Journal of Engineering and Sustainable Development
Vol. 28, No. 06, November 2024
https://jeasd.uomustansiriyah.edu.iq/index.php/jeasd
ISSN 2520-0917
Research Article
https://doi.org/10.31272/jeasd.28.6.10

High-Capacity Video Steganography Based on Chaotic Maps for High-Efficiency Video Coding (HEVC)

Salwan F. Salman Al-Rubaie[1*], Maher K. Mahmood Al-Azawi[2]

[1,2]Electrical Engineering Department, College of Engineering, Mustansiriyah University, Baghdad, Iraq

[1]https://orcid.org/0009-0000-0847-3775
[2]https://orcid.org/0000-0003-3326-8911
[*]Email: salwan7@uomustansiriyah.edu.iq

Article Info

Received	21/06/2023
Revised	02/10/2024
Accepted	17/10/2024

Abstract

Video steganography is a method for concealing information within a video without substantially changing its visual content. The utilization of high-definition videos has garnered considerable interest from industries. H.265/HEVC, the recent video coding technology, is a promising field for video steganography. In this paper, a high concealment capacity based on three chaotic maps for the HEVC video standard is proposed, where the confidential data will be encrypted using two chaotic maps and then concealed in randomly selected Discrete Cosine Transform (DCT) coefficients of Transform Blocks (TBs), which are also randomly chosen using one chaotic map. The technique used in the DCT domain to achieve superior embedding capacity at the same visual quality compared with the state-of-the-art schemes in the compressed domain, and the use of three novel chaotic maps to protect the secret information and get uncrackable security level are the significant contributions of this paper. The simulation findings proved that the proposed approach has an average concealing capacity reaching 41.3 Kbits/frame. This payload exceeds what recent cutting-edge techniques could achieve in 1280 x 720 video frame dimensions with a ΔPSNR (shortened as difference Peak Signal to Noise Ratio) of -0.009 dB and a Bit Rate Increase (BRI) of 0.0747 at a Quantization Parameter (QP) value of 32. Furthermore, the critical space size of the suggested scheme is 2^{448}, which makes it very secure against all types of brute-force attacks.

Keywords: Chaotic maps; Discrete Cosine Transform; High-Efficiency Video Coding; High capacity; Intra-prediction; Video steganography

1. Introduction

The Internet's rapid growth and widespread usage as a source of wanted information have created new opportunities for intruders to quickly gain valuable data from other individuals. Therefore, steganography approaches have developed and worked in a complimentary manner to offer an authentication system that hides contact between an authorized sender and its receiver to guarantee the confidentiality of crucial information [1]. In recent years, considerable attention has been paid to image steganography, whereas just a few investigations have focused on video steganography. Nevertheless, due to rapid developments in computing, digital media, and communication, video compression methods are being actively developed, and video-based applications are progressively gaining popularity, laying the groundwork for developing video steganographic techniques [2]. Due to the endless video sequence, video steganography is advantageous for obtaining a higher embedding capacity than other digital media steganography, mainly when extensive secret data must be transmitted confidentially. Video steganography may be utilized in more practical applications, such as secret communication for the military, security agencies, interactive media, and medical facilities [3]. High-Efficiency Video Coding (HEVC) replaced the H.264/AVC codec standard, becoming a globally accepted standard on January 26, 2013 [4].

H.265/HEVC can reduce the bit rate by around 50 percent compared to H.264/AVC while retaining the same level of visual fidelity. Numerous innovative coding methods and frameworks, including variable coding size, quad-tree partitioning, additional modes for angular prediction, and enhanced inter-prediction, are responsible for the significant enhancements. However, this modern technology is incompatible with its predecessor H.264/AVC, particularly when it comes to video steganography. Therefore, efforts to

investigate video steganography techniques for high-definition video encoded with HEVC are vitally important [5]. Since video is typically transmitted or kept after compression, the footage steganographic approaches in the encoded domain have a higher utility value and garnered greater interest. Fig. 1 shows an overview of video data hiding methods in the encoded domain. In the current literature, most steganography approaches based on encoded domains and specific encoding characteristics use a type of coding procedure, including motion vector estimation, DCT coefficients, intra-prediction modes, etc., to conceal the secret data [6].

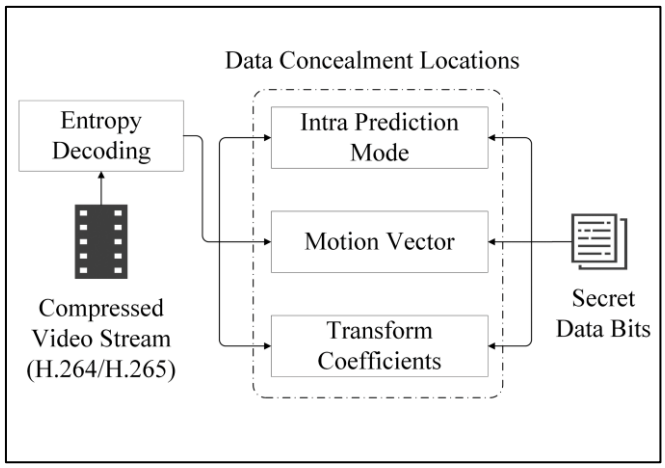


Figure 1. An overview of video steganographic techniques based on encoded domain.

The natural occurrences of chaos may be defined as the combination of the inherently unpredictable nature of a system that is deterministic with the distinctive actions of a complex dynamical process [7]. The key used for encryption is produced via a chaotic map in an encryption system that utilizes chaos. The chaotic maps have been praised for bringing intricacy and sturdiness to methods of encryption. However, the preferable characteristics of maps used in encryption systems are significant nonlinear behavior, extraordinary randomness, and an extensive chaotic interval. These are essential qualities needed to withstand various threats [8].

A novel 2D Logistic-Sine-Cosine Map (2D-LSCM) was presented in [9]. It has a higher +ve Lyapunov exponent, a more extensive chaotic range, and a greater complexity of chaotic dynamics than the standard 2D Logistic map. A new 1-D Sine Chaotic System (1-DSCS) with huge parameter intervals was proposed in [10]. The model showed chaotic solid behavior, a broad range of parameter values, and a high level of sensitivity, according to the 1-DSCS performance evaluation. In [11], a unique 1-D Cosine Polynomial (shortened as 1-DCP) chaotic map was introduced. The evaluation performance of the suggested map shows that it has an unlimited chaotic domain, a simple structure, and a considerably chaotic behavior.

In [12], a unique multiple-level steganography technique that utilizes diamond-encoded Prediction Unit (PU) partitioning modes was developed. The PU modes of the smaller 16 x 16 and 8 x 8 Coding Units (CUs) are adopted as the cover for information concealment. The use of the diamond coding basis improves the concealment capacity of restricted PU types, enabling them to store more data while undergoing minor alteration. Experimental analysis shows that the hiding capacity reached an average of 235 bits per frame in 416 x 240 video resolution with a ΔPSNR of -0.1 dB and a Bit Rate Increase (BRI) of 0.0402 at a QP of 32.

A new, effective solution for HEVC video steganography that is based on transform block choice was introduced in [13]. The hiding error of information concealing was examined by changing the Prediction Block (PB), Transform Block (TB), and Coding Block (CB) partitioning elements as well as the transform block choice in order to conceal confidential information and modify relevant leftovers synchronously. The simulation results demonstrate that the suggested technique has a hiding capacity of 489 bits per frame in 416 x 240 video resolution with a ΔPSNR of -0.2 dB and a BRI of 0.0472 at a QP of 32.

To enhance the imperceptibility performance of the cover video related to HEVC, the suggested approach in [14] employed the avoidance of the intra-prediction distortion drift method that utilized intra- and inter-frames. The simulation evaluation has proven that this technique has a concealment capacity of an average of 108 bits per frame in 416 x 240 video resolution with a ΔPSNR of -0.12 dB and a BRI of 0.0063 at a QP of 32.

HEVC-based new and robust data concealing technique was presented in [15]. The hidden information is first coded utilizing the BCH code to enhance the robustness of the information concealing. Then, the chosen 4 x 4 luminance Discrete Sine Transform (DST) blocks are employed to embed the encoded information into their multi-coefficients. The simulation results show that this technique has a concealing capacity of an average of 94 bits per frame at a ΔPSNR of -0.2 dB and a BRI of 0.0124 at a QP of 32 for 416 × 240 video resolution.

Although the related studies above have worked on new methods to conceal the secret data and enhance the performance of imperceptibility, robustness, and BRI, none of them have focused on improving the embedding capacity performance and security of the system, particularly when a large size of private valuable information is needed to be transmitted secretly and safely. To solve this problem, this paper proposes a superior embedding capacity technique that utilizes the transform domain, where three novel chaotic maps are used to protect the secret data and raise the security efficiency of the system to attain an unbreakable level. In this work, the private information is ciphered utilizing 2D-LSCM and 1-DSCS chaotic maps for confusion and diffusion processes and then embedded in randomly selected DCT coefficients of randomly chosen TBs utilizing a 1-DCP chaotic map. The performance evaluation proves this technique has a high hiding payload of 41.3 Kbits per frame in 1280 x 720 video resolution with a good ΔPSNR of -0.009 dB and a BRI of 0.0747 at a QP of 32. This paper's contributions are considered in the proposed method that achieves supreme hiding payload at the same imperceptibility performance compared with the related studies, and the utilization of 3 new chaotic maps to boost the security level of the system which is not considered in related state-of-the-art works.

The remaining sections of this paper are as follows. Section 2 examines the technical background of block partitioning structure in H.265/HEVC, intra-picture prediction, and intra-picture distortion drift. Section 3 will introduce the proposed technique. The experimental results are presented in Section 4, whereas the conclusion will be provided in Section 5.

2. Related Technical Backgrounds

As the HEVC video codec standard is now widely adopted in various applications, such as broadcasting, video streaming services, video conferencing, and surveillance, this section will present some of its features regarding block partitioning structure, and intra-picture prediction. Furthermore, the intra-picture distortion drift will also be offered to give a clear understanding of how visual quality is degraded when the pixels of TBs in the I-frames are manipulated or embedded with secret information.

2.1. Block Partitioning Structure in HEVC

2.1.1. Coding Tree Units (CTUs) and Coding Tree Blocks (CTBs)

For both the chroma and luma elements of HEVC, every single frame of a video has been partitioned into square-shaped blocks referred to as Coding Tree Blocks (CTBs). A pair of chroma samples and one luma sample make up each CTB, which are combined to produce a Coding Tree Unit (CTU). The fundamental computing unit CTU in HEVC is comparable to macroblocks in the H.264/AVC standard. Fig. 2 illustrates the splitting of an image utilizing HEVC with (64 x 64 CTUs), allowing for more excellent image compression capability. The square sample regions in the image have a size of $2^N \times 2^N$ luma CTB. For various CTU sizes, 16 x 16, 32 x 32, and 64 x 64 samples, which correspond to N = 4, 5, and 6, respectively, larger CTUs will enhance the compression performance since they can be encoded more effectively. Still, they also demand more memory and can add delay to encoder calculations [16].

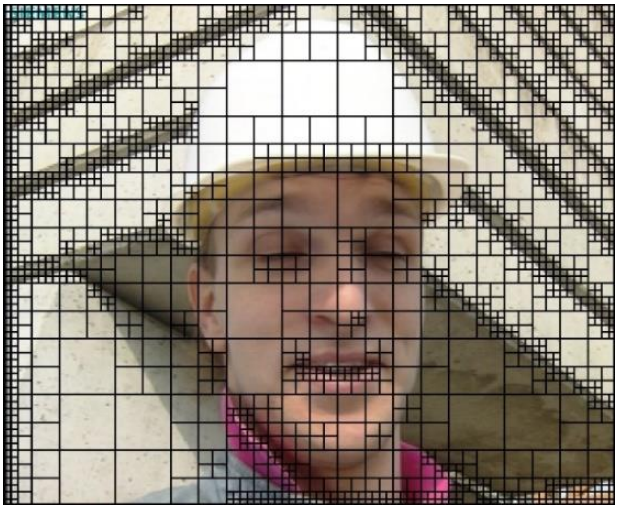


Figure 2. Block partitioning structure of an image in HEVC standard (64 x 64 CTUs).

2.1.2. Coding Units (CUs) and Coding Blocks (CBs)

The CTU could be one CU, or it might be partitioned into four minor units of size N x N, leading to nodes of the CU. If the units are the connected nodes of the coding tree, they turn into CUs. If not, it might be partitioned into four smaller parts. Fig. 3 depicts an instance of CTU splitting and the computation order of CUs if the dimensions of the CTU are 64 x 64 and the minimal CU size is 8 x 8. In Fig. 3(a), each square block denotes CU. In this instance, a CTU is divided into 16 CUs of various sizes and locations. Fig. 3(b) depicts the coding tree structure corresponding to the CTU splitting structure in Fig. 3(a). The digits on the tree indicate whether or not the CU is subdivided further [17]. The CTU's quadtree syntax specifies the dimensions and coordinates of its chroma and luma CBs. Typically, a single luma CB, a pair of chroma CBs, and the related syntax constitute CU. Each CU is partitioned into Prediction Units (PUs) and a tree of Transform Units [18].

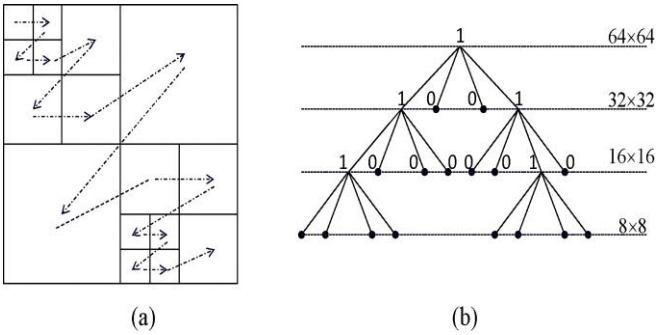


Figure 3. CTU splitting, when the dimensions of CTU are equal to 64 × 64 and the minimum CU dimensions are equal to 8 × 8. (a) CTU division. (b) The equivalent coding tree structure.

2.1.3. Prediction Units (PUs) and Prediction Blocks (PBs)

The CU decides whether an image region should be coded using inter- or intra-image prediction. The root of a PU-splitting structure is the CU level. Based on the type of prediction, the chroma and luma CBs may be further subdivided and predicted from the chroma and luma PBs [18].

2.1.4. Transform Units (TUs) and Transform Blocks (TBs)

The residual error of the prediction is encoded utilizing block transforms. The residual luma CB is the same as the luma TB or can be further subdivided into minor luma TBs. Similarly, for chroma TBs. For squared TB sizes 4 x 4, 8 x 8, 16 x 16, and 32 x 32, integer basis functions analogous to those of DCT/ DST are constructed [18].

2.2. Intra-Picture Prediction in HEVC

This section demonstrates the enhanced intra-prediction technique for H.265 over H.264 since the suggested method conceals the confidential data in intra-predicted pictures of the HEVC-encoded video. H.264/AVC has nine intra-prediction modes for predicting the present block using the preceding decoded blocks. If higher block dimensions are utilized in HEVC, the number of modes is inadequate to effectively forecast the orientation structures found in a video [19]. The

H.265 offers 35 intra modes, which are Planar, DC, and 33 angular prediction modes, as shown in Fig. 4.

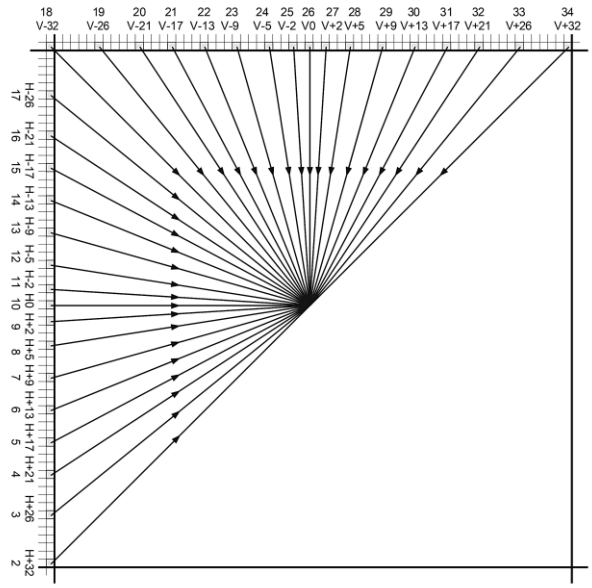


Figure 4. The 33 Angular intra-prediction modes in H.265 are numbered from 2 to 34.

The I-frame of HEVC uses intra-prediction to minimize the spatial redundancy of video frames. As depicted in Fig. 5, the inner pixels of an N x N prediction block are predicted utilizing the top $R_{X,0}$, and left $R_{0,y}$ boundary reference pixels of neighboring blocks, in which the number of neighboring pixels in the standard HEVC will be 2N, resulting in more possible prediction modes, which will efficiently enhance the prediction precision [20].

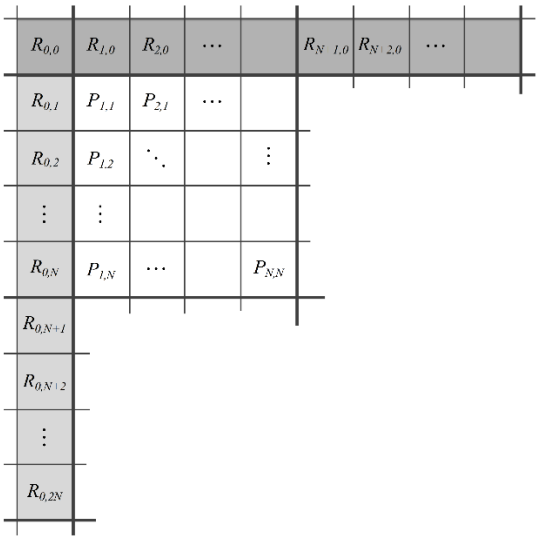


Figure 5. The Top $R_{X,0}$ and left $R_{0,y}$ reference pixels in the intra-prediction of H.265 use a block of dimensions N x N.

2.3. Intra-Picture Distortion Drift in HEVC

By the H.265 codec standard, the intra-frame prediction of neighboring PUs of the current block as depicted in Fig. 6 may result in Error Propagation (EP) if the rightmost column pixels $\{R_{i,N}\}_{i=1,\dots,N}$ and bottom-row pixels $\{R_{N,j}\}_{j=1,\dots,N}$ of the current block have been altered or conceal secret information in them, in either transform domain or spatial domain. This is because each predicted sample of the PUs will be duplicated from the reference pixel of the reconstructed neighboring block utilizing intra-angular modes [21].

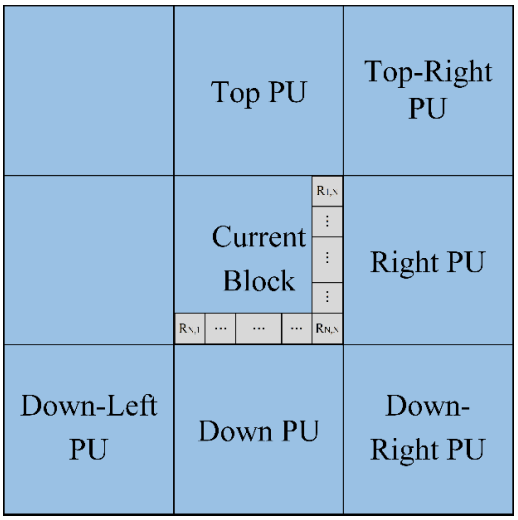


Figure 6. Intra-picture prediction of neighboring PUs from the current block pixels.

3. The Proposed Technique

This section explains the large hiding capacity technique behind the embedding and retrieving procedures for the HEVC video and the utilization of 1-DSCS, 1-DCP, and 2D-LSCM chaotic maps to secure the hidden information.

3.1. Embedding Process

The steps below demonstrate how the encoder conceals the encrypted confidential information within the DCT coefficients of the luma TBs with different sizes in the I-frames. The block diagram of the suggested technique at the encoder side of the H.265/HEVC is shown in Fig. 7.

Step 1: Read the confidential data (picture, video, text, …etc.).

Step 2: Apply the confusion and diffusion operations to cipher the private information by employing the chaotic maps 1-DSCS and 2D-LSCM, respectively, where the mathematical model of the chaotic map 1-DSCS can be defined as:

$$x_{n+1} = (\mu(3 + 2\lambda)(1 - sin(\pi x_n))) \bmod 1 \quad (1)$$

Where $\mu \in [4, +\infty]$ and $\lambda \in [0, +\infty]$ are the control parameters. Whereas the 2D-LSCM mathematical equations are defined as:

$$x_{n+1} = sin(\pi x_n) + a(sin(\pi x_n) - sin^2(\pi x_n) + sin(\pi y_n)) \quad (2)$$

$$y_{n+1} = cos(\pi y_n) + b(cos(\pi y_n) - cos^2(\pi y_n) + cos(\pi x_n)) \quad (3)$$

A, b ϵ [0, +∞] are the control parameters.

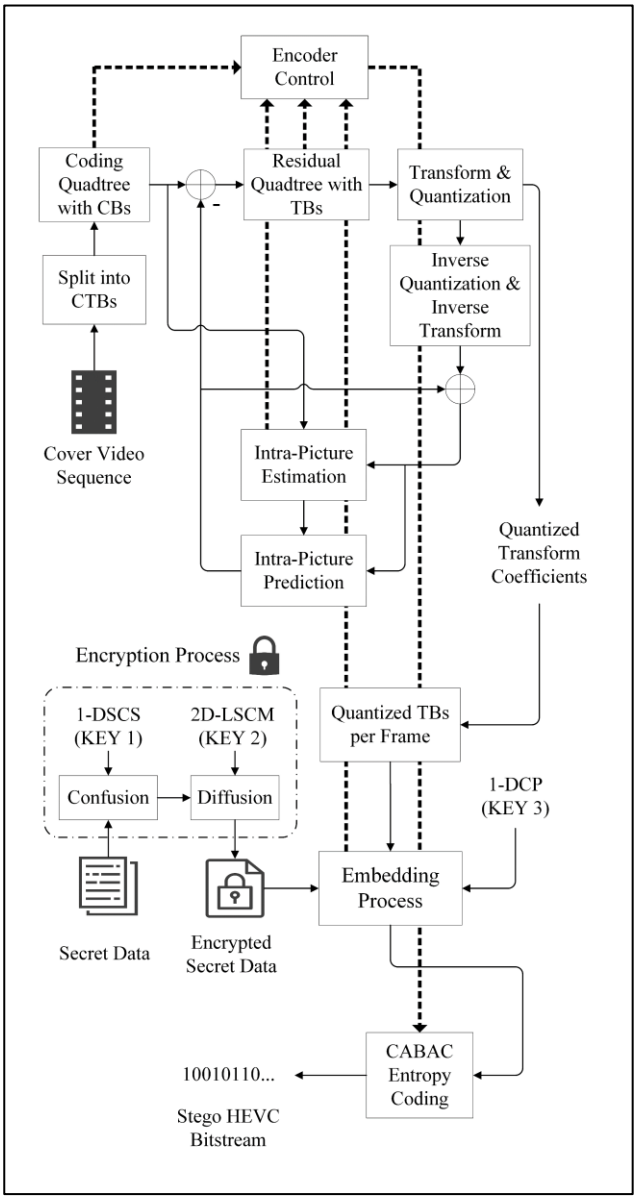


Figure 7. The suggested approach's block diagram in the H.265 encoder.

Step 3: Convert the ciphered private information into binary form, then convert each 3 bits into a decimal number. Store the result in a vector named **SD**. Now, the vector **SD** has decimal elements in the range $[0, 2^3 - 1] = [0, 7]$.

Step 4: Read the frames of the cover video file.

Step 5: Transform each frame from Red, Green, and Blue (RGB) into luminance and chrominance color ranges.

Step 6: Divide each intra-picture (I-frame) into CTBs using H.265/HEVC quadtree decomposition, where each CTB will be further split into smaller CBs. The encoder will decide whether each CB will be divided into smaller PBs or TBs.

Step 7: Apply intra-frame prediction at each PB by utilizing the 35 intra modes of HEVC to generate the best-predicted block. Subtracting the best-predicted and original blocks will generate the residual error blocks, which are transformed into TBs.

To avoid EP in the neighboring PUs, the secret data vector (**SD**) will be concealed in the DCT domain of the pixels of the current block, excluding the rightmost column and bottom row pixels, as shown in Fig. 5. These pixels will be transformed, quantized, and encoded separately without any manipulation.

Step 8: Convert the TBs (residual error) from the domain of pixel (spatial) into the domain of DCT (frequency), where the coefficients of the DCT transform of the luminance TBs are the only ones to be used in concealing the confidential data to obtain large concealing capacity and satisfactory level of content quality since the majority of an image's information may be seen in the luminosity channel. Hence, any minor manipulation in the DCT coefficient values of the luminance channel won't be detected by the Human Visual System (HVS) compared to the chroma samples [22].

Step 9: Apply the quantization operation by dividing the TBs' DCT coefficients by the quantization step size *Qstep* at a QP value assigned by the H.265 video encoder.

Before encoding the Quantized TBs with Context Adaptive Binary Arithmetic Coding (CABAC) to generate the HEVC bitstream, the elements of the vector **SD** have to be embedded in randomly selected DCT coefficients of randomly selected luma TBs.

Step 10: Gather all quantized residual TBs per frame to randomly assign the chosen quantized luma TBs for the embedding operation using the 1-DCP chaotic map.

Step 11: Produce a PRSN (abbreviated as Pseudo Random Sequence Number) with a length (L) equal to:

$L = Total\ No.\ of\ luma\ TBs \times \psi$

Utilizing the chaotic map 1-DCP formula as defined below:

$$x_{n+1} = cos(\mu(x_n^3 + x_n)) \quad (4)$$

Where the control parameter $\mu \in [0, +\infty]$ and the concealing factor $\psi \in [0, 1]$.

Step 12: Using the generated PRSN, choose a random quantized luma TB, and save the output in a block called **EB**.

Step 13: Apply the dequantization operation by multiplying the block **EB** by *Qstep*.

Step 14: Apply the floor/ceil function to all **EB**'s DCT coefficients after multiplying them by 0.1, then multiply the result by ten as shown:

$$\varphi^* = \begin{cases} floor(\varphi^* \times 0.1) \times 10 & ,if\ \varphi^* \geq 0 \\ ceil(\varphi^* \times 0.1) \times 10 & ,if\ \varphi^* < 0 \end{cases}$$

Where φ^* represents the block **EB**'s DCT coefficient, for DCT coefficients ≥ 10, this step will substitute the first figure from the right side with a 0 value. In contrast, DCT coefficients < 10 will be removed, leading to fewer DCT coefficients being encoded, which is beneficial for BRI.

Step 15: Utilizing the same chaotic map 1-DCP, produce a different PRSN whose L equals the number of **EB**'s DCT coefficients≥ 10. Save the result in a vector named **R**.

Step 16: Add the elements of the **SD** to the **EB**'s coefficients that are ≥ 10 randomly using the vector **R** to generate the stego block named **SEB**.

Step 17: To protect the secret data from damage brought on by scaling and rounding procedures for QP > 0, use a unique QP called QP_{stego} with a value of 0 (lossless encoding) to skip the quantization operation for the block **SEB**.

Repeat steps 12 through 17 until the **SD** elements are entirely concealed within the DCT coefficients of the luminance TBs, where both are selected randomly using the vectors **R** and PRSN, respectively.

Step 18: The rest of the luminance quantized TBs, the stego **SEB** blocks, and the chroma quantized TBs, each with their unique QP/QP_{stego} will be encoded using CABAC entropy coding to produce the stego H.265 video bitstream.

The key trick of this technique is to quantize all luma and chroma TBs with the QP specified by the encoder. After hiding the secret information in the randomly chosen luma TBs, a different QP called QP_{stego} will be encoded and sent to the recipient with the rest of the HEVC bitstream.

3.2. Extraction Process

After decoding the stego HEVC bitstream with the CABAC entropy decoding, a reverse procedure is applied by skipping the dequantization process for the stego **SEB** blocks using QP_{stego} to preserve the stego DCT coefficients. Then, the confidential data will be extracted utilizing the 1-DCP map, unlike the rest of the decoded quantized TBs, where QP will be used in the inverse quantization process. After that, the inverse transform is applied to the DCT coefficients of the TBs and the stego **SEB** blocks to construct the stego residual error blocks. The intra-prediction modes are used to generate the best-predicted blocks, where the stego I-frames are built by adding the best-predicted blocks to the stego residual blocks. The block diagram of the suggested technique on the HEVC decoder side is the opposite of that on the encoder side.

4. Experimental Results

This section provides the performance evaluation tests and associated analysis to verify the proposed approach. The H.265/HEVC video codec standard was built utilizing MATLAB R2022b environment to evaluate the suggested method. The simulation is conducted via a PC running Windows with a 1.80GHz Intel (R) Core (TM) i7-8550U processor, 1TB Solid-State Drive (SSD), and 8GB of RAM. The configuration of the primary simulation parameters will be as follows: The group of picture structure is set to all intra, the largest CB size is set to 64, whereas the largest and the most petite TB sizes have been specified as 64 and 4, respectively. The proposed method is evaluated using well-known video sequences from xiph.org and MCL-JCV Dataset. Table 1. illustrates the video sequence dataset in the form of classes.

4.1. Visual Quality Analysis

Video quality evaluation provides two primary parts: subjective perception and objective evaluation. The subjective perception measures the picture's visible distortion of the stego HEVC compressed video. Fig. 8 compares subjective perceptions of the original, HEVC compressed, and stego HEVC compressed frame for (a) Bus. (b) KristenAndSara. and (c) BasketballDrive.

Table 1. The video sequences dataset.

Class	Resolution	Video Sequence
Class A	352 x 288	Akiyo, Bus, Foreman
Class B	1280 x 720	KristenAndSara, Parkrun, Shields
Class C	1920 x 1080	BasketballDrive, Crowd Run, Kimono
Class D	416 x 240	BasketballPass

The objective performance of the video is a quantitative assessment, where the Correlation Coefficient (CC), Structural Similarity Index Measure (SSIM), and PSNR are employed as standard criteria in imperceptibility analysis [23]. When the PSNR is greater than or equal to 36 dB, the HVS cannot differentiate between the original and carrier images [24]. Regarding reducing the content quality of the compressed picture or encoded video, the PSNR values range between 60 to 80 dB for 16-bit depth and from 30 to 50 dB for 8-bit depth [25]. The mathematical equation of the PSNR is defined as follows [26]:

$$PSNR = 10 \log_{10}\left(\frac{B^2}{MSE}\right) \quad (5)$$

Where B represents the highest pixel value (which is equivalent to 255 for 8-bit depth) of the cover video frame F_C, and the MSE (abbreviated as Mean Square Error) is expressed as [27]:

$$MSE = \frac{1}{H \times W} \sum_{i=1}^{m} \sum_{j=1}^{n} [F_C(i,j) - F_S(i,j)]^2 \quad (6)$$

Where W and H denote the Width and Height of the cover frame, n, and m are the number of columns and rows, respectively, and $F_S(i,j)$ and $F_C(i,j)$ are the pixels of the stego and cover video frames, respectively, given by (i, j).

ΔPSNR is utilized to calculate the PSNR difference between the suggested HEVC steganography technique ($PSNR_{stego}$) and the standard HEVC ($PSNR_{default}$). ΔPSNR can be defined as follows:

$$\Delta PSNR = PSNR_{stego} - PSNR_{default} \quad (7)$$

The SSIM can be expressed as [28]:

$$SSIM = \frac{(2\mu_c\mu_s + c_1)(2\sigma_{cs} + c_2)}{(\mu_c^2 + \mu_s^2 + c_1)(\sigma_c^2 + \sigma_s^2 + c_2)} \quad (8)$$

Where μ_c and μ_s denote the mean values of carrier F_C and stego F_S frames, respectively, the covariance between F_C and F_S, the variance of F_C, and the variance of F_S are denoted by the

symbols σ_{cs}, σ_c, and σ_s, respectively, whereas c_1 and c_2 represent constant with values of $(0.01 \times B)^2$ and $(0.03 \times B)^2$, respectively. The CC can be mathematically expressed as [29]:

$$CC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(F_C(i,j) - \overline{F_C})\ (F_S(i,j) - \overline{F_S})}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}[F_C(i,j) - \overline{F_C}]^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}[F_S(i,j) - \overline{F_S}]^2}} \quad (9)$$

$\overline{F_S}$ and $\overline{F_C}$ represent the mean values of the stego and cover video frames, respectively.

The first row of Fig. 9 (a) and (b) shows a trade-off demonstration among the PSNR (in dB) and QP for classes A and B sequences, respectively.

Figure 8. The subjective perception comparison of original, encoded, and stego encoded frame at QP of 26 and ψ of 0.5 for (a) Bus. (b) KristenAndSara. (c) BasketballDrive.

In Fig. 9 (a) and (b), the finest PSNR values per frame are noticed in Akiyo and KristenAndSara from classes A and B video sequences, respectively, where the PSNR value of video sequences of both classes is dropped with the increase in the QP value. Table 2 shows the average value per 30 frames of CC, SSIM, and PSNR of the suggested method at QP of (20, 26, and 32) with ψ of 0.5 for classes A, B, and C video frames. The finest $PSNR_{stego}$ and ΔPSNR values per frame are demonstrated in bold.

4.2. Embedding Capacity Analysis

A metric called capacity measures the number of confidential information bits that can be hidden within the cover video frame or image with a minimal degree of degradation in visual quality [30]. In this study, the number of luma TBs employed in the concealing data stage in each I-frame is controlled via the embedding factor ψ.

In the second row of Fig. 9 (a) and (b), a trade-off illustration among the concealing payload (in Kbits) and QP for sequences of classes A and B, respectively, where the most significant hiding capacity values per video frame are noticed in Bus and

Parkrun with a maximum of over 42.5 Kbits and 510 Kbits, respectively at a QP value of 24 and ψ of 0.5. As seen from the second row of Fig. 9 (a) and (b), the highest concealing payload of video sequences of classes A and B occurred at a QP value of 24. The average value of the concealing payload per 30 frames for several video footages is presented in Table 2, where the best values are shown in bold. It can be noticed from Table 3 that the impact of changing ψ values on the content quality is very minor, whereas it has a considerable effect on the performance of BRI and hiding payload.

4.3. Bit Rate Increase Analysis

The modification of DCT coefficients of the luma TBs caused by embedding the secret data proposed in this study led to a rise in the bit rate of the stego HEVC video. To measure the change in a bit rate of the test videos in classes A, B, and C after the hiding operation, the BRI metric can be expressed mathematically as [31]:

$$BRI = \frac{(BR_{stego} - BR_{default})}{BR_{default}} \quad (10)$$

Where BR_{stego} and $BR_{default}$ are the bit rates of the H.265 video sequence with and without secret information, respectively.

The BRI performance of video sequences in classes A and B is shown in the third row of Fig. 9 (a) and (b), respectively, where the finest BRI can be noticed in Akiyo and KristenAndSara, which have the best PSNR values with the lowest embedding capacity. From the third row of Fig. 9 (a) and (b), the worst BRI value of classes A and B video sequences is observed at a QP value of 24, where the highest embedding payload is achieved. The best average BRI value per frame for different video sequences is shown in Table 2 in bold.

A summary of a comparative analysis of the suggested technique with the related studies is demonstrated in Table 4. Table 5 presents the comparative outcomes per video frame with the recent large-capacity video data hiding schemes, where two video sequences (BasketballPass from class D and KristenAndSara from class B) are adopted for the comparison evaluation test. The best payload, ΔPSNR, and BRI results are presented in bold. It can be noticed from Table 5 that the suggested technique has a superior hiding capacity per frame at different ψ values (0.5 and 1.0) with an acceptable level of BRI and a good ΔPSNR at the same QP values (26 and 32) in comparison with the other cutting-edge data hiding techniques.

4.4. Robustness Analysis

The receiver/decoder side can extract the secret information completely without any corruption if the stego HEVC video has not been attacked by noise, re-compression, or any other signal processing attacks, where any small change in the DCT coefficients values of the luma TBs can cause high altering in the secret data bits. Hence, the confidential information will be damaged entirely on the decoder side. Although the proposed technique has a superior embedding payload with good imperceptibility and an acceptable BRI performance, its drawback is that it is fragile against re-compression, transcoding, and any image processing attack.

4.5. Key Space Size Analysis

The vital space is the entire number of private and secure keys that cryptography techniques can utilize. Brute force attacks are pretty difficult to succeed in breaking the system security if the keyspace size is enormous, where there are 10^k total keys, each of which can be expressed with k binary bits [32].

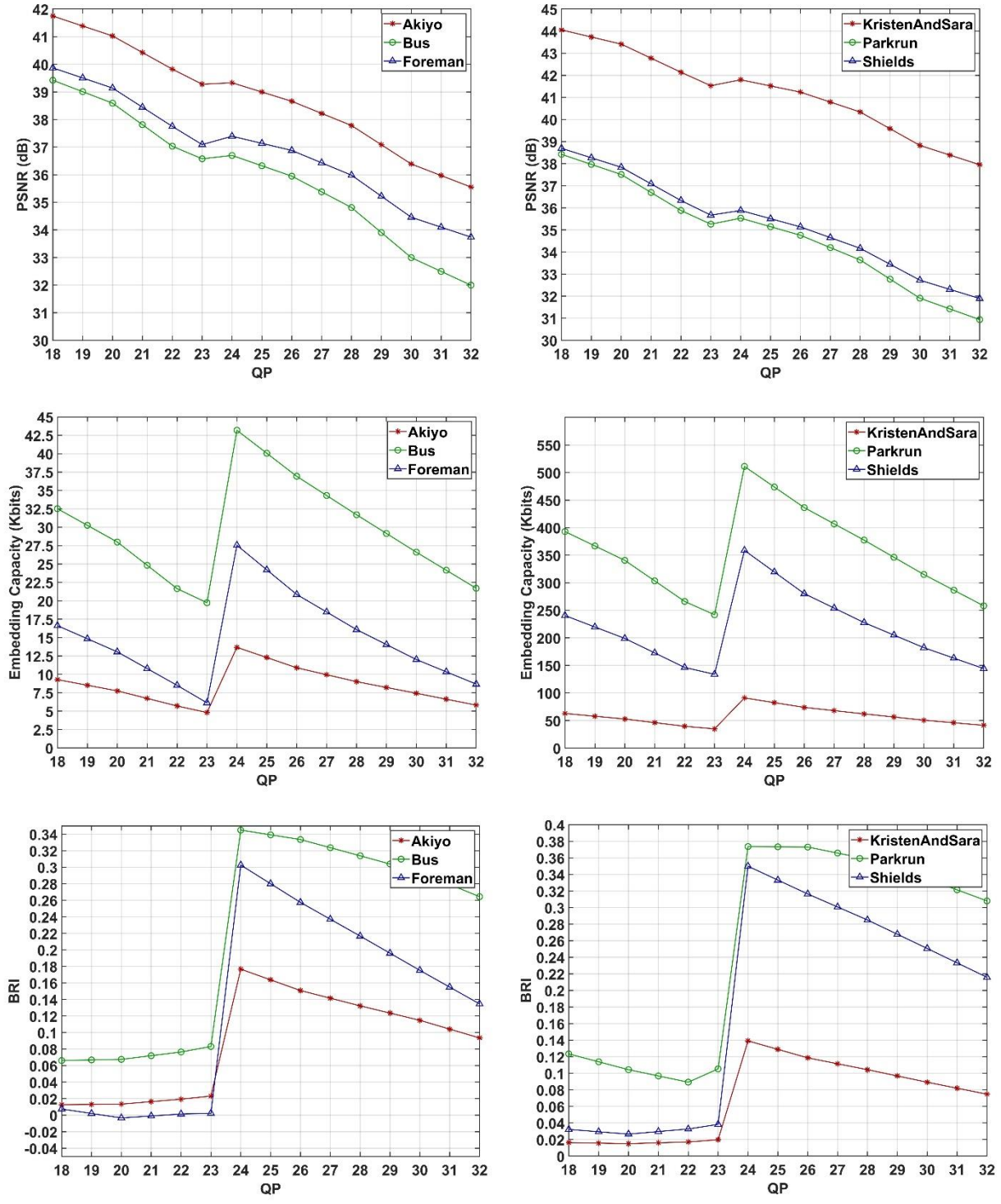
The total number of keys that are utilized in this study is considered as the overall number of parameters and initials for the chaotic maps 1-DSCS and 2D-LSCM that are adopted in the encryption stage and the chaotic map 1-DCP for the concealing stage, where the 1-DSCS map possesses x as an initial value and two control parameters, the 2-D-LSCM map has two initials x and y with two control parameters, the 1-DCP map offers one parameter and one initial value, and consequently, nine keys have been established in the whole stego system at an accuracy of 10^{-15} for each, resulting in a substantial key space size that is equivalent to $10^{15 \times 9} = 10^{135}$ or 2^{448}, where the number of bits to assign a key = $\log_2 10^{135} \approx 448$ bits.

4.6. Stego-analysis of the Proposed Method

As the secret information is hidden inside the DCT coefficients of the Luma TBs, the quantization parameter employed to skip the quantization process for the Stego DCT coefficients is called QP_{stego} with a 0 value (lossless compression) to avoid confidential data loss caused by scaling and rounding operations, as mentioned earlier.

The existence of confidential information is easily detected in this method by the stego-analyzers when they try to analyze the stego HEVC video using video analysis software (like Elecard, CodecVisa, Zond265, …etc.), where the video analyzer software will present the QP used for each TB in the quantization stage. For instance, if the encoder sets the QP value to 28, each TB will be encoded with a QP ≥ 28, whereas the stego TBs will be encoded with QP_{stego}; hence, the significant difference between QP and QP_{stego} values leads the intruder to notice the existence of private information.

However, since the Stego video of the suggested approach has a good visual quality with an acceptable BRI performance, and there are hundreds of millions of uploaded videos on the Internet, it is challenging for the third party to find the Stego video. Even in the worst case, if the intruder has detected the Stego video among hundreds of millions of videos, the private data is protected with a key of length 448 bits.



(a) (b)

Figure 9. A trade-off illustration among PSNR, Embedding Capacity (in Kbits), and BRI against various QP values and at ψ of 0.5 for (a) Class A video sequences. (b) Class B video sequences.

Table 2. The average value per 30 frames of CC, SSIM, PSNR, BRI, and embedding payload of the presented approach at various QP values and ψ of 0.5 for classes A, B, and C video sequences.

Video Sequence	QP	PSNR (dB) (Default)	PSNR (dB) (Stego)	ΔPSNR (dB)	SSIM (Stego)	CC (Stego)	Capacity (Kbits)	BRI
Akiyo (352 x 288)	20	42.5	**41.026**	-1.474	0.97510	0.99924	7.758	**0.01339**
	26	38.813	**38.659**	-0.154	0.96191	0.99871	10.898	0.15083
	32	35.56	35.552	**-0.008**	0.94098	0.99736	5.820	0.09347
Bus (352 x 288)	20	41.284	**38.591**	-2.693	0.97302	0.99820	**27.996**	**0.06754**
	26	36.244	35.948	-0.296	0.95665	0.99669	**36.927**	0.33350
	32	32.016	31.998	**-0.018**	0.91244	0.99182	21.707	0.26441
Foreman (352 x 288)	20	41.532	**39.139**	-2.393	0.97882	0.99872	13.062	**-0.00331**
	26	37.087	36.879	-0.208	0.96733	0.99786	20.864	0.25747
	32	33.72	33.739	**0.019**	0.94381	0.99559	8.681	0.13466
KristenAndSara (1280 x 720)	20	45.341	**43.413**	-1.928	0.98638	0.99962	52.791	**0.01500**
	26	41.467	**41.239**	-0.228	0.97970	0.99938	73.845	0.11861
	32	37.962	**37.953**	**-0.009**	0.96501	0.99869	41.291	**0.07478**
Parkrun (1280 x 720)	20	40.145	**37.51**	-2.635	0.97499	0.99805	**340.695**	0.10433
	26	35.069	34.759	-0.310	0.95955	0.99634	**436.389**	0.37316
	32	30.964	30.94	**-0.024**	0.91572	0.99114	**258.150**	0.30815
Shields (1280 x 720)	20	40.112	**37.837**	-2.275	0.97742	0.99741	198.998	**0.02654**
	26	35.349	35.138	-0.211	0.96140	0.99515	**280.311**	0.31647
	32	31.905	31.895	**-0.010**	0.93178	0.98981	144.275	0.21590
BasketballDrive (1920 x 1080)	20	40.599	**38.59**	-2.009	0.98464	0.99705	195.915	**-0.02992**
	26	36.821	36.67	-0.151	0.97689	0.99542	**319.395**	0.20779
	32	34.415	34.416	**0.001**	0.96427	0.99228	130.298	0.09996
Crowd Run (1920 x 1080)	20	39.467	**37.349**	-2.118	0.96582	0.99869	**546.720**	**0.04411**
	26	34.596	34.388	-0.208	0.94254	0.99745	**728.858**	0.33472
	32	31.091	31.08	**-0.011**	0.90700	0.99452	**399.885**	0.24726
Kimono (1920 x 1080)	20	41.505	**40.268**	-1.237	0.95999	0.99781	133.113	**-0.01986**
	26	38.761	**38.612**	-0.149	0.94296	0.99679	173.879	0.11669
	32	36.603	36.577	**-0.026**	0.92102	0.99488	100.527	**0.07528**

Table 3. The average value per 30 frames of CC, SSIM, PSNR, BRI, and embedding payload of the presented approach at various ψ values and QP of 28 for several video footages.

Video Sequence	ψ	PSNR (dB) (Default)	PSNR (dB) (Stego)	ΔPSNR (dB)	SSIM (Stego)	CC (Stego)	Capacity (Kbits)	BRI
Akiyo (352 x 288)	0.25	36.811	36.795	-0.015	0.95702	0.99842	3.745	0.08133
	0.5	36.811	36.777	-0.033	0.95703	0.99841	8.011	0.13212
	0.75	36.811	36.760	-0.050	0.95706	0.99840	13.681	0.18729
	1.0	36.811	36.733	-0.077	0.95704	0.99839	18.484	0.21611
Parkrun (1280 x 720)	0.25	33.740	33.685	-0.054	0.94976	0.99530	191.473	0.21093
	0.5	33.740	33.637	-0.102	0.94946	0.99526	376.442	0.35848
	0.75	33.740	33.587	-0.152	0.94912	0.99518	568.021	0.47558
	1.0	33.740	33.537	-0.202	0.94872	0.99513	762.706	0.55981
Crowd Run (1920 x 1080)	0.25	33.441	33.416	-0.026	0.93355	0.99680	286.088	0.17128
	0.5	33.441	33.392	-0.050	0.93347	0.99678	608.438	0.30940
	0.75	33.441	33.365	-0.075	0.93345	0.99676	934.550	0.40789
	1.0	33.441	33.342	-0.102	0.93335	0.99674	1238.638	0.46458

Table 4. Summary of the comparative analysis of the suggested technique with the existing state-of-the-art schemes.

Evaluation	Proposed Method	[12] (2021)	[13] (2021)	[14] (2021)	[15] (2018)
Visual Quality	good	good	good	good	good
Embedding Capacity	Very High	Low	Low	Very Low	Very Low
Concealing Location	DCT	PU modes	Coding Syntax	DCT/DST	DST
Coding Scope	Intra	Intra & Inter	Intra & Inter	Intra & Inter	Intra

Table 5. Comparison results per frame with existing extensive capacity video data concealing schemes for HEVC.

Technique	QP	BasketballPass (416 x 240)			KristenAndSara (1280 x 720)		
		ΔPSNR (dB)	Capacity (bits)	BRI	ΔPSNR (dB)	Capacity (bits)	BRI
[12] (2021)	26	-0.120	412	**0.0676**	-	-	-
	32	-0.100	235	**0.0402**	-	-	-
[13] (2021)	32	-0.200	489	**0.0472**	-2.41	2125	**0.0249**
[14] (2021)	32	-0.120	108	**0.0063**	-1.27	502	**0.0141**
[15] (2018)	32	-0.200	94	**0.0124**	-	-	-
The Proposed Method at ψ of 0.5	26	-0.353	**21170**	0.2659	-0.228	**73845**	0.1186
	32	**0.003**	**11958**	0.1791	**-0.009**	**41291**	**0.0747**
The Proposed Method at ψ of 1.0	26	-0.381	**43905**	0.3895	-0.485	**154142**	0.1816
	32	**-0.004**	**23667**	0.2708	**-0.032**	**86772**	0.1171

5. Conclusion

In this paper, an efficient and secure data concealing technique with high embedding payload for H.265/HEVC codec standard is presented, where the private information is ciphered by employing two chaotic maps (2D-LSCM and 1-DSCS) and then hidden within randomly selected DCT coefficients of randomly chosen luma TBs via 1-DCP chaotic map to boost the system security. This paper's contributions can be considered in the technique utilized in the frequency domain and three state-of-the-art novel chaotic maps to get a very high concealing capacity and unbreakable data security, respectively. The simulation results prove that this technique has a superior hiding capacity at the same visual quality compared with the related state-of-the-art studies. Regardless of whether the QP value exceeds 28, the embedding capacity can attain an average value of 41.3 Kbits per frame, which is far beyond what other recent research achieved in 1280 x 720 video quality with a ΔPSNR of -0.009 dB and a BRI of 0.0747 at a QP value of 32. Moreover, due to the large size of the system's key space with a value of 2^{448}, the secret information is protected overall brute-force attacks.

Future work will focus on utilizing both intra- and inter-picture predictions of H. 265 to gain more concealing capacity at the same imperceptibility performance since the default process of the HEVC codec standard utilizes both intra-frame and inter-frame predictions to compress the video sequence.

Acknowledgments

The authors would like to thank the Electrical Engineering Department, College of Engineering, Al-Mustansiriyah University, Baghdad, Iraq, https://uomustansiriyah.edu.iq/, for their support in accomplishing this work.

Conflict of interest

The authors confirm that publishing this paper does not involve any conflicts of interest.

Author Contribution Statement

Each author contributed to the writing and editing of this work. The authors presented the investigation's research question and findings. The introduction and general structure of the paper were developed collaboratively by all contributors.

References

[1] R. J. Mustafa, K. M. Elleithy, and E. Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC," IEEE Access, pp. 1–1, 2017, doi: https://doi.org/10.1109/access.2017.2691581.

[2] A. Jabbar, Shahrin Sahib, and M. Zamani, "An Introduction to Image Steganography Techniques," International Conference on Advanced Computer Science Applications and Technologies, Nov. 2012, doi: https://doi.org/10.1109/acsat.2012.25.

[3] R. J. Mstafa, Y. M. Younis, H. I. Hussein, and M. Atto, "A New Video Steganography Scheme Based on Shi-Tomasi Corner Detector," IEEE Access, vol. 8, pp. 161825–161837, 2020, doi: https://doi.org/10.1109/access.2020.3021356.

[4] S. Liu, Y. Liu, C. Feng, and H. Zhao, "An Efficient Video Steganography Method Based on HEVC," Springer, cham, vol. 12836, pp. 327–336, Aug. 2021, doi: https://doi.org/10.1007/978-3-030-84522-3_26.

[5] H. Zhao, M. Pang, and Y. Liu, "Intra-frame Adaptive Transform Size for Video Steganography in H.265/HEVC Bitstreams," Springer, cham, vol. 12465, pp. 601–610, Oct. 2020, doi: https://doi.org/10.1007/978-3-030-60796-8_52.

[6] S. Liu, Y. Liu, C. Feng, H. Zhao, and Y. Huang, "A HEVC Steganography Method Based on QDCT Coefficient," Springer, cham, vol. 12465, pp. 624–632, Oct. 2020, doi: https://doi.org/10.1007/978-3-030-60796-8_54.

[7] W. Yan, Z. Jiang, X. Huang, and Q. Ding, "A Three-Dimensional Infinite Collapse Map with Image Encryption," Entropy, vol. 23, no. 9, pp. 1221–1221, Sep. 2021, doi: https://doi.org/10.3390/e23091221.

[8] J. S. Muthu and P. Murali, "A new chaotic map with large chaotic band for a secured image cryptosystem," Optik, vol. 242, p. 167300, Sep. 2021, doi: https://doi.org/10.1016/j.ijleo.2021.167300.

[9] H.-Q. Huang, "Novel Scheme for Image Encryption Combining 2D Logistic-Sine-Cosine Map and Double Random-Phase Encoding," IEEE Access, vol. 7, pp. 177988–177996, Dec. 2019, doi: https://doi.org/10.1109/access.2019.2958319.

[10] X. Wang and P. Liu, "A New Image Encryption Scheme Based on a Novel One-Dimensional Chaotic System," IEEE Access, vol. 8, pp. 174463–174479, Sep. 2020, doi: https://doi.org/10.1109/access.2020.3024869.

[11] Mohamed Zakariya Talhaoui, X. Wang, and Mohamed Amine Midoun, "A new one-dimensional cosine polynomial chaotic map and its use in image encryption," Vis Comput, vol. 37, no. 3, pp. 541–551, Mar. 2021, doi: https://doi.org/10.1007/s00371-020-01822-8.

[12] J. Liu, Z. Li, X. Jiang, and Z. Zhang, "A High-Performance CNN-Applied HEVC Steganography Based on Diamond-Coded PU Partition Modes," IEEE Transactions on Multimedia, vol. 24, pp. 2084–2097, 2022, doi: https://doi.org/10.1109/tmm.2021.3075858.

[13] H. Zhao, Y. Liu, Y. Wang, S. Liu, and C. Feng, "A Video Steganography Method Based on Transform Block Decision for H.265/HEVC," IEEE Access, vol. 9, pp. 55506–55521, Feb. 2021, doi: https://doi.org/10.1109/access.2021.3059654.

[14] H. Zhao, M. Pang, and Y. Liu, "An Efficient Video Steganography Scheme for Data Protection in H.265/HEVC," Springer, cham, vol. 12836, pp. 358–368, Aug. 2021, doi: https://doi.org/10.1007/978-3-030-84522-3_29.

[15] Y. Liu, H. Zhao, S. Liu, C. Feng, and S. Liu, "A Robust and Improved Visual Quality Data Hiding Method for HEVC," IEEE Access, vol. 6, pp. 53984–53997, 2018, doi: https://doi.org/10.1109/access.2018.2869148.

[16] T. N. Swamy, Kannadka Ramesha, and K. R. Diwakar, "An efficient algorithm for intra prediction in HEVC/H.265 standard for 16×16 pixels," International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), pp. 226–233, Dec. 2017, doi: https://doi.org/10.1109/iceeccot.2017.8284674.

[17] I.-K. Kim, M. Jung-Hye, T. D. Lee, W. M. Han, and Jeong Hoon Park, "Block Partitioning Structure in the HEVC Standard," IEEE Transactions on Circuits and Systems for Video Technology, vol. 22, no. 12, pp. 1697–1706, Dec. 2012, doi: https://doi.org/10.1109/tcsvt.2012.2223011.

[18] G. J. Sullivan, J.-R. Ohm, W.-J. Han, and T. Wiegand, "Overview of the High Efficiency Video Coding (HEVC) Standard," IEEE Transactions on Circuits and Systems for Video Technology, vol. 22, no. 12, 2013, doi: https://doi.org/10.1109/TCSVT.2012.2221191.

[19] S. Gaj, A. Sur, and P. K. Bora, "Prediction mode based H.265/HEVC video watermarking resisting re-compression attack," Multimedia Tools and Applications, vol. 79, Feb. 2020, doi: https://doi.org/10.1007/s11042-019-08301-w.

[20] S. Liu, Y. Liu, C. Feng, H. Zhao, and Y. Huang, "Blockchain Privacy Data Protection Method Based on HEVC Video Steganography," 2020 3rd International Conference on Smart BlockChain (SmartBlock), pp. 1–6, Oct. 2020, doi: https://doi.org/10.1109/smartblock52591.2020.00015.

[21] M. Z. Konyar, O. Akbulut, and S. Öztürk, "Matrix encoding-based high-capacity and high-fidelity reversible data hiding in HEVC," Signal, Image and Video Processing, vol. 14, pp. 897–905, Jan. 2020, doi: https://doi.org/10.1007/s11760-019-01621-2.

[22] A. A. Elrowayati, M. A. Alrshah, M. F. L. Abdullah, and R. Latip, "HEVC Watermarking Techniques for Authentication and Copyright Applications: Challenges and Opportunities," IEEE Access, vol. 8, pp. 114172–114189, 2020, doi: https://doi.org/10.1109/access.2020.3004049.

[23] B. Peng and J. Yang, "An optimized algorithm based on generalized difference expansion method used for HEVC reversible video information hiding," 2017 IEEE 17th International Conference on Communication Technology (ICCT), pp. 1668–1672, Oct. 2017, doi: https://doi.org/10.1109/icct.2017.8359914.

[24] R. O. El Safy, H. H. Zayed, and A. El Dessouki, "An adaptive steganographic technique based on integer wavelet transform," 2009 International Conference on Networking and Media Convergence, pp. 111–117, Mar. 2009, doi: https://doi.org/10.1109/icnm.2009.4907200.

[25] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," Journal of Computer and Communications, vol. 07, no. 03, pp. 8–18, 2019, doi: https://doi.org/10.4236/jcc.2019.73002.

[26] Y. Zhang, M. Zhang, X. Yang, D. Guo, and L. Liu, "Novel video steganography algorithm based on secret sharing and error-correcting code for H.264/AVC," Tsinghua Science and Technology, vol. 22, no. 2, pp. 198–209, Apr. 2017, doi: https://doi.org/10.23919/tst.2017.7889641.

[27] Y. Cui, Y. Yao, and N. Yu, "Defining Embedding Distortion for Sample Adaptive Offset-Based HEVC Video Steganography," 2020 IEEE 22nd International Workshop on Multimedia Signal Processing (MMSP), pp. 1–6, Sep. 2020, doi: https://doi.org/10.1109/mmsp48831.2020.9287075.

[28] 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, pp. 985–1024, Mar. 2021, doi: https://doi.org/10.1007/s00530-021-00763-z.

[29] V. Kumar and D. Kumar, "A modified DWT-based image steganography technique," Multimedia Tools and Applications, vol. 77, no. 11, pp. 13279–13308, Jul. 2017, doi: https://doi.org/10.1007/s11042-017-4947-8.

[30] Jayakanth Kunhoth, N. Subramanian, Somaya Al-Maadeed, and A. Bouridane, "Video steganography: recent advances and challenges," Multimedia Tools and Applications, Apr. 2023, doi: https://doi.org/10.1007/s11042-023-14844-w.

[31] X. Jia, Jie Jin Wang, Y. Liu, X. Kang, and Y. Q. Shi, "A Layered Embedding-Based Scheme to Cope with Intra-Frame Distortion Drift In IPM-Based HEVC Steganography," ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2720–2724, Jun. 2021, doi: https://doi.org/10.1109/icassp39728.2021.9413728.

[32] I. Hussain, Amir Anees, A. H. Alkhaldi, M. Aslam, N. A. Siddiqui, and R. Ahmed, "Image encryption based on Chebyshev chaotic map and S8 S-boxes," Optica Applicata, vol. 49, pp. 317–330, Jan. 2019, doi: https://doi.org/10.5277/oa190212.