ARTICLE
JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)
Vol.2; No.3.| 2021

# Video Steganography Based on Modified Embedding Technique

Rawaa Abd-alhakem[1*] and Mohammed Abdullah Naser[2]

[1]College of Science for Women, University of Babylon, rawaa.abod.gsci30@student.uobabylon.edu.iq, Babylon, Iraq.
[2]College of Science for Women, University of Babylon, wsci.mohammed.abud@uobabylon.edu.iq, Babylon, Iraq.
*Corresponding author email: mohamed127612@gmail.com; mobile: +9647813030258

# الإخفاء بالفيديو باستخدام تقنية التضمين المعدّلة

رواء عبد الحكيم عبد الشهيد[1]*، محمد عبد الله ناصر[2]
1 كلية العلوم للبنات ، جامعة بابل ، rawaa.abod.gsci30@student.uobabylon.edu.iq ، بابل، العراق
2 كلية العلوم للبنات ، جامعة بابل، wsci.mohammed.abud@uobabylon.edu.iq ، بابل، العراق

Received: 20/10 /2021 Accepted: 20/12 /2021 Published: 31/12/2021

## ABSTRACT

Information security has become the concern of the most famous researchers and the focus of their attention, as they are constantly trying to find the best and most secure way to transfer information through a secure channel to protect it from hacking attempts and common attacks on the Internet. This work is an attempt to suggest a security approach in protecting data by focusing on protection the text sent in Arabic and English from being noticed or modified by attackers, and it is efficiently hidden inside the cover video. the proposed method combines cryptography and steganography by encrypting the secret text before hiding it with the public key encryption system is named after the initials of its co-founders, Rivest - Shamir – Adleman (RSA). In addition, add an extra layer of security and confidentiality, a hash-based least significant bit mechanism that uses a pattern to choose the insertion sites in the least Significant Bit (LSB). In a spatial domain technique, the secret information is embedded in the LSB of the cover frames that are efficiently chosen based on the hash value of the secret key agreed upon between sender and receiver. The secret information is divided into eight bits and then embedded in the Red, Green, and Blue (RGB) pixel values of the cover frames. In comparison to the original cover video, the proposed method is analyzed in terms of both "Peak Signal to Noise Ratio (PSNR) reached to scale (68.582) compared to the original cover video as well as the Mean Square Error (MSE) reached to scale (0.0115) through embedding message with size 2 KB in AVI video. When compared to other ways of concealing common information, the experimental results from our methodology show that it provides stronger embedding capacity as well as improved imperceptibility of stego-videos and boosts security and robustness.

Key words:
Video Steganography, Hash Function, LSB, Stego-Video, Secret Message.

## الخلاصة

أصبح أمن المعلومات محل اهتمام أشهر الباحثين ومحور اهتمامهم ، حيث يحاولون باستمرار إيجاد الطريقة الأفضل والأكثر أمانًا لنقل المعلومات عبر قناة آمنة لحمايتها من محاولات القرصنة والهجمات الشائعة على الإنترنت. . هذا العمل هو محاولة لاقتراح نهج أمني في حماية البيانات من خلال التركيز على حماية النص المرسل باللغتين العربية والإنجليزية من ملاحظته أو تعديله من قبل المهاجمين ، ويتم إخفاؤه بكفاءة داخل فيديو الغلاف. تجمع الطريقة المقترحة بين التشفير وإخفاء المعلومات عن طريق تشفير النص السري قبل إخفائه مع نظام تشفير المفتاح العام الذي سمي على اسم الأحرف الأولى من مؤسسيها Rivest - Shamir - Adleman (RSA). بالإضافة إلى إضافة طبقة إضافية من الأمان و السرية ، وهي آلية بتات أقل أهمية تعتمد على التجزئة وتستخدم نمطًا لاختيار مواقع الإدراج في البتات الأقل أهمية (LSB). في تقنية المجال المكاني ، يتم تضمين المعلومات السرية في LSB لإطارات الغلاف التي يتم اختيارها بكفاءة بناءً على قيمة تجزئة المفتاح السري المتفق عليه بين المرسل والمستقبل. يتم تقسيم المعلومات السرية إلى ثماني بتات ثم يتم تضمينها في قيم البكسل الأحمر والأخضر والأزرق (RGB) لإطارات الغطاء. تم تحليل التقنية المقترحة من حيث "نسبة الإشارة القصوى إلى الضوضاء (PSNR) التي وصلت إلى مقياس (68.582) مقارنة بفيديو الغلاف الأصلي بالإضافة إلى متوسط الخطأ التربيعي (MSE) الذي وصل إلى مقياس (0.0115) من خلال تضمين رسالة بحجم 2 كيلوبايت في فيديو AVI. عند مقارنتها بالطرق الأخرى لإخفاء المعلومات الشائعة ، تُظهر النتائج التجريبية من منهجيتنا أنها توفر قدرة تضمين أقوى بالإضافة إلى تحسين عدم إدراك مقاطع فيديو Stego وتعزز الأمان والمتانة.

الكلمات المفتاحية:
إخفاء المعلومات بالفيديو ، وظيفة التجزئة ، LSB، فيديو Stego ، الرسائل السرية.

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

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
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

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

## 1.Introduction

Security has become a fundamental demand and requirement in many aspects of social life in today's internet-driven world. security is the most crucial criterion for determining whether or not the data is still valid and useable **[1].**

the study of mathematical approaches that provide some amount of security is known as cryptography. encryptions are divided into two types: symmetric encryption and asymmetric encryption one key is utilized for encoding in symmetric encryption. asymmetric encoding uses two sets of keys, to validate the digital signature and encrypt the plaintext, one set of the public key's keys is used. the private key is used to create digital signatures and decrypt ciphertext **[2 and 3]**. information concealing is now regarded as a necessary and significant procedure because of technical innovation, advancement, and the complexity of algorithms. steganography is the process of hiding a secret message in data (cover), such as text, audio, video, and image, and then transmitting it to the receiver, who decodes the message using the stego key and retrieves the original image [4]. mixed data (secret information and the cover) called "Stego Objects" will see the human visual system (HVS) as a single piece of data because (HVS) will not be able to find out that there is a small change to your cover data [5] there has been a significant increase in the use of video as a cover file because it has a high concealing capacity, is more resistant to attacks, and Non-discrimination of cover video and stego video is a major concern for any steganography technique. **[4, 5 and 6]**. Figure 1 shows the standard process of steganography based on image and video between two parties.

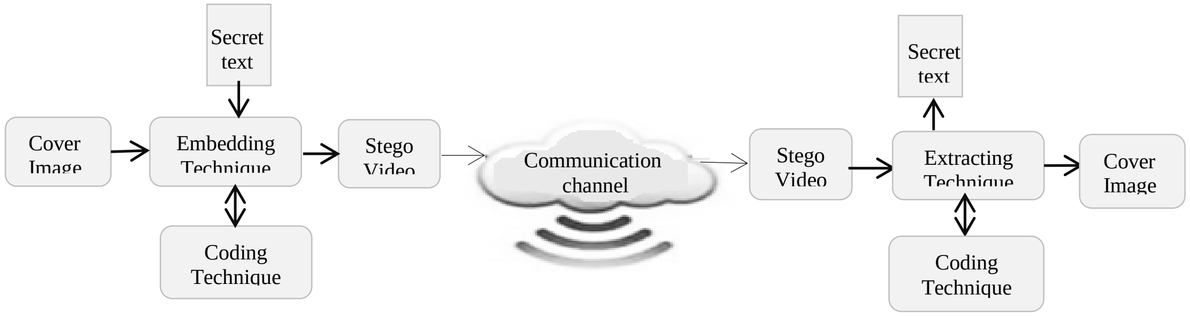

*Figure 1: steganography with video image*

The rest of the paper is as follows: steganography is explained in section 1. Section 2 discusses the related work. section 3 describes the proposed method. The results are shown in Section 4. section 5 also concludes the paper.

## 2. Related Works

This section of the work presents the literature survey carried out. These works are referred to in this project and the gist of each reference has been presented.

Ganesh Aithal et al utilized Cryptography to present the notion of video steganography. Their method divides the secret data into equal halves and encrypts them simultaneously using an XOR function. The encrypted data chunks are subsequently placed in the video frames in parallel (using the LSB technique). Using the Feedback Shift Register (FSR), the video frames utilized to include the data were picked at random. Parallelization is also used in the extraction and decryption processes. This parallelization considerably improves system performance **[7]**.

The authors in **[8]**, **[9]** proposed combined video steganography with cryptography. In 2015, Dixit et al used is 2-2-3 LSB technique [8], In 2013, Sanjeev Sharma et al to offer more secure data transmission, symmetric encryption was implemented.

Khosla et al proposed the video steganography approach, by combining “watermarking” and the least significant bit approaches of steganography to assure information security. The original video is shown as the first stage of the process. The LSB method then embeds data into “the LSB of pixel” of the frame. Following that Watermarking is done with the use of DWT, DCT methods. The final resulting is a stego-video with a watermark. The high and acceptable ratio findings of the PSNR and MSE production rates revealed that the watermarked stego-video provided efficiency and security **[10]**.

Nyo et al used combination of steganography and cryptography techniques in order to improve imperceptibility, robustness to transmit data securely. As the preprocessing step, Arnold scrambling and discrete wavelet transform (DWT) techniques are used over the secret image. Then the referable values are calculated from the values of transformed secret image with the use of a secret key and embed these referable values in the video file by least significant bit (LSB) technique. As the experimental results, performance of the system is tested with various video and measured by different parameters (PSNR, MSE) **[11]**.

Jawad et al. combined the encryption and steganography techniques to secure transmission through unsecured network. In their paper, they proposed a method for encryption images using second-order equations, The image is embedded in the video according to the equations rather than embedding it sequentially in order to increase the security layer. The experimental results suggest that the approach proposed is achieved robustness and increases the safety by encryption and non-sequential selection of frames **[12]**.

Table (1) contains a comparison of embedding methods for previous works with the proposed system performance. It should be noticed that the proposed system accomplished higher performance than the other existing systems, this comes from the fact that the proposed method adopts a strong public-key encryption algorithm in order to encrypt the secret message before embedding it, in addition to improving the traditional LSB technique through the technology of hash-based_LSB technique which was used in embedding.

**Table (1). Comparison of the Proposed Method With Other Related Works**

| # | The author(s) | Technique used | Cover type | Video name | PSNR | MSE |
|---|---|---|---|---|---|---|
| [10] | Khosla et al., in (2016) | LSB Technique and Watermarking | Video | eli_walk.avi | 52.69 | 0.364 |
| | | | | trafic.avi | 52.7 | 0.351 |
| [11] | Nyo et al., in (2019) | Arnold Scrambling and DWT, and LSB Technique | Video | Bird.avi | 60.914 | 0.018 |
| | | | | Canary.avi | 57.990 | 0.069 |
| | Proposed System | The RSA encryption method and HASH Based_ LSB Technique | Video | Rhinos.avi | 68.582 | 0.0115 |
| | | | | Ali.avi | 47.520 | 1.136 |

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

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

## 3. The Proposed Method

The proposed method focuses on the steganography technique using Audio Video Interleave (AVI) digital video, due to the complexity relative to the structure of video files when compared to image files to provide increased security against hacker attacks. we present video steganography, use the hash-based least significant bit (HLSB) approach with the main purpose of embedding encrypted secret information in a random frame of the video file for added security, and then extracting and decrypting it using secret keys. For steganography, an LSB insertion method is used to embed data in a cover video with a change in the lower bit rate. The process of embedding information in a video without affecting its perceptual quality is known as data hiding. The proposed LSB method embeds eight bits of secret data at a time in the LSB of the carrier frame's RGB (Red, Green, and Blue) pixel value in a 3, 3, 2 order. Depending on the hash function is used.Figure 2 illustrates the main processes of the embedding procedure in the proposed system (in sender site).

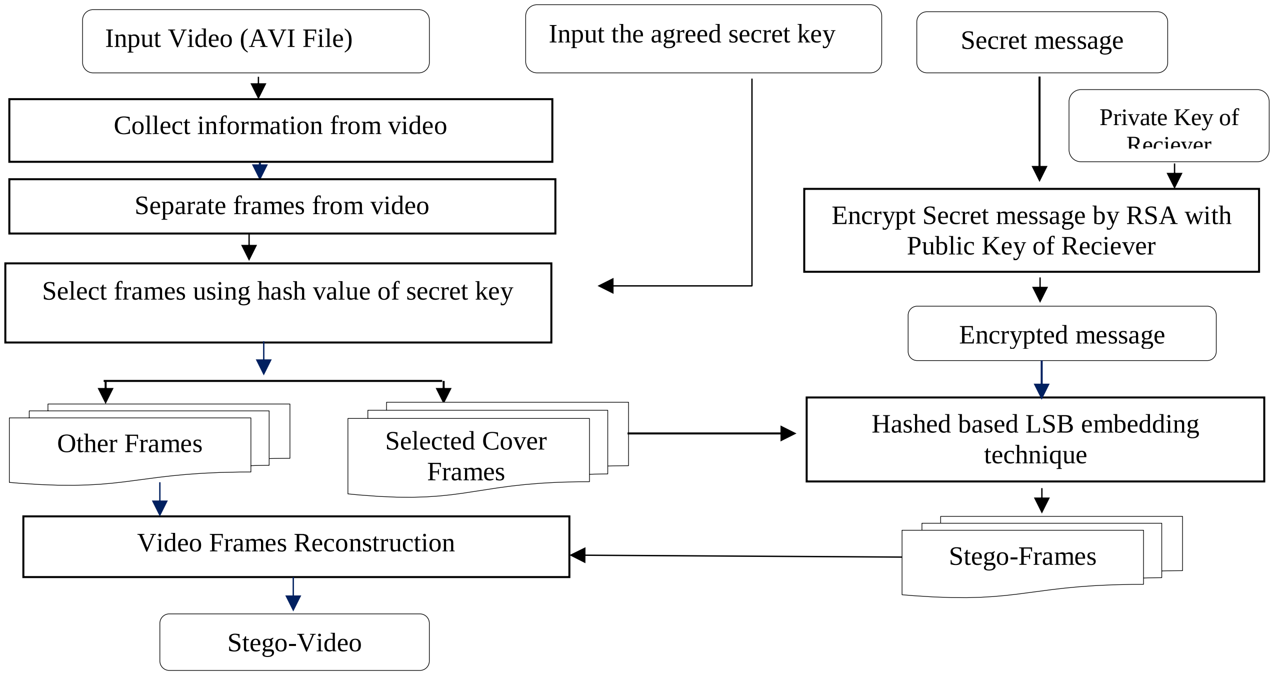
Input Video (AVI File)
Input the agreed secret key
Secret message
Private Key of Reciever
Collect information from video
Separate frames from video
Encrypt Secret message by RSA with Public Key of Reciever
Select frames using hash value of secret key
Encrypted message
Other Frames
Selected Cover Frames
Hashed based LSB embedding technique
Video Frames Reconstruction
Stego-Frames
Stego-Video

**Figure 3: General Block of Extracting Procedure**

The hash function is used again in the suggested (LSB) technique to determine the position of the least significant bit to retrieve secret data in the same order (3, 3, 2). Figure 3 illustrates the main processes of the extracting procedure in the proposed method (in receiver site).

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

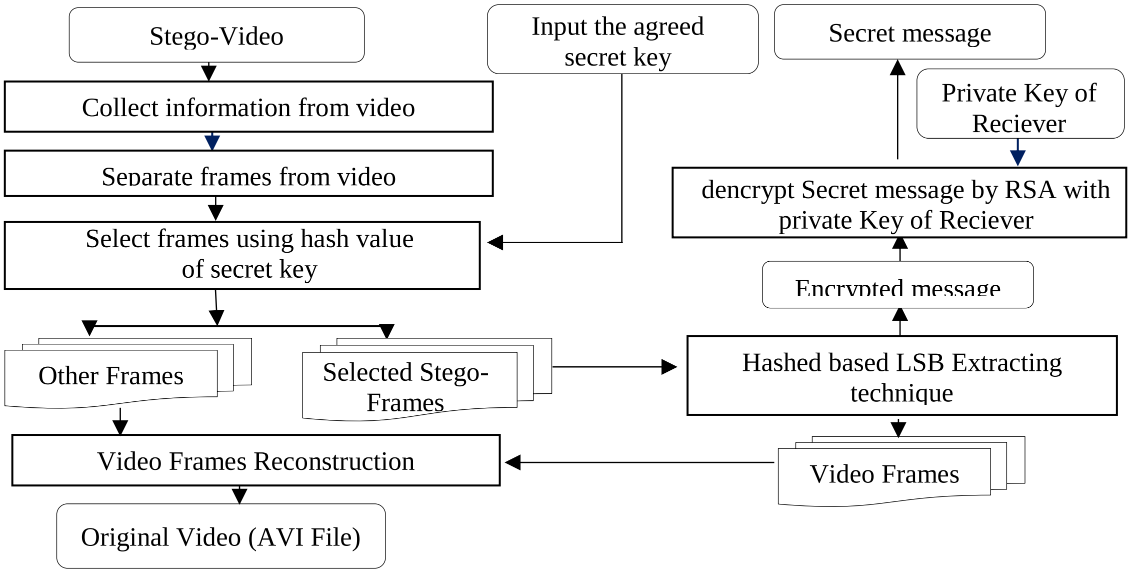
Stego-Video
Collect information from video
Separate frames from video
Select frames using hash value of secret key
Input the agreed secret key
Other Frames
Selected Stego-Frames
Video Frames Reconstruction
Original Video (AVI File)
Secret message
Private Key of Reciever
dencrypt Secret message by RSA with private Key of Reciever
Encrypted message
Hashed based LSB Extracting technique
Video Frames

**Figure 3: General Block of Extracting Procedur.**

### 3.1 Embedding Procedure

On the sender's side, the embedding procedure consists of several steps, the most important of which is to encrypt the secret message using the (RSA) algorithm based on the intended recipient's public key, choosing the cover video file that will be used in hiding, and then collecting information from it, after which the cover video frames are separated from each other, then several frames are selected based on a hash function based on the secret key that is agreed upon between the sender and receiver. The proposed hash-based (LSB) method has been applied to conceal the encrypted secret message in the cover selected frames. Below is a detailed of important steps in sender site.

**Algorithm (1) illustrates the main steps for the embedding procedure**

| **Algorithm (1): Main Embedding Algorithm** |
|---|
| Input:<br>AVI Video // cover carrier<br>secret key // key control of random frames selection<br>Text file // text file contain secret message<br>Encryption key // encrypt the secret message before embedding |
| Output:<br>Stego video // video carrying the encrypted secret message |
| Step1: Segment the video into the frame depending on video frame rate<br>Step2: Select the frames randomly depending on the hash value of secret key<br>Step3: Analyzes the messages and encrypted using RSA encryption algorithm<br>Step4: 4 LSB bits to each RGB pixel in the cover frame should be found.<br>Step5: Using the hash function in equation (1), find the position for embedding the secret data.<br>Step6: Embed the Secret data depend on these positions in the order of 3, 3, 2<br>Step7: Gather stego frame with video frame and create the stego video |

3.1.1 Selection and Encryption the Secret Message

The secret data is encrypted using the (RSA) encryption algorithm for converting it into ciphertext based on the intended recipient's public key to increase security by reading each character from a secret text and converting it to (decimal system) including space. then converted to binary format and divided into blocks according to the size of the hidden message before it is incorporated into the cover video. without the recipient's private key, any intruder will have a difficult decrypting the message. RSA algorithm procedure can be illustrated as follows:

(i) Choose p and q, two large, strong prime numbers. Let's say n = p*q.

(ii) Calculate n's Euler totient value: f (n) = (p - 1)* (q - 1).

(iii) Find a random number e that matches the conditions 1 e f (n) and is relatively prime to f(n), i.e.,gcd(e,f(n)) = 1.

(iv) Find an integer d such that it equals e-1 mod f. (n).

(v) Encryption:C = M e mod n is used to encrypt a plain text (m)

(vi) Decryption: M = Cd mod n is used to decrypt the encrypted text (c).

### 3.1.2 Select and Collect Information from Cover Video

In this step, we use the avi video (uncompressed), as a carrier to conceal the message's encryption. this type is chosen because it provides a higher hiding capacity compared with compressed video files such as MPEG or MP4.

### 3.1.3 Select Video Frames

In this step, a hash function (SHA512) has been used to produce a unique hash value from the input secret key that is agreed upon between the sender and recipient. The hash value is converted to its equivalent binary value. The binary value is used to choose the frames that are used in the hiding, where the cover frames that correspond to the value of "1" are selected in the hiding process, while the frames that correspond to the value of "0" are not used.

Figure (4) example that illustrates the process of choose frames randomly from specified video in detail.

### 3.1.4 Hash-LSB Embedding Process

The hash function is used to determine the LSB location, which is utilized to hide the encrypted text in the (H-LSB) steganography technique With in the selected frames. Each RGB pixel's LSB discovers via the hash function and secret message bits are embedded or hidden in each RGB pixel independently using the values given by the hash function. In this procedure, each 8 bits is inserted in the order of 3, 3, 2 bits at a time, after the secret message is converted to binary form. as illustrated in Figure 4. the first 3 bits of the 8 bits secret message are inserted into red pixel and other 3 bits of the secret message into green pixels and the remaining 2 bits are inserted into the blue pixel. These 8 bits are arranged in this order because blue has a higher chromatic influence on the human eye than red and green. as a result, the distribution pattern chooses the two bits in the blue pixel that will be hidden.

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

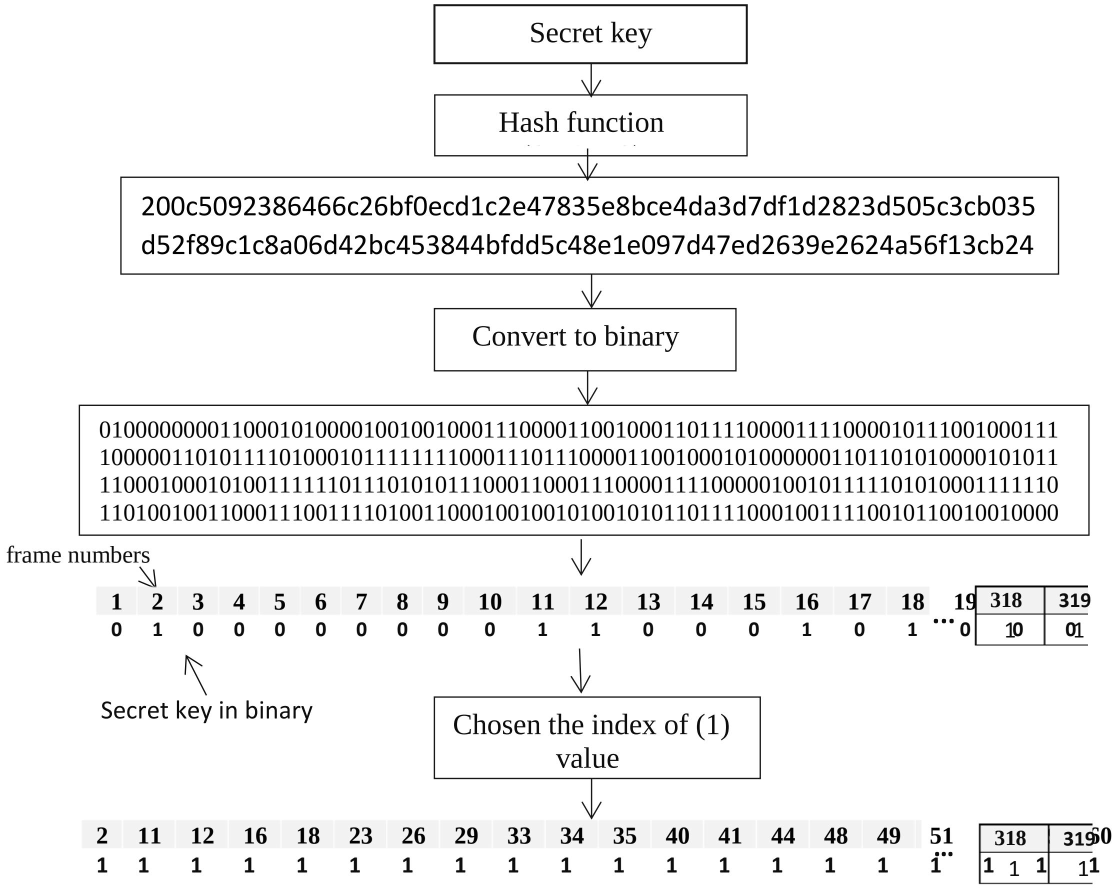

**Figure 4: Illustrates the Process Choose Frames**

As a result, there will be no degradation in visual quality. to determine where data should be hidden in the LSB of each RGB pixel in the cover frame. apply the formula below:

**"k = p % n ………………… (1)"**

Here k denotes the pixel's LSB bit location; p is the location of every hidden frame pixel; and n denotes the count of LSB bits in this case is four . a stego-video will be created after the data has been embedded in the cover video. To retrieve the data storage locations, the recipient of this video must utilize the hash algorithm once more to extract the data in ciphertext format.

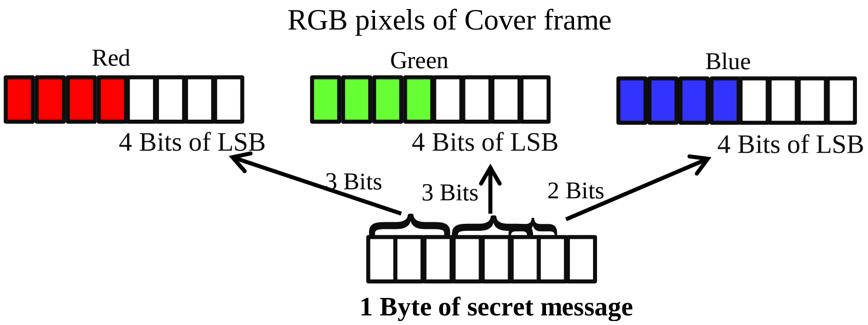

**Figure 5: In the corresponding RGB pixels of the carrier frame, secret data is embedded in 4 bits of LSB in 3,3,2 order.**

Figure (5) shows the mechanism by which the bits that will be selected from the RGB pixels of cover frames, depending on the above equation 1 that was employed in the proposed work.

### 3.1.5 Video Frames Reconstruction

After the process of hiding the encrypted secret text in the specified video frames, it is necessary to reassemble the entire video by reconstructing the unselected frames with the stego- frames to produce stego-video.

### 3.2 Extraction Procedure

On the receiver's side, the extracting procedure consists of several steps, to decrypt the secret data, choosing the stego-video file which carries the secret message, and then collecting information from it, after which the stego frames are separated from other frames based on a hash function value (SHA512) for the secret key that is agreed upon between the sender and receiver. The suggested (HLSB) method was used to extract the encrypted secret message from the selected stego-frames. To decrypt the secret data, the receiver will use his or her private key to execute the (RSA) method. Because the recipient's public key has encrypted the private data. The original message will be transformed into a readable format using the receiver's private key. The Algorithm (2) illustrates the main steps for the extracting procedure (in receiver site).

**Algorithm (2): Main Extraction Algorithm**

```
Input:
AVI Video // stego video
 secret key // for control random frame selection
Private key // for the RSA algorithm
Output:
test file // the original secret message
Step1: Segment the video into frame depending on video frame rate
Step2: select the frame randomly depending on the Hash value secret key
Step3: 4 LSB bits to each RGB pixel in the cover frame should be found
Step4: Using the hash function in equation (1), find the position for embedding the secret data.
Step5: Retrieve the Secret data depend on these positions in the order of 3, 3, 2.
Step6: decrypt the secret message using private key.
Step7: create the original text file
```

## 4. Results

### 4.1 The Experimental Results

The results of the experimental work are discussed in this section. the proposed method's performance is evaluated using a variety of videos of the same file type (avi) and Secret messages of different to insert a hidden message (text) into a video. the suggested system was simulated on a windows 10 platform with an Intel core i7 processor using the matlab program version 2020. The features of the videos are listed in the table1:

**Table (2): Selected Videos Files Used In The Experiments**

| File Name | First Frame | Number of Frames | Size of Each Frame |
|---|---|---|---|
| **Rhinos** | | **114** | **240x320x3 uint8** |
| **Ali** | | **53** | **120 x90 x3 uint8** |

## 4.2 The Results of Random Selection for Video Frame

At this step selected random frame from video based on hash value for the secret key, the frames of the videos as shown in the Tables 3,4:

**Table (3): Selection Step Of Rhinos Avi Video For 3-Time Selection Using Secret Key**

| Random Frame No. | Cover Frame | Secret key |
|---|---|---|
| **5** | | **N.W.2009** |
| **6** | | **stego ff01** |
| **8** | | **FFDE111000** |

Table (4): Selection Step Of Ali Avi Video For 3-Time Selection Using Secret Key

| Random Frame No. | Cover Frame | Secret key |
|---|---|---|
| 4,6,11,13 | <br> <br> <br> | text8e |
| 3,13,15 | <br> <br> | Accept10 |
| 5,7 | <br> | go135 |

## 4.3 The Results of The Embedding Process

After the frame selected based on a hash function based on the secret key that is agreed upon between the sender and receiver, and analyzing the secret message. the embedding process of the secret word to frame to produce stego-frame based on hash function.as shown in Table ( 5,6).

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Table (5): Selection Step Of Rhinos Avi Video For 3-Time Selection Using Secret Key

| Frame No. | Cover Frame | Secret key | Stego Frame |
|---|---|---|---|
| **5** | | N.W.2009 | |
| **6** | | stego ff01 | |
| **8** | | FFDE111000 | |

Table (5): Embedding Process Using Ali Avi Video For 3-Time Selection Using Secret Key

| Frame No. | Cover Frame | Secret key | Stego Frame | Secret message |
|---|---|---|---|---|
| **4,6,11,13** | <br> <br> <br> | Text8e | <br> <br> <br> | M1.text |
| **3,13,15** | <br> | Accept10 | <br> | M2.text |

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com
مجلة جامعة بابل للعلوم الصرفة والتطبيقية

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

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| **5,7** | | | go135 | | | M3.text |

## 4.4 The Results of PSNR and MSE

The basic characteristics of every steganography technique are imperceptibility and capacity viewer must be unable to see embedded data (perceptual invisibility), and “computer analysis (statistical invisibility). with achieving a high embedding capacity to maintain high quality and robust system. PSNR (“Peak Signal to Noise Ratio”), an addition to MSE (“Mean Square Error”) that is used to measure the fidelity of the stego-frame by comparing it to the original frame as shown in Table (6).

**Table (7): PSNR and MSE Calculation**

| Video name | Frame no. | Secret key | Secret Message size | PSNR | MSE |
|---|---|---|---|---|---|
| Rhinos | 5 | NW2011 | 2 KB | 68.582 | 0.0115 |
| | 6 | stego ff01 | 4 KB | 66.446 | 0.0538 |
| | 8 | select135 | 6 KB | 63.237 | 0.0819 |
| Ali | 4,6,11,13 | TEXT | 27.5 KB | 32.582 | 5.464 |
| | 3,13,15 | accept | 21.3 KB | 38.225 | 2.530 |
| | 2,5 | go135 | 9.60 KB | 47.520 | 1.136 |

The values of PSNR are decreasing and the values of MSE are increasing as the message size factor is increased, as shown in the tables above. That means that when the message size grows larger, the frame's fidelity decreases, and the steganography causes the cover frame to distort as shown in Figure (6,7)

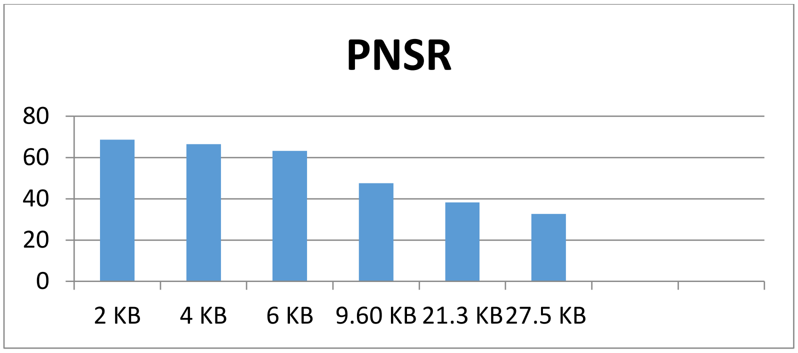

**Figure 6: The Relationship Between Message Size And PSNR For Avi Video**

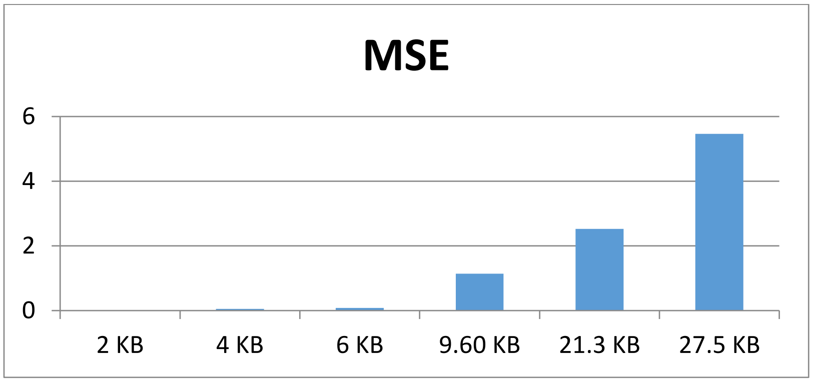

**Figure 7: The Relationship Between Message Size And MSE For Avi Video**

## 5-Conclusions

The primary goal of the research is to develop an information hiding application by merge encryption and steganography to ensure a high level of security while preserving data transection in the public channel from common attacks. secret text is encrypted using the (RSA) public cipher technique, using the recipient's public key before embedding it in an avi video cover, making it impossible for an intruder to decrypt the encrypted text. the frames selection based on hash value to secret key added extra protection to the proposed method, if the attacker suspects that there is a hidden message inside the video, it is difficult to detect the secret message because it is encrypted and scattered randomly. The proposed steganography method (H-LSB) that has been implemented for text embedding is stronger in terms of security, reliability, capacity, and imperceptibility, as well as performance and computing complexity than standard embedding procedures. To evaluate the system's performance, we utilized video files to hide encrypted data using the proposed methods. Video resolution does not change much according to PSNR and MSE. This proposed method can be robust to the "steganalysis process" that is because it encrypts the secret message using the RSA algorithm. In future work is the proposed method can be applied using a new method for randomly selecting frames, pixels or bits. This can be expanded by using a dynamic threshold in the subject of embedding and As a result, the stego image's quality will improve. The suggested method can be applied by embedding the color text message as input message instead of black & white text message. The proposed method can be applied using a new method for randomly selecting frames, pixels or bits.

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

## Acknowledgments:

we extend our sincere thanks to the presidency of the department of computer science and the deanship of the college of science for women, and thanks are also extended to the presidency of the university of Babylon for the unlimited support in completing this work and publishing it in the journal of university of Babylon for pure and applied sciences.

## Conflict of interests.

There are non-conflicts of interest.

## References

[1] Liestyowati, Dwi. "Public Key Cryptography." In Journal of Physics: Conference Series, vol. 1477, no. 5, p. 052062. IOP Publishing, 2020.

[2] Hayouni, Haythem, and Mohamed Hamdi. "A novel energy-efficient encryption algorithm for secure data in WSNs." The Journal of Supercomputing 77, no. 5,2021.

[3] Rao, Umesh Hodeghatta, and Umesha Nayak. The InfoSec handbook: An introduction to information security. Springer Nature, 2014.

[4] Rashid, Rakan Mohammed et al. "Information Hiding in Still Image Based on Variable Steganography Technique to Achieve High Imperceptibility." In 2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC), pp. 171-176. IEEE, 2021.

[5] Liu, Yunxia, Shuyang Liu, Yonghao Wang, Hongguo Zhao, and Si Liu. "Video steganography: A review." Neurocomputing 335 (2019): 238-250.

[6] Pilania, Urmila. "Stable High Capacity Video Steganography in Wavelet Domain." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12, no. 7 (2021): 2142-2158.

[7] Sudeepa, K. B., K. Raju, Ranjan Kumar HS, and Ganesh Aithal. "A new approach for video steganography based on randomization and parallelization." Procedia Computer Science 78 (2016): 483-490.

[8] Dixit, Mrudul, Nikita Bhide, Sanika Khankhoje, and Rajashwini Ukarande. "Video steganography." In 2015 International Conference on Pervasive Computing (ICPC), pp. 1-4. IEEE, 2015.

[9] Yadav, Pooja, Nishchol Mishra, and Sanjeev Sharma. "A secure video steganography with encryption based on LSB technique." In 2013 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-5. IEEE, 2013.

[10] Khosla, Shivani, and Paramjeet Kaur. "Secure data hiding technique using video steganography and watermarking." International Journal of Computer Applications 95, no. 20 (2016): 7-12.

[11] Nyo, Hnin Lai, and Aye Wai Oo. "Secure Data Transmission of Video Steganography Using Arnold Scrambling and DWT." International Journal of Computer Network & Information Security 11.6 (2019).

[12] Jawad, M. J. (2020). Combining A Cryptography and Steganography Techniques–Based Securing Transmitted Video Through Unsecure Channel. Journal of University of Babylon for Pure and Applied Sciences, 207-215.

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