Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

An Enhanced Dual-Layer Video Steganographic Approach: Enhancing Security and Imperceptibility

Md. Maruf Hassan[1,2,*], R. Badlishah Ahmad[1,2], Naimah Yaakob[1,2], Ong Bi Lynn[1,2], Nur Farhan Kahar[1,2]

[1] Faculty of Electronic Engineering & Technology, Universiti Malaysia Perlis, Arau, 02600, Perlis, Malaysia
[2] Department of Software Engineering, Daffodil International University, Dhaka, Bangladesh
[3] Centre of Excellence for Advanced Computing (AdvComp), Universiti Malaysia Perlis, Arau, 02600, Perlis, Malaysia

ABSTRACT

In a digital age where the role of digital information is continually expanding, the imperative to ensure secure communication and data protection has intensified. Steganography, a field that conceals sensitive information within apparently innocuous carriers like multimedia files, holds promise for achieving this goal. Recent times have seen a growing interest in video-based steganography, driven by the proliferation of videos online. However, a review has unveiled a noteworthy gap in efforts to increase the safety of video steganography employing the popular Least Significant Bit (LSB) process. LSB steganography is at risk to exploits that could jeopardize the confidentiality of the concealed message. In this research, we present a video steganographic solution achieved through the integration of advanced encryption algorithms and a dual approach involving randomized frame selection using the Fisher-Yates method and pixel selection utilizing the 8-directional technique. Additionally, we have devised an upgraded imperceptible video steganographic approach in the spatial domain, capitalizing on an XOR-based LSB substitution embedding approach. The outcomes underscore the effectiveness of our proposed methodology, revealing significant imperceptibility when compared to recent solutions, thereby reinforcing data security against unauthorized access. This comprehensive solution holds wide-ranging applications across various domains, providing heightened security and confidentiality for sensitive information. Notable applications include secure communications within intelligence agencies, safeguarding patient data in medical sciences, ensuring privacy in video surveillance, fortifying video transmission against errors and data breaches, securing business communications, preventing data leakage, and enhancing rights management for digital content.

Keywords:
Data hiding; video steganography; least significant bit (lsb); pixel selection technique; dual layered technique

1. Introduction

In today's digital age, ensuring secure communication and data protection is paramount. Steganography, particularly video steganography, offers a way to safeguard sensitive information

* *Corresponding author.*
E-mail address: ancssf@gmail.com

https://doi.org/10.37934/araset.58.1.119

within innocuous carriers like multimedia files. Online activity has increased dramatically since Industry 4.0 and rapid technical breakthroughs have arrived, underscoring the necessity of secure data transfer in an era of continuous digital communication. For example, in the span of a single minute on the internet, we observe an astonishing scale of online interactions, including the uploading of more than 500 hours of content on YouTube, the sharing of 695,000 stories on Instagram, and the exchange of nearly 70 million messages via WhatsApp and Facebook Messenger [2,3]. In that same minute, online transactions totalled $1.6 million, highlighting significant financial activity. The reliance on cloud servers for storing confidential data and providing services has grown with the influx of data over the internet. However, this also creates opportunities for hackers to exploit vulnerabilities, potentially causing financial and reputational damage to businesses. Consequently, data security is crucial for safeguarding organizations and their clients from cyber threats in the evolving digital landscape. In 2022, Malaysia experienced several alarming data breaches affecting prominent companies and services [4]. Among the notable incidents, Maybank, WhatsApp, AirAsia, Carousell, and others fell victim to cyberattacks, resulting in the exposure of millions of Malaysians' personal information, which subsequently found its way to be sold on the dark web. Notably, in May 2022, iPay88, a payment gateway provider, experienced a data breach potentially compromising customers' card data. There are three different technologies that may be used to secure data: steganography, watermarking, and cryptography. Cryptography uses mathematical algorithms and keys to transform data into ciphertext, ensuring security and confidentiality in various applications [5]. Watermarking involves embedding hidden information (watermark) in digital signals like images, audio, or video, preserving content integrity and copyright protection [6]. Steganography conceals secret messages within cover media (images, audio, video, text) in an undetectable manner, serving as a hidden communication method for sensitive information [7]. Steganography has three fundamental requirements: robustness, capacity, and imperceptibility [8]. Imperceptibility is the most crucial requirement of steganography is that the embedded secret message should not be detectable to human senses, such as sight or hearing. The changes made to the cover medium to hide the secret message should be subtle enough to avoid arousing suspicion. It should be possible for the steganographic method to survive standard signal processing procedures like noise addition, resizing, and compression. The embedded secret message should remain intact and retrievable even after these transformations. On the other hand, the steganographic method should have sufficient capacity to accommodate the entire secret message within the cover medium. The embedding process should not significantly degrade the quality or integrity of the cover medium. Meeting these basic requirements ensures that steganography provides a reliable and effective means of concealing and transmitting sensitive information within various cover mediums.

We choose video as a cover object for our steganographic solution due to several beneficial characteristics [9] such as Size and Embedding Capacity, Perceptual Redundancy, and Complex Structure. Videos, with their larger size and pixel count compared to images, offer a higher capacity for hiding secret data, allowing for significant concealment without perceptual quality loss. Their temporal features, like motion and frames, provide redundancy, enabling subtle modifications that go unnoticed to humans. The complex video structure makes it challenging for intruders to detect hidden information. Considering these benefits and the extensive utilization of videos in social media and internet traffic, video steganography emerges as a powerful technique for safeguarded data transmission. Video steganography finds application across numerous domains, delivering heightened security and privacy for sensitive information. Examples include its use in Intelligence Agency communications [10], secure message transfer in military and defence sectors [11], safeguarding patient data in the realm of medical sciences, enhancing privacy in video surveillance,

enabling video error correction and data transmission, securing business communication, preventing data leaks, managing rights for digital content, and a myriad of other possibilities [12].

Lately, video-oriented steganography has garnered significant interest owing to the increasing prevalence of online videos. However, the analysis highlights a concerning weakness in the efforts to improve the robustness of Least Significant Bit (LSB)-based video steganography techniques. Despite being extensively used, LSB steganography has flaws that make hidden data security vulnerable [12]. Combining steganography and cryptography has shown to be a viable method for improving the security of video steganography. The combination of these two disciplines can provide an extra layer of protection for the concealed information [13]. However, the review highlights that the practice of employing frame shuffling mechanisms to randomize solutions and bolster security is rare in the existing literature. Frame shuffling can significantly enhance the complexity of the steganographic algorithm, making it more resilient against attacks [14]. Additionally, specific pixel selection techniques [15], which can further improve the robustness of steganography, were not considered in many of the studies. These techniques involve choosing particular pixels for data embedding, increasing the difficulty of detecting hidden information. Moreover, the review points out a crucial aspect that has been overlooked in most previous works - the embedding of metadata. Embedding cryptographic keys, shuffling keys, secret message size, and other relevant metadata can automate the decryption process and facilitate seamless data extraction. Yet, this vital step is rarely explored in the current literature. The literature study, in short, highlights the critical need for additional efforts aimed at enhancing the resilience of LSB-based video steganography. To improve security and automation, steganography and cryptography should be combined with frame shuffling methods, pixel selection strategies, and information embedding. By tackling these areas for development, we can open the door for future video steganographic systems that are safer and more effective.

It is commonly known that the Least Significant Bit (LSB) method is a simple and straightforward way for hiding confidential data to a cover video. This technique boasts high embedding capacity and maintains an acceptable level of imperceptibility in the stego-video [16]. However, its efficacy is compromised by its susceptibility to common security threats such as compression and noise, rendering it less robust [17]. Furthermore, the reliance on LSB-based steganography opens up the possibility for attackers to exploit stego video files through active steganalysis processes, thereby jeopardizing the security of sensitive data. Also, Current steganographic techniques often adopt frame shuffling mechanisms to introduce dynamic elements to their models. However, these approaches frequently overlook the importance of pixel selection within frames, which is crucial for achieving enhanced reversibility and improved security. The prevalent practice of serially selecting pixels within frames for embedding information not only hampers the efficiency of the technique but also exposes it to electronic attacks. This vulnerability, coupled with the absence of emphasis on pixel selection, underscores the limitations of LSB-based methodologies in the realm of steganography.

By combining Least Significant Bit (LSB) replacement embedding methodology, randomized frame selection, pixel selection, and sophisticated encryption, the research offers an enhanced method for safe video steganography. The following is a summary of this paper's contributions:

i. Incorporates a cryptographic algorithm to add an additional level of security in video steganography.
ii. Introduces a system for randomly choosing frames and pixels to bolster the security of the video steganography technique.
iii. The XOR-based LSB substitution embedding technique is selected to improve the concealment quality of video steganography.

This document is structured into five segments. In introductory section, it highlights the core issue, objectives, scope, and contributions. The second section explores existing video steganography literature, including recent advancements. In third segment, it explains the security-focused method involving cryptography, random frame selection, and LSB-based data embedding. Result and discussion are discussed in fourth section where it displays outcomes and discusses their implications in the context of research objectives. We conclude the paper with summarizes research findings, assesses their significance, and suggests future directions.

2. Related Works

The Least Significant Bit (LSB) embedding technique is preferred by researchers due to its simplicity, minimal information requirements, and avoidance of perceptual distortion. LSB algorithm can be applied to both coloured and grayscale videos for concealing sensitive information. With the widespread availability of coloured cameras, video capturing technology, and viewing devices, grayscale videos are less commonly used. Nonetheless, some researchers utilize grayscale videos to embed classified information. For example, Gupta *et al.,* [18] inserted grayscale graphics and hidden text into grayscale video frames using the LSB Replacement Technique. Although this method offers a simple and fast process, it is not secure and may be easily detected with LSB checks.

The anchoring ability of the LSB approach is one of its main advantages. A spatial domain technique that uses two bits from every single blue, green and red channels to hide concealed data in text, photos, and videos was presented by Hanafy *et al.,* [19]. This confidential data, partitioned into non-overlapping chunks and randomly inserted, was secured using a private key. Despite its limited capacity and vulnerability to attacks, this method improved security.

Bhattacharyya *et al.,* [20] LSB Replacement technique, based on directed graph patterns, was developed to enhance capacity in video steganography. This approach utilized two graph designs for encoding, ensuring data placement within the cover video according to graph orientation. Although statistically unobtrusive and minimally affecting video quality, the technique lacked a thorough statistical analysis to validate its reliability. In the pursuit of enhanced security in video steganography, several researchers have proposed innovative techniques and methodologies. Balaji and Naveen *et al.,* [21] introduced a highly effective and secure approach by utilizing a clip from the cover film as an identifier during extraction. This method involved segregating frames into used and underused categories based on the identifier. To bolster security, empty frames were populated with arbitrary data. However, the method's vulnerability arises from the uniform distance between frame and hidden data pixels. Dasgupta *et al.,* [22] presented a 3-3-2 LSB steganography technique based on hashing to further improve security. In order to use this method, two bits from the blue channel, three from the green channel, and three from the red channel are the least significant bits had to be replaced with hidden data bits. To confirm the integrity of frames, an anti-steganalysis examination was utilized, while an evolutionary method was employed to improve the concealment quality. Although this technique offered improved security, it lacked resistance to deformation.

Paul *et al.,* [23] adopted a 3-3-2 LSB method coupled with scene shift recognition to embed hidden data. They utilized histogram disparities to detect abrupt changes in frame order and a random sequence generator for security enhancement. Despite its merits, this method exhibited significant visual error in the displayed histograms. Quantum video steganography was introduced by Chen and Qu *et al.,* [24], utilizing the LSB technique to insert hidden data bits within RGB components of frames. A method for text insertion in films utilizing LSB methods was recommended by Kapoor *et al.,* [25]. It involved the application of ZIP compression, 2-character chunking, and a frames dispersion mechanism. This method showed significant imperceptibility, with an average

PSNR of more than 52 dB. Ma *et al.,* [26] used chaos theory with the Fisher-Yates scrambling algorithm to create a novel colour picture encryption technique. This technique exhibited excellent encryption performance, high security, and computational efficiency, making it a strong contender for secure image encryption in various applications. However, a drawback was the relatively long encryption time, which might impede practical applications. Using the AES algorithm, Chikouche and Chikouche [27] presented an improved LSB-based picture steganography method. This method combined AES encryption with the LSB substitution method to enhance robustness and security. Although the approach outperformed existing methods in terms of robustness and security, its evaluation was limited to a constrained number of image datasets. Balu *et al.,* [28] and Luo *et al.,* [29] have explored various strategies to enhance security further, including incorporating secret data based on the human visual system and employing encryption algorithms [30-32]. The application of trial and error, as well as the correction of coding errors, has also been considered by Mstafa and Elleithy [33,34]. Moon *et al.,* [35] demonstrated the investigation of substitute methods by utilizing computer forensics and 4LSB approaches to improve concealment in AVI video clips. Sudeepa *et al.,* [37] and Kaur *et al.,* [36] investigated encryption techniques to conceal sensitive information in RGB frames. Meanwhile, Manisha *et al.,* [38] pursued 1real-time concealing through segmentation and encryption of hidden images before embedding. Mstafa *et al.,* [34] focused on security through facial recognition and error-correcting codes, although their embedding capacity was limited. Balu *et al.,* [28] engaged in LSB replacement techniques to hide data in non-interesting regions, highlighting the challenge of incorporating data using human vision regions of interest (ROI). In conclusion, while scholars often employ the basic LSB embedding method in the spatial domain, many explore combinations with cryptography to heighten security.

3. Methodology

In this part, the general structure of the suggested approach is discussed, and the specific theoretical elements are explained. The suggested automated dual-layer secure information hiding method for video steganography, which makes use of 1-bit LSB and one-time XOR with 8 directive image components selecting process, was also presented in this part. Figure 1 displays the workflow of the suggested approach.

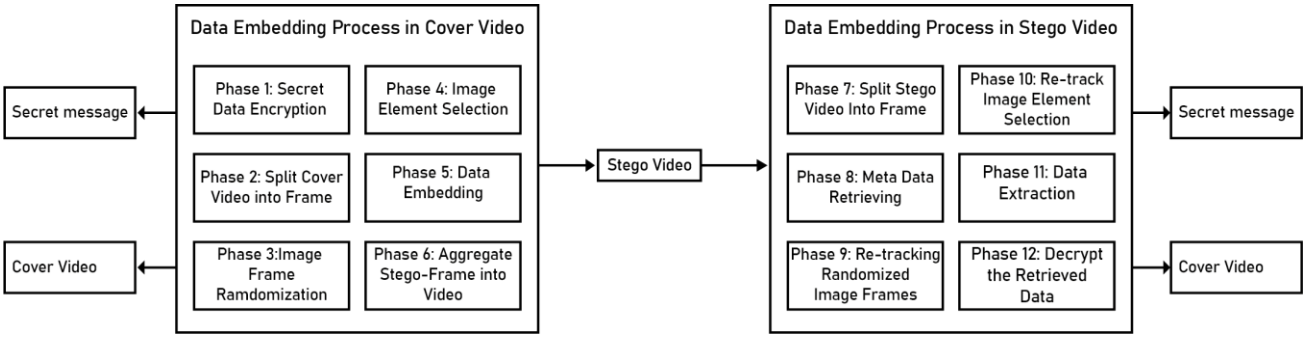


Fig. 1. Workflow of the suggested video steganographic approach

According to Figure 1, the suggested method is made of six essential processes for data embedding and retrieval. When the concealed message and cover video are first received, the cover video is divided into separate frames. The encrypted data is being processed concurrently. A popular technique is used to randomize frames, using metadata present in the first frame. For increased protection, data is contained in the RGB component with the least amount of significance. After that, every frame is put back organized to make a stego video. The stego video is allocated into frames

during retrieval, and the *ffmpeg* module is used to retrieve information. Frames are chosen by utilizing the shuffling key to reassemble the shuffling sequence. Up until all frames are analysed, encrypted data from chosen pixels is obtained. Finally, decryption is applied to unveil the confidential information.

The Embed and Extract procedure is depicted in Figure 2 It entails breaking up the cover video into individual frames, removing the audio, and applying encryption with the AES approach to encrypt the hidden content. The initial frame is created by inserting randomly generated information into the designated pixels. An XOR technique is used to incorporate encrypted data after the frames have been jumbled. The stego video is then created by reassembling the frames together with the audio.

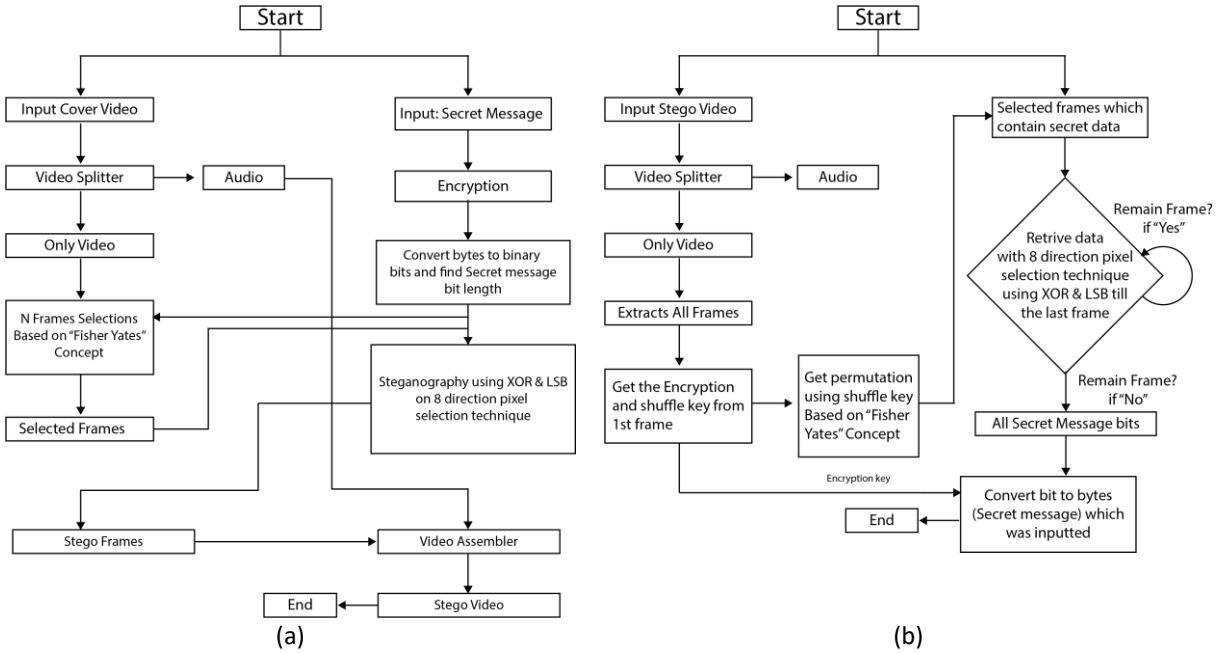


Fig. 2. Flowchart (a) Embed process of the proposed approach (b) Retrieve process of the proposed approach

3.1 Encrypting the Secret Message

Our prototype allows users to input confidential information, which is automatically encoded using the AES technique. AES uses symmetric keys of 128 bits, ensuring security. The system generates the key for users, enhancing security within video frames. The 128-bit AES key undergoes a 10-round cyclic process with stages like Add Round Key, Sub Bytes (byte replacement via an S-box table), Shift Rows (row adjustments), and Mix Columns. AES maintains security through its unique structure, ensuring at least 25 active S-boxes in four consecutive rounds. for every round, a round 128-bit key resulting after the primary key is employed. The procedure is carried out through a unique C# function. First, a video splitting application is applied to encode the message within the video carrier and extract it into BMP image frames. Overall, AES is a reliable and effective encryption technique that is often used in many applications to safeguard the secrecy of data. It is resistant to a variety of cryptanalytic assaults due to the mix of substitution, permutation, and key addition operations that cause confusion and diffusion. Because it offers greater encryption efficiency, we choose the AES algorithm [39] for our suggested strategy. Furthermore, it applies to huge data [40, 41].

3.2 Randomization Frame Selection Method

The Fisher-Yates algorithm for frame selection is incorporated in this model to ensure fair element permutations. The process involves iterating through an array in reverse, swapping elements with randomly generated indices, ensuring an equal probability of each element's final position in the shuffled array. The reason Fisher-Yates is selected is because of its qualities of unbiased randomness [41], the capacity for in-place shuffling [43], and exceptional effectiveness with an O(n) time complexity [26]. We opted for the Fisher-Yates algorithm to randomize our model's picture frames. It is a reliable method, ensuring precise and evenly distributed random ordering of elements. This approach is well-suited for enhancing security in video steganography due to its simplicity and effectiveness. The Fisher-Yates method introduces randomness, making it difficult for attackers to discern which frames hide secret data. It ensures equal frame selection, boosting steganographic security. It's computationally efficient and memory-friendly, seamlessly integrating into the recommended method without performance impact. Fisher-Yates is well-established for generating secure random permutations, making it ideal for enhancing video steganography security. In summary, its unpredictability, uniformity, efficiency, and reliability make it the best choice for randomizing image frames in our suggested approach. The quantity of frames *(Nf)* utilized for concealing the encrypted confidential data *(Sm_L)* and the dimensions *(Dv)* of the cover video are established through the application of Eq. (1) and Eq. (2). The selection of the extracted frames, presented in BMP format, is accomplished employing a randomization approach rooted in the principles of the Fisher Yates concept.

$$MEMB = M_{ax}D_v \times 4CD \times 3\ bits \tag{1}$$

$$Nf = \frac{CB}{MEMB}(Where, (Nf + 1) > 1) \tag{2}$$

The Maximum Embed Message Bit per frame (*MEMB*), the Total Cipher text length in bits (*CB*), and the maximal Size of the Input Video (*MaxDv*)—that can be either width or height—are all shown here. The eight directions are included in the complete direction representation (abbreviated *CD*). The maximum number of pixels that can be included in a frame is the product of *MaxDv* and 4 *CD*. In addition, the embedding capacity of a single pixel is taken into consideration by the 3-bit representation. With the frame selection strategy, we may choose the first *(Nf + 1) > 1* frame from a permutation according to the input key and the number of frames. Moreover, the frame sequence permits a reverse shuffle with the same key, facilitating data retrieval from the frame. Notably, the first frame always serves the purpose of storing metadata, including the shuffle key, length of the secret data, and progressively the cipher text.

3.3 Pixel Selection Method

To make the steganographic process more secure and capable, we employ the 8-directional pixel selection (8DPS) approach, a technique that selects pixels in eight different directions. This method uses the top-left, top-right, right, bottom-right, bottom, bottom-left, and left orientations to choose pixels. For many reasons, this method is effective and perfect for varying the image frames to boost the security of the suggested video steganographic technique. It is possible to significantly boost the steganographic process's capabilities by choosing pixels with eight distinct orientations. This allows for the concealment of more sensitive information while yet preserving the visual appeal of the film. The 8DPS approach makes it challenging for an assaulting party to determine which pixels have been

used to hide data. The steganographic process's unpredictable and random nature, which makes it challenging for an assaulting party to determine if concealed message is there, boosts the procedure's security. The steganographic process is reinforced by the 8DPS technique, which distributes the concealed data throughout various regions of the video frames. In the event that a frame or section of the video is lost or damaged, this enables the extraction of the concealed information from following video frames. The suggested system's one-time XOR and 1-bit LSB steganographic techniques are both compatible with the 8DPS technique. It may thus easily be included into the recommended video steganographic method without having a substantial impact on performance. In conclusion, the 8DPS approach is practical and best suited for randomizing the image frames in an effort to strengthen security of the suggested video steganographic approach because of its increased capacity, improved security, robustness, and compatibility with various steganographic techniques.

We provide two components of the steganographic procedure: the retrieval approach and the embedding strategy. The embedding process of the suggested technique is displayed in Figure 2(a), which comprises extracting video from the cover carrier in the first step and encrypting the message utilizing the AES 128-bit method. The frames are permuted using the frame selection approach in the second stage. Prior to starting to embed data into the selected frames' pixels, the data hiding function has a few phases that must be completed progressively. This function is known as the 8DPS strategy. The technique determines the width *(W)*, height *(H)*, and centre location *(Cx, Cy)* of the frame incrementally *(Cx, Cy)* follow Eq. (3) to identify pixel position, and then applies the 8DPS strategy to the chosen frames. Besides, using Eq. (1), the approach determines the maximum embed secret message bit number for a certain frame. When the message bit length is smaller than the *MEMB*, the following equations will be applied accordingly:

$$\left(C_X, C_y\right) = \left(\frac{Fd}{2}\right) \tag{3}$$

$$T_{np} = \left(\frac{BL}{3}\right) \tag{4}$$

The frame dimensions (*Fd)* in this instance, are what are utilized to discover the *x* and *y* centres. *Tnp* is the overall number of pixels in the image, while *BL* denotes the buried message's still-secret byte length. It will determine the value of Ppn (Pixels Number), for each directive line using Eq. (5) and the value of *Tnp*.

$$P_{pn} = \left\{\frac{\left(T_{np}-1\right)}{8}\right\} \tag{5}$$

$$D_s = \left(C_x \pm a, C_y \pm a\right) [Here\ a\ =\ 0\ to\ Ppn\ for\ every\ frame] \tag{6}$$

After obtaining the P_{pn}, the method will employ Eq. (6) to establish the positions *(Ds)* of the pixels in eight directions. For example, the equation for the downhill direction is (C_x, C_{y+a}), but the equation for the downhill-right direction is (C_{x+a}, C_{y+a}). The determination of the four pixels that encode the size of the confidential information bit in the figure is achieved using Eq. (7) through Eq. (10), which are employed to extract information from the stego frame as needed.

$$1^{st} pixel's\ position, (x_1, y_1) = \left(\frac{W}{2} - 2{,}1\right) \tag{7}$$

$$1^{st} pixel's\ position, (x_1, y_1) = \left(\frac{W}{2} - 2, 1\right) \quad (8)$$

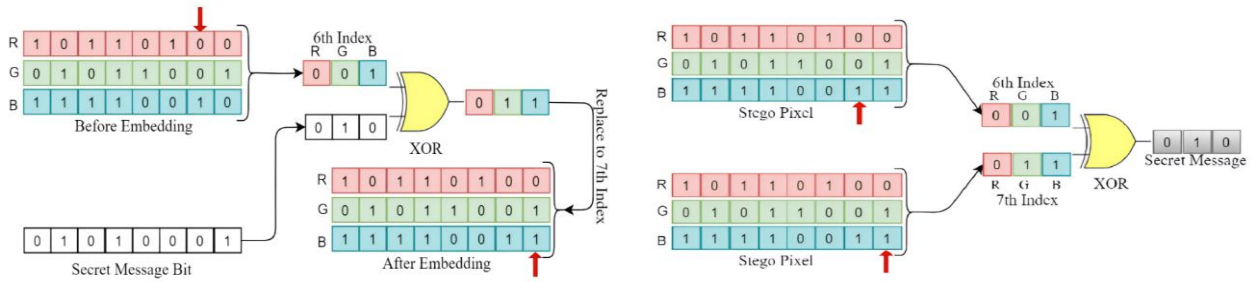
$$2^{nd} pixel's\ position, (x_2, y_2) = \left(W, \frac{H}{2} - 2\right) \quad (9)$$

$$4^{th} pixel's\ position, (x_1, y_1) = \left(1, \frac{H}{2} + 2\right) \quad (10)$$

It is simpler to obtain the encryption and shuffle keys from the first frame since they are always saved as metadata in the 8-direction pixel location of the first frame, and their bit length value is maintained in a specific 4-pixel position. Then, the data bit length of the particular frame and secret data are embedded, respectively, using the remaining selected frames.

3.4 Secret Data Embedding and Extracting Process

Figure 3 represents XOR based LSB substitution embedding and extracting technique of the video frames. In this initial step, the sensitive data that has to be concealed inside the video frame is selected. Before being included into the image, this information is encrypted to increase its security. The cryptographic output is obtained after encryption. After that, the output is binary-formatted. This conversion makes it easier to express the data as series of 0s and 1s. Now that the output has been translated to binary, the video frame may include the output. The least significant bits (LSBs) of certain pixels in a particular frame of the cover are changed throughout the embedding process. A method that combines the XOR operation with LSB replacement is used to accomplish this. The particular pixels and frame for embedding are chosen in accordance with the steganography specifications. The seventh bit of every pixel's Red, Green, and Blue (RGB) [44] element is used as the input for an XOR operation to strengthen the embedding process even more. The last bit of the RGB element is then replaced with the output of this XOR operation. These procedures produce the stego object, a movie that, to the untrained eye, seems just like the original cover but contains hidden information inside its pixel values. The cover image's integrity is preserved while the concealed data is imperceptible thanks to the XOR-based replacement of LSBs in the RGB components.



(a) (b)

Fig. 3. XOR based LSB substitution (a) embedding technique (b) extracting technique

Following the stego operation, the stego picture is formed. To extract the concealed data from it, a series of successive processes that mimic the original embedding process are required. In this process, the same reading procedure is applied in reverse order to achieve the extraction. It begins with Step S1, involving reading the pixel value "n" from the stego image and extracting the 7th bit "Rn7" of the red component of the pixel. Subsequently, an XOR operation is conducted between

(Rn7,1) and (Rn7,0), followed by a comparison between the result and the 8th bit "Rn8" of the red component. If equality holds with (Rn7,1), the extracted message bit "msgbit" is assigned the value 1; otherwise, if equality holds with (Rn7,0), "msgbit" is assigned the value 0. Similar procedures are repeated in Step S2 for the Green component and in Step S3 for the Blue element of the pixel. The hidden message bit "110," as shown in the accompanying figure, is extracted by performing an XOR procedure among the 7th bit of every element and the estimated 8th bit message. Importantly, this method makes sure that the message bit is not included by default in the original cover object, protecting the message's confidentiality even after thorough steganalysis.

3.5 Algorithm for Embedding and Extracting Process

Figure 4 shows the suggested approach's algorithm. As listed below, it includes a number of processes including frame selection, encryption, data hiding [45], and more. The components for the Cover Video (C_v) and Secret Message (S_m) are input during the embedding and retrieval phases. The secret plaintext and a 128-bit encryption key are essential for the AES approach to accomplish secret data encryption. The first frame is devoted to the XOR method of embedding meta data (*MD*) into eight directions ($Ds = (C_{xa}, C_{ya})$). The remaining secret info is embedded using subsequent frames. A second thread is used to extract frames into BMP formats simultaneously. After frame extraction (*FE []),* the Fisher Yates Shuffle function is used to process a series of integers and a random key. This produces a permutation (FL_p *[]*) that is based on user-provided stego video for the retrieval procedure. After that, the stego video is extracted into BMP file types.

The method then extracts metadata from the 8-direction location, including encryption keys, shuffle keys, and the total amount of secret message bits. The system then determines the necessary frames by using the shuffle key to generate random permutations and the message's total bit length.

Result: Stego Video

$S_m \leftarrow input;$
$C_v \leftarrow input;$
$C_t \leftarrow 128 - bitAES(S_m, key);$
$F_E[] = Extract\_Frames(C_v);$
$FL_p[] = FisherYatesShuffle(F_E[], key);$
$S_F = C_B / M_{EMB};$
$M_D = binary(shuffle\ key + salt + encryption\ key + salt + length\ of\ S_m);$
$embedMetaData(S_F[0], M_D);$
$Four\ Secret\ Pixels \leftarrow length\ of M_D;$
$S_{MB} = binary(S_m);$
$v = 0;$
for $S_F[1\ to\ N-1]$& $S_{MB}[0\ to\ N-1]$ **do**
  if $M_{EMB} < S_{MB}$ **then**
    $embedSecretDataXOR(S_F[v], S_{MB}[v\ to\ n])$
  end
  else
    $W = Each\ Frame\ Width;$
    $H = Each\ Frame\ Height;$
    $(C_x, C_y) = (H/2, W/2);$
    $embed((C_x, C_y));$
    $BL = Length\ of\ M;$
    $T_{np} = B_L/3;$
    $P_{pn} = (T_{np} - 1)/8;$
    $S_{MBL} \leftarrow length(S_{MB})$
    $Four\ Secret\ Pixels \leftarrow S_{MBL}$
    $a = 0;$
  end
  while $a \leq P_{pn}$ **do**
    $D_s = (C_{x \pm a}, C_{y \pm a}) embedXOR(D_s);$
    $a++;$
    $embed\ function(position):$
    $RGB\ Color \leftarrow position$
    $UpdateRGB\ color \leftarrow message$
    $stegoFrame.Add(S_F)$
    $stegoVideo \leftarrow videoAssembler(stegoFrame[])$
  end
end

(a)

Result: Secret Message

$S_v \leftarrow input;$
$F_E[] = Extract\_Frames(S_v);$
$M_D = Retrive(F_E[0]);$
$ShuffleKey = M_D.ShuffleKey;$
$EncryptionKey = M_D.EncryptKey;$
$TotalSecretMessageLength = M_D.MLength;$
$FL_p[] = FisherYatesShuffle(F_E[], ShuffleKey);$
$S_F = selectedFrame(FL_p[], M_D.MLength);$
$v = 0;$
for $S_F[1\ to\ N-1]$ **do**
  if $M_{EMB} < TotalSecretMessageLength$ **then**
    $S_{MBL} \leftarrow Four\ Secret\ Pixels$
    $S_D[] = retrieveSecretDataXOR(S_F[v], S_{MBL})$
  end
  else
    $W = Frame\ Width;$
    $H = Frame\ Height;$
    $(C_x, C_y) = (H/2, W/2);$
    $retrieve((C_x, C_y));$
    $BL = Length\ of\ M;$
    $T_{np} = B_L/3;$
    $P_{pn} = (T_{np} - 1)/8;$
    $S_{MBL} \leftarrow Four\ Secret\ Pixels$
    $a = 0;$
  end
  while $a \leq P_{pn}$ **do**
    $D_s = (C_{x \pm a}, C_{y \pm a}) S_D[] = retrieveXOR(D_s, S_{MBL});$
    $a++;$
    $retrieve\ function(position):$
    $secretData.Add(S_D)$
    $encryptData \leftarrow bitToBytes(secretData)$
    $PlainSecretData \leftarrow Dycrypt(encryptData, EncryptionKey)$
  end
end

(b)

Fig. 4. Algorithm of the suggested approach (a) embedding technique (b) extracting technique

4. Results

This section introduces the initial findings regarding visual quality and a comparative assessment of the original and concealed video frames. Six metrics are used in the rigorous statistical analysis applied in the research: Mean Absolute Error (MAE), Root Mean Square Error (RMSE), Mean-Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Mean Absolute Error (MAE), and Signal-to-Noise Ratio (SNR). Time to Complete the Embedding Process (TCEP), also known as the embedding time, is used to assess how effective the suggested solution is. Four videos—*DaffodilVarsity, Saint Martin, Bali*, and *Hobbit*—are chosen for experimental validation, as shown in Figure 5. These five-second films, all in AVI format, have 512 by 512-pixel resolution and a constant frame rate of 25 frames per second (FPS). By using the suggested method, a substantial amount of text is hidden inside the video files. Through the proposed approach, a sizable text is concealed within the video files. The method is implemented and tested using the C# language within the .NET Framework version 4.5.2.

Daffodil Varsity	Saint Martin	Bali	Hobbit

Fig. 5. Cover videos for experiment

The scientific rationale behind the six selected metrics for measuring frame quality, namely, SNR, SSIM, MAE, MSE, RMSE, and PSNR is elaborated in Eq. (11) to Eq. (16). These equations serve as commonly employed factors to assess both the effectiveness and security of the steganographic procedure. The mathematical elucidation of PSNR is as follows:

$$PSNR = 10\ \log_{10}\frac{255^2}{MSE} \tag{11}$$

In this context, the measurement unit for PSNR is expressed in decibels (dB), a metric that relies on the Mean-Square Error (MSE). Numerous studies validate that a PSNR value exceeding 40 dB when comparing the cover and stego frames is generally deemed satisfactory. The technical interpretation of SSIM is as follows:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+C_1)+(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2} \tag{12}$$

In this case, x and y stand in for the image's dimensions. To accommodate for a weaker denominator, two variable values, $C1 = (k_1L)2$ and $C2 = (k_2L)2$, are used to lessen the division. The averages of *x* and *y* are represented by the symbols μ_x and μ_y, respectively. Here, the pixel values' dynamic range known as *L* is specified together with default values for $K_1 = 0.01$ and $K_2 = 0.03$. Below is the mathematical explanation of MAE:

$$MAE = \frac{1}{3MN}\sum_{i=1}^{M}[C(x,y) - S(x,y)] \tag{13}$$

In this case, the location of the pixel is denoted by (*x, y*), and the picture dimension is represented by *M* and N. *C* stands for the cover frame, and S for the stego frame. The city-block standard is corresponding to the notation [1]. The following is the mathematical justification for SNR:

$$SNR = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\int(x,y)^2}{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[\int(x,y)-\int(x,y)]^2} \tag{14}$$

Digital image processing is the field from which the equation originates. *x* and *y* represent the coordinates of a pixel, the original frame is denoted as *f*, and the noisy frame is designated as $\check{f}$. The square root of the Mean-Square Error (MSE), or RMSE, has the following scientific interpretation:

$$RMSE = \sqrt{MSE} \tag{15}$$

The Scientific definition for MSE is:

$$MSE = (1_X M_X N)\sum_{i=1}^{M}\sum_{j=1}^{N}(a_{ij} - b_{ij})^2 \tag{16}$$

The value of the pixel at the cover frame's locations *i* and *j* is represented by the equation a_{ij}, whereas the pixel value at the identical positions *i* and *j* of the stego frame is represented by b_{ij}.

The outcomes of the suggested approach are evaluated using four chosen video frames and a maximum data payload of 15 KB. The results of the PSNR standard assessment for the selected frames are shown in Table 1.

Table 1
PSNR for selected videos

Frame no	DaffodilVarsity (PSNR)	SaintMartin (PSNR)	Bali (PSNR)	Hobbit (PSNR)
01 (M_D)	79.2390	78.9269	78.6890	78.5597
02 (S_{MB})	72.4123	72.3263	72.2630	72.2530
03 (S_{MB})	72.4343	72.3578	72.2835	72.2584
04 (S_{MB})	72.5001	72.3494	72.2958	72.2594
05 (S_{MB})	72.4952	72.3209	72.2094	72.2547
06 (S_{MB})	72.4771	72.3287	72.2906	72.2345
07 (S_{MB})	72.4563	72.3912	72.2523	72.2285
08 (S_{MB})	72.4109	72.4844	72.2712	72.2976
09 (S_{MB})	72.4889	72.3242	72.2944	72.2234
10 (S_{MB})	72.5099	72.3233	72.2203	72.2567
11 (S_{MB})	72.4911	72.3274	72.3965	72.2493
12 (S_{MB})	72.4286	72.3688	72.2945	72.2687
13 (S_{MB})	72.5013	72.3127	72.2099	72.2234
14 (S_{MB})	72.5109	72.4101	72.2506	72.2656
15 (S_{MB})	72.3099	72.3309	72.2054	72.2787
16 (S_{MB})	72.4019	72.3217	72.2470	72.2405
17 (S_{MB})	72.5088	72.3298	72.2694	72.2456
18 (S_{MB})	72.4863	72.3134	72.2547	72.2459
19 (S_{MB})	72.4128	72.3495	72.2231	72.2569
20 (S_{MB})	72.4713	72.3607	72.3458	72.3955
21 (S_{MB})	75.9788	75.7265	74.9949	75.1697

Frames measuring 512 × 512 were used for the movies of Daffodil Varsity, Saint Martin, Bali, and Hobbit, as shown in the table. A payload of fifteen thousand bytes, or fifteen kilobytes, was used. In total, 21 frames were used by our algorithm to hide the secret info. An informational maximum of 765 bytes was gradually hidden in each frame. Among the chosen video frames, DaffodilVarsity frames exhibited slightly improved PSNR values. Notably, the initial video frame was allocated for concealing information such as secret message size, AES and Fisher Yates algorithm keys, which are essential for the retrieval process. Consequently, PSNR values of 79.2390, 78.9269, 78.6890, and 78.5597 were obtained for *DaffodilVarsity, SaintMartin, Bali*, and *Hobbit* frames, respectively, all for the same payload.

Figure 6 visually demonstrates the PSNR values of our proposed model across different frames for various videos. Notably, the PSNR values of the 1st and 21st frames were marginally superior to those of the other frames. The 1st frame contains metadata, while the 21st frame holds the remaining secret data, always less than 765 Bytes. Consequently, these two frames exhibited slightly improved PSNR values.

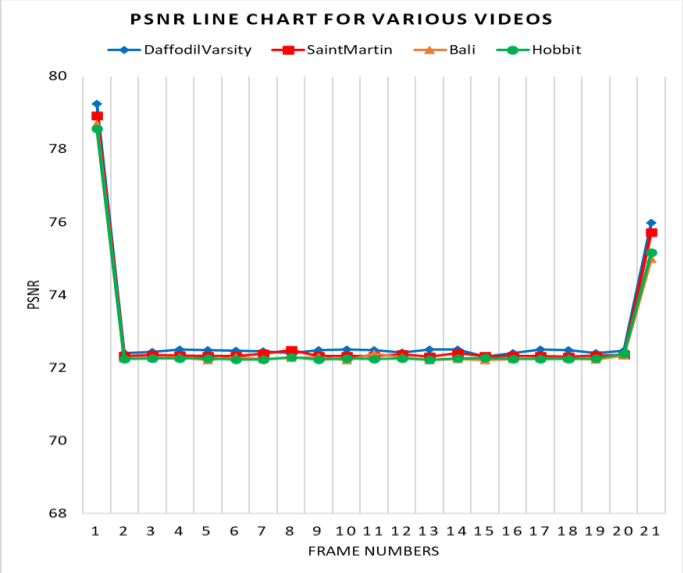


Fig. 6. PSNR values of the Proposed Model (P-Model) for various videos

Table 2 displays the results of six quality assessment metrics for a specific frame, along with the embedding time of the concealed frame, at various payload sizes of 512 bytes, 256 bytes, and 128 bytes. The videos are denoted as DV (DaffodilVarsity), SM (SaintMartin), BA (Bali), and HO (Hobbit). In this table, video frames DV, SM, BA, and HO, each with dimensions of 512 X 512, are used with different payload sizes (512 bytes, 256 bytes, and 128 bytes). Similarly, for DV, PSNR values of 74.0082, 77.1885, and 80.2390 were observed at different payload levels. SM exhibited PSNR values of 74.0079, 77.1467, and 80.2053 in a progressive manner, while BA yielded PSNR values of 74.0189, 76.8467, and 80.1678, and HO showed PSNR values of 74.0112, 76.7438, and 80.0443. Among these frames, DV demonstrated notably high PSNR values.

Table 2
Assessment of quality metrics of the planned approach with various standardized payload sizes

Frame (Bytes)	PSNR	SSIM	MAE	SNR	RMSE	MSE	TCEP
DV (512)	74.00 82	0.999 992913	0.00 26	68.59 91	0.05 09	0.00 26	6.47 s
DV (256)	77.18 85	0.999 997723	0.00 12	71.77 94	0.03 52	0.00 12	5.45 s
DV (128)	80.23 90	0.999 999726	0.00 06	74.82 99	0.02 48	0.00 06	4.52 s
SM (512)	74.00 79	0.999 995854	0.00 26	68.33 56	0.05 09	0.00 26	6.23 s
SM (256)	77.14 67	0.999 999646	0.00 12	70.95 40	0.03 51	0.00 12	5.93 s
SM (128)	80.20 53	0.999 999867	0.00 06	74.81 68	0.02 49	0.00 06	4.45 s
BA (512)	74.01 89	0.999 997803	0.00 26	67.78 20	0.05 09	0.00 26	6.12 s
BA (256)	76.84 67	0.999 999125	0.00 13	70.60 99	0.03 67	0.00 13	5.59 s
BA (128)	80.16 78	0.999 999650	0.00 06	73.93 68	0.02 50	0.00 06	4.56 s
HO (512)	74.01 12	0.999 997403	0.00 26	67.72 34	0.05 09	0.00 26	6.73 s
HO (256)	76.74 38	0.999 998925	0.00 13	70.52 83	0.03 71	0.00 13	5.98 s
HO (128)	80.04 43	0.999 999350	0.00 06	73.85 48	0.02 52	0.00 06	4.56 s

In terms of SSIM, DV achieved values of 0.999992913, 0.999997723, and 0.999999726 gradually, while SM attained SSIM values of 0.999995854, 0.999999646, and 0.999999867. Additionally, BA obtained SSIM values of 0.999997803, 0.999999125, and 0.999999650, and HO presented SSIM values of 0.999997403, 0.999998925, and 0.999999350. MAE values for DV were 0.0026, 0.0012, and 0.0006, in that order; values for the other frames were very comparable. In terms of SNR, SM

displayed values of 68.3356, 70.9540, and 74.8168, whereas DV reported values of 68.5991, 71.7794, and 74.8299. Additionally, BA recorded SNR values of 67.7820, 70.6099, and 73.9368, and HO provided SNR values of 67.7234, 70.5283, and 73.8548. The values of RMSE and MSE were comparable among all frames. However, HO showed better quality during the embedding process, concealing 512 Bytes, 256 Bytes, and 128 Bytes of sensitive data in 6.73 seconds, 5.98 seconds, and 4.56 seconds, respectively. The performance of the final three frames revealed findings that were largely consistent.

Table 3 presents a comparison among two recent steganographic techniques with a payload of 512 Bytes and a frame size of 512 X 512. The XOR substitution model by Bhuiyan *et al.,* [46] is denoted as Model1, the 8 directional-based model by Alam *et al.,* [47] is denoted as Model2, the 4 directional-based model by Sarkar *et al.,* [48] is denoted as Model3, and our suggested model is denoted as P-Model in the table. The chosen frames are represented as DV (DaffodilVarsity), SM (SaintMartin), BA (Bali), and HO (Hobbit). The first to eighth columns of this table present the values of PSNR, SSIM, MAE, SNR, RMSE, MSE, and TCEP in a sequential manner. For the frames of DV, PSNR values of 69.7483, 73.1845, 73.1442, and 74.0082 are achieved by model1, model2, model3, and p-model respectively.

Table 3
Comparison among three recent steganographic techniques

Techniques	PSNR	SSIM	MAE	SNR	RMSE	MSE	TCEP
Model1 (DV)	69.7 483	0.999984985	0.0029	64.4785	0.0539	0.0029	8.4545s
Model2 (DV)	73.1 845	0.999991956	0.0027	67.8686	0.0520	0.0027	5.9646s
Model3 (DV)	73.1 442	0.999991941	0.0027	67.8094	0.0520	0.0027	5.8346s
P-Model (DV)	74.0 082	0.999992913	0.0026	68.5991	0.0509	0.0026	6.4754s
Model1 (SM)	70.0 966	0.999989566	0.0029	65.1299	0.0539	0.0029	8.2331s
Model2 (SM)	73.9 565	0.999991023	0.0026	67.2094	0.0508	0.0026	5.5413s
Model3(SM)	73.9 349	0.999991007	0.0026	67.1958	0.0508	0.0026	5.3866s
P-Model (SM)	74.0 079	0.999995854	0.0026	68.3356	0.0509	0.0026	6.2311s
Model1 (BA)	70.9 856	0.999989803	0.0028	65.7820	0.0529	0.0028	7.4546s
Model2 (BA)	73.6 734	0.999993854	0.0027	66.9943	0.0519	0.0027	5.5112s
Model3 (BA)	73.6 611	0.999993719	0.0027	66.9761	0.0519	0.0027	5.4986s
P-Model (BA)	74.0 189	0.999997803	0.0026	67.7820	0.0508	0.0026	6.1241s
Model1 (HO)	70.9 568	0.999987403	0.0028	65.8455	0.0529	0.0028	7.54 65s
Model2 (HO)	73.8 896	0.999993096	0.0027	67.1959	0.0519	0.0027	5.14 45s
Model3(HO)	73.8 453	0.999992983	0.0027	67.1917	0.0519	0.0027	5.0069s
P-Model (HO)	74.0 112	0.999997403	0.0026	67.7234	0.0509	0.0026	6.7365s

This suggests that, when it comes to image quality metrics for DV frames, the p-model outperforms the other models by a small margin. However, the TCEP values progressively displayed are 8.4545s, 5.9646s, 5.8346s, and 6.4754s, suggesting that Model3 excels in embedding time compared to the proposed and other models. For SM frames, PSNR values of 70.0966, 73.9565, 73.9349, and 74.0079 are obtained by model1, model2, model3, and p-model respectively. In terms of image quality metric performance for SM frames, the p-model shows significant performance to the other models. However, the TCEP values progressively observed are 8.2331s, 5.5413s, 5.3866s, and 6.2311s, highlighting that model3 outperforms the proposed and other models in terms of embedding time. Progressively reported PSNR values of 70.9856, 73.6734, 73.6611, and 74.0189 are observed for BA frames with model1, model2, model3, and p-model respectively. This implies that the p-model exhibits slightly better image quality metric performance for BA frames compared to other models. However, the TCEP values sequentially shown are 7.4546s, 5.5112s, 5.4986s, and 6.1241s, indicating that model3 excels in embedding time compared to the suggested and other

models. For HO frames, rising PSNR values of 70.9568, 73.8896, 73.8453, and 74.0112 are achieved by models 1, 2, 3, and p-model respectively. In terms of image quality metric performance for HO frames, the p-model demonstrates a slightly improved performance to the other models. However, the TCEP values are sequentially depicted as 7.5465s, 5.1445s, 5.0069s, and 6.7365s, where Model3 outperforms the proposed and other models in embedding time.

The suggested model excels in most aspects compared to existing models, emphasizing enhanced security through cryptography, random frame selection, and pixel selection. However, it has a slightly longer execution time. The initial evaluation focused on imperceptibility, where the proposed approach outperformed three known solutions. Yet, further research is needed to test its security and robustness. This research introduces a dual-layer video steganography solution that combines 1-bit LSB replacement and XOR techniques with AES encryption for added security. Random frame selection via the Fisher-Yates algorithm and 8DPS enhance data hiding effectiveness. Comparative studies show the suggested method's superiority in reliability and security. Empirical results demonstrate its improved performance, highlighting its value for secure data embedding in videos. In conclusion, this research presents a comprehensive video steganography approach that employs modern techniques and algorithms to enhance security and resilience.

4. Conclusions

The findings of this study show how much more imperceptible our proposed solution is compared to the recent models. We have proposed a more secure approach by incorporating cryptography into the video steganography. A significant step towards improving data security is the use of the 128-bit key AES algorithm for secret data encryption. Additionally, using a Fisher-Yates-based randomization strategy for frame shuffle not only enhances security levels in video steganography techniques but also foils statistical assaults. The automated technique of hiding and encrypting secret data, together with simplified processes for extraction and decryption, is a major advance of this study. This thorough and automatic framework takes care of possible weaknesses and makes it easier to carry out safe data hiding and retrieval. Additionally, the use of the 8DPS approach in conjunction with the XOR-based 1-bit LSB technique increases the complexity and obscurity of concealed data in video frame, strengthening resistance against steganalysis assaults. In this work, steganographic and cryptographic concepts are combined in such a way, resulting in a complex solution that provides a strong barrier against unauthorized access and data disclosure.

Acknowledgement
This research was partially funded by the Centre of Excellence for Advanced Computing (ADVCOMP), Universiti Malaysia Perlis.

References
[1] European Commission. "Newsroom: Research and Innovation." (2023). https://ec.europa.eu/newsroom/rtd/items/713444/en
[2] Data Breaches Exposed Malaysia. "Exposed: The Alarming State of Data Breaches in Malaysia." (2023). https://www.exabytes.my/blog/data-breaches-exposed-malaysia
[3] BBC News. "Malaysian data breach sees 46 million phone numbers leaked." (2023). https://www.bbc.com/news/technology-41816953
[4] Tech.co. "Data Breaches That Have Happened in 2022 and 2023 So Far." (2023). https://tech.co/news/data-breaches-updated-list
[5] Diffie, Whitfield, and Martin E. Hellman. "New directions in cryptography." In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, pp. 365-390. 2022. https://doi.org/10.1145/3549993.3550007

[6] Boujerfaoui, Said, Rabia Riad, Hassan Douzi, Frederic Ros, and Rachid Harba. "Image watermarking between conventional and learning-based techniques: a literature review." *Electronics* 12, no. 1 (2022): 74. https://doi.org/10.3390/electronics12010074
[7] Mandal, Pratap Chandra, Imon Mukherjee, Goutam Paul, and B. N. Chatterji. "Digital image steganography: A literature survey." *Information sciences* 609 (2022): 1451-1488. https://doi.org/10.1016/j.ins.2022.07.120
[8] Pilania, Urmila, Rohit Tanwar, Mazdak Zamani, and Azizah Abdul Manaf. "Framework for video steganography using integer wavelet transform and JPEG compression." *Future Internet* 14, no. 9 (2022): 254. https://doi.org/10.3390/fi14090254
[9] Kadhim, Mohammed Ayad, and Majid Jabbar Jawad. "A Coverless video steganography: A Survey." In *2022 5th International Conference on Engineering Technology and its Applications (IICETA)*, pp. 522-527. IEEE, 2022. https://doi.org/10.1109/IICETA54559.2022.9888744
[10] Sadek, Mennatallah M., Amal S. Khalifa, and Mostafa GM Mostafa. "Video steganography: a comprehensive review." *Multimedia tools and applications* 74 (2015): 7063-7094. https://doi.org/10.1007/s11042-014-1952-z
[11] AP, Petitcolas Fabien. "Information hiding-A servey." *Proc. IEEE* 87, no. 7 (1999): 1062-1078. https://doi.org/10.1109/5.771065
[12] Dalal, Mukesh, and Mamta Juneja. "A survey on information hiding using video steganography." *Artificial Intelligence Review* 54, no. 8 (2021): 5831-5895. https://doi.org/10.1007/s10462-021-09968-0
[13] Adee, Rose, and Haralambos Mouratidis. "A dynamic four-step data security model for data in cloud computing based on cryptography and steganography." *Sensors* 22, no. 3 (2022): 1109. https://doi.org/10.3390/s22031109
[14] Rijati, Nova, Pulung Nurtantio Andono, and De Rosal Ignatius Moses Setiadi. "Imperceptible Improvement using Edge Area Selection for Robust Video Watermarking Using Tchebichef-Singular Value Decomposition." *International Journal of Intelligent Engineering & Systems* 15, no. 2 (2022). https://doi.org/10.22266/ijies2022.0430.27
[15] Kumari, Manju, and Shailender Gupta. "Performance comparison between Chaos and quantum-chaos based image encryption techniques." *Multimedia Tools and Applications* 80, no. 24 (2021): 33213-33255. https://doi.org/10.1007/s11042-021-11178-3
[16] Patel, Rachna, Kalpesh Lad, and Mukesh Patel. "Novel DCT and DST based video steganography algorithms over non-dynamic region in compressed domain: a comparative analysis." *International Journal of Information Technology* 14, no. 3 (2022): 1649-1657. https://doi.org/10.1007/s41870-021-00788-7
[17] Chandio, Asghar Ali, M. D. Asikuzzaman, Mark R. Pickering, and Mehwish Leghari. "Cursive text recognition in natural scene images using deep convolutional recurrent neural network." *IEEE Access* 10 (2022): 10062-10078. https://doi.org/10.1109/ACCESS.2022.3144844
[18] Gupta, Hemant, and Dr Setu Chaturvedi. "Video data hiding through LSB substitution technique." *International Journal Of Engineering And Science* 2, no. 10 (2013): 32-39.
[19] Hanafy, Amr A., Gouda I. Salama, and Yahya Z. Mohasseb. "A secure covert communication model based on video steganography." In *MILCOM 2008-2008 IEEE Military Communications Conference*, pp. 1-6. IEEE, 2008. https://doi.org/10.1109/MILCOM.2008.4753107
[20] Bhattacharyya, Debnath, Arup Kumar Bhaumik, Minkyu Choi, and Tai-hoon Kim. "Directed graph pattern synthesis in LSB technique on video steganography." In *International Conference on Advanced Computer Science and Information Technology*, pp. 61-69. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. https://doi.org/10.1007/978-3-642-13577-4_6
[21] Balaji, R., and Garewal Naveen. "Secure data transmission using video Steganography." In *2011 IEEE International Conference on Electro/Information Technology*, pp. 1-5. IEEE, 2011. https://doi.org/10.1109/EIT.2011.5978601
[22] Dasgupta, Kousik, J. K. Mandal, and Paramartha Dutta. "Hash based least significant bit technique for video steganography (HLSB)." *International Journal of Security, Privacy and Trust Management (IJSPTM)* 1, no. 2 (2012): 1-11.
[23] Paul, Rahul, Anuja Kumar Acharya, Virendra Kumar Yadav, and Saumya Batham. "Hiding large amount of data using a new approach of video steganography." In *Confluence 2013: The next generation information technology summit (4th international conference)*, pp. 337-343. IET, 2013. https://doi.org/10.1049/cp.2013.2338
[24] Chen, Siyi, and Zhiguo Qu. "Novel quantum video steganography and authentication protocol with large payload." *International Journal of Theoretical Physics* 57, no. 12 (2018): 3689-3701. https://doi.org/10.1007/s10773-018-3882-4
[25] Kapoor, Vivek, and Akbar Mirza. "An enhanced LSB based video steganographic system for secure and efficient data transmission." *International Journal of Computer Applications* 121, no. 10 (2015). https://doi.org/10.5120/21580-4649

[26] Ma, Kaiyun, Lin Teng, Xingyuan Wang, and Juan Meng. "Color image encryption scheme based on the combination of the fisher-yates scrambling algorithm and chaos theory." *Multimedia Tools and Applications* 80 (2021): 24737-24757. https://doi.org/10.1007/s11042-021-10847-7

[27] Chikouche, Sofyane Ladgham, and Noureddine Chikouche. "An improved approach for lsb-based image steganography using AES algorithm." In *2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B)*, pp. 1-6. IEEE, 2017. https://doi.org/10.1109/ICEE-B.2017.8192077

[28] Balu, S., C. Nelson Kennedy Babu, and K. Amudha. "Secure and efficient data transmission by video steganography in medical imaging system." *Cluster Computing* 22, no. Suppl 2 (2019): 4057-4063. https://doi.org/10.1007/s10586-018-2639-4

[29] Luo, Ting, Gangyi Jiang, Mei Yu, Haiyong Xu, and Wei Gao. "Sparse recovery based reversible data hiding method using the human visual system." *Multimedia Tools and Applications* 77 (2018): 19027-19050. https://doi.org/10.1007/s11042-017-5356-8

[30] Bhautmage, Pritish, Amutha Jeyakumar, and Ashish Dahatonde. "Advanced video steganography algorithm." *International Journal of Engineering Research and Applications* 3, no. 1 (2013): 1641-1644.

[31] Ramalingam, Mritha. "Stego machine–video steganography using modified LSB algorithm." *International Journal of Information and Communication Engineering* 5, no. 2 (2011): 170-173.

[32] Yadav, Pooja, Nishchol Mishra, and Sanjeev Sharma. "A secure video steganography with encryption based on LSB technique." In *2013 IEEE international conference on computational intelligence and computing research*, pp. 1-5. IEEE, 2013. https://doi.org/10.1109/ICCIC.2013.6724212

[33] Mstafa, Ramadhan J., and Khaled M. Elleithy. "A new video steganography algorithm based on the multiple object tracking and Hamming codes." In *2015 IEEE 14th International conference on machine learning and applications (ICMLA)*, pp. 335-340. IEEE, 2015. https://doi.org/10.1109/ICMLA.2015.117

[34] Mstafa, 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* 75 (2016): 10311-10333. https://doi.org/10.1007/s11042-015-3060-0

[35] Moon, Sunil K., and Rajeshree D. Raut. "Analysis of secured video steganography using computer forensics technique for enhance data security." In *2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)*, pp. 660-665. IEEE, 2013. https://doi.org/10.1109/ICIIP.2013.6707677

[36] Kaur, Manpreet, and Amandeep Kaur. "Improved security mechanism of text in video using steganographic technique." *International Journal* 2, no. 10 (2014).

[37] Sudeepa, K. B., K. Raju, Ranjan Kumar HS, and Ganesh Aithal. "A new approach for video steganography based on randomization and parallelization." *Procedia Computer Science* 78 (2016): 483-490. https://doi.org/10.1016/j.procs.2016.02.092

[38] Manisha, S., and T. Sree Sharmila. "A two-level secure data hiding algorithm for video steganography." *Multidimensional Systems and Signal Processing* 30 (2019): 529-542. https://doi.org/10.1007/s11045-018-0568-2

[39] Jintcharadze, Elza, and Maksim Iavich. "Hybrid implementation of Twofish, AES, ElGamal and RSA cryptosystems." In *2020 IEEE East-West Design & Test Symposium (EWDTS)*, pp. 1-5. IEEE, 2020. https://doi.org/10.1109/EWDTS50664.2020.9224901

[40] Naif, Jolan Rokan, Ghassan H. Abdul-Majeed, and Alaa K. Farhan. "Secure IOT system based on chaos-modified lightweight AES." In *2019 International Conference on Advanced Science and Engineering (ICOASE)*, pp. 1-6. IEEE, 2019. https://doi.org/10.1109/ICOASE.2019.8723807

[41] Stallings, William. *Cryptography and network security, 4/E*. Pearson Education India, 2006.

[42] Juniawan, Fransiskus Panca, Harrizki Arie Pradana, and Dwi Yuny Sylfania. "Performance comparison of Linear Congruent method and Fisher-Yates Shuffle for data randomization." In *Journal of Physics: Conference Series*, vol. 1196, no. 1, p. 012035. IOP Publishing, 2019. https://doi.org/10.1088/1742-6596/1196/1/012035

[43] Naim, M., and A. Ali Pacha. "A new chaotic satellite image encryption algorithm based on a 2D filter and Fisher–Yates shuffling." *The Journal of Supercomputing* 79, no. 15 (2023): 17585-17618. https://doi.org/10.1007/s11227-023-05346-5

[44] Yusof, Ahmad Anas, Mohd Khairi Mohamed Nor, Nur Latif Azyze Mohd Shaari Azyze, Anuar Mohamed Kassim, Shamsul Anuar Shamsudin, Hamdan Sulaiman, and Mohd Aswad Hanafi. "Land clearing, preparation and drone monitoring using Red-Green-Blue (RGB) and thermal imagery for Smart Durian Orchard Management project." *Journal of Advanced Research in Fluid Mechanics and Thermal Sciences* 91, no. 1 (2022): 115-128. https://doi.org/10.37934/arfmts.91.1.115128

[45] Noroozi, E., S. M. Daud, and A. Sabouhi. "A Security Enhanced Robust Image Hiding Algorithm from Digital Signature."

[46] Bhuiyan, Touhid, Afjal H. Sarower, Rashed Karim, and Maruf Hassan. "An image steganography algorithm using LSB replacement through XOR substitution." In *2019 International Conference on Information and Communications Technology (ICOIACT)*, pp. 44-49. IEEE, 2019. https://doi.org/10.1109/ICOIACT46704.2019.8938486

[47] Alam, Sheikh Thanbir, Nusrat Jahan, and Md Maruf Hassan. "A New 8-Directional Pixel Selection Technique of LSB Based Image Steganography." In *Cyber Security and Computer Science: Second EAI International Conference, ICONCS 2020, Dhaka, Bangladesh, February 15-16, 2020, Proceedings 2*, pp. 101-115. Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-52856-0_8

[48] Sarkar, Anindya, Kaushal Solanki, and B. S. Manjunath. "Further study on YASS: Steganography based on randomized embedding to resist blind steganalysis." In *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, vol. 6819, pp. 459-469. SPIE, 2008. https://doi.org/10.1117/12.767893