Video Steganography Using a Hybrid Schem

Faiz Adheem Hameed [1] Ahmad Taha[2]
Salim Wadi[3]
[1]communication Engineering, engineering technology, Al-Furat Al-Awsat Technical University, Iraq
[2] communication Engineering, engineering technology, Al-Furat Al-Awsat Technical University, Iraq
[3] communication Engineering, engineering technology, Al-Furat Al-Awsat Technical University, Iraq
[1]faiz.hameed.ms.etcn@student.atu.edu.iq
Mob: 07803843546
[2]Coj.abdulsad@atu.edu.iq
[3]coj.sal@atu.edu.iq

Abstract.

The ability to communicate multimedia content quickly has been made possible by recent advancements in Internet speed. However, these technological advancements result in breaches of data security and personal information. Private information protection is made possible through digital steganography, which is crucial in the contemporary Internet era. Due to its high ability to conceal critical data, digital video has drawn the attention of many researchers in all digital media. Recently, a variety of video steganography techniques have been put out to stop the theft of sensitive data. However, there are numerous problems with these approaches' resilience, embedding ability, and visual imperceptibility. This work suggests a novel method for video steganography that relies on the corner location theory and the LSBs algorithm to address these problems. The suggested method initially locates areas of corner points inside the frames using the Shi-Tomasi Technique . Then, it employs the 3-LSBs technique to conceal sensitive information inside the noted corner spots. Additionally, to increase security, the suggested method encrypts sensitive data using the AES cipher method before embedding. The suggested approach is exceedingly secure and almost unnoticeable, and sufficiently robust Salt & Pepper noise, which has an average Structural Similarity Index (SSIM) of more than 0.9998, On the basis of experimental results. The results also showed that the proposed method is superior to the methods developed based on lack of visual imperceptibility, offering good peak signal-to-noise ratios (PSNR) of an average of 57.57 dB while preserving excellent embedding capacities.

Keywords: Private Information, Steganography, Embedding, 3- LSBs, AES
DOINumber:10.14704/nq.2022.20.8.NQ44899 **NeuroQuantology 2022; 20(8): 8765-8784**

1 Introduction

Information security concerns, such as copyright laws, and identity verification, have grown significantly over the past few years as consumers became concerned about the possibility of their data being stolen via the Internet. The fields of cryptography and steganography have developed as solutions to these problems [1]-[3]. Steganography is a technique that uses some media (such as video, image, etc.)In addition to a certain technology to hide confidential information inside the cover. Contrarily, Confidential data by encryption technology is transformed into useless or insignificant information, which leads to the difficulty of decrypting it by intruders [4]-[7]. Although both of techniques work to protect information, Therefore, it is not advisable to work each technique on one side. Therefore, combining the two approaches is occasionally advocated. The hacker even had doubts about the transmission process and succeeded in bypassing the steganography algorithm in this case, the hacker would like to decrypt the message to access the secret data [8]–[11].

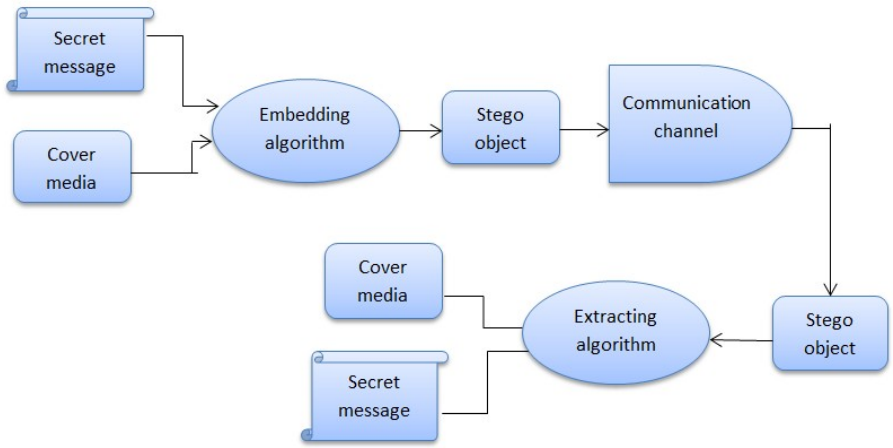

Fig.1. The Steganography Scheme

The general process steps for every steganography algorithm's embedding and extraction are shown in Figure 1. Any good steganography algorithm's effectiveness is mostly determined by four elements: 1. robustness 2. embedding capacity 3. security, 4. imperceptibility. Therefore, these elements must be taken into account both while creating new steganography algorithms and when enhancing the ones that already exist. The term "robustness" describes how well the steganography technique resists attacks and processing. The amount of information that can be embedded into the cover media is referred to as the embedding capacity. Security means that an

attacker cannot extract the data that is embedded. Imperceptibility is the degree of distortion caused by the hiding procedure in the cover [13]–[15].

Digital video has higher redundancy than other digital media, offering a significant capacity for data concealment. A significant volume of HD digital videos are also broadcast over the Inter-

Video steganography techniques can generally be divided into three categories: format-based techniques, video codec-based techniques, and still image-based techniques [8], [20], [21]. . For the goal of data concealment, Still image-based meth-ods convert the video to frames and then apply hiding techniques to the selected frames. The two subcategories of these methods are transform and spatial domain approaches. The cover medium is first translated into the frequency domain in the transform domain procedures. The confidential message is then substituted for a few frequency domain coefficients that have been chosen. The domain is then transformed back into the spatial domain using the modified coefficients. Continuous Wavelet Transform. Examples of transform domain techniques include the discrete cosine transform (DCT) and discrete Fourier transform (DFT). Contrarily, spatial domain approaches immediately encrypt the cover carrier with the secret message. This is because it is mathematically uncomplicated and simple at the same time, Least Significant Bit (LSB) approaches are the most widely used spatial domain methods [8], [22]–[24]. When using LSB methods, Some LSBs are used located inside the frame are used to replace the secret data bits with it. The second subset of video steganography is comprised of format-based methods. By utilizing the compression method and structure of a specific video format, several solutions were created for that format. An illustration of a format-based method is H.264/AVC [25].

net since the big data era came into being. As a result, video steganography has gained popularity and caught the eye of numerous scholars [12], [16]. A secret message can be inserted into a cover video using a technique called video steganography. It is employed in a variety of sectors, including copyright protection, access control, etc. . [17]–[19].

2. Related Works

Because of the high potential of video to embed and hide confidential information, Many scholars in the literature have become interested in steganography. The section here discusses some of the methods relevant to the proposed method.

Hanafy et al., 2008 [27], For embedding, the three color layers (red, blue, and green) were used with two bits of these layers. Before embedding, the hidden information was divided into blocks and generated randomly. With the help of the secret key, pseudorandom places for hiding information were examined. This method was tested on a variety of multimedia data types of different sizes, (such as text, image, audio, and video)and the results showed that the PSNR was greater than 50 dB to include all kinds of high-capacity information.

Sherly and Amritha, 2010 [28], developed a directed graph pattern-based technique for AVI video steganography which is characterized by elevated accuracy. This method used Graph trend for embedding information within the video using LSB replacement after converting the frames of the cover to bitmap format. For the embedding process, The technique suggested two types of graphs, and the results showed that

they have a large embedding capacity. This approach was performed in the spatial domain.

Kapoor and Akbar, 2015 [29], offered a technique based on LSB insertion and RGB model pixel extraction to inject data into cover video frames. Data was encoded in this secret after some capacity and imperceptibility checks were performed. As a cover, With the help of LSB insertion, the secret message was added to MPEG video formats. The results of this approach showed positive results that led to an improvement in imperceptibility, based on measures of MSE and PSNR, with an average PSNR of 52 dB.

Mustafa and Elleithy, 2015 [30], devised two techniques to complete the steganography process using the LSB technique, one of them is called hamming codes that take care of the secret message, and the other is called KLT tracking technology, and its guest is facial recognition and tracking in the video. This method yielded good results.

Bayee Elaf Ali et al., 2018 [31], Propose a new method for hiding the text in all images that uses a randomization mechanism, a secret key, and a basic hash function. While the last row will not hide parts of the text in it, the secret text is evenly distributed over all rows of the image. It employs several techniques, including the randomization approach for selecting pixels in each image row, a reverse reflection of text sections in each row, and the improved LSB algorithm.

Table 1.A comparison study of video steganography in the spatial domain.

Authors	Algorithm method	Type of carrier	Using Key	Type of message
Hanafy et al. [27]	LSB	AVI	Yes	text
Sherly and Amritha [28]	TPVD	MPEG	Yes	Text
Kapoor andAkbar[29]	LSB insertion	MPEG	-	Text
Mustafa and Khaled[30]	LSB	AVI	No	Text
Bayee Elafe-tal.[31]	LSB	Image	Yes	Text

3. Material and Methods

This section provides a detailed explanation of the AES encryption algorithm and the Shi-Tomasi corner detecting technique. This is so that these two techniques are used in the proposed manner.

3.1 Shi-Tomasi Corner Detector

The Shi-Tomasi technique is a popular corner detection method in computer vision. It is considered a developed part of the Harris Detector [32], [33]It entails selecting specific sets of features with an image.

the Harris operator has several advantages over the other corner extract algorithms, when faced with complex and misleading corners, it struggles to meet the target recognition requirements. As a result, to detect corners, this work uses the Shi-Tomasi algorithm. Shi-Tomasi is based on the Moravec algorithm. The Moravec corner detection principle is described below: Make a detection window in the image. The average power of the windows can also be specified by rotating them moderately in all directions. When the energy value exceeds the given threshold, the window's center pixel is chosen as a corner point.

As a result, the Harris technique is based on the notion that as the image reading changes during window shift, the image under the original window matches the corner more. The equation (1) [34] expresses this assumption

$$E(a,b) = \sum_{x,y} w(x,y)\left[I(x+a, y+b) - I(x,y)\right]^2 \qquad (1)$$

Where (E) is the sum of squared differences between the original and moved the window, The x-direction displacement of the window is denoted by the letter (a), and The y-direction displacement of the window is denoted by the letter (b). The weighting function of the window at position (x,y), either a Gaussian or a window of ones, is denoted by, w(x,y), The intensity of the relocated window is represented by I(x+ a,y+b)., The intensity of the original window is represented by I(x, y).

The above equation can be expressed by another equation in the form of a matrix, as shown by Eq (2)

$$E(a,b) \approx [a\ b]\left(\Sigma x \sum_{y} w(x,y)\begin{bmatrix} Ix^2 & IxIy \\ IxIy & Iy^2 \end{bmatrix}\right)\begin{vmatrix} a \\ b \end{vmatrix} \qquad (2)$$

Eq (2) can be written as follows

$$E(a, b) \approx [a\ b]\ F \begin{bmatrix} a \\ b \end{bmatrix} \quad (3)$$

The Harris Matrix (F) can be expressed by Eq (4)

$$F = \Sigma x \sum_{y} w(x, y) \begin{bmatrix} Ix^2 & IxIy \\ IxIy & Iy^2 \end{bmatrix} \quad (4)$$

Corner response (R) can be determined using the formula in Eq (5) [35].

$$R = \det(F) - K(\text{Trace}(F))^2 \quad (5)$$

Where $\det(F) = \lambda_1 * \lambda_2$ and $\text{Trace}(F) = \lambda_1 + \lambda_2$

The eigenvalues of (F) are (λ_1, λ_2), and (k) is a constant

.If :

1– λ1, λ2 are large, the E will increase that lead R is a corner

2- λ1, λ2 are small, the E will be almost constant that lead R is flat

3 – λ1 > λ2 or λ1 < λ2 ,R is Edge

The Shi-Tomasi approach, like the Harris-Stephen technique where the corner is detected depending on the values of(λ1 and λ2), While the corner is detected here according to another principle. R is determined in the Shi-Tomasi technique as follows :

$$R = \min(\lambda 1, \lambda 2) \quad (6)$$

If R exceeds the threshold, then this point can be considered a corner

The Shi Tomasi technique is distinguished in that its points are better tracked than the Harris technique. but this leads to increased computational demand.

3.2. Advanced Encryption Standard (AES)

It is one of the algorithms made in 2001. It was adopted by the National Center for Standards and Technology in America, which is considered one of the parts of symmetric encryption. This algorithm appeared to be an alternative to DES, although both of them are symmetric block ciphers, AES is computationally better because of the key length.[36]

AES has a certain number of cycles depending on the length of the key. Where 10 rounds are

used for a 128-bit key, 12 rounds are used for a 192-bit key, or the last one uses 14 rounds for a 256 key.

The AES algorithm is superior to DES:-

- With strength and speed
- Possibility to work in Java and C
- Key Expansion
- safe against brute-force attacks

transformation initial consists of-[36]
key Expansion: by which he begins to derive the keys of the session from the master key of the cryptography.
initial round: By bitwise, the message bytes are combined with the master encryption key in an array (4 x 4).

A 4-transformation is applied to each cycle and according to the length of the key, as follows:
Sub byte: Each byte is replaced by another byte by a table called S - box
shift row: - by which the bytes of rows - except for the first row - are shifted and rotated.
mix column:- where they are treated as polynomial equations where the byte mix is multiplied by a matrix (4 x 4)
add round key: - in this transformation, it contains the XOR operation, which in turn adds the round key to the result obtained in the previous step.
The stages of transformation are as shown in Figure 2

A

19	a 0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

(S-box)

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	3c

B

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	3c

Rotate Over1 Byte
Rotate Over1 Byte
Rotate Over1 Byte

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

C

D

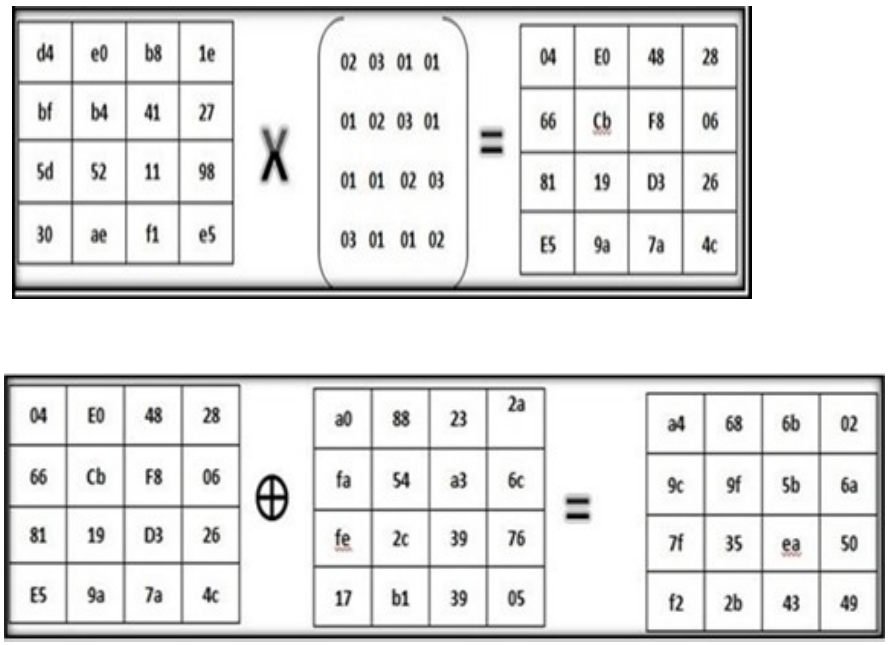

Fig. 2. The general scheme of AES ciphering (a) Sub Byte. (b) Shift Row (c) Mix Column (d) Add Round Ke

4.

The Proposed Methodology

The suggested video steganography method is built on the corner points of the 3-LSBs algorithm and the Shi-Tomasi algorithm, which is described in this section. In the blue channel of each frame of the cover video, corner points regions(i.e., Region of Interests (ROIs))are found Finding a certain threshold and using the Shi-Tomasi detector approach. The specific information embedded in the 3-LSBs method within the pixels is pre-selected. To increase the security level of the proposed technique, the private information is en-

crypted using the AES encryption prior to embedding. Here, the suggested technique employs plaintext as a covert message.
the cover media, private key, and threshold should all be pre-agreed upon by the sender and the receiver before the suggested method is used. The AES encryption algorithm's key is represented by the private key, Shi-Tomasi detector technique finds corners in the frames of the cover using a threshold value, where different threshold values result in different corner points. The cover video is a piece of media having a concealed message in it.
The proposed method's general design is shown in Figure 3. For the recommended technique, the following subsections cover data extraction, encryption, and data embedding.

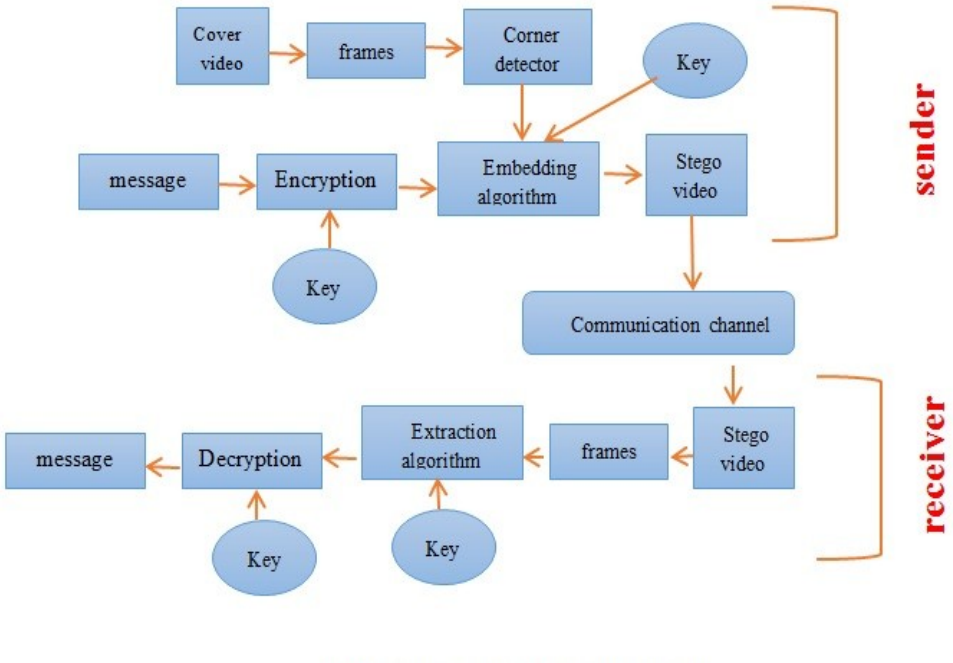

Fig.3. Framework for the Suggested Approach

4.1 Message Encryption and Embedding

The main idea through which the 3LSBs embedding strategy was used is to increase the embedding capacity and transfer the largest amount of information without the hacker feeling the presence of hidden information. In the specified corners. This value is originally a decimal value so that each value is converted to binary values. On the other hand, we have the secret message (plaintext) after it has been encrypted by the AES algorithm. Also, each of its characters is converted to ASCII code, after which each value is converted into values Binary, and thus both the secret message and the pixel value are binary values that will facilitate the working mechanism for embedding. The next stage will divide the secret message bits into segment parts, and each segment is 3 sequential bits long, after which it is

converted into a decimal to show the value of each of these segments. The next step will be returned to the binary values, after which the number of required frames is determined by the number of corners required for embedding based on the number of prepared secret message segments so that each frame can take a sufficient number of bits for embedding. Now start by pulling only the determined locations from each frame to work on them. After the corners are initialized, the first 3 least significant bits are uploaded to be replaced by 3 bits of each segment in the secret message. After this step, the new value of binary bits is converted to decimal values. These new values will replace the old decimal values according to the location of each pixel. Finally, the frames are returned for the reconstruction of the stego video.

4.2 Message Extraction and Decryption

The extraction and decryption for the message block diagram are shown in Figure 4. data, key, and the stego video will be entries here in this stage, with the secret message being the output. Here, Well, the stego video to figure out all the binary bits are concealed in the pixels. The stego video is first partitioned into frames to retrieve the bits that are hidden within the video.

The corner points are then determined by applying a Shi-Tomasi approach to the cover video frames using a defined threshold. The hidden bits are then retrieved from pixels in each frame of the stego video so that their locations match those found in the previous stage. When the binary bits recovered length equals the message length, the extraction procedure ends. To retrieve confidential information, a decryption algorithm and a private key are used.

Figure 4. An example showing the process of embedding a single character in the (3 LSBs) of the secret message B inside the cover after the text is converted to ASCII code.

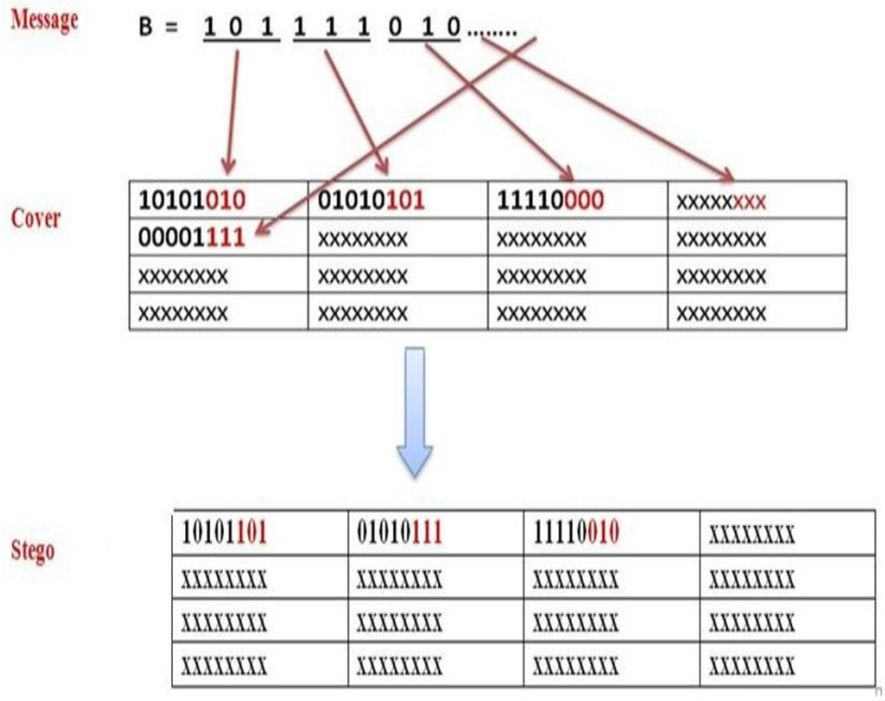

Fig .4. General scheme to hide three bits inside the cover video frame

5. Result

5.1 Result and Database

Thorough performance analysis of the suggested method is provided in this section. First, we describe the dataset and evaluation measures that we employed in our trials. The outcomes of the suggested methodology are then highlighted. The proposed method is then illustrated and compared with other methods that have been published in the literature.

First, The following requirements were used to accomplish our study on a computer using MATLAB (R2021a) software and are as follows:Windows 8Pro 64-bit operating system, Intel Core(TM) i7 (8 CPUs) 2.1GHz, Random Access Memory (RAM): 6144MB, secondly, Using the Shi-Tomasi detector and the LSB algorithm in the MATLAB environment, the steganographic approach provided here effectively hides the secret data in the cover video. Original cover video and embedding data are included in the database. The primary performance evaluation parameters of every Steganographic technique are imperceptibility and capacity. The following parameters are taken into account when determining evaluation results.

Figure 5 shows a set of video files that were used in this study and in AVI format, where the optimal corner locations are detected within the frames of these covers before embedding, while Table 1 shows the number of corners that were detected inside the covers.

Table 2 shows the results obtained for the cover video using the two messages.

Table 2. Clarification the Properties of the Set Cover Files

Cover name	Formatting	NO. of frames	cover resolution	cover size in pixels
Strawberry	AVI	181	1080 x 1920	2,073,600
Tree	AVI	125	960 x 540	518400
Bunny	AVI	92	640 x 360	230400
Beach	AVI	126	640 x 360	230400
Sea	AVI	120	1280 x 720	921600
Flower	AVI	126	1920 x 1080	2073600

5.2 Metrics

The difficulty in developing video steganography techniques is to incorporate as much data as possible in the frames of the cover video with the least amount of change that can be seen in the stego video. As a result, the proposed

method was assessed and contrasted with cutting-edge techniques. They will be discussed in order, using different scales, and as follows:

5.2.1 MSE

The Mean Squared Error is derived by comparing each of the bytes in stego and cover files. The normal of the squares of the errors, or the normal squared contrast between the assessed attributes and what is appraised, is measured by MSE, according to the equation (7) [37]

$$MSE = \frac{\Sigma_{i=1}\sum_{j=1}^{n}\left[O(i,j)-E(i,j)\right]^2}{m \times n} \quad (7)$$

8777

where O is the original frame and E is embedded Stego- frames. m × n represents the size of the video frame which shows several rows and shows several columns of a video frame.

5.2.2 PSNR

The Peak Signal-to-Noise Ratio is a standard metric for determining the difference between transporter and stego data. PSNR is the ratio of a flag's maximum imaginable intensity to the maximum conceivable intensity of debasing clamor that impacts the consistency with which it is depicted and according to equation (8) [37]

$$PSNR = 10 \times \log_{10}\left(\frac{MAXo^2}{MSE}\right) (dB) \quad (8)$$

MAX_O represents the highest pixel value in frame O

5.2.3 SSIM

The robustness metric was used to assess the suggested method's effectiveness against several forms of attacks(such as salt and pepper). The similarities between what is entered (the secret message) and the message that was extracted is computed using this metric. This metric was measured using the structural similarity index

(SSIM) function, which is defined mathematically as Eq (9)

$$\mathrm{SSIM} = \frac{(2\mu o\mu E + S1)(2\sigma 0 + s2)}{(\mu o^2 + \mu E^2 + S1)(\sigma o^2 + \sigma E^2 + S2)} \quad (9)$$

where O and E indicate the video frames of original and embedded stego video, respectively. μ_O and μE are the mean values of original and embedded stego video frames, respectively, while, σ_O and σ_E represent the standard deviation of pixel values in frames O and E. S1 and S2 are the fixed values.

The corner points found in each frame of cover video are displayed in Table 3. Each cover video has a different amount of corner points that can be identified, As is also clear from Table 3, the Flower and Beach cover videos each received 1270836 and 94878, respectively, in terms of the number of detected corner points. This is because each cover video has different frame scenes and sizes in pixels.

Table 3. The number of corners detected, by the Shi-Tomasi technique

Cover Video	No .of Frames	No . of Corners
Strawberry	181	280369
Tree	125	805875
Bunny	92	209300
Beach	126	94878
Sea	120	669120
Flower	126	1270836

5.3

Proposed Method's Results

Table 4 summarizes how well the suggested strategy performed in terms of PSNR on 6 cover videos. The videos "Sea", "Strawberry", and "Flower" It has a large embedding capacity compared to other videos, It has a large embedding capacity compared to the rest of the covers previously shown, due to the abundance of corner points in these covers as shown in Table 3. Embedding capacity for "tree", "Bunny" and "beach" videos with low corner points is less effective than other covers hiding capacity. This is to be expected given that these cover videos lack corner points and have a very small extracted ROI. All of the videos used had PSNR values of more than 47 dB, as can be shown in Table 3. This demonstrates the method's remarkable perceived invisibility. Table 3 further shows that the

average PSNR for all of the user videos is 57.24 dB. This demonstrates how highly imperceptible the suggested strategy is. As a result, we may conclude that the suggested strategy offers a high level of imperceptibility.

Table 4.clarification the properties of the set cover files

Cover name	Format	No .of Frame	Total Corners	MSE	PSNR	SSIM
Straw-berry	AVI	181	270,052	0.034	62.743	1.000
Tree	AVI	125	805,875	0.182	55.517	1.0000
Bunny	AVI	92	209,300	0.161	56.06	0.9999
Beach	AVI	126	94,878	1.12	47.637	0.9994
Sea	AVI	120	669,120	0.01	67.998	1.0000
Flower	AVI	126	1,270,836	0.183	55.485	1.0000

The effectiveness of the suggested strategy in terms of SSIM rates (without and with) the noises on 6 cover videos is shown in Fig. 10. When no noise is applied to the cover video, as shown in Fig. 10, the SSIM rates are nearly "1". This suggests that a small amount of data loss can be used to recover the secret data. The proposed approach can give a large SSIM value that is somewhat similar to the SSIM value for noise-free videos. as seen in Fig. 10 if Salt and Pepper noise is put to the cover videos at a density of 0.002. However, the SSIM rate drops as salt and pepper noise density increases.

The suggested method is strong when the cover video is devoid of noise, but it deteriorates if noises are added to the cover videos, as may be inferred from Figure 6. , the suggested method performed best with salt and pepper.

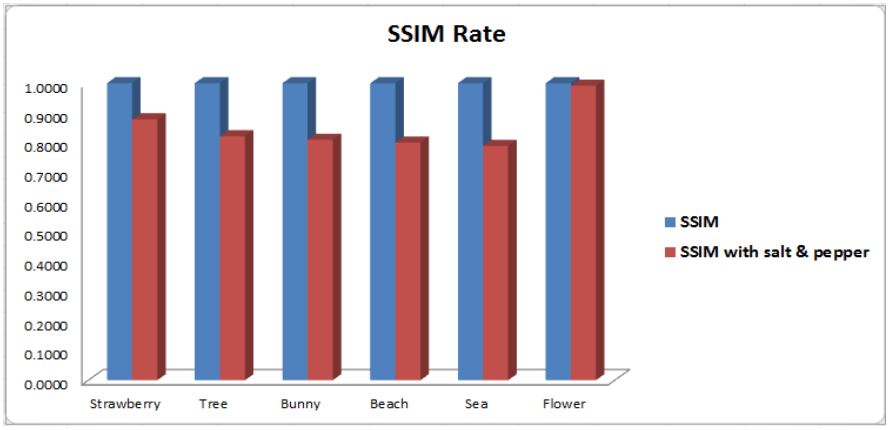

Fig.6. performance analysis of the suggested technique using various video sequences with SSIM Salt and Pepper noise at a density of 0.002.

5.4

Results Comparisons

The perceptual invisibility of the suggested method was contrasted with other ways from the literature in this section. To compare the suggested approach with the methods given in [27]–[31], the PSNR rates of the methods were taken into consideration. We compared the results from six separate videos with results ref. shown in [27] through [31]. The PSNR rates obtained by the suggested approaches and those in [27]-[30] are listed in Tables 5 (A, B, C, D, E). It is clear from Tables 5 (A, B, C, D, E) that, across all used videos, the proposed approaches achieve the highest PSNR rate when compared to the results in [27]-[30]. The results of each stated reference in [27] - [31] were compared with those of the proposed method to further validate its effectiveness in terms of visual imperceptibility.

Table 5. (A, B, C, D, E) Analyzing the PSNR rate and comparing it with previous results

A

cover video	proposed method	Ref. [27]
Strawberry	62.743	50
Tree	55.517	
Bunny	56.06	
Beach	47.637	
Sea	67.998	
Flower	55.485	

B

cover video	proposed	Ref. [28]

	method	
Strawberry	62.743	40
Tree	55.517	
Bunny	56.06	
Beach	47.637	
Sea	67.998	
Flower	55.485	

C

cover video	proposed method	Ref. [29]
Strawberry	62.743	52
Tree	55.517	
Bunny	56.06	
Beach	47.637	
Sea	67.998	
Flower	55.485	

D

cover video	proposed method	Ref. [30]
Strawberry	62.743	36
Tree	55.517	
Bunny	56.06	
Beach	47.637	
Sea	67.998	
Flower	55.485	

E

cover video	proposed method	Ref. [31]
Strawberry	62.743	52
Tree	55.517	
Bunny	56.06	
Beach	47.637	
Sea	67.998	
Flower	55.485	

6
Conclusions

This work is proposed based on video steganography to hide data behind a secure, high-capacity video. For video steganography, 3-LSBs secured corner-based approaches were introduced. This method uses a cover video file in the spatial domain to hide the presence of sensitive data in any format. The proposed technique is used with an AVI file, but it can be modified to work with any other format with small procedural changes. It has been demonstrated that this technique can include the same amount of data as other LSB cloaking techniques with fewer changes in pixel values than other LSB cloaking techniques. As a result of this optimization, there is a greater similarity between the cap and the stego frame, which leads to improved non-perception. This low rate of variability at each pixel chosen by the corner detection also makes LSB masking more resistant to typical detectors. The least significant bit, secret key 1 and key 2 provide double protection. The whole process demonstrates an effective steganography method for encrypting and decrypting confidential data.

7. References

1. Y. Yang, Z. Li, W. Xie, and Z. Zhang, ‘‘High capacity and multilevel information hiding algorithm based on pu partition modes for HEVC videos,’’ Multimedia Tools Appl., vol. 78, no. 7, pp. 8423–8446, Apr. 2019, doi: 10.1007/s11042-018-6859-7.
2. . K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, ''A novel magic LSB substitution method (M-LSB-SM) using multilevel encryption and an achro-matic component of an image,'' Multimedia Tools Appl., vol. 75, no. 22, pp. 14867–14893, Nov. 2016, doi: 10.1007/s11042-015-2671-9.
3. A. Sahu, K. Lakshmaiah, G. Swain, and K. Lakshmaiah, ''Dual stego- imaging-based reversible data hiding using improved LSB matching,'' Int.J. Intell. Eng. Syst., vol. 12, no. 5, pp. 63–73, Oct. 2019.
4. A. T. Bhole and R. Patel, ''Steganography over video file using random byte hiding and LSB technique,'' in Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC), Dec. 2012, pp. 5–10, doi: 10.1109/ICCIC. 2012.6510230.
5. R. J. Mustafa and K. M. Elleithy, ''A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes,'' in Proc. Long Island Syst., Appl. Technol., May 2015, pp. 1–7, doi: 10.1109/LISAT.2015.7160192.
6. 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., to be published, doi: 10.1016/j.jksuci.2019.07.004.
7. M. Ma, D. He, M. K. Khan, and J. Chen, ‘‘Certificateless searchable public key encryption scheme for mobile healthcare system,’’ Comput. Electr. Eng., vol. 65, pp. 413–424, Jan. 2018.
8. M. M. Sadek, A. S. Khalifa, and M. G. M. Mostafa, ''Video steganography: A comprehensive review,'' Multimedia Tools Appl., vol. 74, no. 17, pp. 7063–7094, Sep. 2015, doi: 10.1007/s11042-014-1952-z.
9. R. Das and T. Tuithung, ‘‘A novel steganography method for image based on Huffman encoding,’’ in Proc. 3rd Nat. Conf. Emerg. Trends Appl. Comput. Sci. (NCETACS), Mar. 2012, pp. 14–18, doi: 10.1109/NCETACS. 2012.6203290.
10. R. J. Mustafa and K. M. Elleithy, ''A new video steganography algorithm based on the

multiple object tracking and Hamming codes," in Proc. IEEE 14th Int. Conf. Mach. Learn. Appl. (ICMLA), Dec. 2015, pp. 335–340, doi: 10.1109/ICMLA.2015.117.
11. A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaiah, P. Yang, H. Huang, and G. Hou, ‘‘Secure and robust fragile watermarking scheme for medical images,’’ IEEE Access, vol. 6, pp. 10269–10278, 2018, doi: 10.1109/ACCESS.2018.2799240.
12. R. J. Mustafa and K. M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes," Multimedia Tools Appl., vol. 75, no. 17, pp. 10311–10333, Sep. 2016, doi: 10.1007/s11042-015-3060-0.
13. M. Douglas, K. Bailey, M. Leeney, and K. Curran, ‘‘An overview of steganography techniques applied to the protection of biometric data,’’ Multimedia Tools Appl., vol. 77, no. 13, pp. 17333–17373, Jul. 2018, doi: 10.1007/s11042-017-5308-3
14. R. J. Mustafa and K. M. Elleithy, "A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11)," in Proc. Wireless Telecommun. Symp. (WTS), Apr. 2015, pp. 1–8, doi: 10.1109/WTS.2015.7117257.
15. R. J. Mustafa and K. M. Elleithy, "A highly secure video steganography using Hamming code (7, 4)," in Proc. IEEE Long Island Syst., Appl. Technol. (LISAT) Conf., May 2014, pp. 1–6, doi: 10.1109/LISAT. 2014.6845191
16. M. Zeeshan, M. Majid, I. F. Nizami, S. M. Anwar, I. Ud Din, and M. K. Khan, ‘‘A newly developed ground truth dataset for visual saliency in videos,’’ IEEE Access, vol. 6, pp. 20855–20867, 2018.
17. R. J. Mustafa, K. M. Elleithy, and E. Abdelfattah, "Video steganography techniques: Taxonomy, challenges, and future directions," in Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT), May 2017, pp. 1–6, doi: 10.1109/LISAT.2017.8001965.
18. R. J. Mustafa and K. M. Elleithy, "An efficient video steganography algorithm based on BCH codes," in Proc. ASEE, 2015, pp. 1–10, doi: 10.13140/RG.2.1.4202.7363.
19. Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, ‘‘Video steganography: A review,’’ Neurocomputing, vol. 335, pp. 238–250, Mar. 2019, doi: 10.1016/j.neucom.2018.09.091.
20. M. Shirali-Shahreza, ‘‘A new method for real-time steganography,’’ in Proc. 8th Int. Conf. Signal Process., vol. 4, 2006, doi: 10.1109/ICOSP. 2006.345954.
21. M. K. Khan, M. Zakariah, H. Malik, and K.-K.-R. Choo, ‘‘A novel audio forensic data-set for digital multimedia forensics,’’ Austral. J. Forensic Sci., vol. 50, no. 5, pp. 525–542, Sep. 2018.
22. K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, ‘‘CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method,’’ Multimedia Tools Appl., vol. 76, no. 6, pp. 8597–8626, Mar. 2017, doi: 10.1007/s11042-016-3383-5.
23. R. J. Mustafa, 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, pp. 5354–5365, 2017, doi: 10.1109/ACCESS.2017.2691581.
24. T. Rabie and M. Baziyad, ‘‘The pixogram: Addressing high payload demands for video steganography,’’ IEEE Access, vol. 7, pp. 21948–21962, 2019, doi: 10.1109/ACCESS.2019.2898838.

25. T. Stütz and A. Uhl, ‘‘A survey of H.264 AVC/SVC encryption,’’ IEEE Trans. Circuits Syst. Video Technol., vol. 22, no. 3, pp. 325–339, 2012, doi: 10.1109/ TCSVT.2011.2162290.
26. A. K. Sahu and G. Swain, ''Reversible image steganography using dual-layer LSB matching,'' Sens. Imag., vol. 21, no. 1, p. 1, Dec. 2020.
27. Chaudhary, Jyoti. "A Multi-Phase Model to Improve Video Steganography." In Computational Intelligence and Communication Networks (CICN), 2014 International Conference on, pp. 725–729. IEEE, (2014).
28. Kapoor, Vivek, and Akbar Mirza. “An Enhanced LSB based Video Steganographic System for Secure and Efficient Data Transmission.” International Journal of Computer Applications 121.10 (2015).
29. Mustafa, Ramadhan J., and Khaled M. Elleithy. "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes.” Multimedia Tools and Applications, pp. 1–23 (2015).
30. Bayee Elaf Ali et al. " Text in Image Hiding using Developed LSB and Random Method" in International Journal of Electrical and Computer Engineering • August 2018.
31. Ashty M. Aaref “ Video Steganography Using LSB Substitution and Sobel Edge Detection” Diyala Journal of Engineering Sciences, Vol. 11, No. 2, June 2018, pages 67-73 DOI: 10.26367/DJES/VOL.11/NO.2/9 (2018)
32. S. Wu, A. Oerlemans, E. M. Bakker, and M. S. Lew, ‘‘A comprehensive evaluation of local detectors and descriptors,’’ Signal Process., Image Commun., vol. 59, pp. 150–167, Nov. 2017, doi: 10.1016/j. image.2017.06.010.
33. S. Wu, A. Oerlemans, E. M. Bakker, and M. S. Lew, ''A comprehensive evaluation of local detectors and descriptors,'' Signal Process., Image Commun., vol. 59, pp. 150–167, Nov. 2017, doi: 10.1016/j. image.2017.06.010.
34. Kaviya K, Mridula Bala, and Swathy N P, ‘‘Video Steganography Based on Shi-Tomasi Corner Detection and Least Significant Bit Algorithm,’’ Journal of Image Processing and Artificial Intelligence, DOI: 10.46610/ JOIPAI.2021.v07i02.003
35. V. A, N. Aklecha, Meghana, K. N. B. Murthy, and S. Natarajan, ''On detectors and descriptors based techniques for face recognition,'' Procedia Comput. Sci., vol. 132, pp. 908–917, May 2018, doi: 10.1016/j.procs.2018.05.106.
36. Deshmukh P. Pravin and Smita Kasar ‘‘Security Improvisation in Steganography using AES 128/192/256,’’ International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 11, November-2014
37. Rachna Patel, Kalpesh Lad and Mukesh Patel "Study and investigation of video steganography over uncompressed and compressed domain: a comprehensive review "Received: 14 December 2020 / Accepted: 18 February 2021. © The Author(s), under exclusive license to Springer-Verlag GmbH Germany, part of Springer Nature 2021