




A SECURE DATA HIDING FOR H.264 VIDEO BASED ON CHAOTIC MAP METHODS AND RC4 ALGORITHM

Mustafa M. Mashkour ¹, Lahieb M. Jawad ¹, Ghazali Sulong ²

¹ College of Information Engineering, Al-Nahrain University, Baghdad, Iraq

² Centre of Cyber Security and Big Data, Management and Science University, Kuala Lumpur, Malaysia
muntherm35@gmail.com , lahieb1978@gmail.com

lahieb.m.jawad@nahrainuniv.edu.iq

ghazali_sulong@usm.edu.my

Corresponding Author: Ghazali Sulong

Received: 22/05/2023; Revised: 29/07/2023; Accepted: 28/08/2023

DOI:[10.31987/ijict.6.3.250](https://doi.org/10.31987/ijict.6.3.250)

Abstract- Video steganography is a common field of data security in digital communication where data include text, image, and video. Compressed video is a suitable modern source for hiding huge secret data that will trust security. This work proposes a compressed video steganography scheme for hiding cipher secret data at high-security levels. The proposed work consists of four phases, protected secret data (Text in English, Text in Arabic, Image, and Video) based on the chaotic maps module and RC4 algorithm. The chaotic maps module is a combination of (a Henon map and a sine map) with simple operations for key generation. As for the RC4 algorithm, it is one of the encryption algorithms of stream data, and its weakness has been addressed by strengthening the key in the proposed module for key generation, so it will be strong. Second phase, hidden cipher secret data between the quantized discrete cosine transform (QDCT) and entropy coding from the inter-prediction mode at the H.264/AVC video frames using Least Significant Bit (LSB) replacement. The third phase is transmitting and receiving secret data. The fourth phase, recover plain data from the compressed video steganography. The experimental result shows that the proposed scheme is a high-security level where cipher secret data with an average entropy value of (7.9992), an average PSNR value of (8.790 dB), an average correlation value of (0.0042), a key length is 228 bit and key space is 2^{228} . Moreover, the measured Randomness of the generation key by NIST succeeded in all the tests of Robustness, and imperceptibility. Embedding capacity is high while maintaining visual quality, where the average PSNR value is about (36.65 dB), and the average SSIM value is about (0.95).

keywords: Chaotic maps, Data hiding, RC4 algorithm, H.264, Secret data, Embedding capacity.

I. INTRODUCTION

Data protection plays an important role in protecting and maintaining secrecy in the digital communication world. Data protection techniques were categorized as Steganography, Cryptography, and Watermarking. Steganography is one of the traditional communication-securing techniques [1]. The role of steganography is to hide the secret data inside other data based on various embedding techniques, where the data can be Text, Image, Audio, or Video [2]. The video is more suitable for data hiding than other steganography resources. Hence, transmitting video can hide a large size of secret data such as text, image, video, and audio because the video includes a large number of parameters that can be used in hiding named video steganography [2]. Video steganography is classified into two approaches, uncompressed, and compressed video steganography [1], [3]. The parameters that can hide secret data in compressed video at H.264/AVC are entropy Coding, Transform Coefficients, Motion Vector Estimation, Inter-Frame Prediction, and Intra intra-frame prediction [4]. Each parameter of hiding secret data is different in characteristics from sides: complexity level, quality of the cover video, and embedding capacity [2], [5]. The proposed work consists of four phases, protected secret data based on the proposed chaotic maps module and RC4 algorithm. The chaotic maps module is a combination of (the Hoenn map and Sine map)

with simple operations to protect plain data. The preference for chaotic maps hybrid and RC4 algorithm over any other cryptographic algorithm is due to its ability to provide better security with High speed and Flexibility, Unpredictable and nonlinear Enjoy with high randomness and low computational complexity. Second phase, hidden cipher secret data between the (QDCT) and entropy coding from the inter-prediction mode at the H.264/AVC video frames are used (LSB) replacement. The third phase is transmitting and receiving secret data. The fourth phase, recover plain data from the compressed video steganography. The experiments are conducted to validate the proposed scheme in terms of imperceptibility, robustness, embedding capacity, and embedding efficiency. In the proposed scheme, the chaos encryptions by sine and Hoenn maps with the RC4 algorithm are used to encrypt the secret data for high-security levels, where chaos encryption increases the security of the RC4 algorithm. The input video frames are compressed at H.264/AVC technique and LSB replacement is performed to embed the cipher secret data into the cover compressed video. Then, the cipher secret data are retrieved by H.264/AVC technique with deciphering of the secret data. This paper is structured as follows. The first section introduction, the second section literature review, the third section focuses proposed methodology, the fourth section focuses on experimental results shows analysis and discussion, and finally, section five concludes the paper and suggests future works.

II. LITERATURE REVIEW

Various video steganography techniques have been proposed to enhance H.264/AVC standard. These techniques are implemented to increase protection security levels, improve embedding capacity in compressed video, improve the quality of the cover video, and decrease the bitrate generated from hiding processes. An explanation and short description for each technique are described below these works. In 2019 [7], a steganography technique to increase the capacity of embedded compressed video frames at (H.264/AVC) technique. The coefficients of the (QDCT) were split into two different groups in the suggested method: hiding and preventing groups. The results showed the QDCT with hiding direction table increases better hiding. Analysis was preserving the great PSNR and SSIM of the Stego video. However, the embedding capacity was medium because using I frame from group-of-picture and these types of frames were very rare to return each 10 frames and also using QDCT without encryption to secret data is less secure because of easy discovery. In 2019 [6], Presented a steganography technique based on the (QDCT) coefficient of I-frames at (H.264/AVC) technique and Syndrome-Trellis Code (STC). The results showed an increase in security performance in resisting steganalysis attacks. However, embedding capacity is low due to using I-frames and these types of frames are infrequent and need a more practical technique to achieve better embedding capacity (EC). In 2021[8], Implemented a hiding scheme using discrete sine transform secret bit positions of the non-dynamic region for message to embedding secret RGB image in intra-prediction from (H.264/AVC) advance video coding. Results show that this algorithm has low imperceptibility, robustness, and embedding capacity. In 2021 [9], a steganography technique in (H.264/AVC) video frames. Secret data was encrypted using Cryptography methods before hiding it. The encrypted secret data was embedded into the (DCT) coefficients of (I, B, and P) video frames. The results showed increasing security by encrypting the secret data before embedding it, but the methods used for encryption requires time and optimization technique to achieve better embedding capacity. In 2022 [10], Developed a steganography scheme using (QDCT) coefficients of intra-frame mode at (H.264/AVC) video frames. Secret data was ciphered using a private key. Then, the coefficients pair mapping is used to hide the cipher secret data. The results showed that the proposed

algorithm obtains good visual quality of marked videos; however, the embedding capacity was medium. The results showed maximum embedding capacity was 19,152 bits.

III. PROPOSED METHODOLOGY

This section explains the design of the proposed secure compressed video steganography system. First proposed cipher scheme, and embedding this cipher secret data in compressed video.

A. Proposed Cipher Scheme

The proposed cipher scheme includes two stages, a key generation module based on chaotic maps and cipher secret data.

- **Generation of key:** The proposed key generation module met the criteria for being a suitable and robust key that can be used as the secret key with the RC4 algorithm from the perspective of cryptography. This model employs chaotic map methods (Henon map and sine map), respectively, as illustrated in Fig. 1. The equations for these maps are Henon (1), (2), and sine (3) [11],[12]. To increase the security and the randomness of the generated key, several operations are done between the chaotic paths (X, Y, Z), the first operation is sorting X sequence, and the new positions of its sequence bytes are taken to order Z sequence bytes with it. The following operation is XOR the rearranged Y with Z sequence, then the produced sequence is XOR with the sorted X to key sequence.

$$X_{(n+1)} = 1 - aX_n^2 + Y_n \quad (1)$$

$$Y_{(n+1)} = bX_n \quad (2)$$

$$Z_{(n+1)} = r \sin(\pi Z_n) \quad (3)$$

Where a is the parameter as key together with initial values X_0 , b is the parameter as key together with initial values Y_0 at Hoenn map, and r is the control parameter as key together with initial values Z_0 at sine map.

- **Cipher secret data:** The cipher secret data in the first step must to converted from secret data to binary secret data before hiding in compressed video, the RC4 algorithm is used with the generated key sequence. Based on the RC4 algorithm structure generating a keystream with a length equal to the secret data length then this keystream is XORed with the plaintext in binary level as shown in Fig. 2.

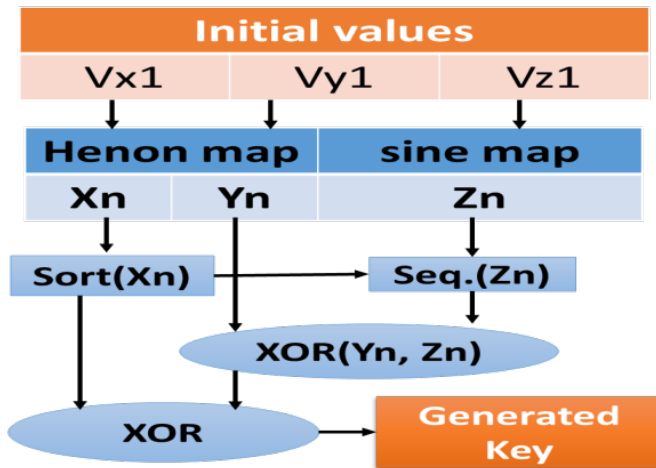


Fig. 1: Generation key based on chaotic maps



Fig. 2: Cipher secret data by keystream

B. *The proposed Hiding Ciphered Secret Data Method*

Consists of three main stages, first, choose the Group of Picture (GOP) structure of compressed video in (H.264/AVC), which is IPPP..., where the first frame is encoded as I-frame and the remaining frames are encoded as P-frames, second stage, is to choose an inter-frame mode of compressed video for hiding ciphered secret data in it, third stage, is to the embedding procedure.

- **GOP:**The video sequence is composed of a header and number of (GOP), the video sequence header defines the video format, picture dimension, number of frames, start frames and size of secret data, and type of secret data. The GOP header contains the starting for the group represented by the first I-frames followed by the number of inter-prediction modes.
- **Region hiding in compressed video:** compressed video has three types of frames (I, P, and B) that are accessible. Furthermore, the frame type influences the choices made for hiding cipher secret data. This study did not use I-frames since these types of frames are very rare to use because they affect compressed video. But have the option to embed in P frames. As shown in Fig. 3.

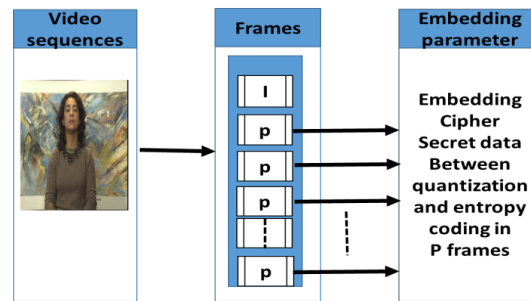


Figure 3: Parameter hiding in compressed video

- **Embedding cipher secret data to cover video:** Let cq be the coefficients quantization matrix of size 4×4 for each block, and csd is the cipher vector of size $(1 \times m)$. Moreover, the coefficient values that are used for embedding cipher data are the set $[2, -2, -1, 3]$ that are used for embedding data via generating a cq new matrix. Hence, the proposed method is

$$cq_{new} = \begin{cases} -2 & \text{where } (csd = 0 \ \& \ (cq = 1 \ \text{or} \ cq = -2)) \\ +2 & \text{where } (csd = 0 \ \& \ (cq = 2 \ \text{or} \ cq = 3)) \\ -1 & \text{where } (csd = 1 \ \& \ (cq = -1 \ \text{or} \ cq = -2)) \\ 3 & \text{where } (csd = 1 \ \& \ (cq = 2 \ \text{or} \ cq = 3)) \\ cq & \text{otherwise} \end{cases} \quad (4)$$

Fig. 4 shows a better explanation of the proposed scheme of the DCT-based embedding algorithm.

1. Assume that Fig. 4 (a) is the original (QDCT) coefficient block, and the cipher secret data in binary (csd) is ...01101101.
2. To embed cipher secret data (csd) into this (QDCT) coefficient block, using Eq. (4) will hide cipher secret data (csd) as shown in Fig. 4 (b).

Where $cq(1, 4) = -1$ with $csd = 1$, the hiding of the $QDCT$ coefficient has no change. $cq(1, 4) = -1$.

And where $cq(4, 3) = -1$ with $csd = 0$, the $QDCT$ coefficients have changed. $cq(4, 3) = -2$. Notice that this block of quantization has a two-bit hide only.



Fig. 4: The QDCT coefficients: (a) before and (b) after the embedding operation

Fig. 5 presents the embedding procedure. For each coefficient pair, the value of coefficient quantization $cq(i)$ is checked through embedding the cipher secret bit by using Eq. (4). Moreover, in the proposed method, to increase the security of the proposed method, before the embedding process, the secret data (sd) should be ciphered with keystream that is described in previous.

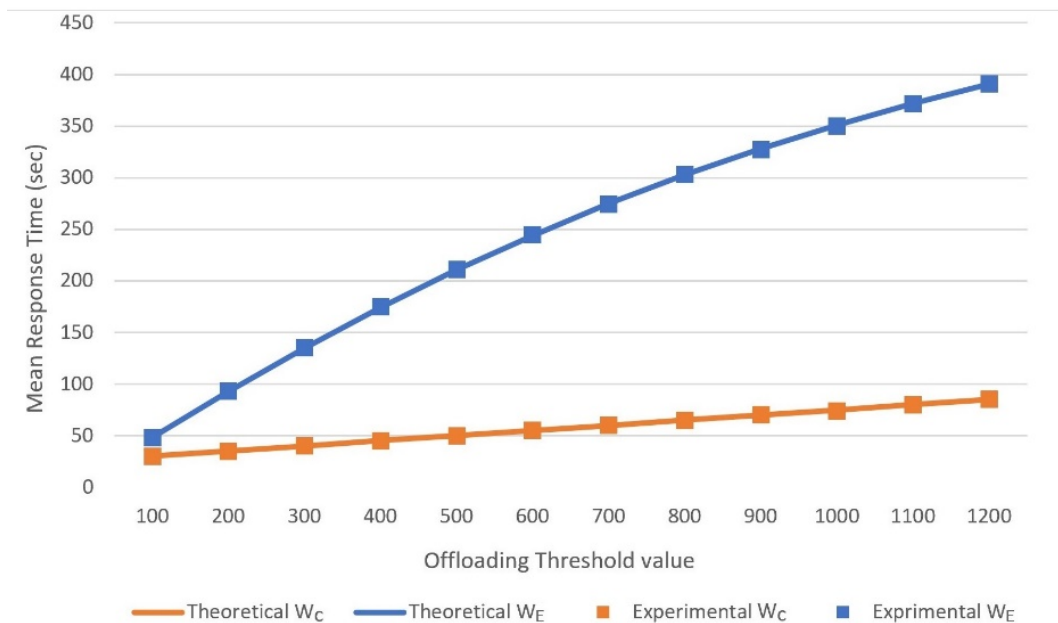


Fig. 5: Embedding operations in (H.264/AVC)

C. Procedure of Extraction

The receiver receives stego bit streams and then applies the extracting algorithm to extract the Cipher Secret Data (csd) as shown in Fig. 6. The stego bit streams are entropy decoded to regenerate the Quantized Discrete Cosine Transform (QDCT) coefficient blocks. The hidden data is extracted from the QDCT coefficient blocks. The hidden cipher secret data ($csd(1), csd(2), \dots, csd(n)$), where $csd(i) \in \{0, 1\}$, is extracted using Eq. (5).

$$csd(i) = \begin{cases} 0, & \text{if } cq(i) = 2, -2 \\ 1, & \text{if } cq(i) = 1, 3 \end{cases} \quad (5)$$

D. Decipher procedure to Secret Data

In terms of the design of the deciphering algorithm, do the inverse process of the cipher steps. Where the same keystream is XORed with the cipher secret data at binary level resulting plaintext in at binary level then after decrypted to reconstruct the secret data to the same type of secret data sent.

IV. RESULTS AND DISCUSSION

The experimental analysis is done using the standard video dataset which consists of fourteen color videos (akiyo, news, bridge-close, mobile, bridge-far, grandma, car phone, hall, Claire, foreman, coastguard, container, grandma, mother-daughter, and salesman) of (176 × 144 pixels/frame). The first 300 frames of each video sequence are encoded at 30 frames per second [<http://trace.eas.asu.edu/yuv/>]. The GOP structure is IPPP..., where the first frame is encoded as an I-frame and the remaining frames are encoded as P-frames. These raw videos are input to (H.264/AVC) for compression and chaos encryption for cipher the secret data and dataset to data secret can be as a text such as (Arabic or English) language, Image using the standard dataset which consists of Lena and cameraman [<https://imageprocessingplace.com/>], or a video that is used in the cover.

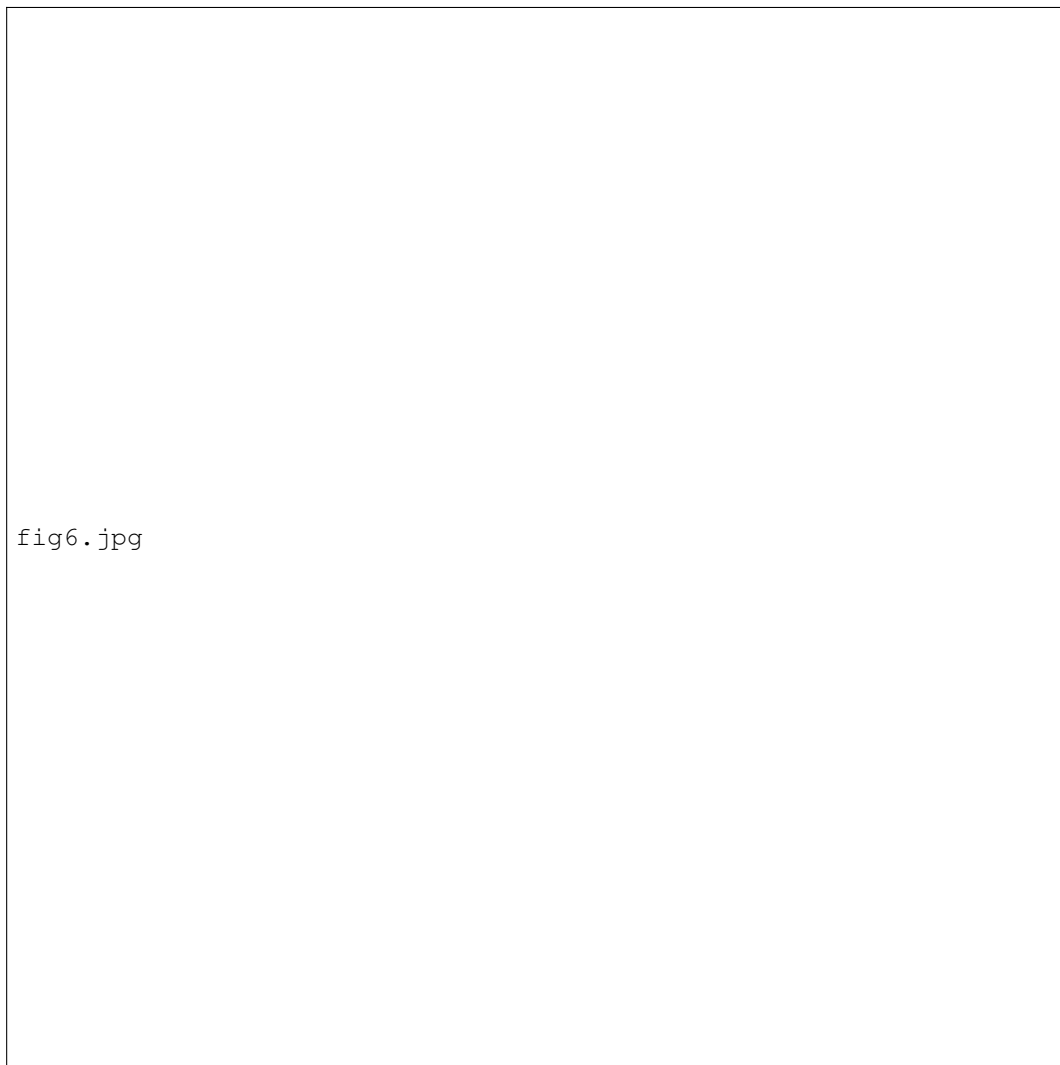


Fig. 6: Extracting cipher secret data from stego. video

A. Performance Analysis Encryption Secret Data

This section shows and analyzes the results of the major objective, which is to demonstrate and evaluate the efficiency of the suggested cipher secret data. In addition, perceptual quality is one of the evaluations for the strength of the cipher as a performance analysis measure.

- 1) **Results of visual intelligibility:** This is a subjective metric that measures the intelligibility quality of the secret data, as shown in Table I, the cipher secret data (Text in Arabic or English, Image, Video) are very noisy and unclear which means that the proposed algorithm encryption guarantees visual perception security.
- 2) **PSNR encryption test:** The PSNR evaluation for the testing secret data (secret image and video) is implemented in Table I as it is obvious that the values of all secret data in the cipher suffer from a strong descending, this indicates

the high level of security and protection that provided by the encryption scheme proposed. Eq. (6) used to calculate The PSNR [2].

$$PSNR(dB) = 10 \cdot \log_{10} \left(\frac{\text{MAXIMUM PIXEL}_X^2}{\text{MEAN SQUARE ERROR}} \right) \quad (6)$$

Where X; is the original frames, and MAXIMUM PIXEL x shows the value of the highest pixel in frames X.

- 3) **Information entropy:** The entropy analysis determines how random the encryption process is. As can be seen, the result values of the two encrypted secret data (Images) is about 7.9992, indicating both a high degree of unpredictability and a high degree of degradation in the quality of the data, as shown in Table I. Eq. (7), used to calculate it [10].

$$H(m) = \sum_{i=0}^{n-1} P(S_i) \log_1 \left(\frac{1}{P(S_i)} \right) \quad (7)$$

Where (Si) indicates the pixel values, P(Si) refers to the probability of the symbol (Si), and (n) is the total number of symbols which is equal to (256) for the grayscale images.

- 4) **Correlation:** Correlation in selected secret data (images and video) and their encryption secret data obtained from encryption are given in Table I the results of the two images of the encrypted secret data refer to the very small values. This means that the encryption process is capable of hiding the details of the original image. Function corr () in Matlab is used to calculate it.
- 5) **Randomness:** The National Institute of Standards and Technology (NIST) is a statistical test to measure the randomness of the output pseudo-random number generator sequence in binary form. NIST test includes 15 tests that focus on a variety of different randomness types that could exist in a sequence If the computed test value of all 15 tests is smaller than (0.01), then this sequence is non-random. Otherwise, conclude that the sequence is random. In Table II, all fifteen tests are practiced to the generated key by the chaotic system and the computed results values of all tests are larger than (0.01) which indicates the high randomness of the chaotic sequence [11].

TABLE I
 RESULTS OF PERFORMANCE ANALYSIS ENCRYPTION SECRET DATA

Seq	Original	Encryption	Decryption	MSE	PSNR (dB.)	Entropy	Corr.
Lena	5/L1 .png	5/L2 .png	5/L3 .png	7831.9	9.1845	7.9993	-0.0060
cameraman	5/C1 .png	5/C2 .png	5/C3 .png	9405.8	8.3969	7.9990	0.0014
miss-America(video)	5/M1 .png	5/M2 .png	5/M3 .png	8928.9	8.6181	_____	0.00021
English (txt)	5/TE1 .png	5/TE2 .png	5/TE1 .png	_____	_____	_____	_____
Text Arabic	5/T1 .png	5/T2 .png	5/T3 .png	_____	_____	_____	_____

B. Performance Analysis of the Hiding Method

The main goal of this section is to analyze the efficiency of the proposed compressed video steganography. The performance analysis includes measuring capacity embedding, imperceptibility of PSNR and SSIM, similarity, embedding efficiency, and robustness with different quantization parameters (QP). The QP is either 18, 28, or 38.

TABLE II
 RESULTS RANDOMNESS OF NIST TESTS

1	Frequency Test	1.000	9	Universal	0.971
2	Block Frequency	0.013	10	Linear Complexity	0.436
3	Runs	0.425	11	Serial	0.064
4	Longest Run	0.030	12	Approximate Entropy	1.000
5	Rank	0.298	13	Cumulative Sums	1.000
6	FFT	0.076	14	Random Excursions	0.072
7	Non-Overlapping Template	0.980	15	Random Excursions Variant	0.025
8	Overlapping Template	0.604			

- 1) **Results of visual intelligibility:** This is a subjective metric that measures the intelligibility quality of cover video. The cover videos that hide secret data guarantee visual perception security. As shown in Table III frame number two of videos before and after embedding secret data with QP=28.

TABLE III
 VISUAL INTELLIGIBILITY

Seq.	Original image	Stego. image
bridge-close	5/br1.png	5/br2.png
Coastguard	5/co1.png	5/co2.png
Container	5/con1.png	5/con2.png

- 2) **Embedding capacity block:** The Embedding capacity block (ECB) to the proposed Algorithm in terms of the number of bits per 4x4 block between quantization and entropy. As shown in Table IV. Eq. (8), is used to calculate the embedding capacity block [14]. As shown focused on the Embedding capacity blocks values of the embedded secret data in cover videos, it will be noticed that the embedding capacity in cover videos with the highest values when the smallest amount of quantization parameter (QP) is the proportion between the embedding capacity and the QP is opposite proportional and proportion between the compressed rate and the QP is directly proportional. In this

case, one must balance between compressed rate and embedding capacity. There are also differences in embedding capacity between cover videos, result show the number of pixels in the quantization block that have these values (3, 2, -1, -2).

$$ECB = \left(\frac{\text{BIT USED FOR STEGO.}}{\text{number of } 4 \times 4 \text{ blocks}} \right) \times 100\% \quad (8)$$

TABLE IV
 RESULTS EMBEDDING CAPACITY

Sequence	QP	QP	QP
	18	28	38
Akiyo	0.55	0.16	0.015
bridge-close	3.9	1.33	0.19
bridge-far	2.9	0.99	0.2
Car phone	2.6	0.62	0.18
Claire	2.12	0.17	0.02
Coastguard	2.1	0.90	0.15
Container	2.7	0.29	0.04
Foreman	3.2	0.60	0.09
Grandma	2.7	0.30	0.03
Hall	3.5	0.59	0.12
Mobile	2.6	1.99	0.42
mother-daughter	3.5	0.24	0.03
News	1.7	0.35	0.02
Salesman	3.1	0.55	0.10

- 3) **PSNR video steganography test:**The PSNR evaluation for the testing cover videos is implemented in Table V. As it is obvious that the values of all cover videos do not affect then one can compare between PSNR after and before embedding (PAE /PBE), which are small. This indicates the high level of security and protection provided by the scheme proposed. The PSNR values of the difference between after and before embedding are ranged between (2.2958) and (0.7542) decibels. Eq. (6), is used to calculate the ratio (PSNR)[2].
- 4) **SSIM video steganography test:**The SSIM analysis for testing cover video sequences is given in Table V. The values of average SSIM are ranged between (0.986-0.885) and as the SSIM values are closer to one, the similarity between two cover video after and before are being higher and the security is high. The SSIM values of the after-embedding cover videos are very close to one which means that the quality of these cover videos is very good. These results ensure that the proposed system guarantees high protection of the embedded secret data in the cover videos. Eq. (9) is used to compute structural similarity (SSIM) [2].

$$SSIM = \frac{(2\beta_X\beta_Y + \rho_1)(2\sigma_X + \rho_2)}{(\beta_X^2 + \beta_Y^2 + \rho_1)(\sigma_X^2 + \sigma_Y^2 + \rho_2)} \quad (9)$$

Where X is the original frame, Y is the embedded frames, ρ_1 and ρ_2 are the fixed values, β_X and β_Y are the

mean values of original and embedded frames, and σ_X and σ_Y represent the standard deviation of pixel values in frames X and Y .

TABLE V
 SSIM AND PSNR VIDEO STEGANOGRAPHY TEST

Sequence	SSIM			PSNR with QP=28	
	QP=18	QP=28	QP=38	PBE	PAE
Akiyo	0.990	0.970	0.898	39.7961	37.5003
bridge-close	0.989	0.960	0.857	36.3958	35.3646
bridge-far	0.991	0.962	0.839	37.3106	36.5342
Car phone	0.978	0.976	0.914	38.4944	37.7402
Claire	0.978	0.978	0.922	41.0486	38.4140
Coastguard	0.995	0.965	0.850	36.6457	35.6475
Container	0.987	0.962	0.883	37.9037	35.8716
Foreman	0.988	0.972	0.912	37.8869	37.0244
Grandma	0.989	0.964	0.881	38.5131	36.4013
Hall	0.970	0.971	0.884	38.0954	36.3189
Mobile	0.980	0.969	0.908	35.5804	33.5319
mother-daughter	0.979	0.971	0.895	39.4164	37.6439
News	0.987	0.970	0.915	38.4055	35.68
Salesman	0.996	0.965	0.838	37.5221	35.9741
Average	0.986	0.968	0.885	38.07	36.40

- 4) **Bitrate steganography video test:** The Bitrate for the testing covers videos that are implemented by using Eq. (10) in Table VI with QP=28. Bitrates directly affect the file size, quality of cover videos, internet connection speed, and the cost of bandwidth. There is a bit rate increase for Stego. The video is very low. This is one of the advantages of the proposed approach it has resulted from the mechanism of data hiding [7].

$$\text{Increase bit rate} = \left(\frac{\text{bitrate after embedding} - \text{bitrate before embedding}}{\text{bitrate before embedding}} \right) \times 100\% \quad (10)$$

C. Comparative Evaluation

This section compares the performance of the proposed system with various compressed video steganography approach in different quantitation parameter (QP) 18, 28, and 28. Table VII shows the comparison of (ECB) between the proposed method with existing methods [13], [14], [4], and [7]. The ECB value obtained by the proposed methods is always higher than that of [13]. Table VII shows a comparison of the average ECB. The average of improvement of the proposed method from method [13] is 32.4%.

TABLE VI
BITRATE VIDEO STEGANOGRAPHY TEST WITH 28

Sequence	Bit rate(kb/s) (Org. Video)	Bit rate(kb/s) (Stego. Video)	Bitrate increment %
Akiyo	1122	1134	1.06
bridge-close	1365	1388	1.66
bridge-far	859	921	6.7
Car phone	1268	1276	0.63
Claire	947	963	1.66
Coastguard	1475	1488	0.87
Container	1323	1333	0.75
Foreman	1395	1390	-0.36
Grandma	1142	1147	0.45
Hall	1321	1334	0.97
Mobile	2425	2434	0.37
mother-daughter	1106	1111	0.45
News	1406	1405	-0.07
Salesman	1450	1453	0.21
Average	1228	1341	1.09

TABLE VII
COMPARISON OF THE EMBEDDING CAPACITY

QP	[13]	[14]	[4]	[7]	Proposed	Improvement with [13] %
18	0.97	1.03	0.93	1.29	2.7	64%
28	0.50	0.73	0.54	0.97	0.65	23.1%
38	0.10	0.35	0.22	0.54	0.11	10%
Avg.	0.52	0.70	0.575	0.93	1.15	32.4%

Table VIII shows the comparison of PSNR and SSIM between the proposed schemes and existing schemes [13], [4], [14], and [7]. Table VIII shows the average of the PSNR proposed scheme is 36.65 dB. The PSNR value obtained by the proposed scheme is always higher than that of existing schemes and the average SSIM of the proposed scheme is 0.95. The SSIM value obtained by the proposed scheme is higher than that of other schemes [13], [4], and [7].

TABLE VIII
COMPARISON OF PSNR AND SSIM

QP	[13]		[4]		[14]		[7]		proposed	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
18	42.66	0.994	42.41	0.991	42.69	0.991	42.70	0.991	44.56	0.986
28	36.05	0.976	35.04	0.958	34.81	0.961	34.34	0.955	36.40	0.968
38	30.07	0.924	28.78	0.884	27.81	0.882	26.89	0.867	29	0.89
Avg.	36.26	0.964	35.41	0.944	35.10	0.944	34.64	0.937	36.65	0.95

Table IX the comparison performance of the proposed scheme with six previous schemes [4], [13], [3],[14],[7], and [10] when the (QP) = 28 is used. The average PSNR, the SSIM, and the maximum capacity of the proposed scheme is

higher than the other six schemes [4], [13], [3], [14], [7], and [10]. However, the maximum capacity of the proposed methods is up to 15 times larger than that of the scheme [13].

Table IX the comparison performance of the proposed scheme with six previous schemes [4], [13], [3],[14],[7], and [10] when the (QP) = 28 is used. The average PSNR, the SSIM, and the maximum capacity of the proposed scheme is higher than the other six schemes [4], [13], [3], [14], [7], and [10]. However, the maximum capacity of the proposed methods is up to 15 times larger than that of the scheme [13].

TABLE IX
 COMPARISON BETWEEN SIX SCHEMES AND THE PROPOSED SCHEME WITH QP = 28 AVERAGE

metrics	2014[4]	2010[13]	2016[3]	2016[14]	2019[7]	2022[10]	Proposed
Parameter hiding in H.264	Inter prediction	Intra prediction	Inter prediction	Intra Prediction	Intra Prediction	Intra prediction	Inter prediction
No. of frames used to hide	99	30	99	—	30	30	299
Bitrate increment	0.75	1.71			1.04		1.09
PSNR (dB)	32.72	35.31	33.05	34.17	34.34	34.34	36.40
SSIM	0.920	0.935	0.943	0.987	0.932	0.842	0.968
Maximum Capacity (bits)	63,757	11,559	63,757	141	19,077	19,551	(49,203) from 165,019

V. CONCLUSION & FUTURE WORK

The results show in this study, it can be concluded that when cryptography is combined with steganography joined with compression video increased security levels, robustness, and capacity are achieved. The encryption experienced in this research is highly secure. The steganography joined compressed video: the study achieved increased security low bitrate increase and high embedding capacity. Future work, dividing the secret data into sets of values and encrypting and decrypting each set with different chaotic maps with compressed it then dividing the sequence frames into sets and embedding and extracting encrypted secret data in each set with different embedding methods and locations with (H.264 / H.265) techniques. His has implications on security and throughput.

Funding

None

ACKNOWLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

- [1] R. Patel, K. Lad, and M. Patel, "Study and investigation of video steganography over uncompressed and compressed domain: a comprehensive review," *Multimedia Systems*, vol. 27, no. 5, pp. 985-1024, 2021.
- [2] M. M. Mashkour and L. M. Jawad, "Compressed and Uncompressed Video Steganography," in *IEEE International Conf. on Electrical, Computer and Energy Technologies*, Prague, Czech Republic, pp. 1-9, 2022.
- [3] Y. Yao, W. Zhang, and N. Yu, "Inter-frame distortion drift analysis for reversible data hiding in encrypted H. 264/AVC video bitstreams," *Signal Processing*, vol. 128, pp. 531-545, 2016.
- [4] T. J. Lin, K. L. Chung, P. C. Chang, and Y. H. Huang, "An improved DCT-based perturbation scheme for high capacity data hiding in H.264/AVC intra frames," *Journal of Systems and Software*, vol. 86, pp. 604-614, 2013.
- [5] D. Xu and R. Wang, "Efficient reversible data hiding in encrypted H.264/AVC videos," *Journal of Electronic Imaging*, vol. 23, pp. 053022-053022, 2014.
- [6] Y. Xue, J. Zhou, H. Zeng, P. Zhong, and J. Wen, "An adaptive steganographic scheme for H.264/AVC video with distortion optimization," *Signal Processing: Image Communication*, vol. 76, pp. 22-30, 2019.
- [7] D. C. Nguyen, T. S. Nguyen, F. R. Hsu, and H. Y. Hsien, "A novel steganography scheme for video H.264/AVC without distortion drift," *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 16033-16052, 2019.
- [8] R. Patel, K. Lad, M. Patel, and M. Desai, "A hybrid DST-SBPNRM approach for compressed video steganography," *Multimedia Systems*, vol. 27, no. 3, pp. 417-428, 2021.
- [9] V. DR and A. Babu J, "A Cryptographic based Approach for Data Hiding in Advanced Video Sequences," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 6, pp. 2031-2038, 2021.
- [10] T. Nguyen, "Reversible Data Hiding Scheme Based on Coefficient Pair Mapping for Videos H.264/AVC without Distortion Drift," *Symmetry*, vol. 14, no. 1768, pp.1-13, 2022.
- [11] D. W. Ahmed, T. M. Jawad, and L. M. Jawad, "An effective color image encryption scheme based on double piecewise linear chaotic map method and RC4 algorithm," *Journal of Engineering Science and Technology*, vol. 16, no. 2, pp. 1319-1341, 2021.
- [12] H. N. Abdullah, S. F Yousif, and A A Valenzuela, "Efficient steganography scheme for color images," *Iraqi Journal of Information and Communication Technology*, vol. 2, no. 4, pp. 1â10, 2019.
- [13] X Ma., Z Li., H Tu., and B Zhang., "A Data Hiding Algorithm for H.264/AVC Video Streams Without Intra-Frame Distortion Drift," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 20, pp 1320-1330 , 2010.
- [14] Y Liu., M Hu., X Ma., and H Zhao., "A new robust data hiding method for H264/ AVC without intra-frame distortion drift," *Neurocomputing*, vol 151 , pp 1076-1085 , 2015.