-3896. http://doi.org/10.15662/ijareeie.2015.0405015

[2] Nandi, B., Ghanti, M. (2017). Lossless steganography: An approach for hiding text under image cover. In 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, pp. 436-441. https://doi.org/10.1109/ICICI.2017.8365389

[3] Thakur, A., Singh, H., Sharda, S. (2015). Secure video steganography based on discrete wavelet transform and Arnold transform. International Journal of Computer Applications, 123(11): 25-29. https://doi.org/10.5120/ijca2015905596

[4] GR, M., RB, S. (2021). Video steganography: A survey of techniques and methodologies. In Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021), Tamil Nadu, India. http://doi.org/10.2139/ssrn.3851241

[5] Kadhim, A.M., Jawad, H.M. (2021). Studying audio capacity as carrier of secret images in steganographic system. Iraqi Journal of Physics, 19(49): 53-61. https://doi.org/10.30723/ijp.v19i49.648

[6] Duan, X., Gou, M., Liu, N., Wang, W., Qin, C. (2020). High-capacity image steganography based on improved Xception. Sensors, 20(24): 7253. https://doi.org/10.3390/s20247253

[7] Pan, Y.L., Wu, J.L. (2022). Rate-distortion-based stego: A large-capacity secure steganography scheme for hiding digital images. Entropy, 24(7): 982. https://doi.org/10.3390/e24070982

[8] Sumathi, C.P., Santanam, T., Umamaheswari, G. (2014). A study of various steganographic techniques used for information hiding. arXiv:1401.5561 https://doi.org/10.48550/arXiv.1401.5561

[9] Rajkumar, G.P., Malemath, V.S. (2017). Video steganography: Secure data hiding technique. International Journal of Computer Network and Information Security, 9(9): 38-45.

https://doi.org/10.5815/ijcnis.2017.09.05
[10] Younus, Z.S., Younus, G.T. (2019). Video steganography using knight tour algorithm and LSB method for encrypted data. Journal of Intelligent Systems, 29(1): 1216-1225. https://doi.org/10.1515/jisys-2018-0225
[11] Mstafa, R.J., Younis, Y.M., Hussein, H.I., Atto, M. (2020). A new video steganography scheme based on Shi-Tomasi corner detector. IEEE Access, 8: 161825-161837. https://doi.org//10.1109/ACCESS.2020.3021356
[12] Hussien, S.A.S., Hussien, T.A.S., Noori, M.A. (2021). A proposed algorithm for encrypted data hiding in video stream based on frame random distribution. Iraqi Journal of Science, 62(9): 3243-3254. https://doi.org/10.24996/ijs.2021.62.9.37
[13] Samiappan, D., Bhubaneswar, P. (2019). Video steganography using IWT, DWT, LBP methods and its research. International Journal of Engineering and Advanced Technology, 8(6S3): 2022-2026. https://doi.org//10.35940/ijeat.F1287.0986S319
[14] Shaik, A., Thanikaiselvan, V. (2021). Comparative analysis of integer wavelet transforms in reversible data hiding using threshold based histogram modification. Journal of King Saud University-Computer and Information Sciences, 33(7): 878-889. https://doi.org/10.1016/j.jksuci.2018.06.001
[15] Miri, A., Faez, K. (2018). An image steganography method based on integer wavelet transform. Multimedia Tools and Applications, 77: 13133-13144 https://doi.org/10.1007/s11042-017-4935-z
[16] Keshavarzi, B., Zarpak, B., Javadi, S.H.H.S., Jandaghi, G.R. (2019). Adaptive steganography based on integer wavelet transform using block standard deviation. Journal of Information and Optimization Sciences, 40(7): 1457-1473. https://doi.org/10.1080/02522667.2018.1522797
[17] Mamatha, P., Venkatram, N. (2016). Watermarking using Lifting Wavelet Transform (LWT) and Artificial Neural Networks (ANN). Indian Journal of Science and Technology, 9(17): 1-7. https://doi.org/10.17485/ijst/2016/v9i17/93088
[18] Hariyanto, E., Rahim, R. (2016). Arnold's cat map algorithm in digital image encryption. International Journal of Science and Research, 5(10): 1363-1365. https://doi.org/10.21275/ART20162488
[19] Liao, X.F. (2015). Improved tent map and its applications in image encryption. International Journal of Security and Its Applications, 9(1): 25-34. http://doi.org/10.14257/ijsia.2015.9.1.03
[20] Mishra, M., Routray, A.R., Kumar, S. (2014). High security image steganography with modified Arnold's cat map. arXiv:1408.3838. https://doi.org/10.48550/arXiv.1408.3838
[21] Al-Husainy, M.A.F., Uliyan, D.M. (2017). Image encryption technique based on the entropy value of a random block. International Journal of Advanced Computer Science and Applications, 8(7): 260-265. https://doi.org/10.14569/IJACSA.2017.080735
[22] Schober, P., Boer, C., Schwarte, L.A. (2018). Correlation coefficients: appropriate use and interpretation. Anesthesia & Analgesia, 126(5): 1763-1768. https://doi.org/10.1213/ANE.0000000000002864
[23] Abdmouleh, M.K., Khalfallah, A., Bouhlel, M.S. (2012). Image encryption with dynamic chaotic Look-Up table. In 2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), Sousse, Tunisia, pp. 331-337. https://doi.org/10.1109/SETIT.2012.6481937
[24] Tripathi, S., Ramesh, N., Bernito, A., Jayaraj, N.K. (2011). A DWT-based dual image watermarking technique for authenticity and watermark protection. Signal & Image Processing an International Journal, 1(2): 33-45. https://doi.org/10.5121/sipij.2010.1204
[25] Sun, Y., Wong, A.C.M. (2007). Interval estimation for the normal correlation coefficient. Statistics & Probability Letters, 77(17): 1652-1661. https://doi.org/10.1016/j.spl.2007.04.004