

DOI: <https://dx.doi.org/10.21123/bsj.2023.7926>

Building a Statistical Model to Detect Foreground Objects and using it in Video Steganography

Mithal Hadi Jebur*¹  Fanar Ali Joda²  Mohammed Abdullah Naser¹ 

¹Department of Computer Science, College of Science for Women, University of Babylon, Babylon, Iraq.

²Department of Air Conditioning and Refrigeration Techniques Engineering, Al-Mustaqbal University College, Babylon, Iraq.

*Corresponding author: mithal.jebur.gsci13@student.uobabylon.edu.iq

E-mail addresses: fanaralijoda@uomus.edu.iq , wsci.mohammed.abud@uobabylon.edu.iq

Received 9/10/2022, Revised 25/2/2022, Accepted 26/2/2023, Published Online First 20/4/2023,
Published 01/12/2023



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Abstract:

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. 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 XOR technique is used with reverse bits between the secret image bits and the detected moving object bits for embedding. The proposed method 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. The experimental results showed the better visual quality of the stego video with PSNR values exceeding 58 dB, this indicates that the proposed method works without causing much distortion in the original video and transmitted secret message.

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

Introduction:

Data transfer over the internet is becoming increasingly frequent in today's digital media. This means that data security is now the most important issue on the internet. The number of invasions is closely connected to the volume of data that is sent. This necessitates that the data be sent over the internet in a secure way. Confidential data transmission over internet is one of the most challenging difficulties in the contemporary digital era. Therefore, there are two separate kinds of security measures accessible for transferring secret information^{1,2}.

- The art of steganography, and
- The science of cryptography.

Steganography is by far the most popular method used for the protection of sensitive data. It is used for the purpose of concealing the confidential data behind a cover medium. The cover media concealed the confidential data by encoding it in such an effective manner that it is next to impossible to extract the primary data from it. There are several different cover media to choose from while engaging in steganography. The specifics of it are shown in Fig. 1.

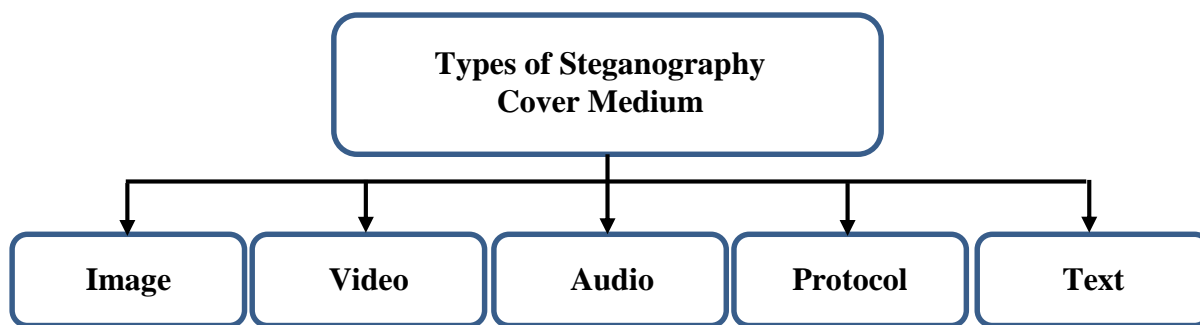


Figure 1. Different kinds of cover mediums for steganography

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. There are some of techniques used nowadays LSB Coding, Phase Coding, ECHO Hiding, Spread Spectrum, and Tone Insertion as steganography techniques³. However, 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 intact⁴. 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. Several academics have come up with a slew of different methods for detecting objects in a video⁵. The drawbacks of basic background removal approaches have been solved by using the statistical properties of individual pixels. They are motivated by background removal techniques in terms of maintaining and dynamically updating statistics of pixels that are part of the background process. Comparison of pixel statistics with those of the background model helps to identify foreground pixels. This method is becoming more popular because of its dependability in scenarios with noise, shifting light, and shadows of any kind⁶. However, the current work is as an attempt to embed sensitive data inside the digital video, based on the technology of detecting the moving object in the video.

The rest of the paper is organized as follows. The Section 2 provides a brief introduction to objects detection. Section 3, describes related works. The proposed approach is discussed in Section 4. Whereas Section 5 presents the evaluation of the performance of the proposed approach.

Object Detection:

Computer vision is concerned with the detection of moving objects and their subsequent classification and recognition. The primary goal of moving object detection is to identify objects in a video sequence that are moving in relation to the background scene. The background is assumed to be stationary in the case of a stationary camera. In order to detect moving objects, optical flow, temporal differencing, and background subtraction are all used in tandem⁷.

Visual elements (i.e., shape, texture, and color) and motion information are the two primary sources of information in a video that may be utilized to recognize and track objects. The statistical analysis of visual characteristics and the temporal analysis of motion information have been suggested as robust methodologies. Color and texture may be used to segment a frame into many sections, which can then be combined based on motion vectors that are comparable to each other⁸. This is a usual method, and it can be used to a wide range of images. Several academics have come up with a slew of different methods for detecting objects in a video. There is a lot of overlap and interconnection between distinct approaches in some of them which makes it extremely difficult to classify current techniques in a consistent manner^{9, 10}.

Related Works:

Some of the latest contributions proposed in the field of video steganography discussed in this section where embedding is applied in a video using various embedding techniques.

In Hashim *et al*¹¹, this approach contains an AVI hidden information system development. The AVI file is divided 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 methods are used in this approach, the first method is the least significant bit (LSB) to embed one bit into blue channel of a pixel, and the second method is the Haar Wavelet Transform (HWT). HWT scans the pixel in horizontal and vertical directions (i.e., from left to right, and from top to bottom, respectively) to perform addition and subtraction on neighboring pixels.

Vinay and Ananda¹², 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.

Mstafa *et al*¹³, proposed secure video steganography algorithm using the multiple object tracking (MOT) algorithm and error correcting codes. In the 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.

In Paramesh *et al*¹⁴, they proposed an approach for hiding secret information in video. LSB is used to embed data in video frames. XOR operations were also used to encrypt information with using keys.

In Rajkumar *et al*¹⁵, another approach was proposed for embedding information at the background of video frames. Where an encryption algorithm is used to encrypt the data, and then LSB encoding is applied to embed the encrypted data in the video frames.

In M.Hemalatha *et al*¹⁶, 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 relevant key used to select the pixel coefficient, and the encryption key used to decrypt it to get the original data.

Nilizadeh *et al*¹⁷ proposed an approach called Adaptive Matrix Pattern (AMP), which divides an image into blocks (i.e., non-overlapped square-sized), and generates matrix pattern (i.e., a unique codebook) for each ASCII character in each image block. Where each ASCII character receives a different 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.

Mirah and Majid¹⁸ proposed an approach for embedding the secret message using the Least Significant Bit (LSB). In this approach, the XOR operator is used for embedding stage with three keys. However, this approach is designed for embedding the secret message in a frame without identifying or detecting the objects.

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

Table 1. Summary of Reported Literature

Author(s) and Year of Publication	Embedding Technique	Detection Moving Objects	Embedding in Objects	Embedding in Background
Hashim <i>et al</i> ¹¹	LSB and HWT	No	No	Yes
Vinay and Ananda ¹²		No	No	Yes
Mstafa <i>et al</i> ¹³	LSB, DWT, and DCT	Yes	Yes	No
Paramesh <i>et al</i> ¹⁴	LSB	No	No	Yes
Rajkumar <i>et al</i> ¹⁵	LSB	No	No	Yes
M.Hemalatha <i>et al</i> ¹⁶	AES	No	No	Yes
Nilizadeh <i>et al</i> ¹⁷	AMP	No	No	Yes
Mirah and Majid ¹⁸	LSB	No	No	Yes

The Proposed Approach

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. Fig. 2, shows main tasks of the proposed approach for embedding images in moving objects. The technique consists of

moving object detection, sorting objects, and embedding sorted objects through applying least significant bit. More details are explained in below.

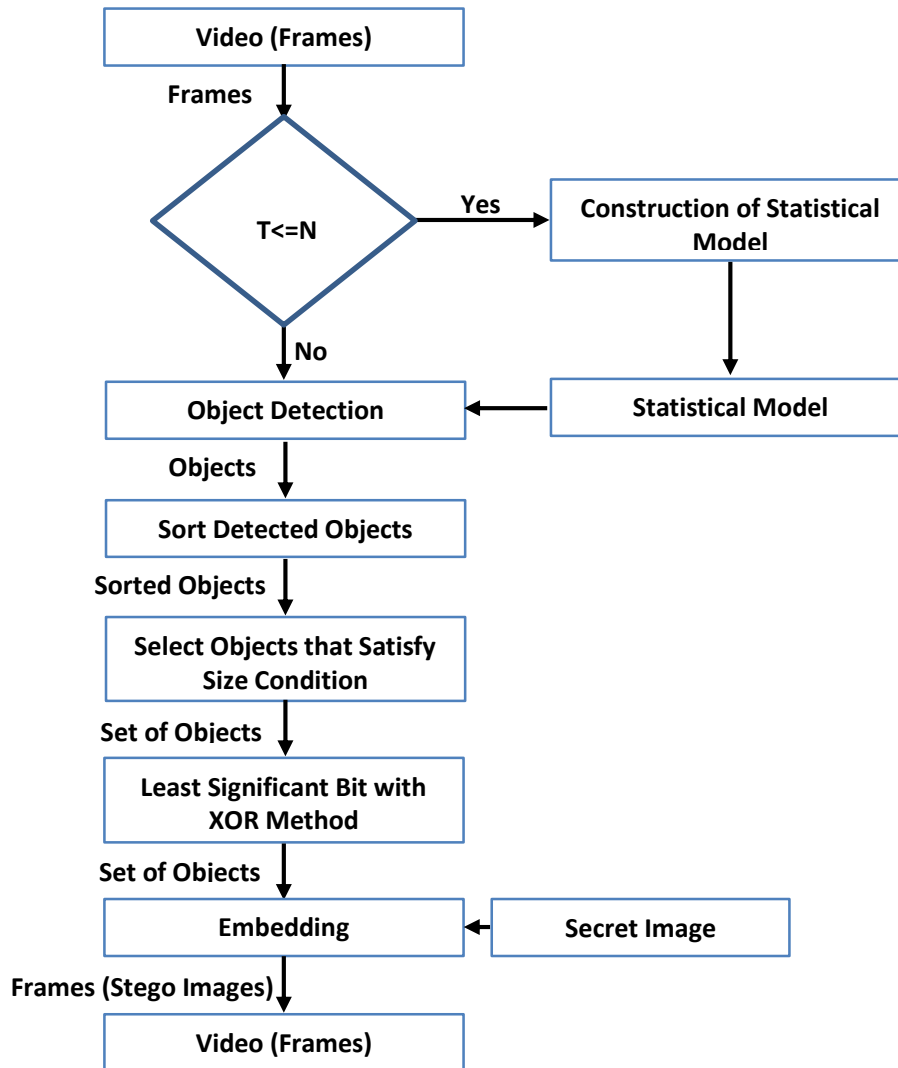


Figure 2 . The General structure of the proposed approach

Moving Object Detection:

In this stage, objects are detected through applying statistical model. Eq. 1, shows calculation difference between 2 pixels from different images to detect object. Hence, image frame difference (Eq. 1) at time t + 1 is defined as:

$$V(x, y, t + 1) - V(x, y, t) > (\sigma * 3) + \mu \quad 1$$

Where calculating three-sigma, there are three standard deviations above the mean of 10 frames as default, x and y refer to position, t refers to current time. At time t, a frame is considered as background model. 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 moving object detection, as shown in Fig. 3.

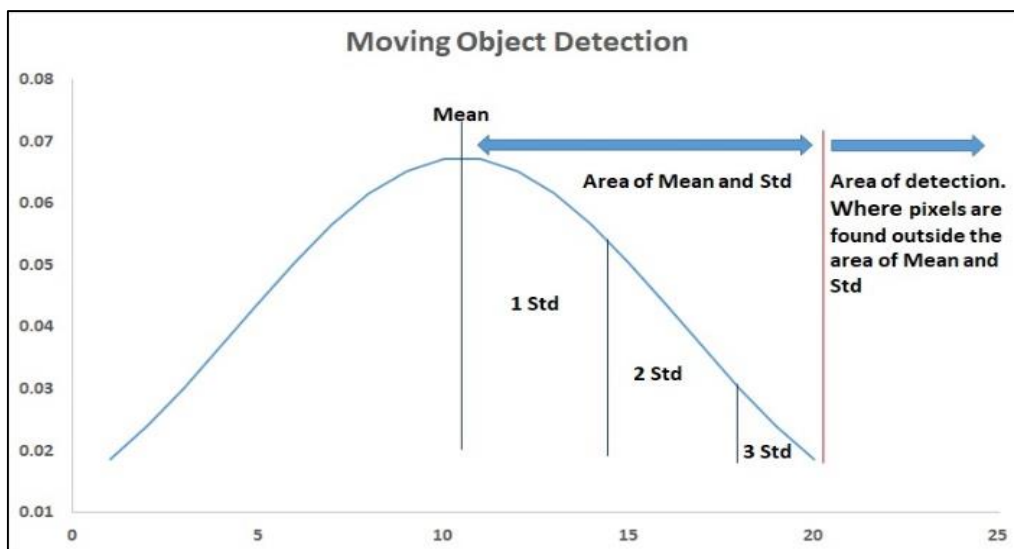


Figure 3. Moving Object Detection

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

Algorithm 1: Object Detection

Input: Video

Output: Stego Objects

Step 1: reading and splitting the video cover into frames, and selecting a group of frames (n frames, as example) to generate mean frame (X),

Step 2: selecting a specific frame of cover image (Y).

Step 3: converting the pixels of X and Y into binary.

C = 0, pixels counter of stego object

T = {}, stego objects with pixels and positions // Objects Detection

For i = 1 to n

For j = 1 to n

Step 4: Calculating μ and σ from group of frames (n frames, as example)

Step 5: Pixel1 = pixel of X(i,j)

Step 6: Pixel2 = pixel of Y(i,j)

If (Pixel1 - Pixel2) > ($\sigma * 3$) + μ then // Eq. 1

Step 7: C = C + 1

Step 8: T = object with main components pixels and positions

End if

next j

next i

Step 4: End.

If Eq. 1 achieved, then a counter is kept incremented by 1, in addition to saving 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.

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. 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 pixel of cover image, embedding 2 bits with G of pixel of cover image, and embedding 3 bits with B of pixel of cover image. The steps of embedding can be listed as follows.

Algorithm 2: Embedding Secret Image

Input: Cover Image, Secret Image, Stego Objects

Output: Stego Image

Step 1: reading cover image (C), and reading secret image (S)

Step 2: converting R, G, and B of each pixel of S into binary

Step 3: reversing binary of R, G, and B of each pixel of S

Step 4: T = stego objects of C with main components pixels and positions // Objects Detection

Step 5: sorting T based on a size from high to low

m = 0 // an index counter for pixels of T

For i = 1 to n

For j = 1 to n

Step 6: P1 = pixel of S(i,j)

If current pixel of T is the last one then

Step 7: get bigger object of T

Step 8: m = 0

End if

Step 9: m = m + 1

Step 10: P2 = pixel of T(m)

Step 11: applying XOR operation between 5th, 6th, and 7th bit of R of P1 and P2

Step 12: replacing the resulted bits with 5th, 6th, and 7th bit of R of P2

Step 13: applying XOR operation between 6th and 7th bit of G of P1 and P2

Step 14: replacing the resulted bits with 6th and 7th bit of G of P2

Step 15: applying XOR operation between 5th, 6th, and 7th bit of B of P1 and P2

Step 16: replacing the resulted bits with 5th, 6th, and 7th bit of B of P2

next j

next i

Step 17: End.

Step 1: reversing binary of 8 bits to become 11011110 = 222,

Step 2: embedding the reversed binary (in Step 1), generating 3 groups of bits (8 bits = 3R – 2G – 3B LSB) as follows:

Group 1 = 3 bits 110 to be embedded with R of pixel P,

Group 2 = 2 bits 10 to be embedded with G of pixel P,

Group 3 = 3 bits 110 to be embedded with B of pixel P.

Step 3: Assuming R of pixel P = 11111010, applying XOR between Group 1 and the last 3 bits of R, and replacing the resulted bits with R of cover image, as shown in Fig. 4,

Worked Example:

Assuming that a pixel of an image with R equals to 123 = 01111011, G equals to 123 = 01111011, and B equals to 123 = 01111011.

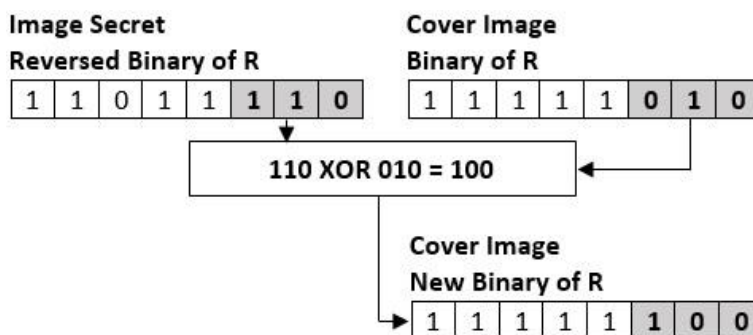


Figure 4. XOR Operation of R Value

Step 4: Assuming G of pixel P = 10110100, applying XOR between Group 2 and the last 2 bits

of G, and replacing the resulted bits with G of cover image, as shown in Fig. 5.

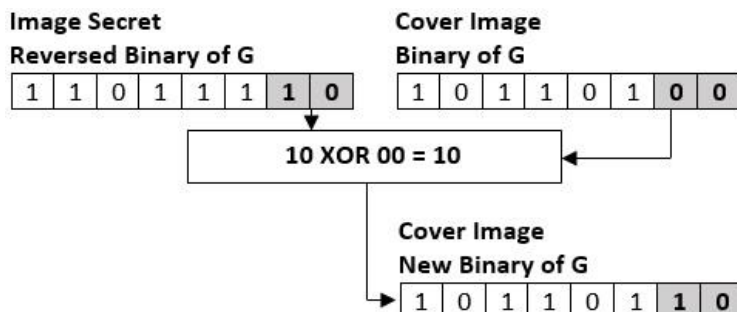


Figure 5. XOR Operation of G Value

Step 5: Assuming B of pixel P = 00111100, applying XOR between Group 3 and the last 3 bits

of B, and replacing the resulted bits with B of cover image, as shown in Fig. 6.

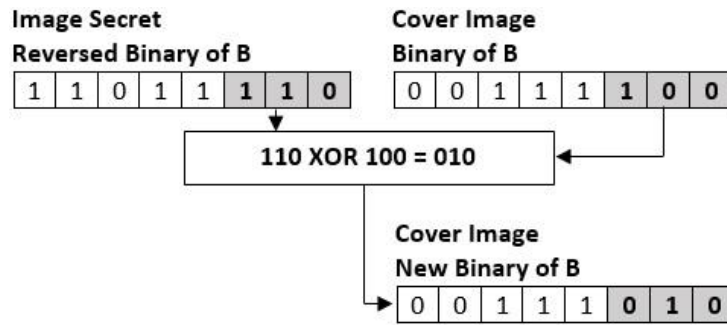


Figure 6. XOR Operation of B Value

Extracting Stage

In order to extract hidden images from stego video, some of the main stages of the proposed approach

Fig. 3 are re-applied which are background subtraction, sort objects, and least significant bit, as shown in the figure below.

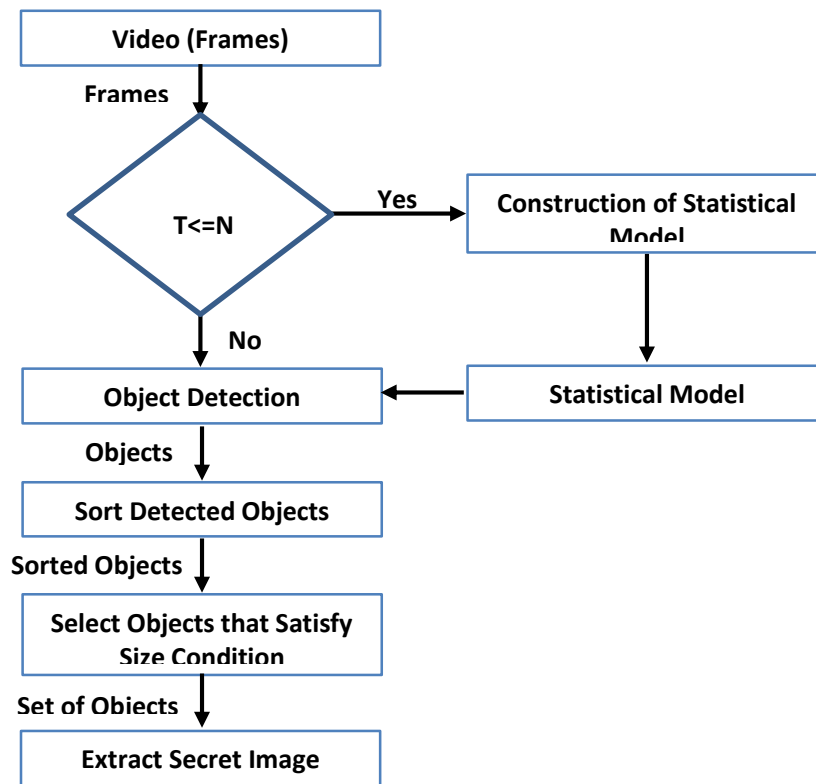


Figure 7. Flow Chart of Extracting Secret Image

The steps of extracting secret image can be listed as follows.

Algorithm 3: Extracting Secret Image

Input: Stego Video

Output: Secret Image

Step 1: selecting a frame randomly from stego video as cover image (C), and $S = \{ \}$ // secret image

Step 2: converting R, G, and B of each pixel of C into binary

Step 3: T = get stego objects with main components pixels and positions from the stego video (see steps in Algorithm 2 in Section 4.2)

Step 4: sorting T based on a size from high to low
 $m = 0$ // an index counter for pixels of T

For $i = 1$ to n

For $j = 1$ to n

Step 5: $P1 = \text{pixel of } C(i,j)$

If current pixel of T is the last one then

Step 6: get bigger object of T

Step 7: $m = 0$

End if

Step 8: $m = m + 1$

Step 9: $P2 = \text{pixel of } T(m)$

Step 10: applying XOR operation between 5th, 6th, and 7th bit of R of P1 and P2

Step 11: replacing the resulted bits with 5th, 6th, and 7th bit of R of S(i,j)

Step 12: applying XOR operation between 6th and 7th bit of G of P1 and P2

Step 13: replacing the resulted bits with 6th and 7th bit of G of S(i,j)

Step 14: applying XOR operation between 5th, 6th, and 7th bit of B of P1 and P2

Step 15: replacing the resulted bits with 5th, 6th, and 7th bit of B of S(i,j)

next j
next i

Step 16: reversing binary of R, G, and B of each pixel of S

Step 17: End.

Please note that here in this stage, XOR is also applied between new binary of cover image and the original one as shown in the figures below.

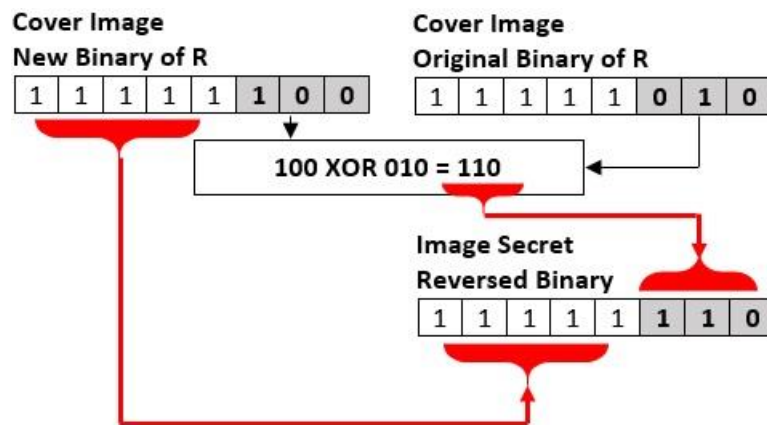


Figure 8. XOR Operation of R Value (Extracting Stage)

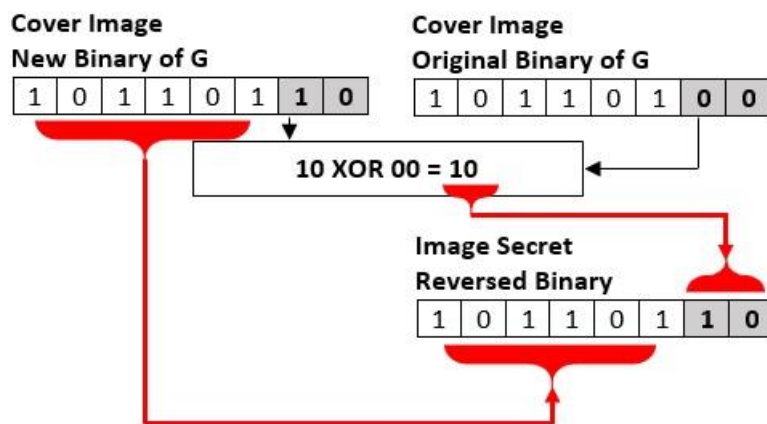


Figure 9. XOR Operation of G Value (Extracting Stage)

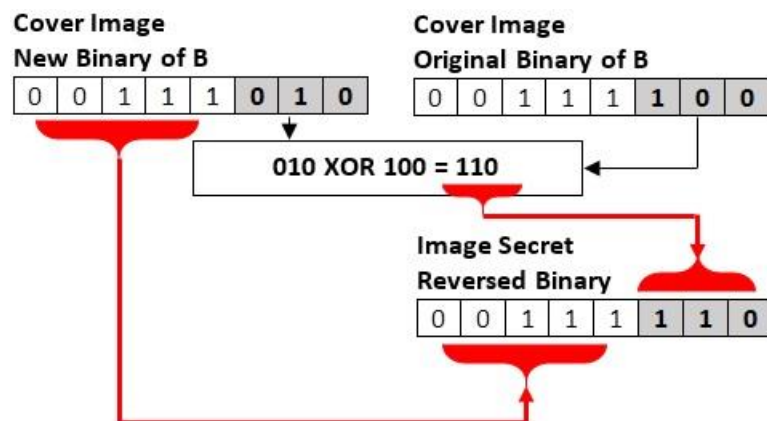


Figure 10. XOR Operation of B Value (Extracting Stage)

Experimental Results:

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://www.cvg.rdg.ac.uk/>¹⁹ was used which consists of some ground truth dataset. Two different movies were used Highway and Office. Where Frame 258 and Frame 1124 were used as cover image, respectively.

The proposed approach is implemented using Visual Studio 2012, C# programming language. The experiments of this research study are run on a computer with an Intel Core i7 -8550U CPU @ 1.80GHz 2.00 GHz frequency and 8 GB of memory.

Secret Image

Three different types of secret images were used Bird, Baboon, and Pepper where high equals to 70 and width equals to 60, size equals to 3.55 kb, 7.01 kb, and 4.97 kb, respectively.

Evaluation

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

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

$$PSNR = 10 * \log_{10} \frac{MAX_A}{MSE}$$

Experimental Results:

Table 2. Reported results with Highway
































Cover Image	Secret Image	LSB Style	Stego Image	Stego Object	Extracted Image	MSE	PSNR
		323LSB				0.10321	57.99378
		233LSB				0.15173	56.32021
		332LSB				0.18273	55.51262
		323LSB				0.10879	57.76502
		233LSB				0.14565	56.49770
		332LSB				0.17298	55.75080
	323LSB				0.11179	57.64672	
	233LSB				0.13651	56.77926	
		332LSB				0.18373	55.48899

Table 3. Reported results with Office

Cover Image	Secret Image	LSB Style	Stego Image	Stego Object	Extracted Image	MSE	PSNR
		323LSB				0.09287	58.45203
		233LSB				0.13789	56.73538
		332LSB				0.16692	55.90577
		323LSB				0.09627	58.29609
		233LSB				0.13362	56.87211
		332LSB				0.15862	56.12714
		323LSB				0.09808	58.21513
		233LSB				0.12420	57.18956
		332LSB				0.16500	55.95584

Tables 2 and 3 show the reported results of Highway and Office with different secret images and LSB styles. It can be seen that high PSNR is registered with 323 LSB style (Table 3), where PSNR equals to 58.45203. Although lower PSNR is reported at the other LSB styles, secret images are extracted successfully without distortion and accurately from stego images which consists of stego objects.

Table 4. Comparison of Results

Approach	PSNR
Proposed Approach	58.45
Mirah <i>et al</i> ¹⁷	55.97
Vinay and Ananda ¹²	55.43
Hashim <i>et al</i> ¹⁶	50.00
Mstafa <i>et al</i> ¹³	49.01
Paramesh <i>et al</i> ¹⁴	30.00

The embedding of secret image of the proposed approach was compared with the previously proposed approaches in the literature in terms of PSNR rate. Table 4 shows comparison of results between existed approaches and the proposed approach of this research study. It can be seen that the proposed approach reported higher PSNR

comparing to the other approaches. The existed approaches are either designed for a specific LSB style or require keys at the receiver side. In addition, in some of these approaches, the higher the *n*-bit LSB size or the data size, the PSNR value decreased. The reason behind this is that it might be designed for embedding secret data in a specific part of an object only which may identify or selected in advance, i.e., human faces or any other parts of objects.

Conclusions:

This paper introduced an approach to hide images inside the moving object in a video on the basis of separating the objects from the background of the frame, selecting and arranging them according to size for the purpose of embedding secret image. This approach is to be distinguished from existing steganography techniques in that, the proposed approach is also capable of detecting the moving objects and extracting the secret images without distortion. Where no keys are used or required at the receiver side. The approach can thus be exploited for the implementation of different LSB styles. 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. However, future work in video steganography set out by this research paper can be conducted in the following directions. Further development to the proposed approach in this area can be done by applying spatial model in combination with statistical model. Applying additional LSB styles to evaluate the ability of the proposed approach in detecting moving objects, evaluating the robustness of the proposed approach against different attacks such as salt and pepper noise and median filtering.

Authors' Declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in University of Babylon, Iraq.

Authors' Contributions:

FAJ and MAN designed the study. MHJ performed coding, experiments, and validation. Fanar and Mithal analyzed the data. Mithal wrote the paper. FAJ and MAN reviewed the paper. FAJ and MAN did revision and proofreading.

References:

1. Raju R, Philip FM. Video steganography in haar wavelet domain based on multiple object tracking and error correction codes. *Int Res J Eng Technol.* 2018; 5(04): 3985-3990. <https://www.irjet.net/archives/V5/i4/IRJET-V5I4890.pdf>.
2. Msallam MM. A Development of Least Significant Bit Steganography Technique. *Iraqi J Comput, Comm, Control and Sys Eng.* 2020 Jan 1; 20(1): 31-9. <https://doi.org/10.33103/uot.ijccce.20.1.4>.
3. Dalal M, Juneja M. A survey on information hiding using video steganography. *Artif Intell Rev.* 2021 Dec; 54(8): 5831-95. <https://doi.org/10.1007/s10462-021-09968-0>.
4. Jenifer JM, Ratna SR, Loret JS, Gethsy DM. A survey on different video steganography techniques. In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE. 2018 May 11: 627-632. <https://doi.org/10.1109/ICOEI.2018.8553847>.
5. Pal SK, Pramanik A, Maiti J, Mitra P. Deep learning in multi-object detection and tracking: state of the art. *Appl Intell.* 2021 Sep; 51(9): 6400- 6429. <https://doi.org/10.1007/s10489-021-02293-7>.
6. Shtayt BA, Zakaria NH, Harun NH. A comprehensive review on medical image steganography based on LSB technique and potential challenges. *Baghdad Sci J.* 2021 Jun 20; 18:957-974. [http://dx.doi.org/10.21123/bsj.2021.18.2\(Suppl.\).0957](http://dx.doi.org/10.21123/bsj.2021.18.2(Suppl.).0957).
7. Chapel MN, Bouwmans T. Moving objects detection with a moving camera: A comprehensive review. *Comput Sci Rev.* 2020 Nov 1; 38: 100310. <https://doi.org/10.1016/j.cosrev.2020.100310>.
8. Naser MA, Al-alak SMK, Hussein AM, Jawad MJ. Steganography and Cryptography Techniques Based Secure Data Transferring Through Public Network Channel. *Baghdad Sci J.* 2022 Dec. 1; 19(6): 1362. <https://bsj.uobaghdad.edu.iq/index.php/BSJ/article/view/6142>.
9. Sahib MG. Foreground Object Detection Based on Chrominance and Texture Features with Enhancement by Canny Filter. *Iraqi J Inf. Technol.* 2018; 9(2): 171-193. <https://www.iasj.net/iasj/download/a247a1734195fd25>.
10. Ogla RA. Symmetric-Based steganography technique using spiral-searching method for HSV color images. *Baghdad Sci J.* 2019 Dec 1; 16(4): 0948-9060. <https://doi.org/10.21123/bsj.2019.16.4.0948>.
11. Hashim AT, Ali YH, Ghazoul SS. Developed method of information hiding in video AVI file based on hybrid encryption and steganography. *Eng Tech J.* 2011; 29(2): 359-373. <https://uotechnology.edu.iq/depts/mypdf/research/2011/r9.pdf>.
12. Vinay DR, Ananda BJ. A Novel Secure Data Hiding Technique into Video Sequences Using RVIHS. *Int J Commun Netw Inf Secur.* 2021 Apr 1; 13(2): 53-65. <https://doi.org/10.5815/ijcnis.2021.02.05>.
13. Mstafa RJ, Elleithy KM, Abdelfattah E. A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC. *IEEE access.* 2017 Apr 6; 5: 5354-5365. <https://doi.org/10.1109/ACCESS.2017.2691581>.
14. Paramesh G, Pavithra KV, Ranjitha N, Swetha S, Anushalalitha T. Video Steganography using MATLAB. *EAI Endorsed Trans. cloud syst.* 2017 Dec 20; 3(10): 1-7. <https://doi.org/10.4108/eai.20-12-2017.153493>.
15. Rajkumar GP, Malemath VS. Video Steganography: Secure Data Hiding Technique. *Int J Comput Net Info Sec.* 2017 Sep 1; 9(9). <https://doi.org/10.5815/ijcnis.2017.09.05>.
16. Hemalatha M, Manisha G, Mounika P, Saleema SK, Prasanna KL. Matlab Code for Video Steganography. *J Info Comput Sci.* 2020; 10(6): 87-92. <https://doi.org/10.12733/JICS.2020.V10I6.535569.12510>.
17. Nilizadeh A, Nilizadeh S, Mazurczyk W, Zou C, Leavens GT. Adaptive matrix pattern steganography on RGB images. *J. Cyber Secur. Mobil.* 2021; 11(1): 1-28. <https://doi.org/10.13052/jcsm2245-1439.1111>.

18. Mirah SR, Jawad MJ. Secure Video Steganography Method Using LSB and MSB with Triple XOR Operation. J Univ Babylon pure appl Sci. 2021 Dec 1; 29(3): 243-56. <https://www.journalofbabylon.com/index.php/JUBPAS/article/view/3981/2998>.
19. Paul M, Haque SM, Chakraborty S. Human detection in surveillance videos and its applications-a review. Eurasip J Adv Signal Process. 2013 Dec; 2013(1): 1-6. <https://doi.org/10.1186/1687-6180-2013-176>.

بناء نموذج إحصائي لكشف الأجسام الأمامية واستخدامه في إخفاء المعلومات بالفيديو

مثال هادي جبر¹ * فخر علي جودة² محمد عبدالله ناصر²

¹قسم علوم الحاسوب، كلية العلوم للبنات، جامعة بابل، بابل، العراق.
²قسم هندسة تقنيات التبريد والتكييف، كلية المستقبل الجامعة، بابل، العراق.

الخلاصة:

أصبح إخفاء المعلومات بالفيديو خيارًا شائعًا لحماية البيانات السرية من محاولات القرصنة والهجمات الشائعة على الإنترنت. ومع ذلك ، عند استخدام إطار (إطارات) الفيديو بالكامل لتضمين بيانات سرية قد تؤدي إلى تشويه بصري. 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. أظهرت النتائج التجريبية جودة بصرية أفضل لفيديو stego مع قيم PSNR تتجاوز 58 ديسيبل ، وهذا يشير إلى أن الطريقة المقترحة تعمل دون التسبب في تشويه كبير في الفيديو الأصلي والرسالة السرية المرسل.

الكلمات المفتاحية: إخفاء الصور بالفيديو ، LSB ، تضمين الصورة السرية ، استخراج الصورة السرية، تشفير XOR ، كشف الأجسام المتحركة.