Received: January 23, 2021 Revised: March 20, 2021.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Video Steganography Using Chaos Encryption Algorithm with High Efficiency Video Coding for Data Hiding

Jaladi Vivek[1]* **Baswaraj Gadgay[2]**

[1]*Department of Electronics & Communication Engineering, Lingaraj Appa Engineering College, Bidar, India*
[2]*Department of PG Studies in Electronics & Communication,*
Visvesvaraya Technological University, Kalaburagi, India
* Corresponding author's Email: vivekjaladi@outlook.com

Abstract: Steganography is also known as data hiding, is a method of ensuring the security and confidentiality of digital data by hiding sensitive data in digital media. In video steganography, compression is the most demanding research area in block based video encoders. With the improvement of video coding equipment, the High Efficiency Video Coding (HEVC) delivers better coding efficiency. However, a large proportion of video frames showed system complexity and required a larger Coding Unit (CU) during encoding. Also, as the larger number of video frames were encoded, the time consumption was increased. To overcome such an issue, this research introduced the chaos with enhanced mapping technique to reduce computational complexity and fast encoding. In this research study, the position of each pixel of the secret video frame is calculated by the ELSB technique, where the existing LSB techniques have not considered this secret video frame's position which leads to high video distortion. In proposed chaos encryption with mapping method, the input video frames are encrypted by using logistic and henon mapping that simultaneously maintains quality and efficiency of the model. The HEVC technique compresses the input video frames and the proposed ELSB performs two functions namely replacement of LSB and matching of LSB which effectively embeds the secret video frames into cover video frames. Finally, the secret video frames are retrieved by HEVC technique with chaos decryption which provides security to the model. The results proved that proposed compression technique achieved PSNR of 35.81dB with average execution time of 40 seconds, but the existing H.264 compression technique achieved PSNR of 32.72dB with average execution time of 45 seconds.

Keywords: Coding unit, Digital data, Encryption algorithm, Enhanced least significant bit, Quality, Steganography.

1. Introduction

The development of the Internet and the advancement in the field of information and communication have made information security essential [1]. Digital images are the most popular file format due to their high availability on the Internet. The important data in the form of text, images, audio or video can be encrypted and hidden in another format of text, image, audio or video [2]. The combination of steganography and cryptography technologies can be a prime solution to strengthen security and maintain the confidentiality of data [3], where the main purpose of cryptography and steganography methods is to protect data from unauthorized persons. The process of getting the secret message (extracting the message) can be done by applying the cryptography and then the steganography based on the methods used in the hiding phase, where the selected methods for data hiding-extraction and data encryption-decryption must be secure and efficient [4].

The main disadvantages of cryptographic methods are the ability of hackers to find text messages and try to decrypt them using automatic counters based on computational mathematics or research experiments. Therefore, cryptographic techniques still have gaps in security, e.g. based only the decryption keys [5]. To address these issues, researchers use steganography, in which the security achieved by concealing confidential data on cover

media so that no one can doubt the existence of hidden data. The stenography technique has the ability to embed the cover and secret frames well and video degradation cannot be seen with the naked eye [6]. Video encryption usually requires an encryption scheme has low processing complexity, which is based on an encrypted bit stream format. Therefore, the research study uses the HEVC technique for compression that is one of the widely used video coding scheme for compression and its efficiency is compared with H.264/AVC [7]. The proposed ELSB technique considered the position selection of the secret video frames, while embedding into the cover video frames. Therefore, the proposed ELSB is used to improve the embedding rate as well as PSNR values, which is harder to detect the secret video frames in the stego video frames. For encrypting the secret video frames, the research study uses the chaos technique with enhanced mapping and used the ELSB for embedding process. The chaos decryption and HEVC decompression techniques are used to retrieve the secret frames from the cover video frames. The embedding capacity of HEVC technique is improved by the chaos technique with enhanced mapping. The experiments are conducted to validate the proposed method in terms of PSNR and structure similarity (SSIM). In the proposed method, the chaos encryption with logistic and henon mapping are used to encrypt the input video frames that maintains quality and efficiency of the system. The input video frames are compressed by HEVC technique and ELSB performs two functions such as replacement of LSB and matching of LSB to embed the secret video frames into cover video frames. Then, the secret video frames are retrieved by HEVC technique with chaos decryption that maintains security of the video frames.

The organization of the research work consists of: The study of existing video stenography is presented in the Section 2. The explanation of the proposed compression technique with encryption for stenography is illustrated. in Section 3. The validation of the proposed method with existing techniques for secret video frames is described. in Section 4. Finally, the conclusion of the research study with its future work is presented in Section 5.

2. Literature review

In this section, study of different existing techniques for steganography is presented, which are used for securing the information. In addition, the major advantages of existing techniques along with its limitations are also described.

Yao [8] implemented an efficient scheme for hiding encrypted H.264/AVC video bit stream data. During the encryption phase, the intra-prediction mode code words, motion vector variation and partial coefficients were encrypted without increasing the bit rate of the video to protect the privacy of the video content. When the receiver decrypts the encrypted video bit stream and removes the embedded data, the unique video bit stream was fully restored. However, when making reversible video data, it has still been a challenge to determine the optimal variation in the quantized DCT ratio to achieve superior visual quality and compression efficiency at an assumed embedding rate.

Nguyen [9] developed a new steganography scheme to improve the ability to embed H.264/AVC video sequences. In the proposed scheme, the coefficients of the quantized discrete cosine transform (QDCT) were divided into two distinct clusters: hiding clusters and preventing clusters. The simulation results showed that QDCT with embedding direction table provides better embedding performance while preserving great visual quality of the Stego video. However, the QDCT scheme was not related to restoring the original version of the video sequences.

Younus and Younus [10] proposed a method of hiding data in a video using the LSB and modified it with the knight Tour algorithm (KTA), which used a method to encrypt key features for encrypting secret messages. Then, the knight tour algorithm was used to randomly select pixels in the frame to embed secret messages and to improve the developed method. Finally, using the LSB method, the encrypted secret message was embedded in bits (7 and 8) in the selected pixels. However, the usage of the key should be a set of arbitrary values for selecting frames and embedded image or audio file within a video for better performance.

Tabash, and Izharuddin [11] developed a chaos encryption technique with the logistic map for encrypting the H.264 video data. The various modules of the compression pipelines were applied by the encryption technique, where the compression pipelines included residues transformation, Motion Vector Difference (MVD), entropy coding and Context-Adaptive Binary Arithmetic Coding (CABAC). The results proved the encrypted video was highly chaotic, where the information was completely opaque. However, due to the large proportion of encoding video frames, the system was complex and increased Coding Unit (CU) requirement.

Xue [12] implemented a QDCT coefficient of I-frames based on Syndrome–Trellis Code (STC). A

distortion optimization strategy was developed according to the block distortion analysis to avoid the distortion of inter and inner blocks. The results proved that developed method secured the steganographic scheme and minimized the block distortion. In this paper, the embedding coefficients were selected by calculating the cost function that was required to incorporate the secret message in the cover frame. However, the cost function needs an optimization technique to achieve better embedding capacity.

3. Proposed methodology

Initially, preliminaries of HEVC i.e. basic ideas that are essential to recognise the process of hiding and recovering the HEVC-coded videos are explained, before embedding the information using the proposed method.

Video pixels are a series of frames built together. The colour space is a reflection of the light and color that make up a frame. The research study uses the YUV Planar format in 4:2:0 modes. YUV can be thought of as a set of three metrics, one representing light (y or brightness) and the other two representing colour (dark), one red and the other blue, correspondingly. HEVC process provides two main encoding approaches that can be used simultaneously or separately. Intramode is a space compression technique that encodes each frame separately. The frames used in this method are in-frames (pictures within coding) that clearly indicate the compression technique. The subsequent mode is called intermode and there is time compression, in which each coded frame / field can refer to past and future frames / fields. The P frames (forecast pictures or delta frames) and B frames (bi-directional forecast pictures) enter to the intermode. The encoding process is not random, and frames are sorted by specific Group of Pictures (GoP) [13]. Two main key variables have a significant impact on the encoding process that causes lossy compression.

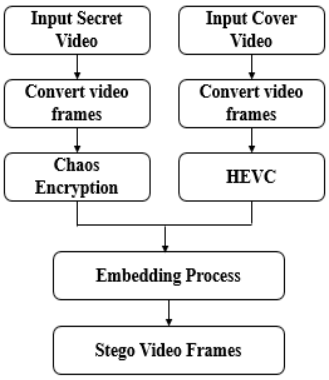

Figure. 1 Flowchart of Encoding Process

First, the index of the Quantization Parameter (QP) is the value at which the least significant information is extracted. The high quality loss occurred due to the high value of QP. Second, the adaptive of sample feature aims to improve visual (subjective) quality by reducing distortions between the original samples and the retrieved samples. The HEVC process [14] ultimately has a small bit stream, and its proportion is well defined. It has three main headers namely Network Abstraction Layers (NALs), which contain the necessary information about the video, images and parameters that can be transmitted as part of the bit stream or distinctly. Following these headings, the bit stream has a sequence of truncated NAL data for each encoded video frame.

3.1. Encoding process

In this research study, the proposed encryption algorithm consists of the following phases: video collection, convert the videos into frames, chaos encryption for encrypting the video frames and HEVC for compression, embedding and extraction phase. Fig. 1 shows the work flow of proposed encoding process and the explanation about the proposed encoding process is described below.

3.1.1. Data collection

In the Quarter Common Intermediate Format (QCIF) format, the experiments use eight video sequences (e.g. car phone, coast guard, container, foreman, hall, harbor, mobile and salesman). The first 100 frames of each video sequence are encoded at 30 frames per second (http://trace.eas.asu.edu/yuv/). IPPP is a GoP structure, where first frame is encoded as I-frame and the remaining frames are encoded as P-frames. These video frames are given as input to HEVC for compression and Chaos encryption for encrypting the secret images. In this research study, among the eight collected videos any one will act as secret images. Fig. 2 shows the sample images of video sequences.

3.1.2. Chaos encryption with enhanced mapping

After collecting the video frames, the secret image is encrypted using chaos encryption with enhanced mapping (logistic map and henon map). The logistic map and henon map simultaneously maintains security and efficiency of the model. These maps generate a simpler and stronger chaotic maps compared to other maps.

Figure. 2 Sample Video Sequence Data.

The threats of the system based on larger extent threats are avoided by logistic and henon maps. Due to the properties of discrete map, the cryptosystem shows higher performance in efficiency and it will be served as key stream generator for the encryption.

In this research, the permutation and diffusion phases are performed using the generated keys K_i and the value of logistic map and henon map. In chaos encryption, the simplest chaotic maps are mathematically given in the Eq. (1) and (2). Logistic map is a polynomial mapping of two grades that exhibits chaotic actions. The logistic map is mathematically given in Eq. (1).

$$l_{map} = \mu x_n(1 - x_{n-1}) \tag{1}$$

where, l_{map} is logistic map, and μ is represented as control parameter that ranges $\mu \in (3.57,4)$ and x_n is represented as chaos sequence that ranges between [0, 1]. The chaotic system exhibits better sensitivity to initial conditions, when the parameter approaches are four. Correspondingly, the henon map is a two dimensional reversible non-linear chaotic map that iterates the point (x_n, y_n), which is mathematically denoted in Eq. (2).

$$h_{map} = 1 - ax_n^2 + y_n, \;\; y_{n+1} \to bx_n \tag{2}$$

where, h_{map} is henon map, a and b are control parameter ranges from $a\epsilon(0,1.4)$, $b\epsilon(0.2, 0.314)$, x_n and y_n are the chaos sequence points. The working process of henon map mainly depends on the parametric values. Besides, iterate the hybrid mapping (logistic map and henon map) for five times in order to accomplish rid of the transient effect using the parameter value of hybrid mapping and generated keys K_i. In addition, sort the chaotic orbit which attained from the previous steps and then permutated the diffused or plain-image using Eq. (3) and (4).

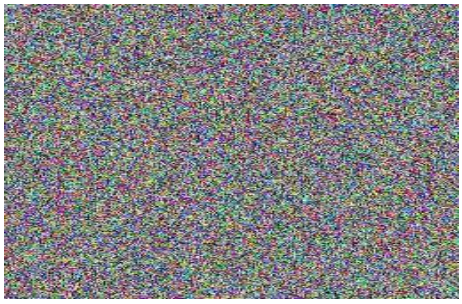

Figure. 3 Sample encrypted secret video frame

$$x_{n+1} = l_{map} + h_{map} \tag{3}$$

$$mim(i) = permute + K_i\big(x_{n+1}p(i)\big)$$
$$i \to 1,2,3,\ldots . p \times q \tag{4}$$

where, l_{map} is logistic map and h_{map} is henon map, and x_{n+1} is represented as chaos sequence, p and q are represented as width and height of plain-image, $p(i)$ is indicated as original image pixel value, and $mim(i)$ is represented as image pixel value.Finally, generate the cipher key for permuted image and then diffuse the permuted image using hybrid chaotic orbit. The output of diffusion stage is cipher-image $c(i)$ that is mathematically signified in Eq. (5).

$$c(i) = mim(i)\,, i \to 1,2,3,\ldots p \times q \tag{5}$$

where, $c(i)$ is the cipher image, $mim(i)$ is the image pixel value, p and q are represented as width and height of cipher image.

Fig. 3 shows the encrypted video frames of secret data. By using the chaos encryption techniques, the input secret video frames are encrypted for secure data transmission. The Fig. 3 shows the encrypted secret video frame of input data: Foreman. Once the secret video frames are encrypted, then the cover video frames are compressed using HEVC process that is explained below section.

3.1.3. HEVC process

Similarly, the cover frames are compressed by the compression technique called HEVC, which remains similar as H.264 and the block based coding methodology efficiently exploits the temporal and the spatial statistical dependencies [15], which allows large and multiple predictions, coding and block sizes to be effectively converted.

The quad-tree block partitioning [16] is based on Coding Tree Unit (CTU) structure, where CTU is made up of luma Coding Tree Block (CTB), two

chroma CTB and quad-tree syntax, where the luma CTB is a block of size of $N \times N$ and chroma CTBs are about the size $\left(\frac{N}{2}\right) \times \left(\frac{N}{2}\right)$. The largest supported coding block (CB) size is CTB size. A CTB consists of one or more CUs associated with Prediction unit (PU) and Transformation Unit (TU). Therefore, the encoding mode is chosen at the level of intra or inter prediction CU. With N, the flow is slightly selected, which can be 8, 16, 32 or 64. The CTUs are divided into hidden areas called CUs. Assuming using intra or inter predictions, the first image at each random access point of the video number is encoded using only intra prediction so that there is no reliance on other images. Most of the remaining frames are accurately encoded and mapped to the TU using the remaining DCT [17]. The computational complexity is reduced by using HEVC intra coding technique, initially depth range is predicted by using the CTU. Then, CUs are used to decide whether the current CU will be divided further or not. At last, intra prediction models are utilized for distortion optimization reduction based on the relation among the CUs.

Inter prediction in HEVC

HEVC supports more prediction block (PB) sections than the intra prediction mode. When a CU is skipped, the CU is characterised as a PU that does not have important transform coefficients and rate parameters derived from the overlay mode. In PU inter coding, the encoders use the merge mode or pure motion parameter transmission for each PU. The merge mode applies to PU coding and skip mode. The connection mode is to identify the neighbouring inter-coded PU so that it can be moved out of the current PU. HEVCs have motion vectors with units that are 1/4 the distance between Luma and Chroma samples.

Intra prediction in HEVC

The inner block uses a spatial relation with each PU and adjacent pixels for a better estimate. In order to effectively eliminate local redundancy and achieve high levels of compression, HEVC defined some new features such as CTU, CU, PU and TU. In addition, frequency distortion optimization was repeated to find the best forecast mode for each CU. The RD cost function is expressed mathematically in the Eq. (6).

$$RD = SSE + (\lambda \times R) \tag{6}$$

where, λ is indicated as quantization parameter, SSE is denoted as sum of squared distances between reconstructed and original pixels, and R is stated as bit rate.

In addition, HEVC uses a quad tree and structural design for dividing CUs. Each CU is separated into four PUs, with an intra-prediction being achieved for each PU. The maximum CU is 64 x 64 to 8 x 8 pixels, so that the maximum PU is 64 x 64 to 4 x 4 pixels. Thus, HEVC predicts intra to 64x64 to 4x4 pixel blocks. If the distance between the structure within the predicted routes and the horizontal or vertical mode is greater than the threshold value, a bi-linear filter is possible.

By using the HEVC techniques, the cover images are compressed and finally, the secret video frames and cover video frames are embedded using ELSB technique.

3.1.4. Enhanced least significant bit

After cover frame transformation and secret frame encryption, embedding mechanism is carried-out for hiding the secret frames in cover frames, which is called as stego data. In embedding process, ELSB is used as the bit position of the integer unit value. Here, the pixel values of cover and secret frames are transformed into binary values by applying ELSB. The proposed ELSB has two techniques namely replacement of LSB and matching technique of the LSB. The following below section describes these ELSB techniques.

3.1.4.1. Replacement of LSB

By placing the secret video on the cover frame, the secret video's two bits are simply overlaps the two bits' pixel value of cover video frame, i.e. the bit planes of first and second, while preserving the high bit planes. The recipient will be shared with secret key that are generated from embedding order, hence the pixel positions are reconstructed for retrieving the secret video frames from the corresponding bits of the stego video frames. Consider a set of match and mismatch as W and W' in this method, therefore four various cases are occurred i.e. WW, W'W', WW' and W'W. According to these four cases, the probability of changing the cover pixel values as 0.5 in this method and the following Eq. (7) shows the bit change of cover video frames as

$$C_b = \frac{1}{2}\sum_{i=0}^{2} P_i \times N_i \tag{7}$$

where, C_b is the bit change for cover video frames, the probability of occurrence is defined as P_i and total number of changed bits as N_i. Based on Eq. (7),

the match and mismatch cases are described in the Eq. (8).

$$C_b = \frac{1}{2}[P_0(WW) \times 0 + \{P_1(WW') + P_1(W'W)\} \times 1 + P_2(W'W') \times 2] \quad (8)$$

Here, C_b is the bit changes of cover video frames, $P_0, P_1\ and\ P_2$ is the probability of occurrence of match and mismatch as W and W', the four cases (W/W') have the same occurrence probability as $(P_0(\theta) = 0.25 \forall \theta)$. Therefore, Eq. (8) will be changed into Eq. (9).

$$C_b = \frac{0+0.5+0.25+0.25}{2} = 0.5\ bits \quad (9)$$

According to the following Eq. (9), the overall bit changes is 0.5 that are obtained from the replacement of LSB techniques. The next section presents the matching of LSB technique.

3.1.4.2. Matching of LSB

The video distortion will be high in the stego video frames due to embedding changes by the replacement of LSB technique, therefore, to solve these issues, matching of LSB technique is developed in this research study. This method considered the two bits of secret video frames and W with W' between the cover video frames for embedding process. During embedding, this technique considered a single W' as SW' and modified the pixel value of cover video frames of third LSB in some cases to point the W' index. According to the third LSB bits' binary value, the embedding process changes in the WW and WW' cases. The W' would be in the first LSB, when the selected pixel value of third LSB is zero, hence after embedding the result will be WW'. Suppose, the pixel value is one, the W' will be occurred in the second LSB and after embedding the result will be W'W.

The embedding method varies the selected pixel value of third LSB based on the W' index for another two cases i.e. WW' and W'W. Therefore, set the value of third LSB is 1 for W'W case and 0 for WW' case. Here, the probability is 50% that is the third LSB has a correct index value and hence, no changes are required to pixel value. The embedding process will be occurred based on the secret cover frames' two bit and W'W cases between replacements of LSB of the selected pixel value. Therefore, the transition of pixel value is different from the replacement of LSB. In the mathematical equation (10), the bit change of cover video frame for this method is stated as:

$$C_b = \frac{1}{2}[2 \times P_1(WW') + P_2(WW') \times 2] \quad (10)$$

Here, the total number of bits changed for WW' and W'W cases is 0.5 bits, because the correct value in the cover pixel of third LSB has the probability as 50%. Therefore, the occurrence of probability as $(P_0(\theta) = 0.25 \forall \theta)$ and the overall bit changes to 0.375 that is explained in the Eq. (11).

$$C_b = \frac{1}{2}[2 \times 0.25 + 1 \times 0.25] \quad (11)$$

When comparing with the replacement of LSB technique, this technique modifies the cover video frames with the probability of changing only 0.375 bits of LSB replacement of the pixel values of the cover video frames.

3.2. Decoding process

After embedding process, the extraction process is performed on the chaos with enhanced mapping encrypted stego frames for retrieving the secret frames from the cover frames.

From the decoding process, encrypted secret and compressed cover video frames are obtained. In this research study, the decryption phase is a single stage process that is directly proportional to the encryption phase. Here, HEVC decompression algorithm and chaos decryption using enhanced mapping are applied subsequently to extract the secret video frames from the cover video frames. The extracted secret frames must be the exact copy of the original secret frames.

4. Results and discussion

In this experimental section, the proposed approach is simulated using MATLAB (version 2018a) with 3.0 GHZ-Intel i5 processor, 1TB hard disc, and 8 GB RAM. The performance of the proposed methodology is compared with other existing methods for estimating the efficiency and effectiveness of the proposed compression algorithm. The performance of proposed compression algorithm is validated in light of embedding capacity (EC), PSNR, mean of SSIM (MSSIM) and SSIM. Here, the size of the cover image is 256×256 and the size of secret image is 128×128.

4.1. Performance measure

Performance metrics are defined as regular measurements of results and outcomes to provide reliable information about the effectiveness of the proposed compression algorithm. In addition,

efficiency is a process of collecting and analysing information about the performance of a group or an individual. The mathematical equation of PSNR, MSE, SSIM and EC are represented in the Eq. (12), (13), (14) and (15), respectively.

$$PSNR = 10\ log_{10}(\frac{255^2}{MSE}) \quad (12)$$

$$MSE = 1/mn \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(x,y) - k(x,y)]^2 \quad (13)$$

where, $m\ and\ n$ are represented as width and height of the image, $k(x,y)$ is denoted as the decrypted image, and $I(x,y)$ is indicated as the input image.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad (14)$$

where, $x\ and\ y$ were stated as windows of filter image k and original image I,$\sigma\ and\ \mu$ were denoted as standard deviation and mean of x and y, $c_1\ and\ c_2$ were indicated as constants.

$$EC = \frac{NEb}{NB} \quad (15)$$

where, the number of embedded bits is represented as NEb and number of 4×4 luminance blocks is defined as NB that are used for embedding the secret data. The EC will be increased based on the QP [8, 9].

4.2. Quantitative analysis of proposed encryption method

In this section, the performance of proposed chaos with HEVC for eight secret frames is validated in terms of PSNR, SSIM and Mean of SSIM as (MSSIM) are given in the Table 1. In this eight secret video sequence, the hall and container had higher PSNR value, i.e. 35.42dB for container and 35.29dB for hall.

Table 1. Performance Analysis of Proposed Chaos with HEVC technique for Secret Frames

Secret Video Frames	PSNR(dB)	SSIM	MSSIM
Car phone	34.71	0.97	0.86
Coastguards	34.09	0.95	0.84
Container	35.42	0.96	0.86
Foreman	34.81	0.96	0.85
Hall	35.29	0.96	0.87
Harbor	33.18	0.95	0.85
Mobile	33.49	0.98	0.88
Salesman	34.62	0.95	0.85

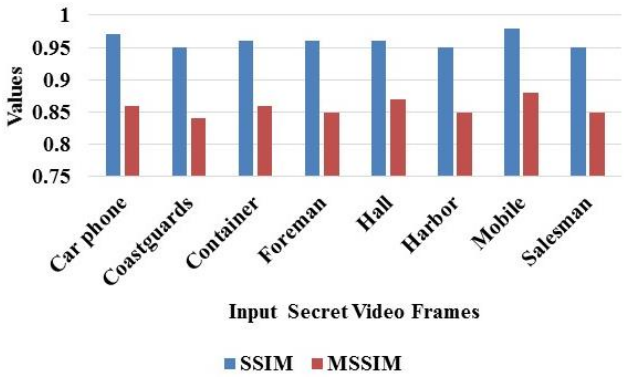

Figure. 4 Graphical Illustration of Proposed Method by means of SSIM and MSSIM for secret video frames

Table 2. Embedding Capacity of Proposed HEVC compression Technique

QP	Embedding Capacity (bit per pixel(bpp))
18	1.34
23	1.21
28	1.01
33	0.87
38	0.67
43	0.45

The harbor and mobile video frame have the lowest PSNR value (i.e. 33.18dB and 33.49dB), while comparing with other six video frames. The performance of the any encryption method on stenography highly depends on the higher PSNR value, but the proposed chaos with enhanced mapping technique has lower PSNR value. This is compensated by the EC of HEVC compression technique, which is explained in the comparative analysis. Fig. 4 presents the graphical representation of the proposed stenography algorithm by means of SSIM and MSSIM.

From the Table 1, it is clearly stated that the proposed method achieved better SSIM than MSSIM for eight secret video frames. The mobile frame has the highest SSIM and MSSIM than other secret video frames and three video frames, such as coastguards, harbor and salesman has the lowest SSIM and MSSIM (i.e. 0.95SSIM and 0.85MSSIM). The encryption chaos technique is improved by using the enhanced map, which is used to improve the performance of stenography video techniques. The EC of proposed HEVC compression methods based on QP is presented in Table 2.

4.3. Comparative analysis of proposed compression technique

In this section, the proposed compression method is compared with the existing techniques called H.264 bit streams [8] and QDCT [9] in terms of

PSNR and SSIM for secret images based on various QP, which is shown in Table 3.

From the comparative analysis, it is clearly stated that the proposed HEVC compression technique achieved better PSNR than the QDCT [9] and H.264 bit streams [8] for various QP. The reason is that the encryption technique (chaos with enhanced mapping) used in the proposed compression techniques increases the EC that leads to minimize the PSNR values. For instance, the QDCT achieved 42.70dB and 0.99SSIM, where proposed compression HEVC technique achieved only 46.70dB and 0.99SSIM for the QP=18. The existing H.264 and QDCT achieved nearly 34dB and 0.95SSIM, where the proposed method achieved 39.42dB and 0.97SSIM for the QP=28. This shows that the proposed compression technique achieved better performance due to the use of the chaos encryption technique with an enhanced map for secret video frames. In addition, the performance of proposed HEVC compression technique is compared with existing H.264 [12] in terms of PSNR and SSIM of varying QP parameters for all cover images, which is shown in Table 4.

From the Table 4, it is clearly proved that the proposed HEVC technique achieved higher PSNR and SSIM values for all sample video frames, even the QP has changed. For instance, proposed HEVC achieved 36.22dB and existing H.246 achieved 35.40dB on Container video frames, when the QP is 28. In addition, the SSIM of proposed HEVC is nearly 93% to 98% on all eight sample video frames.

Table 3. Comparative Analysis of Proposed Compression Technique

QP	H.264 bit streams [8]		QDCT [9]		Proposed Compression HEVC Technique	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
18	-	-	42.70	0.991	46.70	0.99
23	-	-	38.39	0.979	43.09	0.98
28	34.99	0.95	34.34	0.955	39.42	0.97
33	32.72	0.93	30.05	0.917	35.81	0.96
38	-	-	26.89	0.867	33.29	0.89
43	-	-	23.93	0.812	31.18	0.86

Table 4. Comparative Analysis of Proposed HEVC compression technique with existing H.264 in terms of PSNR and SSIM by varying QP

Sample Video Frames	QP	Embedding Capacity	PSNR			SSIM		
			Cover	H.264 [8]	Proposed HEVC	Cover	H.264 [8]	Proposed HEVC
Car phone	24	52355	39.89	36.80	37.57	0.98	0.97	0.98
	28	22915	36.95	34.99	36.45	0.97	0.96	0.97
	32	8934	33.98	32.72	34.49	0.95	0.94	0.94
Coastguard	24	200428	37.12	33.12	33.23	0.96	0.93	0.95
	28	92213	33.94	31.18	31.46	0.92	0.90	0.91
	32	31162	30.89	29.21	30.94	0.85	0.84	0.85
Container	24	26131	38.71	37.26	38.10	0.96	0.95	0.98
	28	9887	36.05	35.40	36.22	0.94	0.94	0.95
	32	3389	33.38	33.10	35.02	0.93	0.93	0.93
Foreman	24	60827	38.86	35.97	37.47	0.98	0.96	0.97
	28	29686	36.15	34.04	36.00	0.96	0.95	0.96
	32	14221	33.42	31.84	32.31	0.94	0.93	0.93
Hall	24	24700	39.84	37.87	38.06	0.98	0.98	0.98
	28	13461	37.35	35.97	36.74	0.97	0.97	0.98
	32	7252	34.51	33.53	34.53	0.96	0.96	0.96
Harbor	24	295230	36.95	31.97	33.11	0.99	0.95	0.96
	28	160100	33.65	29.46	31.41	0.97	0.93	0.95
	32	67074	30.27	27.32	28.31	0.93	0.90	0.92
Mobile	24	329938	36.70	31.63	32.43	0.99	0.96	0.97
	28	169418	33.13	29.74	31.73	0.97	0.95	0.98
	32	65460	29.42	27.51	28.03	0.94	0.93	0.95
Salesman	24	25661	38.62	35.80	37.13	0.98	0.97	0.97
	28	12378	35.60	33.59	35.52	0.95	0.95	0.97
	32	5600	32.55	31.38	32.72	0.91	0.90	0.92

Table 5. Comparative Analysis of Proposed HEVC technique with ELSB in terms of PSNR and Execution time

Authors	Methods	PSNR (dB)						Average execution time (secs)
		Coastguard	Container	Foreman	Harbor	Salesman	Mobile	
Tabash, and Izharuddin, [11]	Chaos encryption-CABAC	-	-	22.8	20.7	18.4	14.4	93
Xue [12]	QDCT-STC	33.85	34.64	31.61	32.47	-	33.14	45
Proposed	HEVC-ELSB	34.09	35.42	34.81	33.18	34.62	33.49	40

4.4. Comparative analysis of proposed compression technique with embedding technique

The performance of proposed HEVC technique along with ELSB is validated with existing techniques, namely chaos encryption technique with CABAC [11] and QDCT-STC [12] on secret video frames in terms of PSNR and Average Execution time which are shown in Table 5.

From this experiment, it is clearly stated that the proposed HEVC technique with ELSB achieved better performance than existing techniques. The existing LSB technique focused only on encryption technique and didn't use the compression technique called HEVC for secure steganography. In addition, the pixel value is fixed in existing LSB technique for embedding process. The Chaos encryption [11] and QDCT-STC [12] technique used the HEVC compression technique for improving the security of the steganography process. However, the embedding capacity was minimum due to the large proportion of the encoding complexity consumed by CU and achieved less performance than the proposed HEVC-ELSB for all input video samples. For example, the chaos encryption with CABAC achieved 22.8dB on Foreman and 20.7dB on Harbor samples, the QDCT-STC achieved 31.61dB on Foreman and 35.29dB on Harbor samples, where the proposed HEVC with ELSB achieved 34.81dB on Foreman and 33.18dB on Harbor samples. The reason is that the position of the pixel value of the secret video frames is either make constant or calculated by cost function. In addition, the match and mismatch cases are not considered by the existing LSB techniques and that the cost function in QDCT-STC [12] requires optimization for better embedding capacity. But, the proposed ELSB considered both match and mismatch cases and identify the probability values for placing the secret video frames in the cover video frames, which does not require any optimization function. The average execution time of Chaos encryption [11] and QDCT-STC [12] technique was 93 and 45 seconds respectively. Whereas, in proposed chaos encryption with mapping method the average execution time is 40 seconds. Therefore, the proposed HEVC-ELSB achieved better PSNR and fast encoding than existing techniques [11] and [12].

5. Conclusion and future work

A highly secured transmission network is developed in this research study for real-time applications. The effective video compression technique called HEVC with encryption algorithm is implemented for video stenography. The cover video frames are compressed by the HEVC technique, where the secret video sequences are encrypted by chaos technique with enhanced mapping to ensure the data integrity and privacy of the data. The ELSB method is applied to embed the secret video frames into cover video frames and chaos decryption with decompression techniques are used to retrieve the secret video frames from the cover video frames. The fast encoding and less computation time are achieved by the proposed chaos encryption algorithm with enhanced mapping. The proposed chaos encryption algorithm with enhanced mapping, improved the decryption of stego videos and preserves the integrity of the secret video frames which are evaluated in terms of PSNR. The proposed compression with chaos encryption technique uses a limited number of video sequences as input, so this technique can be developed in the future to handle more number of video frame sequences. In future work, the video compression is further improved by developing enhanced HEVC technique.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd author.

References

[1] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and Balusamy B. "Securing data in Internet of Things (IoT) using cryptography and steganography techniques", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 50, No. 1, pp. 73-80, 2019.

[2] C. Rangaswamaiah, Y. Bai, and Y. Choi, "Multilevel data concealing technique using steganography and visual cryptography", In: *Proc. of Future of Information and Communication Conference*, pp. 739-758, 2019.

[3] J. C. T. Arroyo, J. A. Espadero, M. A. Ganas, R. F. Ardeña, R. N. Vilchez, and A. J. P. Delima, "An Efficient Least Significant Bit Image Steganography with Secret Writing and Compression Techniques", *International Journal*, Vol. 9, No. 3, pp. 3280-3286, 2020.

[4] R. J. Rasras, Z. A. AlQadi, and M. R. A. Sara, "A methodology based on steganography and cryptography to protect highly secure messages", *Engineering, Technology & Applied Science Research*, Vol. 9, No. 1, pp. 3681-3684, 2019.

[5] K. N. Jassim, A. K. Nsaif, A. K. Nseaf, B. Priambodo, E. Naf'an, M. Masril, I. Handriani, and Z. P. Putra, "Hybrid cryptography and steganography method to embed encrypted text message within image", In*: Proc. of Journal of Physics: Conference Series*, Vol. 1339, No. 1, pp. 012061, 2019.

[6] H. L. Nyo and A. W. Oo, "Secure Data Transmission of Video Steganography Using Arnold Scrambling and DWT", *International Journal of Computer Network & Information Security*, Vol. 11, No. 6, pp. 45-53, 2019.

[7] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H. 264/AVC video coding standard", *IEEE Transactions on circuits and systems for video technology*, Vol. 13, No. 7, pp. 560-576, 2003.

[8] 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.

[9] 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.

[10] Z. S. Younus and G. T. Younus, "Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data", *Journal of Intelligent Systems*, Vol. 29, No. 1, pp. 1216-1225, 2019.

[11] F. K. Tabash and M. Izharuddin, "Efficient encryption technique for H. 264/AVC videos based on CABAC and logistic map", *Multimedia Tools and Applications*, Vol. 78, No. 6, pp. 7365-7379, 2019.

[12] 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.

[13] D. R. Galiano, A. A. Del Barrio, G. Botella, and D. Cuesta, "Securing high-resolution train videos encoded with HEVC and inter prediction mode", *Computers in Industry*, Vol. 121, pp. 103258, 2020.

[14] D. R. Galiano, A. A. Del Barrio, G. Botella, and D. Cuesta, "Efficient embedding and retrieval of information for high-resolution videos coded with HEVC", *Computers & Electrical Engineering*, Vol. 81, pp. 106541, 2020.

[15] M. Wang, J. Li, L. Zhang, K. Zhang, H. Liu, S. Wang, S. Kwong, and S. Ma, "Extended quad-tree partitioning for future video coding", In: *Proc. of Data Compression Conference*, pp. 300-309, 2019.

[16] V. Argyriou and T. Vlachos, "Quad-tree motion estimation in the frequency domain using gradient correlation", *IEEE Transactions on Multimedia*, Vol. 9, No. 6, pp. 1147-1154, 2007.

[17] S. Kumar, B. Panna, and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function", *Medical & biological engineering & computing*, Vol. 57, No. 11, pp. 2517-2533, 2019.