JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)

ARTICLE
Vol.29; No.3. October-December | 2021

# Secure Video Steganography Method Using LSB and MSB with Triple XOR Operation

**Shahad Rafeeq Musa Mirah[1]** **Majid Jabbar Jawad[2]**

**[1] Department of Computer Science, College of Science for Women, Babylon University, Iraq**
shahad.jaffer.gsci33@student.uobabylon.edu.iq .
2 Department of Computer Science, College of Science for Women, Babylon University, Iraq
wsci.majid.jabbar@uobabylon.edu.iq

Corresponding author Email: shahad.jaffer.gsci33@student.uobabylon.edu.iq .

**Received:** 25/10/2021 **Accepted:** 29/11/2021 **Published:** 1/12/2021

## Abstract

Steganography is the science and art of hiding a secret message in a cover media, without any imperceptible changing in the it. Steganography can be applied in several media such as image, audio, video. This project suggested video steganography method for preserving the confidentiality which is the important requirement in the security field. Two domains namely spatial and frequency domains can be used in the video steganography for embedding the secret message. In this method, a spatial domain basing on the Least Significant Bit (LSB) is used for embedding the secret message. In order to satisfying the security requirement, the philosophy of cryptography is used in the suggested method. In this method the XOR operator is used with embedding operation. XOR is used with three keys in order to increase the security layer. In addition, according to the experimental results, the suggested method satisfied the imperceptibility requirement which is very important requirement in the image steganography field. The experiment results show that the value of all PSNR values (after embedding the secret message in more than cover image) are more than 50dB which mean that the suggested method reduced the distortion that may be occur in the cover after embedding the secret message.

## Key words:

Video Steganography, Information Hiding, Information Security

## Citation:

**Shahad Rafeeq Musa Mirah[1]&Majid Jabbar Jawad[2]. Secure Video Steganography Method Using LSB and MSB with Triple XOR Operation.** Journal of University of Babylon for Pure and applied science (**JUBPAS**). October-December , 2021. Vol.29; No.3: 243-256

## 1. Introduction

It is wildly known the internet importance and its impact on everyday life in all the fields of life. Since it provides the speed and ease of communication and information processing, however, this revolution in the internet world came with many challenges is One of the most important challenges in internet security. Since it has a large impact on the privacy, integrity, and accessibility of the internet, therefore, many theoretical and practical approaches to secure communication between the internet application is developed since the invention of the internet. And it is still updated field because of the many challenges arise each time a new solution is given. One of the very important parts of internet security is data encryption. Data encryption is a subfield of information security. Which is concerned about reconstructing the data in a way that only the intended party could access it. The motivation is that the data is hidden from unauthorized parties. Thus, the field of information hiding occurred.

Information hiding general field consists of two subdisciplines, steganography and watermarking. For the first glance, they may seem similar to each other. But steganography is an approach to hide data in other data. For example, they were hiding data (e.g. message, image, audio) in another data form, like hiding a secret message in image. So, if an unauthorized person accesses the image, he/she will not be able to access the secret message. While watermarking has the goal of protecting the intellectual property of the media (e.g. books, images, audio) [1].

## 2. The Existing Working

A large number of schemes have been suggested for hiding image in video based on the Steganography techniques. Herein some works related to the above procedure.

In 2020, M.Hemalatha, G.Manisha, P.Mounika, SK.Saleemaand ,Mrs. K.L Prasanna [2] This article aims to improve the security of secret data that communicate through video files by hiding the data using the technology cryptography .The input video file is converted into frames , and then the video is encrypted using AES encryption. And choose one of the frames to hide the secret data for secure data communication. Suggested technology After the data is encrypted, the data concealer uses an adaptive embedding algorithm to hide the secret encrypted data in the selected frame. Encryption improve many security aspects , it makes secret information difficult to identify and has no meaning. In the extraction, the secret data is extracted using the relevant key used to select the pixel coefficient, and the encryption key is used to decrypt it to obtain the original data. Finally, using images and data to analyze the performance of the program in terms of encryption and hidden data.

In 2017 , Paramesh.G1, Pavithra.K.V2 , Ranjitha.N3, Swetha.S4 and T.Anushalalitha5[3] This article discusses a video steganography technique that can provide acceptable security and high computational speed by embedding secret information in video uses LSB technology to embed data in video frames. Prior to this, symmetric XOR operations were used to encrypt confidential information, this way provides two levels of security : Data Hiding and Extraction procedure, With the amount

of data that can be embedded in it, this method is more efficient than other methods and shows a PSNR of more than 30 dB.

In 2017,Gat Pooja Rajkumar and Dr V. S. Malemath.[4] This article makes use of the idea of video steganography, wherein information is hidden at the back of video frames. This article gives tiers of safety for the facts : Steganography and cryptography. The data is encrypted using an encryption algorithm, and then the encrypted data is embedded in the video frame. The LSB encoding technique used to embed data. And it is used very commonly , because it can embed a large amounts of data in simply and efficient way.

In 2016, Bharti Chandel , Dr.Shaily Jain [5] , Steganography is a technology for concealed protection and concealment of multimedia information. It can also be said to be the study of invisible communication. Steganography is a mixture of compression, encryption, watermarking and cryptography. Generally Steganography uses images, text, video, and audio to hide confidential information. In this research , video steganography is analyzed . Video steganography involves including secret information in a video to protect it from intruders. In this article, the basic concepts, performance indicators and security of video steganography is analyzed. Various methods are being explored to protect confidential information by using video as cover .

In 2011, Ashawq T. Hashim, Dr.Yossra H. Ali [6] This article contains an AVI hidden information system development. Based on steganography technology to prevent attacker from accessing the secret information. This work use the combination of steganography and cryptography techniques to improve security so that the information can't be accessed by attackers. In this work, the AVI file is divided into two parts, video and audio. The video is a combination of frames ; each frame is saved as a BMP file image, and several frames that are needed or needed are selected as the cover. The Type-3 Feistel network is the encryption algorithm that used, it is used domestically and used to make exportable use useful, and the variable length key will make it more difficult for attackers to perform cryptanalysis. Two concealment methods are used in this work, the first method is the least significant bit (LSB), and the second method is the Haar wavelet transform (HWT). The proposed hidden information system was tested using standard subjective measurement methods, such as mean square error (MSE) and peak signal-to-noise ratio (PSNR). All measurement results gained as test results show good results for PSNR (over 50 dB) and increase with the number of frames used for coverage.

## 3. The Proposed Method

Figure 1 illustrates the overall block diagram of the suggested project. The suggested project includes two schemes:

- Embedding process
- Extraction process

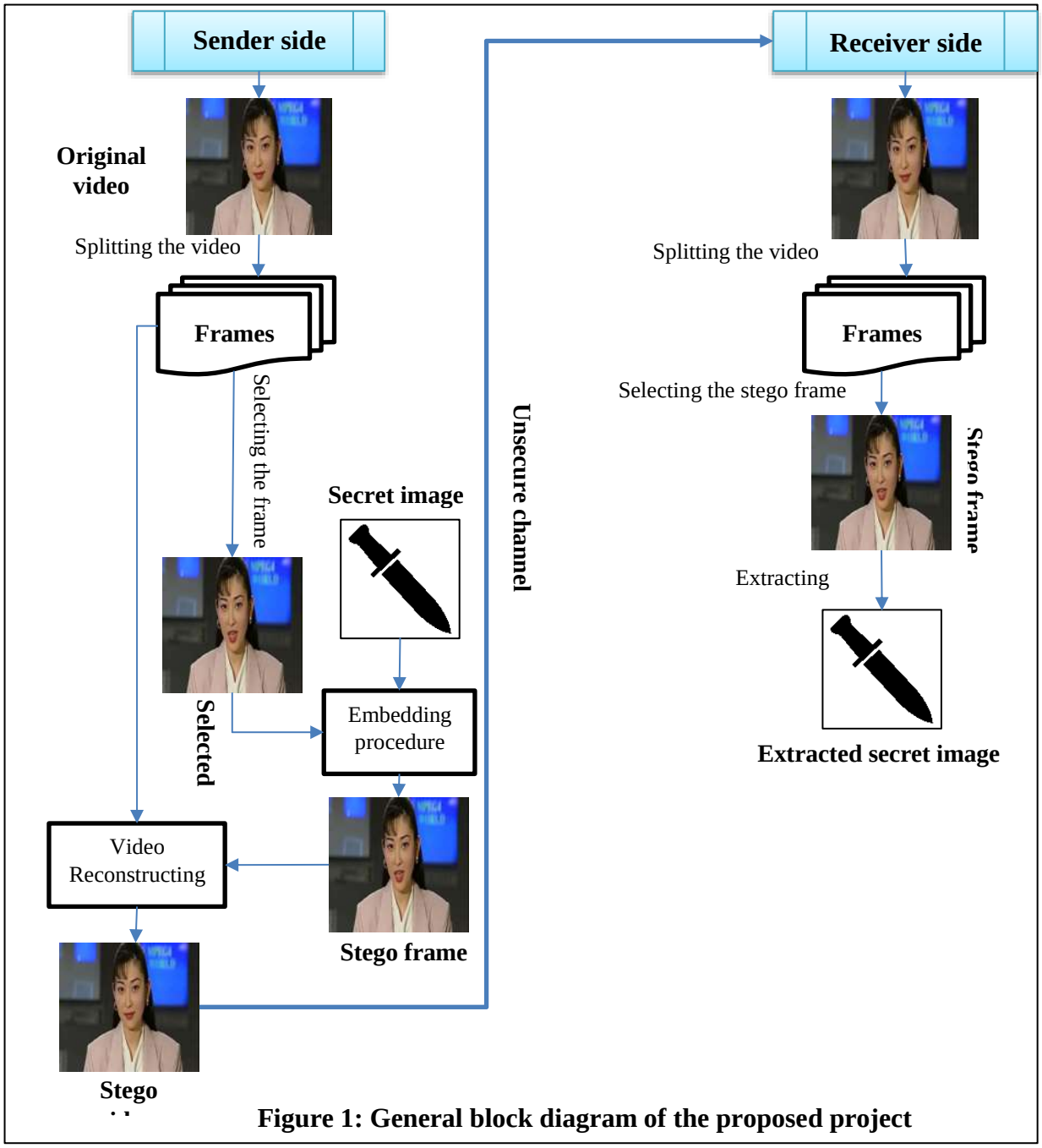


**Figure 1: General block diagram of the proposed project**

### 3.1 The Embedding process

Figure 2 illustrates the embedding process. In this process, the video chosen firstly. Then a desired frame is selected in order to be cover for embedding the secret image.

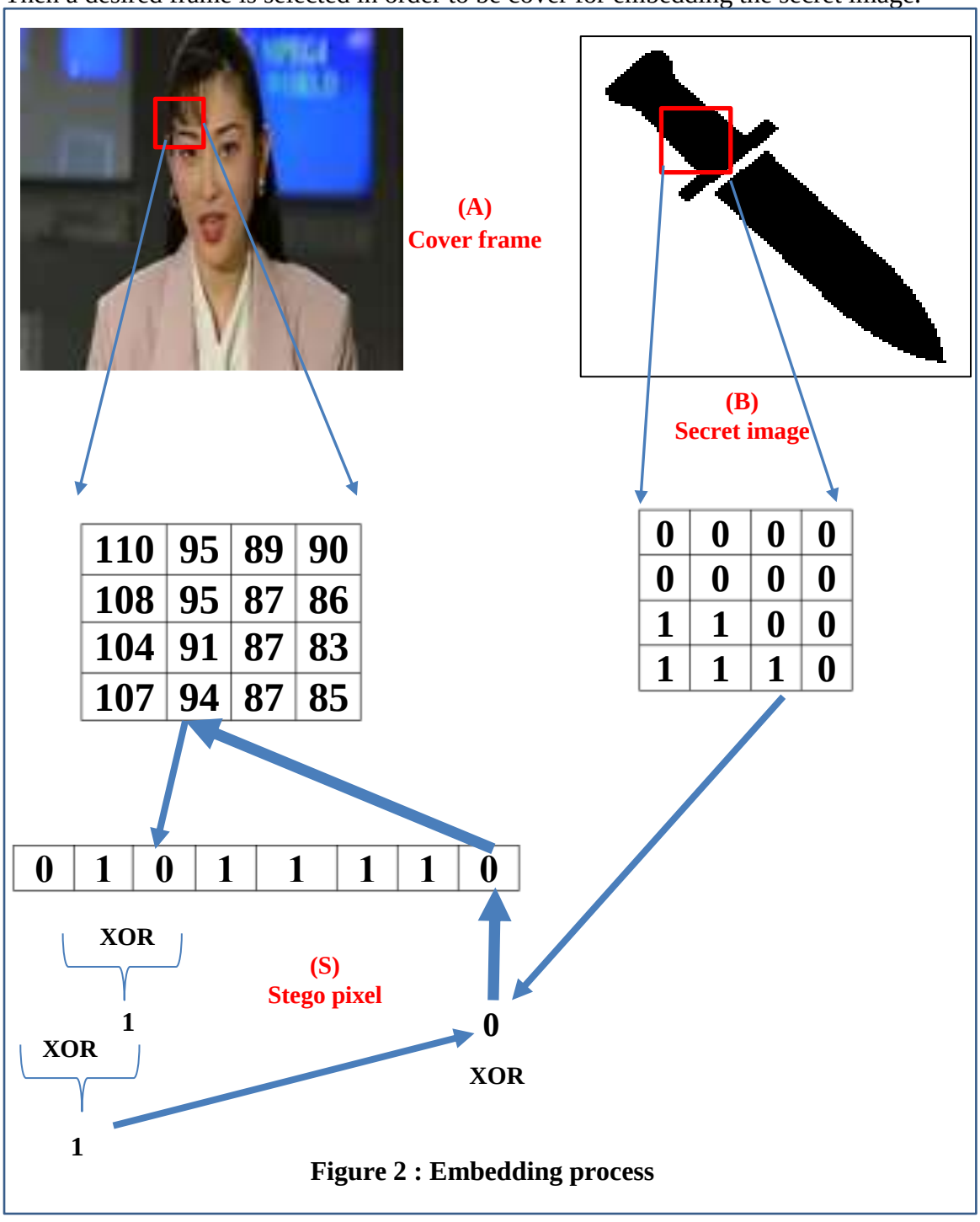


**Figure 2 : Embedding process**

In this process, the secret binary image is embedded in the cover frame Also, this process requires an image in a binary for to be as a secret message. The secret image and video must the same size. The embedding process is illustrated in the Figure (3.2). The steps of the embedding process can be listed as follows:

Step 1: read the video cover (V).
Step 2: split V into frame and select a specific cover frame (A).
Step 3: read the secret binary image (B)
Step 4: convert the pixels of A into binary.
For i =1to n
For j =1to n
Step 5: doing XOR operations between $7^{th}$ and $6^{th}$ bit of A(i,j).
Step 6: doing XOR operation between bit $8^{th}$ of A(i,j) and the result of step 5.
Step 7: doing XOR between secret message bit of B(i,j) and result of step 6.
Step 8: substitute the result of step 7 with $1^{st}$ bit (LSB) of pixel A(i,j) to get stego pixel S(i,j).
next j
next i
Step 9: get the stego frame S.
Step 10 : combine S with other frames of V to create stego video SV

**3.2 The Extraction process**

Figure 3 illustrates the extracting process. In this process, the stego video chosen firstly. Then the stego frame is selected in order to extract the secret image. Extraction process is listed as follows:

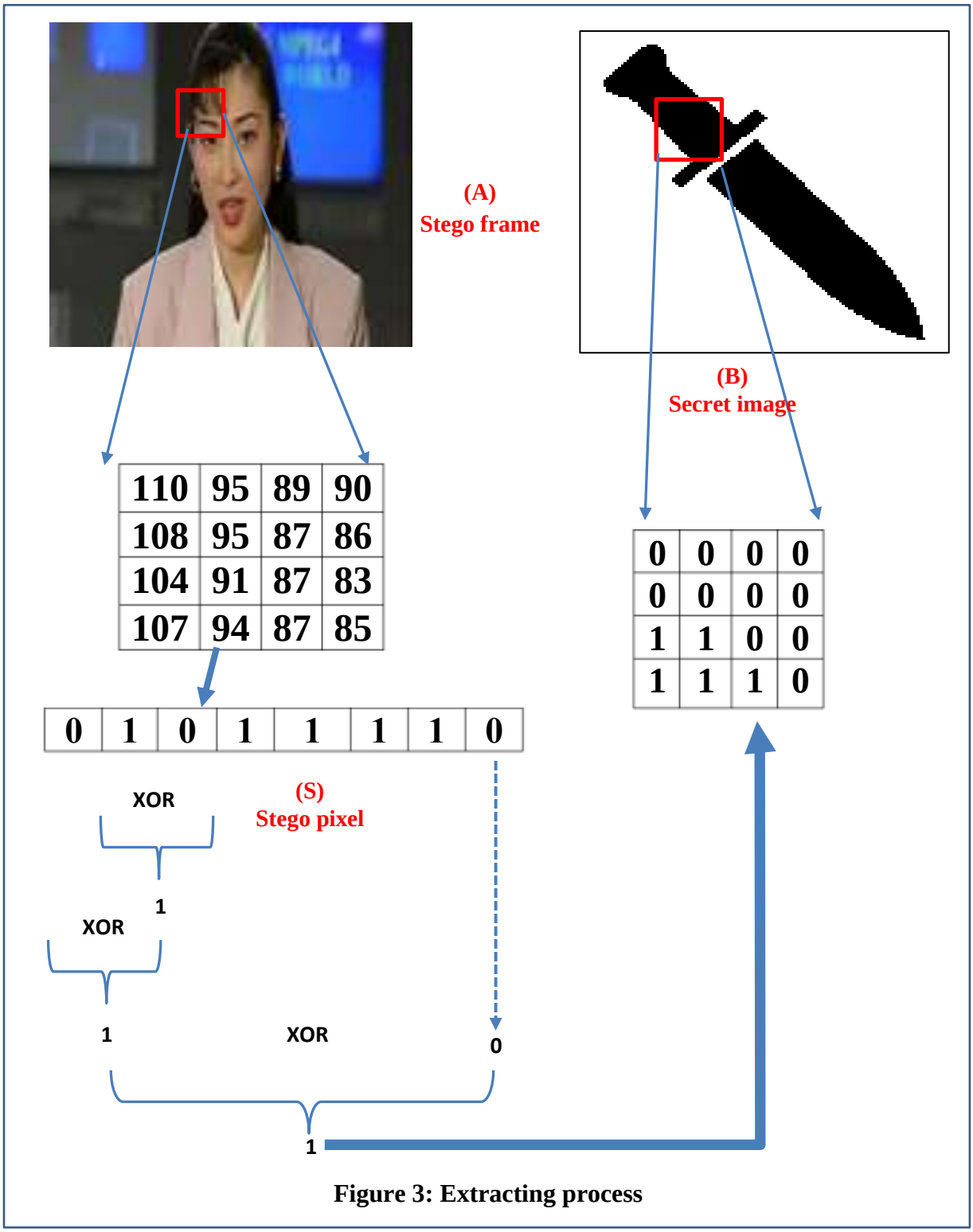


**Figure 3: Extracting process**

Step 1: read the stego video (VS)
Step 2: select the stego frame (S).
Step 3: convert the pixel of S into binary.
For i =1 to n
For j =1 to n
Step 4: doing XOR operations between 7th and 6th bit of S(i,j).
Step 5: doing XOR operation between bit 8th of S (i , j) and the fourth step result
Step 6: doing XOR between 1th bit of S (i , j) and the fifth step result.
Step 7: Saving the result of step 1 in the E(i.j)
Next j
Next i
Step 7: get the extracted secret image E.

## 4. Experimental Results

the results are discussed implementing the suggested method. some figures and table are displayed for showing the performance of the suggested method.

### 4.1 Test Material

The suggested project uses two types of materials. The first one is binary image of size (128*128) bits which represent the secret image. The second one is AVI video of size (128*128) pixels which the cover video. Figures 4 and 5 represent the secret image and AVI cover video respectively.

a) secret1

b) secret2

c) secret3

Figure 4: Secret images


a) boy


b)traffic


c ) two men

Figure 5: AVI videos

**4.2 Experiential Results**

In this section different results will be reviewed for different test videos. Tables bellows shows the results after applying the suggested project.

**Table 1: (boy video-Red band of frame)**

| Secret Image | Frame no. | Cover frame | Stego frame | PSNR | MSE |
|---|---|---|---|---|---|
|  | 1 |  |  | 55.9748 | 0.16429 |
| | | |  | 51.2036 | 0.49286 |
| | | |  | 55.9176 | 0.16646 |

| | | | | | |
|---|---|---|---|---|---|
| | 26 |  |  | 51.1464 | 0.49939 |
| | 53 |  |  | 55.964 | 0.16469 |
| | | |  | 51.1928 | 0.49408 |

**Table 2: (Traffic video-Green band of frame)**

| Image Secret | Frame no. | Cover frame | Stego frame | PSNR | MSE |
|---|---|---|---|---|---|
|  | 1 |  |  | 55.8743 | 0.16813 |
| | | |  | 51.1031 | 0.50439 |

| | | | | | |
|---|---|---|---|---|---|
| | **60** |  |  | 55.9001 | 0.16713 |
| | | |  | 51.1289 | 0.5014 |
| | **120** |  |  | 55.9304 | 0.16597 |
| | | |  | 51.1592 | 0.49792 |

**Table 3: (Two men video-Blue band of frame)**

| Secret image | Frame no. | Cover frame | Stego frame | PSNR | MSE |
|---|---|---|---|---|---|
|  | 1 |  |  | 55.8617 | 0.16862 |
| | | |  | 51.0905 | 0.50586 |
| | 141 |  |  | 55.7357 | 0.17358 |
| | | |  | 50.9645 | 0.52075 |
| | 250 |  |  | 55.7797 | 0.17183 |
| | | |  | 51.0085 | 0.5155 |

## 5. The Conclusions

After applying the suggested method, the following concussions are recorded:

1- A steganography method has been suggested for satisfying the confidentiality demand which is the most important need security requirements.
2- The secret message is embedded in the spatial domain of frame that was selected from a specific video. Also, XOR operation is used for applying the philosophy of encryption. By combining the cryptography and steganography techniques the security layer is increased.
3- According to experimental results, another security requirement is satisfied which is imperceptibility. The value of all PSNR values (after embedding the secret message in mor than cover image) are more than 50dB.
4- Two keys are used for embedding the secret message which means that the suggested method satisfied the security requirement.

## 6. Future works

After applying the suggested project, it is good idea to do the following:

1. Discuss the capability of applying suggested process with sensitive images like medical or military images.
2. Attempt to apply the suggested procedure in the digital watermarking applications.
3. study the effect of using the suggested technique in different types of video such compressed video.
4. Increasing the layer of security by encrypting the secret image before doing the embedding procedure.
5. Studying the ability of suggested project in the other media such as sound file.
6. Doing the XOR operation on the other bits rather than ($6^{the}$,$7^{the}$, and $8^{the}$ ) in order to enhancing the PSNR value.
7. Studying the ability of choosing the desired frame randomly by using key rather than choosing it directly in order to increase the layer security

## Conflict of interests.

There are non-conflicts of interest.

## References.

1. M. Hussain, A. W. Abdul Wahab, and Y. I. Bin Idris, A. T. S. Ho, and K. Jung, "Image steganography in spatial domain: A survey", Signal Processing: Image Communication, volume (65), p. ( 46-66), 2018.
2. .M.Hemalatha, G.Manisha, P.Mounika, SK.Saleema and Mrs. K.L Prasanna," Matlab Code for Video Steganography, 2020
3. Paramesh.G,*, Pavithra.K.V , Ranjitha.N, Swetha.S and T.Anushalalitha," Video Steganography using MATLAB",2017.
4. .Gat Pooja Rajkumar and KLE Dr M S Sheshgiri," Video Steganography: Secure Data Hiding Technique", 2017.
5. .Bharti Chandel, Dr.Shaily Jain," Video Steganography: A Survey", 2016
6. .Ashawq T. Hashim, Dr.Yossra H. Ali && Susan S. Ghazoul, " Developed Method of Information Hiding in Video AVI File Based on Hybrid Encryption and Steganography", 5/1/2011

## الخلاصة

Steganography هو علم وفن إخفاء رسالة سرية في وسائط الغلاف، دون أي تغيير غير محسوس فيها. يمكن تطبيق Steganography في العديد من الوسائط مثل الصورة والصوت والفيديو. اقترح هذا المشروع طريقة إخفاء المعلومات بالفيديو للحفاظ على السرية والتي تعد مطلبًا مهمًا في مجال الأمن. يمكن استخدام مجالين هما المجالات المكانية والترددية في إخفاء المعلومات بالفيديو لتضمين الرسالة السرية. في هذه الطريقة، يتم استخدام مجال مكاني يستند إلى بت أقل أهمية (LSB) لتضمين الرسالة السرية. من أجل تلبية متطلبات الأمان، يتم استخدام فلسفة التشفير في الطريقة المقترحة. في هذه الطريقة، يتم استخدام عامل التشغيل XOR مع عملية التضمين. يتم استخدام XOR مع ثلاثة مفاتيح لزيادة طبقة الأمان. بالإضافة إلى ذلك، وفقًا للنتائج التجريبية، فإن الطريقة المقترحة تفي بمتطلبات عدم الإدراك وهو مطلب مهم جدًا في مجال إخفاء الصور. أظهرت نتائج التجربة أن قيمة جميع قيم PSNR (بعد تضمين الرسالة السرية في أكثر من صورة الغلاف) تزيد عن 50 ديسيبل مما يعني أن الطريقة المقترحة قللت من التشويه الذي قد يحدث في الغلاف بعد تضمين الرسالة السرية.

الكلمات الدالة: إخفاء المعلومات بالفيديو، إخفاء المعلومات، أمن المعلومات.