Article

JOURNAL OF UNIVERSITY OF BABYLON

For Pure and Applied Sciences (JUBPAS)

Vol.31; No.2.| 2023

Video Steganography Technique Based on Enhanced Moving Objects Detection Method

Mithal Hadi Jebur[1*], Fanar Ali Joda[2], and Mohammed Abdullah Naser[3]

[1]College of Science for Women, University of Babylon, mithal.jebur.gsci13@student.uobabylon.edu.iq, Babylon, Iraq.

[2] Al-Mustaqbal University, fanaralijoda@uomus.edu.iq, Babylon, Iraq.

[3]College of Science for Women, University of Babylon, wsci.mohammed.abud@uobabylon.edu.iq, Babylon, Iraq.

***Corresponding author email:** mithal.jebur.gsci13@student.uobabylon.edu.iq; mobile: 07725572892

تقنية إخفاء المعلومات بالفيديو على أساس طريقة محسنة لاكتشاف الأجسام المتحركة

مثال هادي جبر [1]، فنر علي جودة [2]، محمد عبد الله ناصر [3]

1 كلية العلوم للبنات ، جامعة بابل، mithal.jebur.gsci13@student.uobabylon.edu.iq، بابل، العراق

2 كلية المستقبل الجامعة ، fanaralijoda@uomus.edu.iq، بابل، العراق

3 كلية العلوم للبنات، جامعة بابل، wsci.mohammed.abud@uobabylon.edu.iq، بابل العراق

Received:	26 /4/2023	Accepted:	6/6/2023	Published:	30/6/2023

Background:

Video steganography has become a popular option for protecting secret data from hacking attempts and common attacks on the internet. However, when the whole video frame(s) are used to embed secret data, this may lead to visual distortion.

Materials and Methods:

This work is an attempt to hide sensitive secret image inside the moving objects in a video based on separating the object from the background of the frame, selecting and arranging them according to object's size for embedding secret image. The proposed approach reverses the secret image bits and uses XOR technique between the reversed bits and the detected moving object bits for embedding. The proposed approach provides more security and imperceptibility as the moving objects are used for embedding, so it is difficult to notice the changes in the moving objects instead of using background area for embedding in the video. Further development to the proposed approach in the area of video steganography has been done by applying spatial model in combination with statistical model. Additional LSB styles have been also applied to evaluate the ability of the proposed approach in detecting moving objects. In addition to evaluating the robustness of the proposed approach against different attacks such as salt and pepper noise and median filtering.

Results:

The experimental results showed the better visual quality of the stego video with PSNR values exceeding 70 dB, this indicates that the proposed method works without causing much distortion in the original video and transmitted secret message.

Conclusion:

The experimental proof of the proposed approach can successfully detect and embed secret image. Also, it provides more security and imperceptibility as the data was hidden in the moving objects and the updates in the moving objects are difficult to notice rather than the static region in a video.

Key words:

Video Steganography, LSB, Embedding Secret Image, Extracting Secret Image, XOR Coding, Moving Object Detection.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

الخلاصة

مقدمة:

أصبح إخفاء المعلومات عن طريق الفيديو خيارًا شائعًا لحماية البيانات السرية من محاولات القرصنة والهجمات الشائعة على الإنترنت. ومع ذلك ، عند استخدام إطار (إطارات) الفيديو بالكامل لتضمين بيانات سرية ، فقد يؤدي ذلك إلى تشويه بصري.

طرق العمل:

هذا العمل هو محاولة لإخفاء صورة سرية حساسة داخل الأجسام المتحركة في مقطع فيديو بناءً على فصل الكائن عن خلفية الإطار واختيارها وترتيبها حسب حجم الكائن لتضمين الصورة السرية. يتم استخدام تقنية XOR مع البتات العكسية بين بتات الصورة السرية وبتات الكائن المتحرك المكتشفة للتضمين. توفر الطريقة المقترحة مزيدًا من الأمان وعدم الإدراك حيث يتم استخدام الكائنات المتحركة للتضمين ، لذلك من الصعب ملاحظة التغييرات في الكائنات المتحركة بدلاً من استخدام منطقة الخلفية للتضمين في الفيديو. تم إجراء مزيد من التطوير للطريقة المقترحة في مجال إخفاء المعلومات بالفيديو من خلال تطبيق النموذج المكاني مع النموذج الإحصائي. تم أيضًا تطبيق أنماط LSBالإضافية لتقييم قدرة النهج المقترح في اكتشاف الأجسام المتحركة. بالإضافة إلى تقييم متانة الطريقة المقترحة ضد الهجمات المختلفة مثل ضوضاء الملح والفلفل والتصفية المتوسطة.

الاستنتاجات:

أظهرت النتائج التجريبية جودة بصرية أفضل لفيديو stego مع قيم PSNR تتجاوز 70 ديسيبل ، وهذا يشير إلى أن الطريقة المقترحة تعمل دون إحداث تشويه كبير في الفيديو الأصلي والرسالة السرية المرسلة.

الكلمات المفتاحية:

اخفاء المعلومات ، تقنية LSB ،تضمين رسالة سرية ،استرجاع الرسالة السرية ،تشفير باستخدام xor،تحديد الكائنات الموجودة داخل الفديو

مجلة جامعة بابل للعلـــوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

INTRODUCTION

Digital Image steganography is commonly used for hiding a secret data in an image as it is very well-known technique [1, 2]. High capacity is the main characteristic of images which could be suitable for the purpose of steganography. Hence images are commonly applied in various domains such as social media. Using images for hiding secret data is categorized into three main categories which are spatial domain, transform domain, and adaptive steganography [3]. Various digital mediums such as text, image, video, and audio employ their properties to hide secret data [4, 5]. In text steganography applies the line which consists of strings of words and characters shifting encoding, and applies a representation of a facial expression in textual chat to secure connection. In audio steganography, it is widely utilized coding, extent spectrum, and low-bit encoding for embedding secret data. Embedding secret data is also achieved using packet headers in another carrier such as network protocol. The embedding process can be done by using the characteristic of resending of packets which is called retransmission steganography. Whereas embedding secret data using images in combination with audio is commonly applied in video steganography [6, 7]. The reason behind this is that videos have a several combination of images in view of the video stream. However the transformation in the cover carrier must not be recognized through unauthorized access [8]. There are several different cover media to choose from while engaging in steganography. The specifics of it are shown in Figure (1) [9, 10].

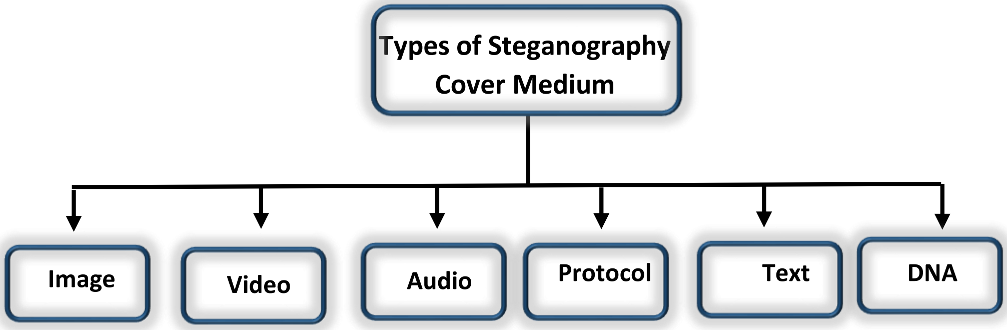


Figure 1: Different Kinds of Cover Mediums for Steganography.

Steganography is a solution to this dilemma since it enables us to transmit news and sensitive information without risk of the signals being intercepted and traced back to us. Data security is to prevent unauthorized access, use, disclosure, interruption, change, or erasure of data and data structures. In a way that does not allow the human vision system to detect it. The data hiding can be done in two domains: spatial and transform. In the spatial domain embedded directly on the values pixels, and in the field of transformation, transformed operands are used to hide data with a slew of different methods for detecting objects in a video [4]. There are some of techniques used nowadays in steganography such as word shit and line shift in text steganography, LSB (Least Significant Bit) and Redundant Pattern Encoding in image steganography, spread spectrum in audio steganography, utilizing the properties of randomness in DNA to embed the secret data,

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

network protocol can be used as a medium to hide secret data in packet payload [6, 11, 12]. These techniques use a cover media to conceal sensitive information in such a manner that it is impossible for unauthorized individuals to discern whether or not the data is there. A technique of steganography makes use of a video file as the cover medium. Converting the video file into individual video frames is the first step. Access to video processing software is a major factor in the rise of videos as a means of online communication. Using video steganography, data may be hidden in a video while leaving the video's visual quality intact [13]. The statistical analysis of visual characteristics and the temporal analysis of motion information have been proposed as robust methodologies. Color and texture attributes may be used to segment a frame, and then motion vectors can be merged across sections depending on particular requirements, such as how close the pixels are to each other in the frame.

In some research studies the focus has been on the process of embedding a secret image within an image, and some of another research studies have been interested in including an image or text within a group of video frames, as the embedding process was in the background of the frames, while others embedded an image or text inside the human face within the video. Hence in this research study focus is given more on embedding the secret image within moving objects of a group of video frames. Where this gives another dimension of safety with additional layer of protection, as an object is a group of extraneous pixels on the video scene and makes it difficult to trace it.

Related Works

The recent research studies proposed in the field of embedding secret data in a video are discussed in this section according to various embedding approaches.

Hashim et al (2011) [14], this proposed an approach contains an AVI hidden information system development. The AVI file is converted into two parts, video and audio. Where each frame is saved as a BMP file image, and several frames are selected as cover frames. Two hiding techniques are applied in this approach, the first technique is the Least Significant Bit (LSB) to embed one bit into blue channel of a pixel, and the second technique is the Haar Wavelet Transform (HWT). HWT scans the pixel in horizontal direction (left to right) and vertical direction (top to bottom) to perform addition and subtraction on neighboring pixels. However, maximum value of PSNR reported in this approach is 53.43. owever

Mstafa and Elleithy (2016) [15] proposed a method with four tasks for embedding messages in a video. In this first task, hamming code is applied to produce an encoded message through pre-processing the secret message through converting it into ASCII codes. In the second task, faces on the cover movies are detected and tracked. The region of interest is also determined. Whereas LSB applied in the third task to embedding the secret message. However, this method is

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

designed for embedding messages in the detected faces only. However, maximum value of PSNR reported in this approach is 53.93 with 1-bit LSB.

Mstafa et al (2017) [16], proposed a secure video steganography algorithm using the Multiple Object Tracking (MOT) algorithm and error correcting codes. In pre-processing stage, the algorithm applies Hamming code for encoding the secret data. The algorithm uses LSB, Discrete Wavelet Transform (DWT), and Discrete Cosine Transform (DCT) for embedding the secret data based on foreground masks. However, maximum value of PSNR reported in this approach is 49.01 with 1-bit LSB, i.e., the higher the n-bit LSB size, the PSNR value decreased.

Muhammad et al (2017) [17], have proposed an approach for embedding secret data in an image using stego key-directed adaptive LSB substitution. A Two-Level Encryption Algorithm (TLEA) applied for encrypting key (i.e., stego key). Whereas a Multi-Level Encryption Algorithm (MLEA) applied for encrypting secret data. LSB substitution is then applied for embedding encrypted information according to secret key, red channel, and MLEA. However, maximum value of PSNR reported in this approach is 58.29.

Rajkumar et al (2017) [18], it is another approach proposed for embedding information at the background of video frames. Where an encryption algorithm is applied to encrypt the data, and then LSB is applied to embed the encrypted data in the video frame.

Hemalatha et al (2020) [19], video is encrypted using Advanced Encryption Standard (AES). The video converted into frames firstly, and one frame is selected to embed the secret encrypted data. Where AES also applied for embedding purposes. In the extraction stage, the original data is extracted by using the relevant key to identify and decrypt the pixel coefficient. However, maximum value of PSNR reported in this approach is 52.58.

Vinay and Ananda 2021 [20], proposed an approach for embedding secret data in video. Firstly, a public key, i.e., without encryption, is required to perform data embedding. A secret image is divided into non-overlapped blocks. XOR operation is then applied for each block of the image with the public key. Whereas, in extracting stage, from the non-overlapped blocks, six main features are extracted entropy, variance, histogram, directional features, correlation and standard deviation. Two class Support Vector Machine (SVM) classifier is then performed to retrieve secret image using the resulted features. However, maximum value of PSNR reported in this approach is 55.43.

Dalal et al (2021) [21], have proposed an approach for embedding and tracking secret data in 323LSB style of moving objects. Where objects that possess motion are detected through applying Gaussian Mixture Model for Background subtraction, which divides a frame into two groups of pixels, removes the background pixels through subtraction and thresholding, and keeps pixels of the objects of interest. However, maximum value of PSNR reported in this approach is 42.32.

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

Mirah and Majid (2021) [22] proposed an approach for embedding the secret message using the LSB. In this approach, the XOR operator applied with three keys for embedding purposes to achieve higher security layer. However, this approach designed for embedding the secret message in a frame without identifying or detecting the objects. However, maximum value of PSNR reported in this approach is 55.97.

Roselinkiruba et al (2022) [23] have proposed an approach for embedding information in a video based on four main steps. (1) Video compression using Discrete Cosine Transform (DCT) to generate frequencies from each image pixel value. (2) Moving object detection using Adaptive Gaussian Mixture Model (AGMM) to separate the background and foreground masks. (3) Kalman filter (KF) applied to detect object's motion through tracking position of each object. (4) Embedding secret information using LSB through dividing image into non-overlapping pixel blocks, i.e., 2×3 pixel blocks. 4-bit LSB is used for embedding the data when a block comprises of only one pixel as moving object. In addition, the data embedding within the blocks are achieved by up-scaling each block. Where the weight of each pixel is calculated using Pixel Value Differencing (PVD), which calculates the difference between the current and the neighboring of a particular pixel. However, maximum value of PSNR reported in this approach is 44.57.

Nilizadeh et al (2022) [24] have proposed an approach called Adaptive Matrix Pattern (AMP), which converts an image into blocks (i.e., non-overlapped square-sized), and generates matrix pattern called codebook for each ASCII character in each image block. Where each ASCII character receives a various codebook matrix pattern. For embedding secret message, the most suitable image blocks identified through applying a pre-processing algorithm, and the blue channel of selected blocks is used. However, maximum value of PSNR reported in this approach is 58.53.

Naser et al (2022) [25], have proposed an approach for hiding secret data in a video using LSB. Firstly, secret data encrypted using Rivest Cipher 4 (RC4) through generating keys and performing XOR operation with plain text to produce the cryptographic text. Secondly, in the embedding stage, a number of frames and pixels selected randomly. Where two keys generated to perform this process, one for selecting frames, and another for selecting pixels. However, maximum value of PSNR reported in this approach is 65.38 when size of secret data is 2kb, i.e., the higher the data size, the PSNR value decreased.

Accordingly, the related works referred to above can be summarized in addition to the proposed work as indicated in the Table 1 and Figure 2 below.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

Table 1: Summary of Reported Literature

Author(s) and Year of Publication	Embedding Technique	Moving Objects Detection (Yes/No)	Embedding in Objects (Yes/No)	Embedding in Background (Yes/No)	Embedding using Statistical and Spatial Model (Yes/No)	Embedding in Video (Yes/No)	Performance Measures (PSNR)
Hashim et al 2011 [14]	LSB and HWT	No	No	**Yes**	No	**Yes**	53.43
Mstafa and Elleithy 2016 [15]	LSB	**Yes**	**Yes**	No	No	**Yes**	53.93
Mstafa et al 2017 [16]	LSB, DWT, and DCT	**Yes**	**Yes**	No	No	**Yes**	49.01
Muhammad et al 2017 [17]	LSB	No	No	**Yes**	No	No	58.29
Rajkumar et al 2017 [18]	LSB	No	No	**Yes**	No	**Yes**	---
M.Hemalatha et al 2020 [19]	AES	No	No	**Yes**	No	**Yes**	52.58
Vinay and Ananda 2021 [20]	XOR and SVM	No	No	**Yes**	No	**Yes**	55.43
Dalal et al 2021 [21]	LSB	**Yes**	**Yes**	No	No	**Yes**	42.32
Mirah and Majid, 2021 [22]	LSB	No	No	**Yes**	No	**Yes**	55.97
Roselinkiruba et al 2022 [23]	LSB and PVD	**Yes**	**Yes**	No	No	**Yes**	44.57
Nilizadeh et al 2022 [24]	AMP	No	No	**Yes**	No	No	58.53
Naser et al 2022 [25]	LSB	No	No	**Yes**	No	**Yes**	65.38

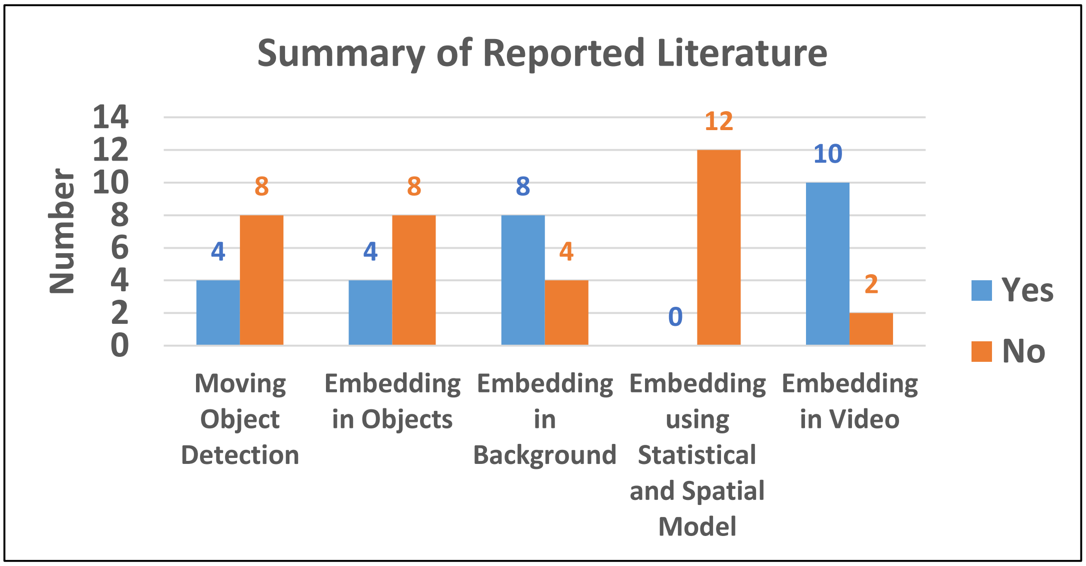


Figure 2: Summary of Reported Literature

Materials and Methods

In this work, an improved approach has been proposed to hide sensitive secret image inside the moving objects in a video on the basis of separating the object from the background of the frame, selecting and arranging them according to size for the purpose of embedding secret image. All details can be followed below. Figure 3 shows main structure of the proposed video steganography approach.

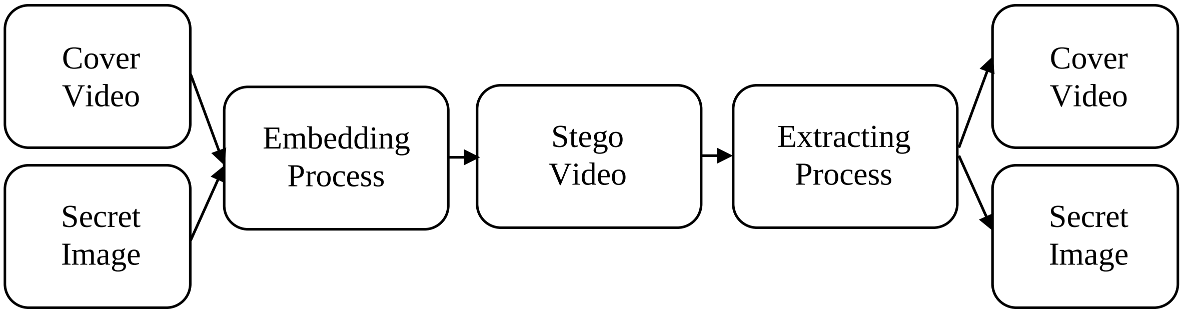


Figure 3: Main Structure of the Proposed Video Steganography Approach

- **The Embedding Process**

This process is carried out at sender side in which, a secret image is embedded inside the cover video using embedding algorithm and generate a stego video. Figure 4 shows main tasks of the proposed approach for embedding images in moving objects. Where N refers to number of frames which can be used for building background model, i.e., 10 frames as default. The technique consists of moving object detection, sorting objects, and embedding sorted objects through applying least significant bit. More details are explained in below.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

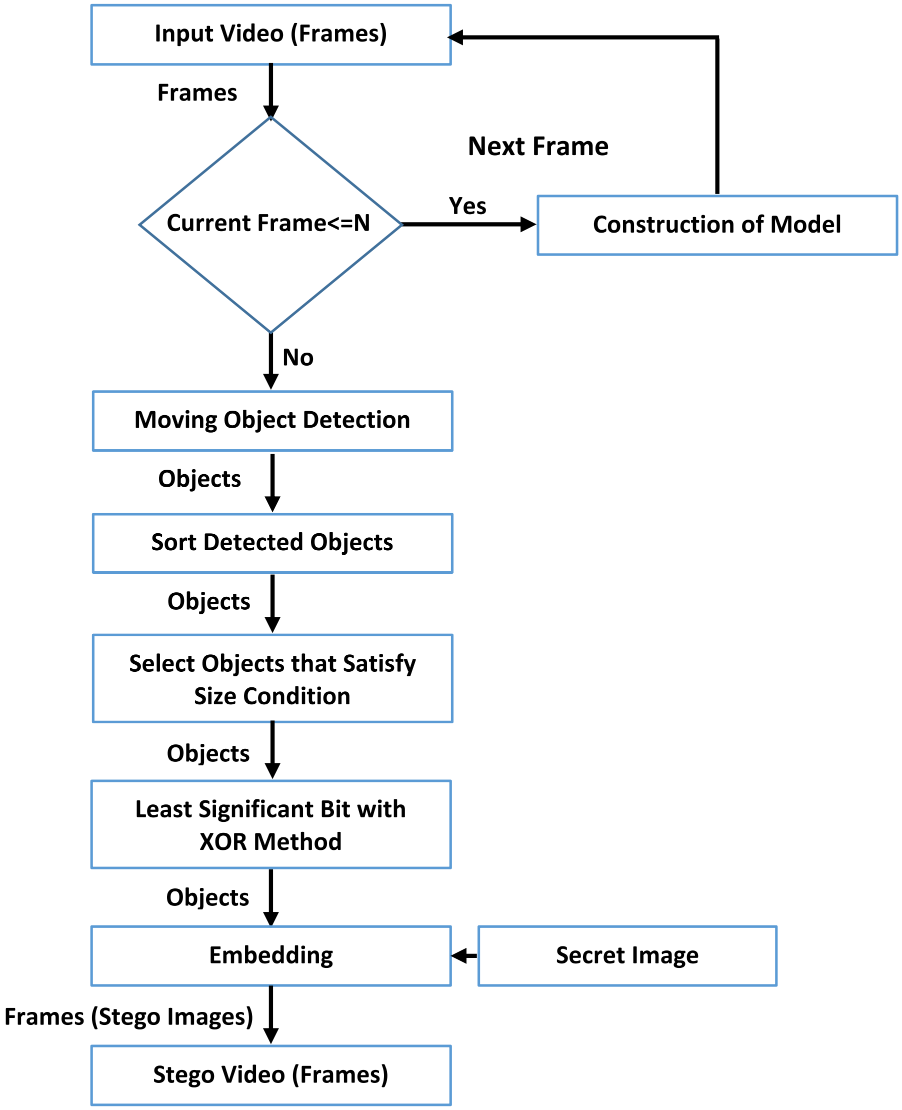


Figure 4: The General Structure of the Embedding Process of the Proposed Approach

- **Generating Background Model**

After selecting the video that is used for embedding a secret image, it is converted into frames, and the first 10 frames (as default) are used to build a background model by averaging pixels over time in an initialization period, as shown in Eq. 1 and Eq. 2. Background model can be used later in detecting a moving object, which is considered an intruder on the video and the difficulty of detecting it, and this added a layer of security to the system.

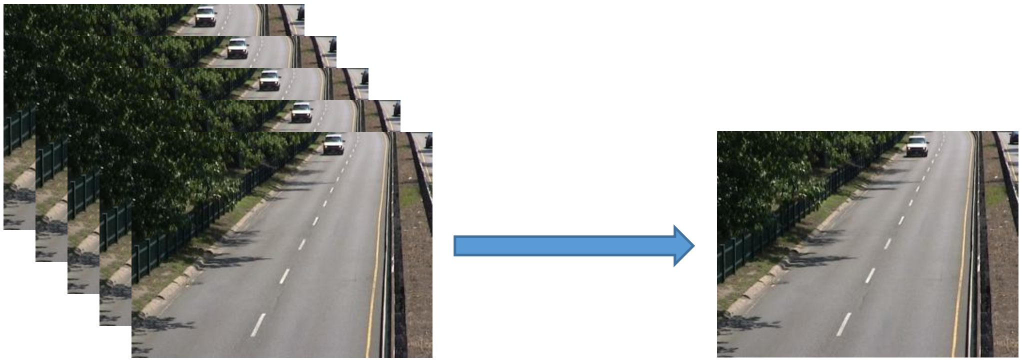
$$\mu\ (x, y, t) = \frac{\sum_{i=1}^{n} P}{n} \qquad (1)$$

$$\sigma\ (x, y, t) = \sqrt{\frac{\sum_{i=1}^{n}\ (P_i - \mu)^2}{n}} \qquad (2)$$

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

Where x and y refer to position, t refers to current time, P refers to pixel. Figure 5 shows example of generating background model.



a) n Frames selected to build background model

b) Background model

Figure 5: Example of Building Background Model from n Frames

- **Moving Object Detection**

For the purpose of accurate detection of a moving object, a hybrid model was adopted between the statistical model and the spatial model. Where the statistical model detects the object with easy and fast mathematical operations. Although the object may detected accurately, critical areas in the parts of the moving object require more analysis such as the spatial model. Here and through work integration with these two models, a good detection of the object could be achieved, and this in turn is reflected in the success of the embedding process, which provides a high embedding capacity. Eq. 3 shows calculation difference between 2 pixels from different images to detect object. Hence image frame difference (Eq. 3) at time t + 1 is defined as:

$$S\,(x, y) = |\,P\,(t+1) - \mu\,(t)\,|, \qquad (3)$$

$$S = \begin{cases} \boldsymbol{True}: Background, & if\ \ s < \sigma * 1 \\ \boldsymbol{True}: Foreground, & if\ \ s > \sigma * 3 \\ \boldsymbol{True}: Critical\ Area: Apply\ Spatial\ Model, & if\ \ s > \sigma * 1\ and\ s \le \sigma * 3 \end{cases}$$

Where x and y refer to position. t refers to current time. P refers to pixel. Calculate the mean and the sigma of 10 frames as default, i.e., background model, see previous section. s < σ * 1 means that pixels are closely distributed around the mean. Whereas s > σ * 3 means that pixels are widely spread around the mean. This image frame difference would only present some strength for the pixel positions which have updated in the two frames. Sigma can be calculated to be put on this difference image to enhance the process of object detection. At time t, if S, i.e., difference value between current pixel and mean, lies between one-sigma and three-sigma, spatial model is applied. If S greater than three-sigma, this is considered as foreground. Hence, a group of object's pixels is then created. Whereas, if S less than one-sigma, this is considered as background. Figure 6 shows flowchart of object detection using statistical model in combination with spatial model.

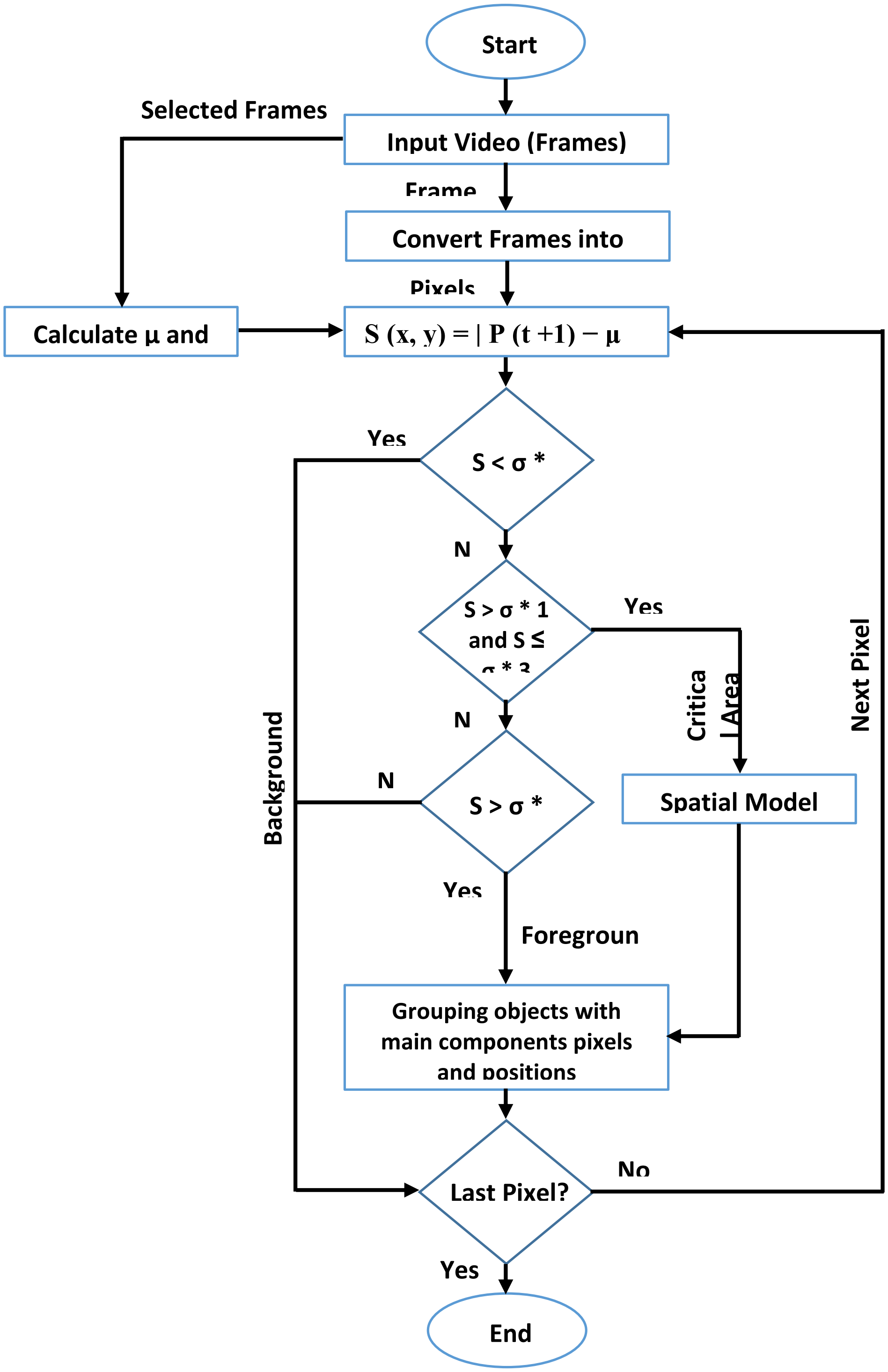
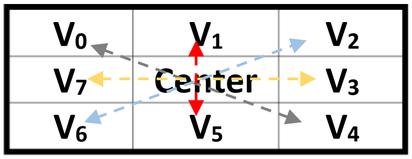


Figure 6: Flowchart Object Detection using Statistical Model in combination with Spatial Model

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

In stage of applying spatial model in this research study, Center Symmetric Local Binary Patterns (CS-LBP) can be applied to enhance the process of object detection [32]. CS-LBP provides higher stability comparing to original LBP in grey level. It calculates differences between pairs of pixels opposite with respect to the center, as shown in Figure 7.



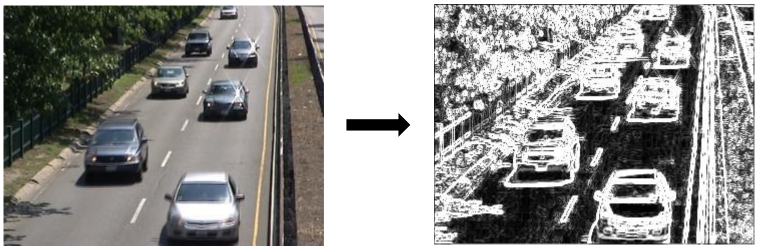
$$\longrightarrow \text{CS-LBP} = S(|V_0 - V_4|) * 2^0 + S(|V_1 - V_5|) * 2^1 + S(|V_2 - V_6|) * 2^2 + S(|V_3 - V_7|) * 2^3$$

Figure 7: CS-LBP Calculates Differences of Opposite Pixels.

Eq. 4 shows the formula of CS-LBP.

$$\mathrm{CS-LBP_T}(i,j) = \sum_{i=0}^{\left(n/_2\right)-1} S\left(|V_i - V_{i+\left(n/_2\right)}|\right) 2^i \qquad (4)$$

Where Vi and $V_i - V_{i+\left(n/_2\right)}$ are pairs of pixels that are positioned at a distance from one another on a circle of radius R. Figure 8 shows example of applying CS-LBP.



a) Highway
Frame No. 828

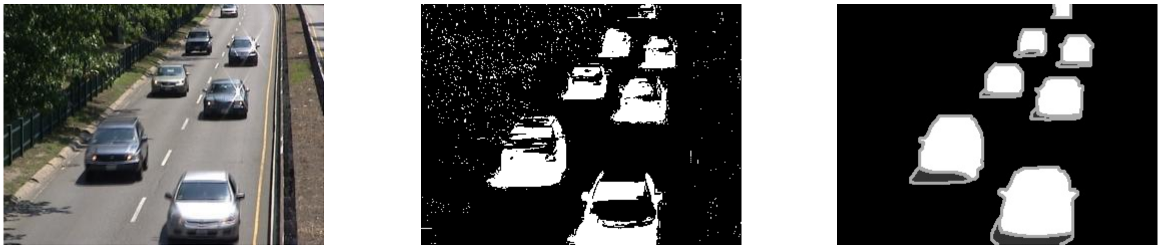
b) Highway
Frame with CS-LBP

Figure 8: Example of Applying CS-LBP.

If Eq. 3 achieved then a counter is kept incremented by 1, in addition to save current position (x, y) of pixel. If the counter is not changed, not incremented by 1, then this means that the previously analyzed pixels are considered as a new object and the counter is reset to zero for new incoming pixels. Each detected object is attached with main components pixels, and positions. Figure 8 shows example of extracted moving objects from video of highway (Frame No. 828), as well as ground truth of the frame.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652



a) Highway Frame No. 828

b) Frame with Moving Objects

c) Ground Truth Frame

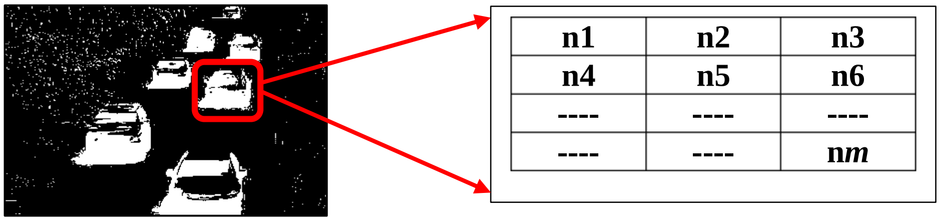
Figure 8: Example of Moving Object Detection

The steps of moving objects detection can be listed as follows:

```
Algorithm 1: Moving Object Detection
Input: Video
Output: Stego Object(s)
Step 1: Split the video cover into frames
Step 2: A is a background model initialized using n frames, i.e., 10 frames as default
Step 3: B is a cover image selected randomly from video with moving objects
Step 4: initialize T is as a set of moving objects with pixels and positions
T = {}
For each pixel in a ∈ A and b ∈ B
        Step 5: Apply Eq. 3.3 (a, b) // Moving Object Detection
        Step 6: Apply Eq. 3.4 (a, b) // CS-LBP
      Step 7: T ⟵ object with main components pixels and positions
End for
Step 6: End.
```

- **Embedding Stage**

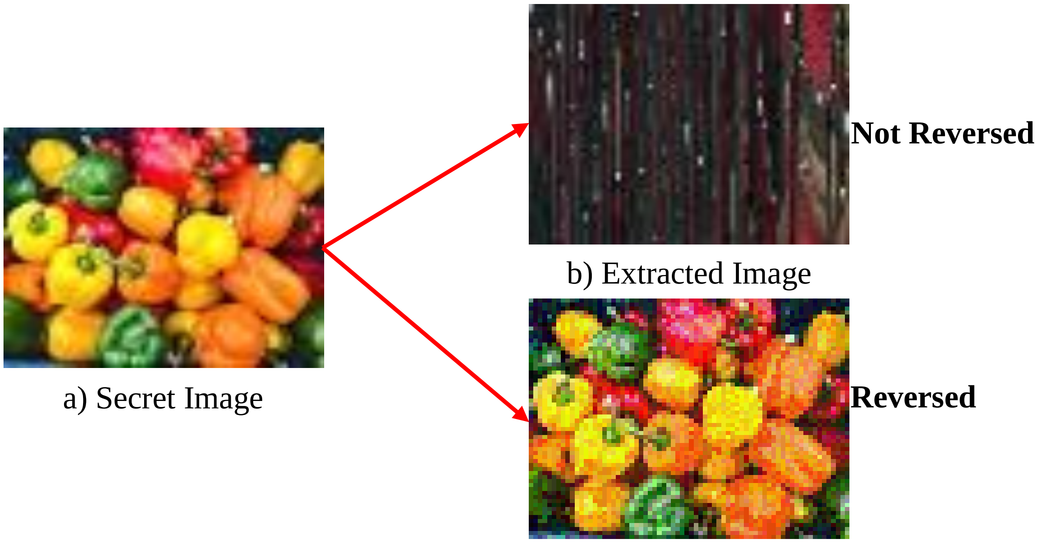
For the purpose of embedding, sort stego objects based on a size from high to low, reverse binary of pixels of image secret which can be embedded in one or more sorted stego objects. For example, assume that stego object A with 20 pixels, and stego object B with 18 pixels, and secret image S with 25 pixels. Firstly, A will be selected as biggest stego object in order to embed S. Hence, 20 pixels of S will be embedded in A, and the rest pixels (5 pixels of S) will be embedded in B._Figure 9 shows example of detected moving object with its pixels. The proposed approach chooses objects with maximum number of pixels for embedding secret data.



n1	n2	n3
n4	n5	n6
----	----	----
----	----	n*m*

Figure 9: Example of Detected Moving Object with its Pixels.

On the other hand, reversing binary of pixels of a secret image is required in order to get or retrieve the original image when extraction is applied. Figure 10 shows example of secret image with/without reversing pixels' bits.



a) Secret Image

b) Extracted Image

c) Extracted Image

Figure 10: Example of Extracted Secret Image with/without Reversing.

Example below shows example of reversing pixels' bits of a secret image in comparison with not reversing it.

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

Without Reversing Pixels' Bits

→ ***Embedding*** :

Image Secret
Pixel: 124 = 01111**011**

Cover Image
Pixel: 250 = 11111**010**

XOR Operation
011 XOR **010** = **001**

Cover Image
New Pixel = 11111**001**

→ ***Extracting*** :

Cover Image
New Pixel = 11111**001**

Cover Image
Original Pixel= 11111**010**

XOR Operation
001 XOR **010** = **011**

Image Secret
Pixel: 11111**011** = 251

→ ***Matching*** :

Image Secret
Original Pixel = 124
Extracted Pixel = 251

→ ***Differences*** :

251 – 124 = **127**

With Reversing Pixels' Bits

→ ***Embedding*** :

Image Secret
Pixel: 124 = 01111011
Reversing = 11011**110**

Cover Image
Pixel: 250 = 11111**010**

XOR Operation
110 XOR **010** = **100**

Cover Image
New Pixel = 11111**100**

→ ***Extracting*** :

Cover Image
New Pixel = 11111**100**

Cover Image
Original Pixel= 11111**010**

XOR Operation
100 XOR **010** = **110**

Image Secret
Pixel: 11111**110** = 254
Reversing = 01111111 = 127

→ ***Matching*** :

Image Secret
Original Pixel = 124
Extracted Pixel = 127

→ ***Differences*** :

127 – 124 = **3**

From the example above, it can be seen that minimum difference of original and extracted pixel may achieve through reversing bits. Hence, this may lead to extract image secret with minimum distortion. On the other hand, this process may also lead to embedding the secret image securely, and the unauthorized access may not able to reach and discover embedded data.

From the reversed bits, 3 groups are generated, 3 bits, 2 bits, and 3 bits (323 LSB, as example), embedding 3 bits with R of cover image's pixel, embedding 2 bits with G of cover image's pixel, and embedding 3 bits with B of cover image's pixel. The embedding steps are listed as follows.

```
Algorithm 2: Embedding Secret Image
Input:
S is a set of secret image's pixels
T is a set of stego objects with main components pixels and positions
C is a cover image with moving object(s)
Output: Stego Image
Step 1: initialize I as stego image
Step 2: I ← replace C's pixels
Step 3: convert R, G, and B of S's pixels of into binary
Step 4: reverse binary of R, G, and B of S's pixels
Step 5: sort T based on size, i.e., number of objects' pixels, from high to low
Step 6: initialize t ∈ T as a set of bigger object's pixels
For each secret image's pixel s ∈ S do
    If current pixel of t is the last one then
        Step 7: t ← select next bigger object's pixels
    Else if current object of T is the last one then
        Step 8: Exit Loop
    End if
    Step 9: apply XOR operation between 5th, 6th, and 7th bit of R of s and t
    Step 10: t ← replace the resulted bits with 5th, 6th, and 7th bit of R
    Step 11: apply XOR operation between 6th and 7th bit of G of s and t
    Step 12: t ← replace the resulted bits with 6th and 7th bit of G
    Step 13: apply XOR operation between 5th, 6th, and 7th bit of B of s and t
    Step 14: t ← replace the resulted bits with 5th, 6th, and 7th bit of B
    Step 15: I ← replace R, G, and B of t at current position
End for
Step 16: End.
```

- **The Extracting Process**

In order to extract hidden images from stego video, some of the main stages of the proposed approach (Figure 4) are re-applied which are background subtraction, sort objects, and least significant bit, as shown in the Figure 11. Where N refers to number of frames which can be used for building background model, i.e., 10 frames as default.

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

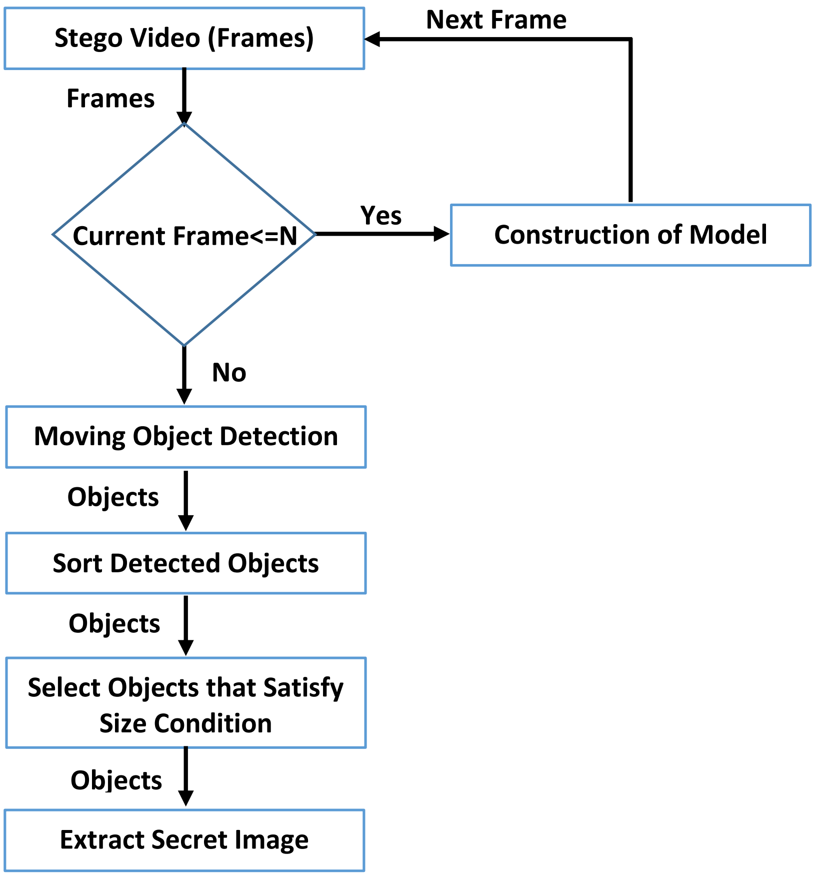


Figure 11: Flow Chart of Secret Image Extraction

The steps of extracting secret image are listed as follows.

Algorithm 3: Extracting Secret Image

Input: Stego Video
C is an original cover image
T is a set of stego objects with main components pixels and positions through applying Algorithm 3.1 (Step 1 to Step 6)
Output: Secret Image

```
Step 1: Split the stego video into frames
Step 2: initialize S as a secret image
Step 3: sort T based on size, i.e., number of objects' pixels, from high to low
Step 4: initialize t ∈ T as a set of bigger object's pixels
For each pixel c ∈ C do
    If current pixel of t is the last one then
        Step 5: t ⟵ select next bigger object's pixels
    Else if current object of T is the last one then
        Step 6: Exit Loop
```

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلـــوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

```
        End if
       Step 7: initialize s ∈ S as a pixel
       Step 8: apply XOR operation between 5th, 6th, and 7th bit of R of c and t
       Step 9: s ⟵ replace the resulted bits with 5th, 6th, and 7th bit of R
       Step 10: apply XOR operation between 6th and 7th bit of G of c and t
       Step 11: s ⟵ replace the resulted bits with 6th and 7th bit of G
       Step 12: apply XOR operation between 5th, 6th, and 7th bit of B of c and t
       Step 13: s ⟵ replace the resulted bits with 5th, 6th, and 7th bit of B
   End for
   Step 14: convert R, G, and B of S's pixels into binary
   Step 15: reverse binary of R, G, and B of S's pixels
   Step 16: End.
```

Results and Discussion

- **Experimental Environment**

The experimental results conducted for studying the performance of the proposed approach are presented and discussed in this section. A series of experiments have been carried out to explore the impact of the different features involved in the overall verification performance of the suggested approach. The suggested system is implemented using a Dell Laptop with Processor: Intel(R) Core™ i7-8550U CPU of .80 GHz, Memory: RAM 8 GB, and Storage: 500 GB. The software used to implement the system based on several programs like Visual Studio 2012, C# programming language to get results from used datasets. In addition to using an operating system consisting of Microsoft Windows 10 Professional 32-bit.

- **Dataset Description**

In this section, we present details of the experiments followed by discussion. To evaluate the proposed approach of moving object detection, the following web page http://changedetection.net/ [26] was used which consists of some ground truth dataset. Three different movies were used Highway (1700 frames), Office (2050 frames), and PETS2006 (1200 frames). Where Frame 828, Frame 1124, and Frame 982 were used as cover frames, respectively. In addition, a S2L1 video from Crowd_PETS09 dataset (220 frames) was also used for the purpose of comparison with previously proposed approaches [27].

- **Secret Image**

Three different types of secret images were used Bird (3,635 bytes), Baboon (7,178 bytes), and Pepper (5,089 bytes). The resolution is 70x60.

- **Evaluation**

The parameters used to evaluate the proposed approach are Mean Square Error (MSE) and Peak Signal Noise Ratio (PSNR).

$$MSE = \frac{1}{m * n} \sum_{m=0}^{m-1} \sum_{n=0}^{n-1} [A(i,j) - B(i,j)]^2 \qquad (5)$$

$$PSNR = 10 * log_{10} \frac{MAX_A}{MSE} \qquad (6)$$

On the other hand, evaluation metrics (Accuracy, Precision, Recall, F_Measure) are used to evaluate the proposed approach for detecting objects

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (7)$$

$$Precision = \frac{TP}{TP+FP} \qquad (8)$$

$$Recall = \frac{TP}{TP+FN} \qquad (9)$$

$$F_{Measure} = 2 * \frac{Precision \times Recall}{Precision + Recall} \qquad (10)$$

To measure the robustness of the proposed approach, two measures were used, namely the Normalized Correlation (NC) and the Bit Error Rate (BER). NC is used to measure the similarity between original and extracted secret image [28, 29]. NC is calculated as follows:

$$NC = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left[S_{original(i,j)} \times S_{extracted(i,j)}\right]}{\sum_{i=1}^{m} \sum_{j=1}^{n} S^2{}_{original(i,j)}} \qquad (11)$$

Whereas BER is used to measure the error rate between original and extracted secret image. BER can also be defined as ratio between number of incorrectly decoded bits (i.e., bit errors) and total number of bits [30, 31]. BER is computed as follows:

$$BER = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left[S_{original(i,j)} \oplus S_{extracted(i,j)}\right]}{m \times n} \qquad (12)$$

- **Experimental Results**

Figures 12 to 14 show comparison between the proposed approach with applying CS-LBP and without applying CS-LBP based on Accuracy, Precision, Recall, and F_Measure.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

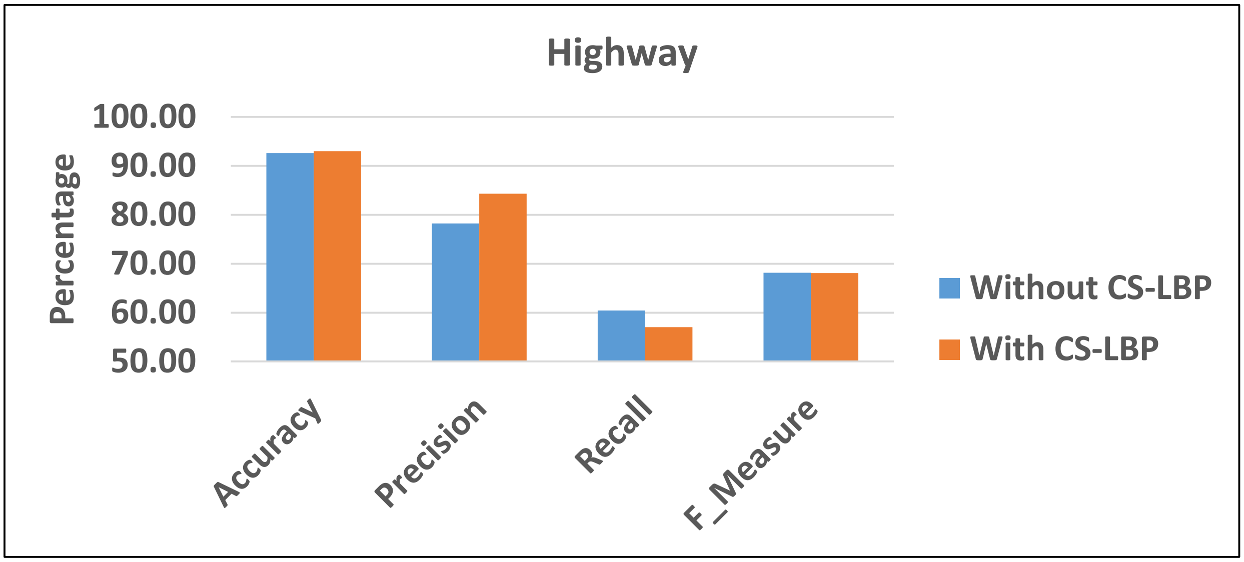


Figure 12: Reported results with Highway

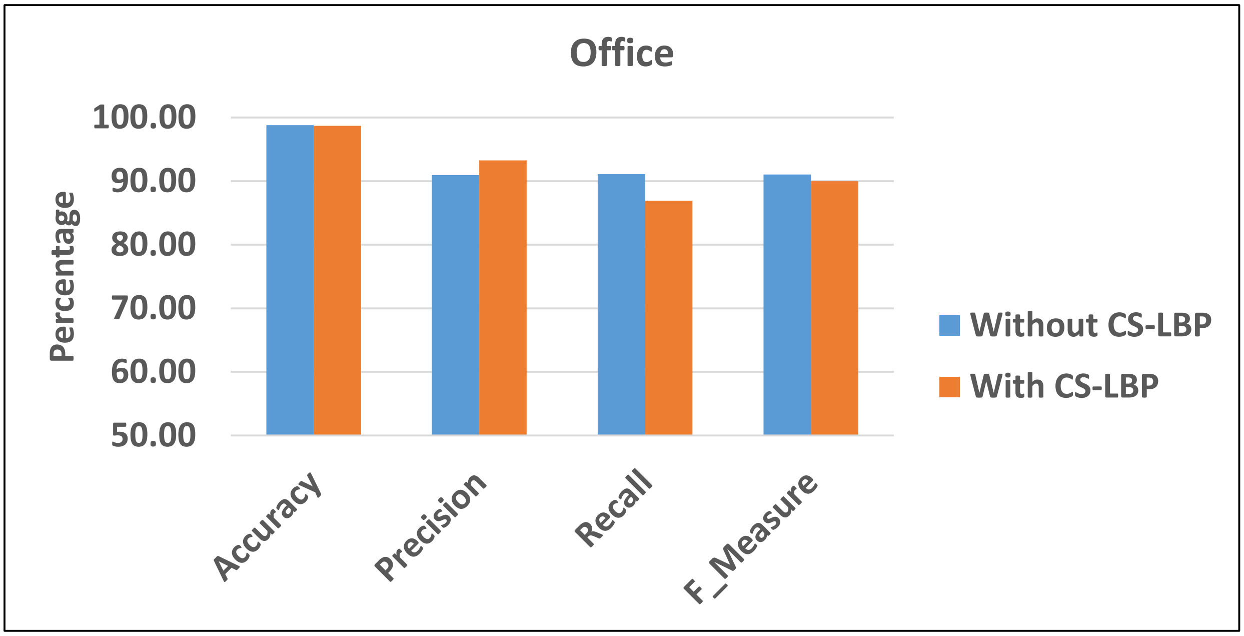


Figure 12: Reported results with Office

مجلة جامعة بابل للعلـــوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

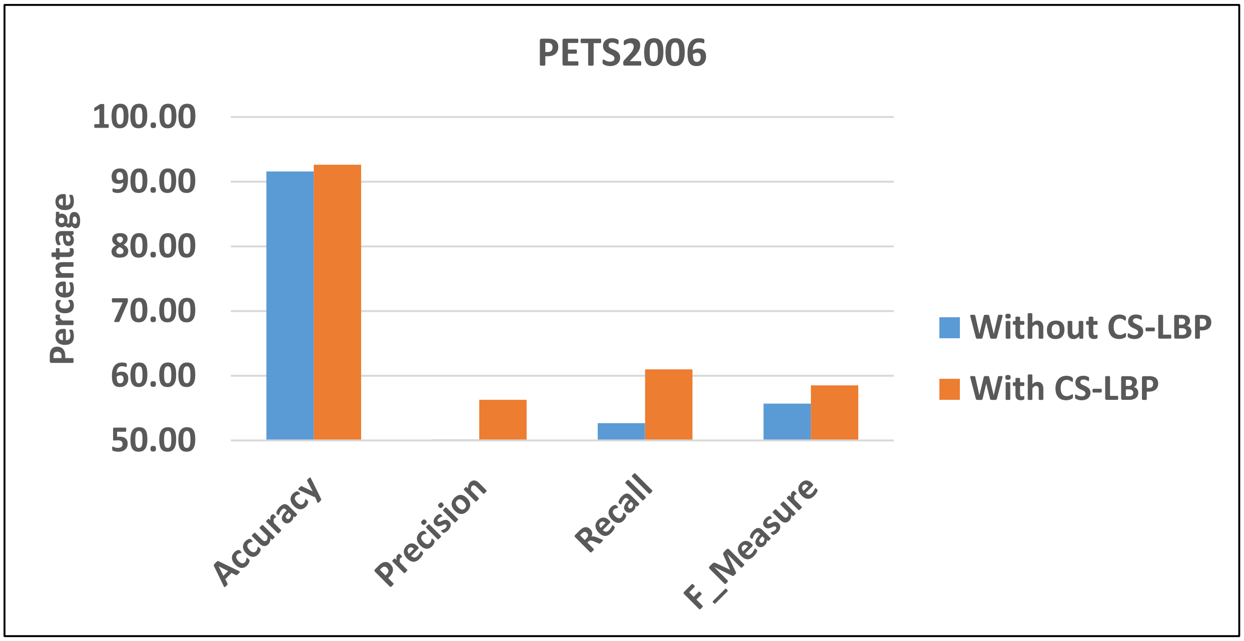


Figure 14: Reported results with PETS2006

The reported precision with applying CS-LBP is higher in all aspects. If an approach is designed and developed for high accuracy and precision, then the feasibility of detecting all moving objects on a given video enhances, i.e., detects region of interest for embedding purposes. On the other hand, if recall is increased it is possible that some of the region of interest left undetected.

Crowd_PETS09 dataset has been also used for the purpose of comparison with previously proposed approaches Mstafa et al 2017 [16] and Roselinkiruba et al 2022 [23]. The average value of reported PSNRs is 61.47. It is higher comparing to the reported PSNR of Mstafa et al 2017 [16] and Roselinkiruba et al 2022 [23], 49.01 and 44.57, respectively.

To test the robustness of the proposed approach, the well-known steganalysis attacks were applied on stego-image which are Salt and Pepper noise (i.e., white and black), Gaussian Noise, and Median filter [16]. Where the attack was applied after embedding the secret images. Figure 16 shows reported results in terms of NC and BER. Where d refers to density, and v refers to variance. They were set to two different values 0.01 and 0.001, respectively as stated in [16], and applied with 323LSB style.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

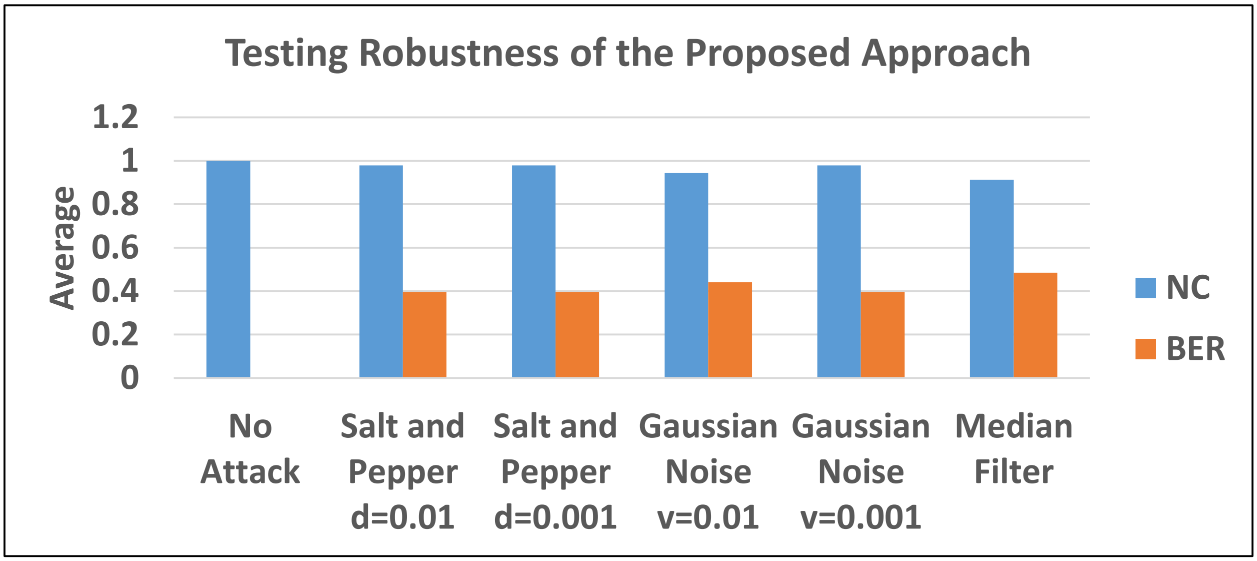


Figure 15. Testing Robustness of the Proposed Approach

According to the reported results in Figure 15, the proposed approach is considered as robust against attack according to the reported values of NC and BER.

The experiments were re-conducted with embedding in movie (more than one frame, or multi-frames). The experiments labelled as Experiment A, Experiment B, Experiment C, and Experiment D as shown in Table 2 which illustrates types of the experiments that are used to evaluate the proposed approaches. These four experiments used the same data set, and applied with 323LSB style. For the purpose of evaluation, average values of MSE and PSNR were calculated, respectively.

Table 2: Types of the Experiments

Experiment	Type of Experiment
Experiment A	Embedding secret image in one frames of video, where a frame hiding 100% of the secret image.
Experiment B	Embedding secret image in two frames of video, where each frame hiding 50% of the secret image.
Experiment C	Embedding secret image in four frames of video, where each frame hiding 25% of the secret image.
Experiment D	Embedding secret image in ten frames of video, where each frame hiding 10% of the secret image.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

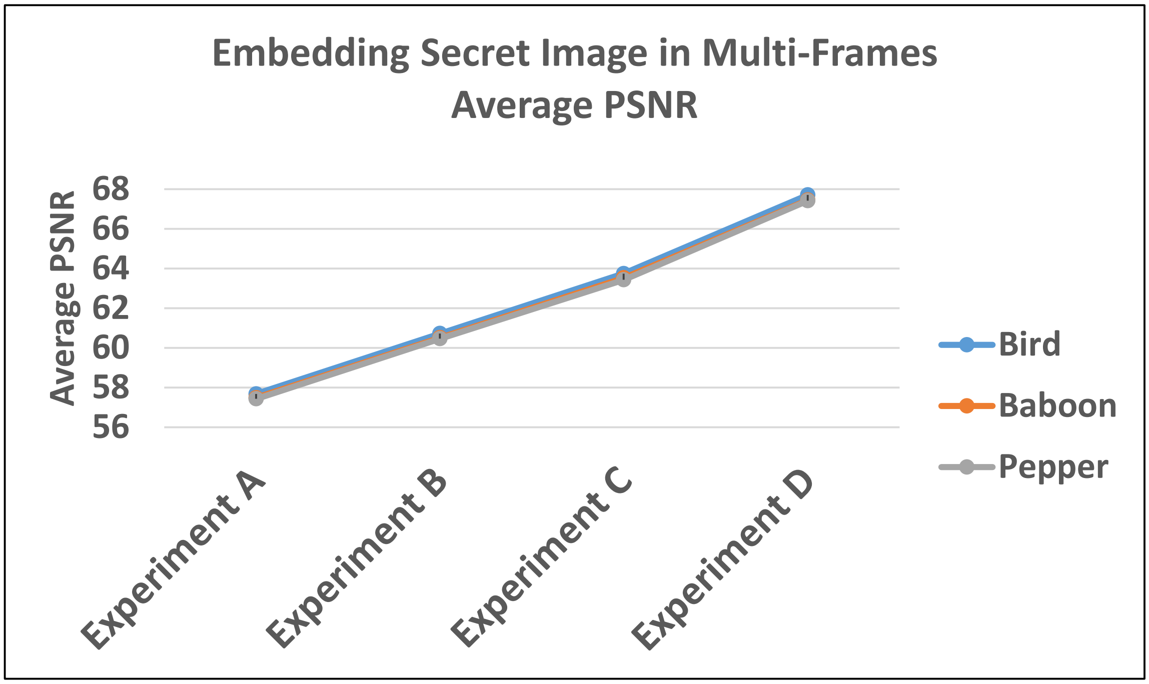


Figure 16: Reported results with Embedding in Videos (Multi-Frames)

Figures 16 shows comparison in terms of average PSNR, it can be seen that PSNR increased gradually, when a secret image embedded in many frames. Hence, the maximum the number of frames, the maximum the PSNR value. Also, it provides more security and imperceptibility as the data was hidden in the moving objects and the updates are difficult to notice rather than the static region in a video.

Steganography is a technique to protect sensitive data. It enables a system to transmit information without the risk of the signals being intercepted. Data security is to prevent unauthorized access, use, disclosure, interruption, change, or erasure of data and data structures. In a way that does not allow the human vision system to detect it, thus the effective method of data hiding using steganography. This research study introduced an approach with the following properties:

1. Hide images inside the moving object in a video by separating the objects from the background of the frame. As the moving object is considered an intruder on the scene, and the difficulty of tracking it.
2. Selecting and arranging objects according to size for the purpose of embedding secret image.
3. This approach is to be distinguished from existing steganography techniques in that, the proposed approach is also capable of detecting moving objects and extracting the secret images without distortion. Where no keys are used or required at the receiver side.
4. The approach can thus be exploited for the implementation of different LSB styles.

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

5. In moving object detection, using the statistical model may not achieve its goal of correct and integrated detection of the moving objects. Hence the spatial model was applied in combination with the statistical model in this research study to achieve this goal and for a critical area only, where the moving objects are detected in an integrated and correct manner.
6. The experimental proof of the proposed approach can successfully detect and embed a secret image. Also, it provides more security and imperceptibility as the data is hidden in the moving objects and the updates in the moving objects are difficult to notice compared the static region in a video.

Conflict of interests.

There are non-conflicts of interest.

References

[1] S. Kumar, “Image Steganography Using Improved LSB And Exor Encryption Algorithm,” Master thesis, Thapar University Patiala, 2014.

[2] E. Cole, *Hiding in plain sight steganography and the art of covert communication*. Indianapolis: Wiley, 2003.

[3] A. Nilizadeh, S. Nilizadeh, W. Mazurczyk, C. Zou, and G. T. Leavens, “Adaptive matrix pattern steganography on RGB images,” *Journal of Cyber Security and Mobility*, vol. 11, no. 1, pp. 1-28, Sep. 2021.

[4] M. G. Abdul Sahib, “Foreground Object Detection Based on Chrominance and Texture Features with Enhancement by Canny Filter,” *Iraqi Journal of Information Technology*, vol.9, no. 2, p. 171, 2018.

[5] G. Paramesh, K. V. Pavithra, N. Ranjitha, S. Swetha, and T. Anushalalitha, “Video Steganography using MATLAB,” *EAI Endorsed Transactions on Cloud Systems*, vol. 3, no. 10, p. 153493, 2017.

[6] M. Hussain, A. W. Wahab, Y. I. Idris, A. T. S. Ho, and K.-H. Jung, “Image steganography in spatial domain: A survey,” *Signal Processing: Image Communication*, vol. 65, pp. 46-66, Aug. 2018.

[7] S. K. Pal, A. Pramanik, J. Maiti, and P. Mitra, “Deep learning in multi-object detection and tracking: State of the art,” *Applied Intelligence*, vol. 51, no. 9, pp. 6400–6429, May 2021.

[8] H. S. T. Al-Dmour, Enhancing information hiding and segmentation for medical images using novel steganography and clustering fusion techniques, PhD Thesis, 2018.

[9] M. M. Msallam, “A Development of Least Significant Bit Steganography Technique,” *Iraqi Journal of Computer Communications Control and System Engineering*, vol. 20, no. 1, pp. 31–39, 2020.

[10] P. Bose, S. K Bandyopadhyay, and V. Goyal, “A graphical based video steganography,” *Preprints*, Jun 2021, doi: 10.20944/preprints 202105.0176.v1.

[11] M. Dalal, M. Singh, A. Kumar, Charu, and M. Juneja, “An approach of data hiding in video steganography using object detection,” *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5, pp. 2460–2466, 2019.

[12] N. Rabade and Y. S. Thakur, “Different Steganography Techniques and Stego Keys used in Digital Images Processing-A Review,” *International Research Journal of Modernization in Engineering Technology and Science*, vol. 5, no. 2, pp. 852-859, 2023.

[13] S. Prabhsimran, S. Nitish, and K. Sukhmanjit, "A Brief Study of Steganography on Different Cover Media's Using LSB Substitution Method," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 5, 2015.

[14] A. T. Hashim, H. A. Yossra, and S. G. Susan, "Developed method of information hiding in video AVI file based on hybrid encryption and steganography," *Eng. & Tech. Journal*, Vol. 29, No. 2, 2011.

[15] R. J. Mstafa and K. M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes," *Multimedia Tools and Applications*, vol. 75, no. 17, pp. 10311–10333, Dec. 2015.

[16] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, "A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC," *IEEE Access*, pp. 5354-5365, 2017.

[17] 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 and Applications*, vol. 76, no. 6, pp. 8597–8626, May 2016.

[18] G. P. Rajkumar and V. S. Malemath, "Video Steganography: Secure Data Hiding Technique," *International Journal of Computer Network and Information Security*, vol. 9, no. 9, pp. 38-45, 2017.

[19] M. Hemalatha, G. Manisha, P. Mounika, S. K. Saleema, and K. L. Prasanna, "Matlab Code for Video Steganography," *Journal of Information and Computational Science*, vol. 10, no. 6, pp. 78-92, 2020.

[20] V. D R and A. B. J, "A Novel Secure Data Hiding Technique into Video Sequences Using RVIHS," *International Journal of Computer Network & Information Security*, vol. 13, no. 2, pp. 53-65, May 2021.

[21] M. Dalal and M. Juneja, "A survey on information hiding using video steganography," *Artificial Intelligence Review*, 54(8), 5831-5895, Mar. 2021.

[22] S. R. M. Mirah and J. J. Majid, "Secure Video Steganography Method Using LSB and MSB with Triple XOR Operation," *Journal of University of Babylon for Pure and Applied Sciences*, pp. 243-256, 2021.

[23] R. Roselinkiruba, T. S. Shar, and J. K. J. Julina, "A novel pattern-based reversible data hiding technique for video steganography," *Preprint*. 2022.

[24] A. Nilizadeh, S. Nilizadeh, W. Mazurczyk, C. Zou, and G. T. Leavens, "Adaptive matrix pattern steganography on RGB images," *Journal of Cyber Security and Mobility*, vol. 11, no. 1, pp. 1-28, Sep. 2021.

[25] M. A. Naser, S. M. Al-alak, A. M. Hussein, and M. J. Jawad, "Steganography and cryptography techniques based secure data transferring through Public Network Channel," *Baghdad Science Journal*, vol. 19, no. 6, p. 1362, 2022.

[26] Y. Wang, P.-M. Jodoin, F. Porikli, J. Konrad, Y. Benezeth, and P. Ishwar, "CDnet 2014: An expanded change detection benchmark dataset," *2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 387-394, 2014.

[27] J. Ferryman and A. Shahrokni, "PETS2009: Dataset and Challenge," *2009 Twelfth IEEE International Workshop on Performance Evaluation of Tracking and Surveillance*, pp. 1-6, 2009.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

[28] H. B. Karaman and S. Sagiroglu, “An application based on Steganography,” In *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, pp. 839-843, Sep.012.

[29] J. Mary Jenifer, S. Raja Ratna, J. B. Shajilin Loret, and D. Merlin Gethsy, “A survey on different video steganography techniques,” In *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, pp. 627-632, 2018.

[30] Y. He, G. Yang, and N. Zhu, “A real-time dual watermarking algorithm of H.264/AVC video stream for video-on-demand service,” *AEU - International Journal of Electronics and Communications*, vol. 66, no. 4, pp. 305–312, May 2012.

[31] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, “A Robust and imperceptible dual watermarking for telemedicine applications,” *Wireless Personal Communications*, vol. 80, no. 4, pp. 1415-1433, 2015.

[32] D. Chandraja, “Methodology and Extensions of Local Binary Pattern: A Survey,” *International Journal of Advance Computational Engineering and Networking (IJACEN)*, vol. 3, no. 10, pp. 17-24, 2015.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652