DOI: 10.24996/ijs.2022.63.12.38

ISSN: 0067-2904

Steganography Encryption Secret Message in Video Raster Using DNA and Chaotic Map

Maisa'a Abid Ali Khodher[1], Ashwak Alabaichi[2], Ammar A. Altameemi[2]
[1]Computer Sciences, University of Technology-Iraq, Bagdad, Iraq
[2]Biomedical Engineering, College of Engineering, University of Kerbala, Kerbala, Iraq

Received: 2/10/2021 Accepted: 10/11/2021 Published: 30/12/2022

Abstract

Recently, much secured data has been sent across the internet and networks. Steganography is very important because it conceals secure data in images, texts, audios, protocols, videos, or other mediums. Video steganography is the method of concealing data in frames of video format. A video is a collection of frames or images used for hidden script messages. This paper proposes a technique to encrypt secret messages using DNA and a 3D chaotic map in video frames using the raster method. This technique uses three steps: Firstly, converting video frames into raster to extract features from each frame. Secondly, encryption of secret messages using encoded forms of DNA bases, inverse/inverse complements of DNA, and utilizing 3D chaotic maps, Thirdly, hiding encryption secret messages in that raster video frame by using a secret key in the four corners of each video frame. This technique hides large amounts of secret data because the video frame is large and accepts any message size. The outcomes are efficient, robust, highly secure, and can tolerate high capacity. These outcomes have been obtained from a set of tests like: peak signal to noise ratio (PSNR), mean square error (MSE), entropy, correlation coefficient, and histogram and capacity.

Keywords: *3D Logistic Map, DNA, Encryption, Raster, and Steganography.*

تشفير الرسائل السرية باستعمال الحمض النووي والفوضى في الفديو النقطي

ميساء عبد علي ، اشواق محمود ، عمار عبد الجبار
قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق
الهندسة الحياتية/كلية الهندسة ،جامعة كربلاء، كربلاء، العراق

الخلاصة

الهدف من هذا البحث ، هو إرسال بيانات آمنة عبر الإنترنت والشبكات. إخفاء المعلومات مهم جدًا ، حيث يمكن إخفاء البيانات بشكل آمن في أي وسائط ، صورة ، نص ، صوت ، بروتوكول ، أو فديو. إخفاء المعلومات عن طريق الفديو هي وسيلة لنقل البيانات المخفية في إطار الفديو بتنسيق. الفديو عبارة عن مجموعة من الإطارات أو الصور تستعمل للرسائل النصية المخفية. تقترح هذه الورقة تقنية لتشفير الرسائل السرية باستخدام الحمض النووي والخريطة الفوضوية ثلاثية الأبعاد في إطار الفديو باستعمال طريقة المسح. توظف هذه التقنية ثلاث خطوات: أولاً ، تحويل إطارات الفديو إلى طريقة نقطية لاستخراج شكل او هيئة من كل إطارات الفديو. ثانيًا ، تشفير الرسالة السرية باستعمال شكل مشفر لقاعدة الحمض النووي، ومكملات

*Email: 110044@uotechnology.edu.iq

عكسية / ومعكوس للحمض النووي ، واستعمال خرائط فوضوية ثلاثية الأبعاد، ثالثًا، إخفاء رسالة سرية مشفرة في إطار فديو نقطي ، باستعمال مفتاح سري هو أربع زوايا في كل إطارات النقطية للفديو. هذه التقنية تخفي بيانات كبيرة من الرسائل السرية لأن إطار الفديو كبير ويقبل أي حجم للرسالة. النتائج هي فعالة وقوية وآمنة للغاية وتتحمل قدرة عالية. تم الحصول على هذه النتائج من مجموعة من الاختبارات مثل نسبة إشارة الذروة إلى الضوضاء (PSNR) ، متوسط الخطأ المربع (MSE) ، الانتروبيا ، معامل الارتباط ، الرسم البياني والسعة.

Introduction

The video steganography conceals secured letters without affecting the visible goodness or tampering with the contents of the video file. In this research, the second goal was accomplished. The video consists of audio and images. Work can be done on those two elements, and video information can be extracted [1]. Data security is becoming increasingly important for newly developed computing systems. Mostly, the secret data-hiding methods are utilized to protect the data from attackers. Cryptography and steganography are the most common and widely used techniques to protect data from invaders. DNA ciphering is utilized to cipher letters for secret peer-to-peer telecommunication through nets [2]. More data is hidden when using multimedia communication for the openness and sharing of the network. Therefore, the security and confidentiality of images have become increasingly important [3]. DNA utilizes data load methods, and new biological technology can be utilized as an instrument for execution. The encryption of data is needed whilst transmitting to guarantee the security of the information post and during transmission [4].

This research is organized as follows: introduction; literature review; video steganography; 3D logistic map; DNA encoding and complementary rules; evaluating system performance; proposed system; experimental results; and conclusions.

Literature Review

This section presents the most works that related with proposed system as following

In 2016, Ruhan BA et al. [2] proposed a modern algorithm dependent on DNA ciphering, which enhances the problems that are related to the transmission of secure data through nets. This is accomplished by using a Feistel-inspired form as input and adding complex processes to it. Moreover, this article discusses DNA cipher system notions depending on the classical Vigenère encryption for interchange. A One-Time Pad is used for key obstetrics when only one key is supplied each time using a random function.

In 2017, Ramadhan M. J. et al. [5] discrete wavelet transforms (DWT) and discrete cosine transforms (DCT) are used in the proposed system. They depended on the multiple object tracking (MOT) algorithm and error-correcting codes. The motion-based MOT algorithm is executed in steward video to recognize the domains of benefit of the moving objects. The data conceal operation is complete via hiding secure letters into the DWT and DCT coefficients of every moving domain in the video relying on the visor. The result is improved embedding capacity and imperceptibility, which promotes its secure data and power through encoded secure letters.

Srushti et al. [6] proposed face recognition technologies using image and sound data collected in 2018. They are used as a tool for authentication. They proposed concealing the secured data behind sound and the recipient’s face image in video, which would require the application of numerous fixed frames of images and sound. The RSA algorithm is used to conceal encrypted scripts and images. The Whereas PCA algorithm is utilized for face recognition. The result is highly secure data. Authentication is obtained at the receiver and sender sides, which are nicely similar, so the data security can be increased.

In 2018, Shanthi et al. [7] primeframe in video is used in this proposal. It was used as a portion of envelops whenever the confidentiality of data was the first significance in correspondence. In this proposal, various kinds of information hiding are utilized depending on the medium, such as audio, video, content, images, etc. The information hidden is which letter is embedded inside the video. As well as mid-point and circle algorithms are utilized in LSB. The results show that we can use this method to enhance the efficiency of the embedding process with low distortion.

In **2018.** Alabaichi A., proposed plan, block reproduction is executed to mix image pixels through the exchange of these locations into an image. The encoded form of the DNA rule and reverse/reverse complements of the DNA are behavers to the exchange of pixel values. That way, they diffuse the image. A 3D chaotic map is then used to generate a secure key for mixing and diffusing the pixels of the image. The S-box of AES is shuffled through exchanges of the coordination values of the DNA S-box of AES to keep it mysterious. The result shows that the proposed algorithm satisfies the entire mentioned standard. This indicates that it is resistant to a variety of offensive strategies, including inclusive differential, statistical, and exhaustive offensives [8].

Al-Dabbas et al. [9] utilize 2 force secure (2FS) to cipher the images; 2SF is frequent twice on an image, which takes out strong ciphering; then hiding of the secure letter is done into the cipher of an image, which has execution utilizing a secure key (cosine curve). The stego-ciphering image has been converted for the Internet of Things into IoTs, whereas the personal requirements of any data can be obtained through IoTs. The results show the suggested system has gained the ability to be evaluated during various tests, like peak signal noise ratio (PSNR), mean square error (MSE), entropy, correlation coefficient, and histogram. The system is good; it is efficient, fast, and has high security, robustness, and transparency.

In 2020, Albaichi et al. suggested image information hiding utilizing least significant bits and secure map methods be executed through the application of 3D chaotic maps, namely, 3D Chebyshev and 3D logistic maps, in order to gain highly secure. The method has depended on the notion of executing random insertion and selecting a point from an image. The suggested is evaluated by various criteria like correlation coefficient, data entropy, homogeneity, contrast image, histogram, key sensitivity, hiding capacity, quality index, MSE, PSNR, and image fidelity [10,11,13].

Video Steganography

Information hiding in video uses a manner of hiding information or data in a set of frames in video format. The video is a set of frames or images used to hide script characters. There are numerous varied techniques utilized to hide data in various video frames, which are kept from the human eye [14]. In a varied manner, directly embedded information in the covering frame with no exchanges to good quality. Today, the information hidden in video frames plays a substantial role in data hiding [12, 13].

This safe information will be hidden in the script, images, sound and video files. Hiding secret data in all video files is called stego-video. LSB [12], Modified Least Significant Bit, and Hash-Based Least Significant Bit (HLSB) [13] were among the methods used.

1. 3D logistic Map

The logistic map function described in Equation (1) is one of the most popular and useful chaotic functions.

$$X_{n+1}=RX_n\,(1-X_n) \qquad \ldots\ldots\ldots\ldots(1)$$

This one dimensional logistic map can be extended to a 3D as definite in Equations (2) and (4).

$$X_{n+1}=RX_n\,(1-X_n) + \beta\, Y_n^2\, X_n + \alpha\, Z_n^2 \qquad \ldots\ldots\ldots\ldots(2)$$
$$Y_{n+1}=RY_n\,(1-Y_n) + \beta\, Z_n^2\, Y_n + \alpha\, X_n^2 \qquad \ldots\ldots\ldots\ldots(3)$$
$$Z_{n+1}=RZ_n\,(1-Z_n) + \beta\, X_n^2\, Z_n + \alpha\, Y_n^2 \qquad \ldots\ldots\ldots\ldots(4)$$

The parameters of the system are nonlinear and are valued in the range [$0.53 < R < 3.81$, $0 < \beta < 0.022$,
$0 < \alpha < 0.015$] where X_0, Y_0, and Z_0 are in [0, 1] [4, 10,14].

2. DNA Encode and Complementary Rule

As mentioned in the previous section, a DNA sequence has four nucleic acid bases, namely, A, C, G, and T, where A and T and C and G are complementary pairs. In a binary system, 0 and 1, 00 and 11, and 10 and 01 are complementary. If 00, 11, 10, and 01 are encoded with nucleic acid bases A, C, G, and T, then we can obtain 4! = 24 types of encoding schemes. However, only 8 types of them suit the Watson−Crick complementary rule, as indicated in Table 1 [8,14].

Table 1: Eight types of encoding and decoding rule

Rule	1	2	3	4	5	6	7	8
A	**00**	**00**	**01**	**01**	**10**	**10**	**11**	**11**
T	**11**	**11**	**10**	**10**	**01**	**01**	**00**	**00**
C	**01**	**10**	**00**	**11**	**00**	**11**	**01**	**10**
G	**10**	**01**	**11**	**00**	**11**	**00**	**10**	**01**

A RGB image can be encoded using a DNA code. Each pixel can be expressed as a DNA sequence with a length of 4 (the length of its binary sequence is 8). To improve understanding, a grayscale pixel example with 213 = (11010101)2 is provided. Depending on Table 1, the DNA code of the pixel is as follows: Rule 1 (TCCC), Rule 2 (TGGG), Rule 3 (GAAA), Rule 4 (CAAA), Rule 5 (GTTT), Rule 6 (CTTT), Rule 7 (ACCC), and Rule 8 (AGGG). DNA decode form rules are the opposite operation of DNA encode form rules. However, if Rule 2 is used to decode a pixel instead of Rule 1, for example, then another binary sequence of the pixel 11101010 will be obtained. That means the pixel value is 234 [8,15].

Evaluate System Performance

That system is assessed through the application of measures like MSE, PSNR, correlation coefficient, histogram, and entropy [10, 11, 16, and 17]. These measures are in demand to assess any modern algorithm. The modern algorithm that is overriding these measures could be an excellent algorithm.

1. Mean Square Error

MSE is computed through a comparison between two images by bytes. A point comparison, 8 bits, and so on. There are 256 levels to cover different gray levels. The most valuable MSEs are the bytes compared in an image with the matching bytes of other images. Equation (5) illustrates MSE computation as follows [18, 19, 20];

$$MSE=\frac{\sum_{m\times n}\ \ [I1(m\times n)-I2(m\times n)]}{m\times n} \qquad \ldots\ldots\ldots\ldots(5)$$

2. Peak signal to noise ration

The parameter of PSNR is utilized for measuring imperceptions in decibels. It measures the quality between two images. The value of big PSNR indicates that a tiny variation exists between two images. The value of small PSNR indicates a massive distortion between two images, as shown in Equation (6) below [21,22]:

$$PSNR= \underline{1}\text{-}\ Log_{10}\ R^{2} \qquad \ldots\ldots\ldots\ldots\ldots\ (6)$$

$$MSE$$

3. Correlation Coefficient

The measure of correlation coefficient (r) computes the range and direction of the linear collection of two randomized variables. If the two variables' values are close, then the value of the correlation coefficient is close to the value of 1. If the value coefficient is close to 0, then the two variables are not related. The value of coefficient r can be computed according to Equation (7) [23, 24].

$$r=\frac{\sum_i \quad (x_i-x_m)(y_i-y_m)}{\sum_i \quad \sqrt{\sum_i \quad (x_i-x_m)^2}\sqrt{\sum_i \quad (y_i-y_m)^2}} \qquad \ldots\ldots\ldots\ldots.(7)$$

4. Histogram

A histogram is a graph that shows the frequency of numerical data using rectangles. The height of a rectangle (the vertical axis) represents the distribution frequency of a variable (the amount or how often that variable appears). It can represent grayscale or color images. A histogram is indispensable for image normalization. Long bars mean an image has a high frequency of pixels in that value, which gives a sensible variation [20, 25]. The histogram normalized, which will increase the area of the pixels and give the best variation of the image. Equation (8) defines the balance of a new pixel value when used in this manner [19, 24, 25].

$$p(m,n) = \frac{number\ of\ pixels\ with\ scale\ level \leq (m,n)}{Total\ number\ of\ pixels}\ x(maximum\ scale\ level) \qquad \ldots\ldots.(8)$$

5. Information Entropy(IE)

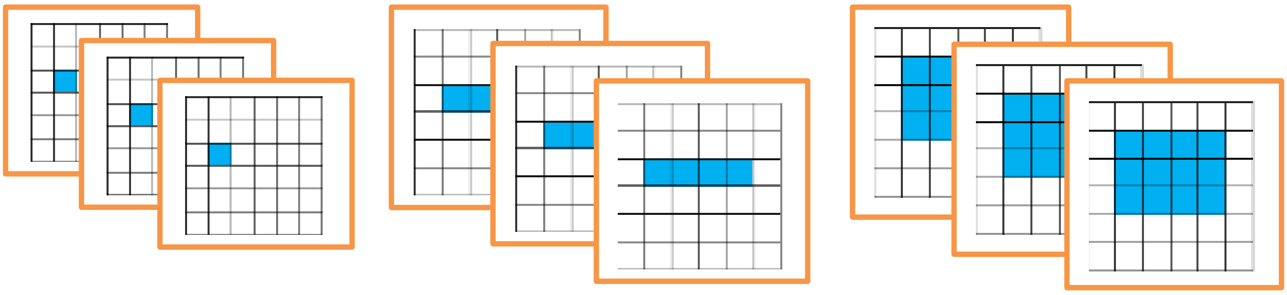
IE is the base random shape that is applied in different fields, like lossless data compression, statistical inference, machine learning, and cryptography. It measures the distribution of grey values in the image. While IE has risen, the distribution of grey values is regular. A secure hiding system is a measurement in the expression of IE. Let e1, e2,..., em be m possibility items for :probability P (e1), P (e2), ..., P (em). The entropy is given as;

$$H(e) = -\sum_{i=0}^{m-1} \quad P(e_i)log_2P(e_i) \qquad \ldots\ldots\ldots\ldots.(9)$$

The neutralization outputs a rating of the area of lower numerical bits in order to encipher a string of bits on the basis of frequency of character [8, 24,25].

Proposed System

This system encrypts secret messages and hides them in video raster. The first step of the system starts with dividing the video into many frames. Then all video frames are converted by the raster method. A video frame is a collection of objects and areas that are represented in raster format by disjointing them into their constituent points. Each point is characterized by its position in a row and a column that have appeared as (space objects) in a raster or vector video frame. The raster video frame contains more convergent locations of the represented structure in each frame, which is a collection of raster data in frames. This layer includes known coordinates such as points, lines, and areas. As shown in Figure 1, the video frame raster in color gradation is 12, 4, and 1. As shown in Figure 2, the color gradation is 4.



(a) (b) (c)

Figure 1: The video frames raster, (a) is point raster, (b) is line raster, and (c) is area raster.

(a) (b) (c)

Figure 2: The video frames raster color gradation is 4, (a) is video frame raster 1, (b) is video frame raster 2, (c) is video frame raster 3.

The next step, it is using encryption secret message in technique DNA and 3D chaotic map, convert all message to binary by using ASCII, as the following:

Convert secret message to ASCII then convert it to binary

Initialize the secret parameters of the 3D logistic map to generate secret keys using the following

equation:

$$Xi= fl\ (Xi.\ 104\ mod\ 2) \qquad \ldots(7)$$

Generate another secret key from the following equation:

$$yi= floor\ (yi.\ 104\ mod\ 7) \qquad \ldots.(8)$$

perform DNA encoding on secret message and keys in step 1 and step 2 using one of the eight

rules in Table 1 as the following:

If the value of the secret key is 0, then rule 0 will be used to encode the secret message and keys; if the value of the secret key is 1, then rule 1 will be used to encode the secret message and keys; and so, on until all secret keys and message are encoded as shown in table 2.

Table 1 in Section 2 the rules 0 to 7. Let each rule from 0 to 7 take 2^2 is equal 4 probabilities are 00, 11,01, 10. The rule 0 the A is 00, T is 11, C is 01, and G is 10, the rule 1 the A is 00, T is 11, C is 10, and G is 01, ….., and rule 7 the A is 11, T is 00, C is 10, and G is 01. In the other words, let A is inverse T, and C is inverse G always in 4 probabilities in each rule, for obtained encode and decode in the same rule in secret message.

Perform XOR between secret keys and secret messages in step 4 based on table 2.

The XOR operation in Table 3 is similar to 0 and different values of 1 among A, T, C, and G. Let A be equal 00, G be equal 10, C be equal 01, and T be equal 11.

Table 2: Performance XOR

XOR	A = 00	G =10	C = 01	T =11
A = 00	A	G	C	T
G = 10	G	A	T	C
C = 01	C	T	A	G
T = 11	T	C	G	A

Generate secret keys from the 3D logistic map using equation 4, then apply reverse and reverse complement to every four DNA sequences as follows:

$\{ reverse\ complement \qquad if\ key\ value \geq 0.5\ reverse$

$if\ key\ value < 0.5$ reverse complement = A=00, 2'S=11 become T

C= 01, 2'S =10 become G

Reverse only the value minimum 0.5 to Z make to reverse the key left to right is to reverse right to left.

And the applied 3D chaotic map in section 3 uses equations 1, 2, and 3. To obtain encryption for secret messages

The final step is embedding encryption secret messages in video frame raster using secret keys in four corners: upper left, upper right, bottom left, and bottom right. selected locations in each video frame to hide 3-bits in RGB from the video frame raster. Using the OR gate after the reset LSB in (RGB) in each location, and adding three bits. After completing all encryption secret messages, the complete embedded operation in all video frames is obtained to stego-video frame raster. As shown in Figure 3.

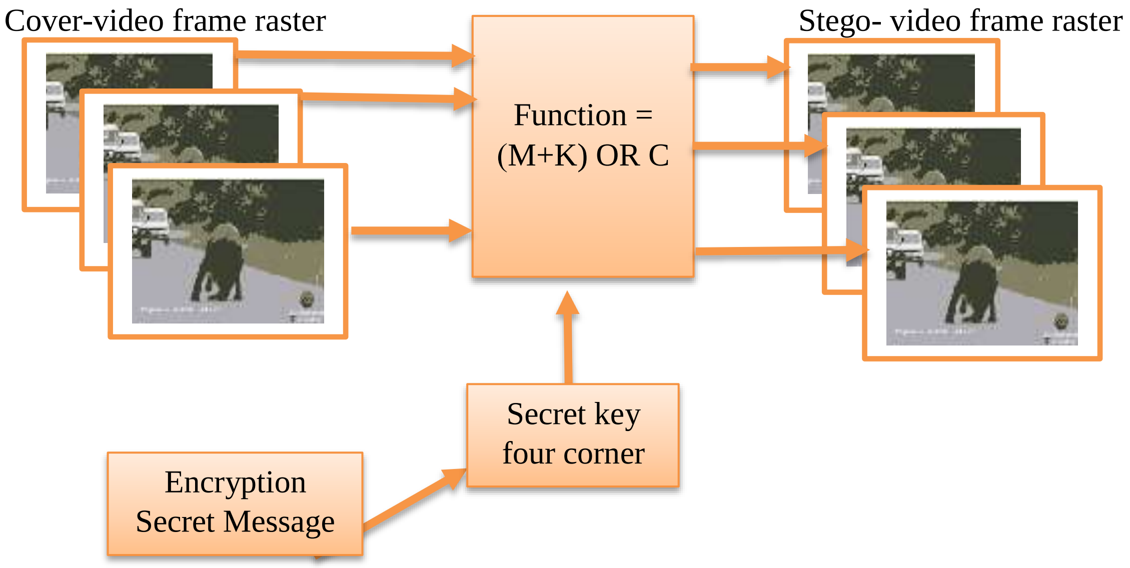


Figure 3: The stego-video frame raster.

Figure 4. explain the flowchart of embedding of proposed system after converted video to raster. And encryption secret message. Figure 5. Explain extraction secret message.

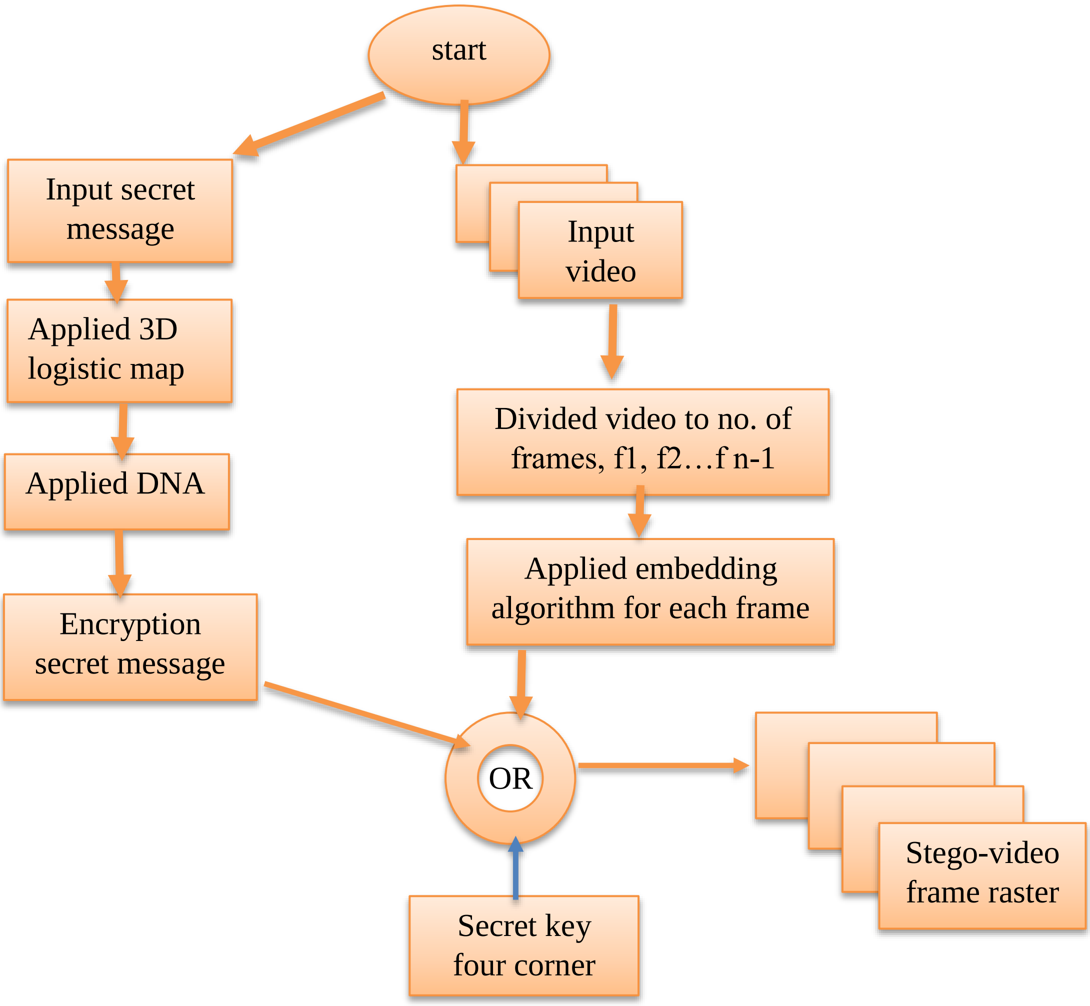


Figure 4: The embedding algorithm.

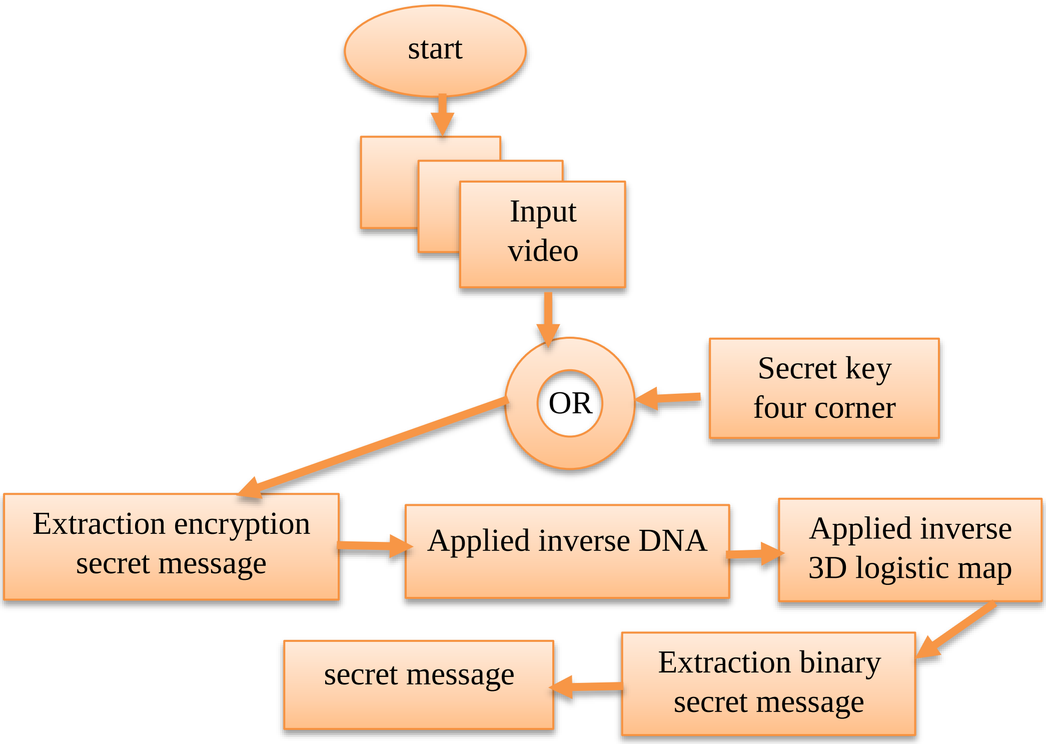

start
Input video
OR
Secret key four corner
Extraction encryption secret message
Applied inverse DNA
Applied inverse 3D logistic map
secret message
Extraction binary secret message

Figure 5: The extraction algorithm.

A- Embedding Algorithm

```
Operation:
Input: Video, Secure key, Encryption secret message.
Output: Stego- frame of video rater
    Initial:
A = Load video.
B = Load video frames.
C = Load video raster.
D = Load secret key.
E = Load secret message.
F = Load stego-frame of video raster.
Step 1: Upload video into A.
Step 2: Divided video to number of frames into B.
Step 3: Applied raster algorithm A in first step, in each video frame into C.
Step 4: Applied secure key four corners to selection locations in each frame of video raster
        into D.
Step 5: Load secret message in next step, and covert to ASCII and convert using DNA and
        3D logistic map, to embedded using location from secret key in video frame raster,
        using 3-bits in (RGB) in LSB using OR gate from encryption secret message when
        complete all message put into E.
Step 6: Put (The outcome of stego-frame of video raster) into F.

        End
```

B- Extraction Algorithm

```
Operation:
Input: Stego – frame of video rater, secure key,
Output: Secret message.
    Initial:
A = Upload stego-frame of video rater.
B = Upload secret key.
        C = Selected location from secret key four corners.
        D = extraction encryption secret message.
        E = Decryption secure letter.
        F = Secure letter.
        Step 1: Upload stego-video frame raster into A.
        Step 2: Upload secret key four corners into B.
    Step 3: Selection location from four corners in each stego-video frame raster into C.
    Step 4: extraction encryption secret message from LSB in each video frame raster using
            OR gate from each location 3-bits from (RGB) in four corners into D.
    Step 5: Applied inverse of DNA and inverse 3D logistic map, to extraction binary secret
            message, and using ASCII to extraction character of secret message into E.
    Step 6: Put (The outcome of secret message) into F.
            End
```

Experimental of Results

These experimental results explain the details of the outcomes of the proposed system and its analysis. The proposed system is based on the encryption of secret messages in DNA and 3D logistic maps. The secret message is hidden in video frames raster in color gradation 4, to prevent attackers from detecting it. Table 4 indicates differences in implementation systems among original video frame, transforming video frame to raster, and stego-video frame raster. Table 3 indicates the time of embedding and time of extraction as in Table 5. The measurements indicate the set of measurements to evaluate the power of the system when concealing secure messages into the frame of video, and the measurements rely on PSNR, MSE, entropy, correlation coefficient, histogram, and capacity. Furthermore, Table 6 shows the histogram between the original video frame, the transformed frame of video to raster, and the stego-video frame raster, whereas Table 7 shows the correlation coefficient between the original video frames, the transformed frames of video to raster, and the stego-frames of video raster.

● From the analyses of the proposed system, it can be seen that the time of embedding of secret messages is lower than the time of extraction of secret messages because the extraction algorithm is found at each location in the frames to retrieve all bits. The PSNR in three experimental frames ranged from 17.4793 to 17.5369, while the average in video frame rasters ranged from 17.4436 to 17.9369. In addition, the range of stego-video frames rasters from 17.4686 to 17.9480. In addition, it can be observed from the results that the MSE in three tests in original video frames from 30.7164 to 56.0660, the range in video frame raster from 26.3180 to 62.5795, and the range in stego-video frame raster from 26.3210 to 62.5795. Finally, from the results, it can be seen the entropy in three tests as follows: 6.7428 to 7.3158, 5.7811 to 3.5680, and 5.7831 to 3.5680 in original video frames, video frames raster, and stego-video frames raster, respectively.

Table 3: Indicates time of embedding and time of extraction.

Name of frame video	Capacity=2560 bit/size of frames	Time of embedding /second	Tim extraction /second
Tigger	0.05113	Sec.	50 Sec.
Elephant sleep	0.04732	Sec.	46 Sec.
Elephant walking	0.07820	Sec.	40 Sec.
Elephant sited	0.04723	40 Sec.	48 Sec.

Table 4: Indicates difference among original video frame, transform video frame to raster, and stego-video frame raster.

Name of video frame	Original video	Video frame raster	Steg-video frame raster
Tigger			
Elephant sleep			
Elephant walking			

Elephant sited			

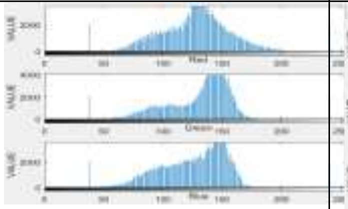
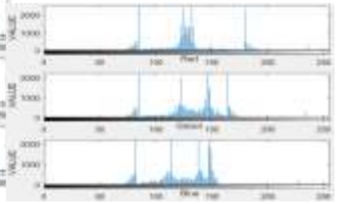
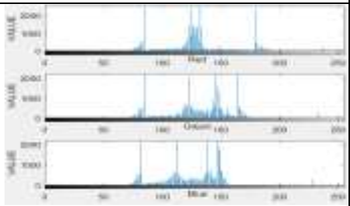
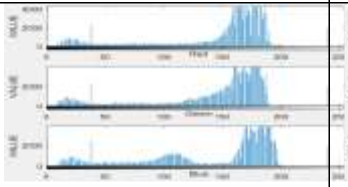
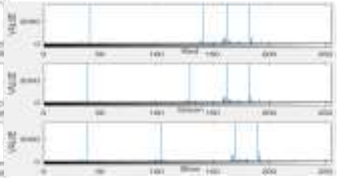
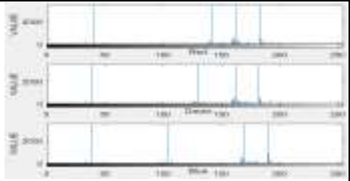
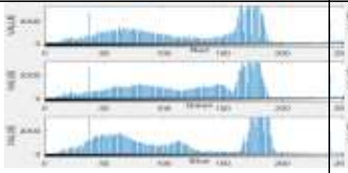
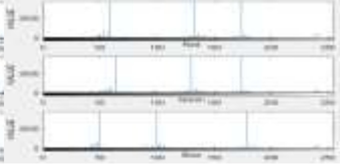
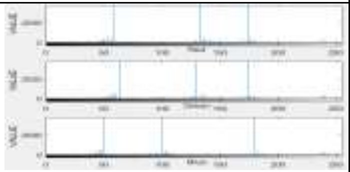
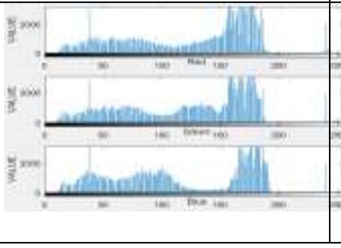
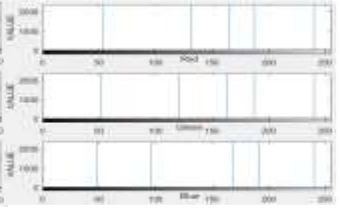
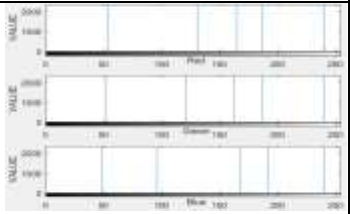
Table 5: Indicates evaluation system for PSNR, MSE, Entropy, and Correlation coefficient

Name of video frame	Measurements	Original video frame	Raster of video frame	Stego- video frame raster
Tigger	PSNR	17.4793	17.4436	17.4686
	MSE	30.7164	26.3180	26.3210
	Entropy	6.7428	5.7811	5.7831
	Correlation coefficient	0.8671	0.8525	0.8336
Elephant sleeping	PSNR	17.5489	17.5163	17.5353
	MSE	51.6485	49.1877	49.1887
	Entropy	6.9163	4.6923	4.6951
	Correlation coefficient	0.9721	0.9740	0.9764
Elephant walking	PSNR	17.6003	17.5749	17.5916
	MSE	58.1325	56.7808	56.7816
	Entropy	7.3625	4.6606	4.6635
	Correlation coefficient	0.9680	0.9381	0.9363
Elephant sited	PSNR	17.5369	17.9369	17.9480
	MSE	56.0660	62.5768	62.5795
	Entropy	7.3158	3.5549	3.5680
	Correlation coefficient	0.9847	0.9807	0.9768

1. Histogram

Histograms can be seen to appear precisely at every point in video frames. Table 6 shows the histograms of original video frames, video frame rasters, and stego-video frame rasters. It can be seen the difference between the proposed system, original video frames, video frames raster, and stego-video frames raster, as well as it can be concluded that the proposed system is better for hiding the secret letter. In addition, the large likeness among video frame rasters and the stego-video frame rasters indicates that to prevent detected secret messages from attackers. As shown in Table 6.

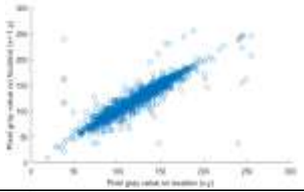
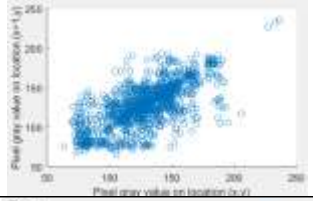
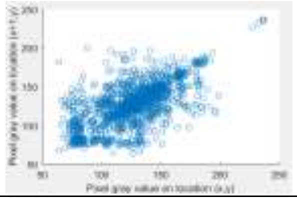
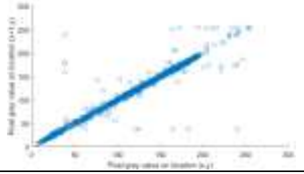
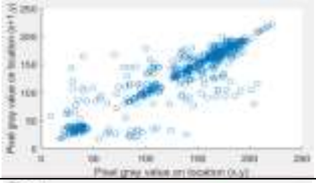
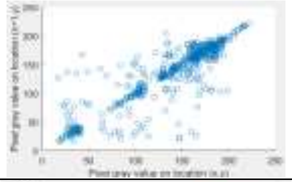
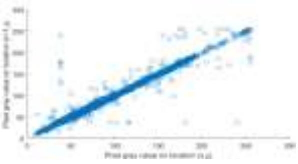
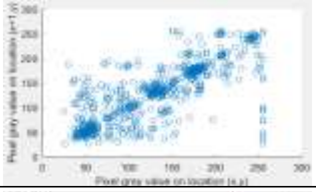
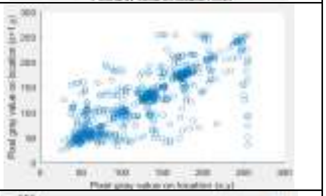
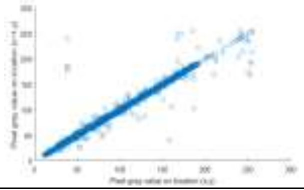
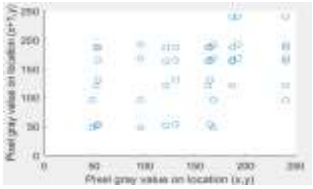
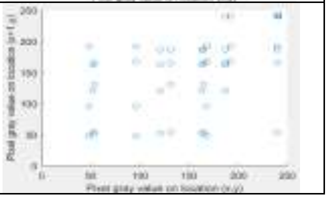
Table 6: Indicates variations histogram among original video frame, video frame raster, and stego-video frame raster.

Name of video frame	Original video	Video frame raster	Steg-video frame raster
Tigger			
Elephant sleep			
Elephant walking			
Elephant sited			

2. Correlation Coefficient

The value of the correlation coefficient is a range between one and zero. The correlation coefficients in the original video frames, video frame raster, and stego-video frame raster are 0.8671-to- 0.9847, 0.8525-to- 0.9807, and 0.8336-to- 0.9768, respectively, as shown in Table 7. From the results, it can be seen that the values of the proposed system are excellent because of the use of transforming the original video frame to raster and hiding the encryption secret message.

Table 7: shows correlation coefficient among original video frame, transform video frame to raster, and stego-video frame raster.

Name of video frame	Original video	Video frame raster	Steg-video frame raster
Tigger			
Elephant sleep			
Elephant walking			
Elephant sited			

3. High Capacity

The capacity defines the maximum number of bits that can be hidden in a video frame raster and the number of bits in secure letters. The proposed system had the capacity to hide the equivalent of 80 characters, or 640 bits, in each frame. In addition, the average capacity hidden in the proposed system is equivalent to the number of alphabets/volume of each frame of video. The size of Tigger's frame is 298168. 640 bits/50064 equals 0.01278, 322168 in Elephant Sleep, 640 bits/54096 equals 0.01183, and other images are the same. From the above results, it can be seen the total message is 320 characters, or 2560 bits' average capacity to conceal data into video frames. This average capacity can be considered excellent.

Comparing with Other studies

This section analyzes the proposed system and compares it with previous systems. The size of the farm, PSNR, and MES are used. Table 8 presents these comparisons. From the outcomes in table 8, it can be seen the best results were of the proposed system. The PSNR was decreased and MSE was increased in the stego-video frame raster. That gives the best results in comparison between the original and the stego-video frame raster. Video frame raster is used to hide secure letters in a manner that is different from the proposed system in references [5, 6, 7]. These references have used concealed to hide secure letters in video frames without converting video to video frame raster, while the proposed system uses converted video to raster and hiding secure letters is robust.

Table 8: Comparison with another previous studies

References	Size of frames	PSNR	MSE	Average time of embedding /extraction
Ref. 5 in 2017	768 × 576	35.95	-	-
Ref. 6 in 2018	16.9KB	-	-	-
Ref. 7 in 2018	-	81.9556	0.0004	-
Proposed system	248×132	17.9480	62.5795	40.5/ 46

Conclusion

This article proposed a system to conceal encrypted letters in video frames using LSB, after transforming video frames to raster. In this system, you can send 80 encrypted characters. The proposed system uses DNA and LOGISTIC maps in the encryption process. This makes the proposed system very robust. This leads the attackers to shut out the presence of secure messages from video frame raster, where any person trying to retrieve a secure message from video frame raster must have a secure key. as well as not allowing anyone unauthorized to view secure messages. The proposed system presents better efficiency, speed, power, security, transparency, and capacity as shown in table 5. The proposed system was evaluated by measures of PSNR, MSE, correlation coefficient, entropy, histogram, and capacity and gave excellent results.

References

[1] N. Gitanjali, G. Ankit, K. Vikram, W. Pooja, "A Survey of Video Steganography Techniques," *International Journal of Network Security*., Vol. 7, No. 5, pp. 33-35, 2017.

[2] BA. Ruhan, S. Malarvizhi, P. Kathan, "Information Coding and its Retrieval using DNA Cryptography," *Journal of Engineering Science and Technology Review*., Vol. 9, No, 3, pp. 86 – 92, 2016.

[3] Z. Shuqin, Z. Congxu, "Secure Image Encryption Algorithm Based on Hyperchaos and Dynamic DNA Coding," *Entropy MDPI*., Vol. 22, No. 772, pp. 1-20, 2020.

[4] G. A. Omar, G. K. Shawkat, "DNA Computing and Its Application to Information and Data Security Field: A Survey," *International Journal of Academic Engineering Research (IJAER).*, Vol. 3, No. 1, pp.1-5, 2019.

[5] M. J. Ramadhan, E. M. Khaled, Eman A., "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC," *IEEE. Translations and content mining are permitted for academic research only*., Vol. 5, pp. 5354- 5365, 2017.

[6] S. Srushti, R. Pracheta, J. Prajakta, Y. Tejaswini, "Data Security using Audio-Video Steganography," *International Journal of Engineering Research & Technology (IJERT)*., Vol. 7, No. 02, pp. 105-108, 2018.

[7] R. M. Mary Shanthi, L. S, D. G., "Video Steganography Using Mid-Point Circle Algorithm and Spatial Domain Technique," *International Journal of Engineering and Techniques*., Vol. 4, No. 1, pp. 98-105, 2018.

[8] AL. Ashawk, "True Color Image Encryption Based on DNA Sequence, 3D Chaotic map, And Key-Dependent DNA S-BOX of AES," *Journal of Theoretical and Applied Information Technology*., Vol. 96, No. 2, pp.304-321, 2018.

[9] K. Maisa'a Abid Ali, AL. Ashawk, A. Ahmed Saleem,"Dual method cryptography image by two force secure and steganography secret message in Iota," *TELECOMNIK Telecommunication, Computing, Electronics and Control*., Vol.18, No.6, pp. 2928-2938, 2020.

[10] AL. Ashawk, K. Maisa'a Abid Ali Al-Dabbas, and S. Adnan, "Image steganography using least significant bit and secret map techniques," *International Journal of Electrical and Computer Engineering (TTECE).*, Vol.10, No. 1, pp. 935-946, 2020.

[11] S. Aditya Kumar, S. Monalisa, "Digital Image Steganography Techniques in Spatial Domain: A study," *IJPT*., Vol. 8, No. 5, pp.5205- 5217, 2017.

[12] A. Mohammed Sabri, R. C.B.M, R. Rafikha Aliana A., H. Safa. Saad, "Digital Image Steganography in Spatial Domain a Comprehensive Review," *Journal of Theoretical and Applied Information Technology*., Vol. 97, No. 19, pp. 5081- 5102, 2019.

[13] R. Abdul Monam Salah, Khodher. Maisa'a Abid Ali, "Proposing an Analysis System to Monitoring Weightlifting Based on Training (Snatch and Clean and Jerk)," *Baghdad Science Journal*, 15(4): 493-502, 2018.

[14] S. Adnan. Ibrahem, Al. Ashawk, A. Ahmed Saleem., "A Novel Approach for Enhancing Security of Advance Encryption Stand using Private XOR Table and 3D Chaotic Regarding to Software Quality Factor," *ICIC Express Letters*., Vol. 10, No. 9, pp. 823-832, 2019.

[15] S. Aditya kuma, S. Mmonalisa, "Digital Image Steganography and Steganalysis: A journey of the past three decades," *Open Compute Sci*., Vol. 10, pp. 296–342, 2020.

[16] A. Aung Myint, "LSB Based Image Steganography for Information Security System," International *Journal of Trend in Scientific Research and Development*., Vol. 3, No. 1, pp. 394-400, 2018.

[17] S. Ansam, H. Shaymaa, K. Maisa'a Abid Ali, "Key Generation Based on Henon Map and Lorenz system," *Al-Mustansiriyah Journal of Science*., Vol. 31, No. 1, pp. 41-46, 2020.

[18] H. Mohammed Mahdi, R. Mohd Shafry Mohd, J. Fadil Abass, T. Mustafa Saba, H. Salman Hamad., "Performance Evaluation Measurement of Image Steganography Techniques with Analysis of LSB Based on Variation Image Formats," *International Journal of Engineering & Technology*., Vol. 7, No. 4, pp. 3505-3514, 2018.

[19] G. Mamad, K. Ali, "A robust Chaotic Algorithm for Digital Image Steganography," Communicat *-ions in Non-linear Science and Numerical Simulation*., Vol. 19, No. 6, pp. 1898-1907, 2014.

[20] H. Iman I., "Image Steganography Based on Discrete Wavelet Transform and Chaotic Map," *International Journal of Science and Research IJSR*, Vol. 2016, pp.588-591, 2016.

[21] K. Maisa' Abid ali, J. Shatha Habbeb, "Concealed Secret Letter Using a 2D Wavelet Packet," 2nd CIMS *AIP Conference Proceedings*., pp. 030007-1- 030007-4, l 2019.

[22] K. Maisa'a Abid Ali, R. Abdul Monem. Salah, "Suggesting an Analysis System for Monitoring Free Hand Gymnastics for Training Youth," *2nd Scientific Conference of Computer Sciences (SCCS).*, 2019.

[23] K. Maisa'a Abid Ali, "Hide Secret Messages in Raster Images for Transmission to Satellites Using a 2-D Wavelet Packet," *Iraqi Journal of science*., Vol. 59, No. 2B, pp. 922-933, 2018.

[24] M. Sally. Adana, K. Maisa'a Abid Ali, "An Improved Method for Combine (LSB and MSB) Based on Color Image RGB," *Engineering and Technology Journal*, Part B, Vol. 39, No. 01, pp. 231-242, 2021.

[25] S. Khadeeja Gebor, Al. Saif M. Kh., J. Majid Jabbar, "Improved Image Security in Internet of Thing
(IOT) Using Multiple Key AES," *Baghdad Science Journal*., Vol. 18, No. 2, pp. 417-429, 2021.