Multimedia Systems (2018) 24:419–437
https://doi.org/10.1007/s00530-017-0568-3

REGULAR PAPER

# Efficient HEVC selective stream encryption using chaotic logistic map

**Ahmed I. Sallam[1] · El‑Sayed M. El‑Rabaie[2] · Osama S. Faragallah[1,3]**

Received: 1 February 2017 / Accepted: 6 October 2017 / Published online: 11 November 2017


**Abstract** At present, the digital video encryption technology has become an interest research topic as a result of very rapid evolution in the application of real-time video over the Internet. So this paper presents a new method for encrypting the selective sensitive data of the latest video coding standard, which called High-Efficiency Video Coding (HEVC). The High-Efficiency Video Coding was founded in 2013 by the Joint Collaborative Team on Video Coding (JCT-VC) from the ISO/IEC Moving Picture Experts Group (MPEG) and ITU-T Video Coding Experts Group (VCEG). The proposed selective encryption HEVC video technique uses the low complexity overhead chaotic logistic map (CLM) to encrypt the sign bits of the Motion Vector Difference (MVD) and the Discrete Cosine Transform (DCT) coefficients in the entropy stage of the process of video encoding. The contribution of the proposed CLM-based HEVC SE is to encrypt the sensitive video bits with the features of low complexity overhead, fast encoding time, keeping the HEVC constant bitrate and format compliant. Also, this paper introduces a comparative study between the proposed CLM-based HEVC SE and the Glenn HEVC SE that uses the Advanced Encryption Standard (AES). Experimental results demonstrate the main feature of the proposed CLM-based HEVC SE, which turned out to save the time of the video encoding with remaining of the near visual distortion of the encrypted video stream by Glenn HEVC SE. This feature is due to the low complexity of the CLM-based encryption employed in the proposed CLM-based HEVC SE scheme instead of using the AES in the Glenn HEVC SE. A course of security investigation experiments is performed for the proposed CLM-based HEVC SE including the main security performance metrics like encryption quality, key space, statistical and sensitivity tests. The achieved test results ensured the superiority of the proposed CLM-based HEVC SE for digital video streams.

**Keywords** Video compression · HEVC · Video encryption · Selective encryption · Chaotic logistic map

## 1 Introduction

To enhance the video coding efficiency, a lot of the video coding schemes have been developed. The most common video coding standards have been developed by the International Telecommunications Union (ITU-T) and the International Standardization Organization (ISO), the International Electro technical Commission (IEC) standards organizations. The ITU-T developed the H.261 [1] and H.263 [2] video coding standards, the ISO/IEC developed the MPEG-1 [3] and MPEG-4 [4] video coding standards, and the two organizations jointly developed the H.262/MPEG-2 [5], H.264/AVC [6] and HEVC [7]. The HEVC is developed to enhance the coding efficiency of the video compared to the H.264/AVC and to decrease the required bit rate of the video for storage or transmission by about 50%. The HEVC video

Communicated by T. Plagemann.

✉ Osama S. Faragallah
osam_sal@yahoo.com; o.salah@tu.edu.sa

1 Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

2 Department of Electronic and Communication Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

3 Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 888, Al-Hawiya 21974, Kingdom of Saudi Arabia

coding standard provides various operation modes like low delay mode that is utilized in real time applications and the random access mode that frames can be randomly accessed to provide efficient video compression.

The HEVC is the most recent video coding standard which is developed by JCT-VC. The JCT-VC is a joint video project team between the ITU-T VCEG and the ISO/IEC MPEG. The HEVC is defined as MPEG-H Part 2 in the ISO/IEC and H.265 in the ITU-T standardization organizations. The ITU-T and ISO/IEC published the first version of the HEVC video coding standard in 2013 [8]. The main feature of the HEVC is to increase the compression ratio of the video with keeping the same video quality compared to the H.264/AVC standard. The HEVC achieves such feature by changing the core of the coding layer from macroblock with fixed size to the coding tree unit (CTU) with flexible larger size. In the H.264/AVC, the macroblock consists of one $16 \times 16$ block of luma and two $8 \times 8$ blocks of chroma but the CTU in the HEVC standard consists of coding tree block (CTB) of luma and CTB of chroma with size $16 \times 16$, $32 \times 32$ or $64 \times 64$. The HEVC standard introduces the concept of the tile as another feature to improve the capability of the parallel processing of video coding on the multicore processors. Tiles are formed by dividing the video frame into rectangular regions and each region can be coded independently. Also, the HEVC adds more filters like adaptive SAO (Sample Adaptive Offset) filter to decrease the visual distortion between the raw video frame and the coded frame.

In the last years, the video data confidentiality has become a challenging research topic. The simple way for securing the video data is to encrypt all the video bitstream using encryption scheme without considering the video compression structure that is defined as Naive Encryption Algorithm (NEA) [9–11]. The NEA has some disadvantages like the large computationally cost of the encryption/decryption process especially for the high-resolution videos and unsuitable for performing the transcoding and watermarking post-processing operations on the encrypted video bitstream. So, there is a bad need for video SE that may be considered as a good alternative for the NEA. The video SE depends on the structure of the video coding and encrypts only the data with high sensitivity in the video bitstream. The video SE protects the video content access from the unauthorized users and should guarantee the following criteria [10, 11]:

- Tunability: The video encrypted parts and the encryption parameters should be flexible to be modified dynamically.
- Visual degradation: The video should be destroyed in visual after the encryption process.
- Cryptographic security: The encryption algorithm should not be weak.
- Encryption ratio: The ratio of the size of the encrypted parts of the video and the size of the original video.
- Compression friendliness: The encryption algorithm should have little impact on the video compression efficiency.
- Format compliance: The encrypted video should be decoded by the standard decoder without the decryption process.

Using the encryption standard algorithms has the disadvantage of significant processing overhead during the encryption/decryption processes that is not suitable for encrypting the real time video applications [11].

Nowadays, using the chaotic theory for video encryption has become an interest research topic. The main advantage of the encryption using chaotic theory lies in the low complexity processing overhead that make it suitable for encrypting real-time video applications [11].

This paper is to present a new proposed HEVC SE using the feature of low complexity overhead of the chaotic logistic map (CLM) to encrypt the sensitive video bits like the DCT coefficients signs and the MVD signs. The contribution of the proposed CLM-based HEVC SE is to encrypt the sensitive video bits with the features of low complexity overhead, fast encoding time, keeping the HEVC constant bitrate and format compliant.

The paper rest is arranged as follows: Sect. 2 explains the basic concept of the HEVC video coding structure and introduces an overview of the previous HEVC SE techniques. Section 3 gives the full details about the proposed CLM-based HEVC SE scheme. Section 4 introduces the instrumented performance studies to compare the proposed CLM-based HEVC SE scheme and the Glenn HEVC SE scheme [19]. Section 5 presents the security investigation of the proposed CLM-based HEVC SE scheme. Section 6 concludes the paper.

## 2 HEVC selective encryption related work

The HEVC has a unified flexible syntax architecture and multiple profiles or levels that are used to support various ranges of applications. The HEVC has the main profile that is used for the most popular applications and present video sample by 8 bit and one luma and two chromas. The other profile is the main still picture profile that is used for taking snapshots from the video sequences [12]. The third profile is the main ten profile that is used to present video sample by 10 bit. The HEVC video coding structure uses the hybrid video coding structure that is used for developing most of the video coding standards since the H.261. This structure is the efficient way to coding the video signal and converts it to bitstream with a small size. Figure 1, shows the HEVC hybrid video coding structure [12].

From Fig. 1, the HEVC video coding standard is developed based on the concept of the block-based hybrid video coding. In the HEVC, the video is divided into a sequence of pictures, each picture is divided into blocks and each block is predicted by using either intra prediction or inter prediction. The intra prediction removes the spatial redundancy between neighboring blocks inside a picture and the inter prediction removes temporal redundancy between pictures. The subtraction between the original block and the predicted block forms the prediction error that is defined as the residual. The prediction error (residual) is transformed from the spatial domain to the frequency domain using the Discrete Cosine Transform (DCT). Then the DCT coefficients are quantized and coded with the prediction information by the entropy process to be transmitted as a bitstream.

The HEVC provides the concept of video picture partitioning into variable units sizes. In the HEVC the video is divided into a sequence of pictures, each picture is divided into coding tree blocks (CTBs) with a square shape with the same component of the luma and chroma and each luma CTB and its associated chroma CTBs is grouped and defined as code tree unit (CTU). The CTU is the basic coding unit in the HEVC. The size of the luma CTB is variable of $2^N \times 2^N$ and the size of each chroma CTB is $2^{N-1} \times 2^{N-1}$ where $N = 4$, 5 and 6 [12].

In the HEVC, the coding unit (CU) is the level that the prediction mode is decided to be intra or inter. In the intra

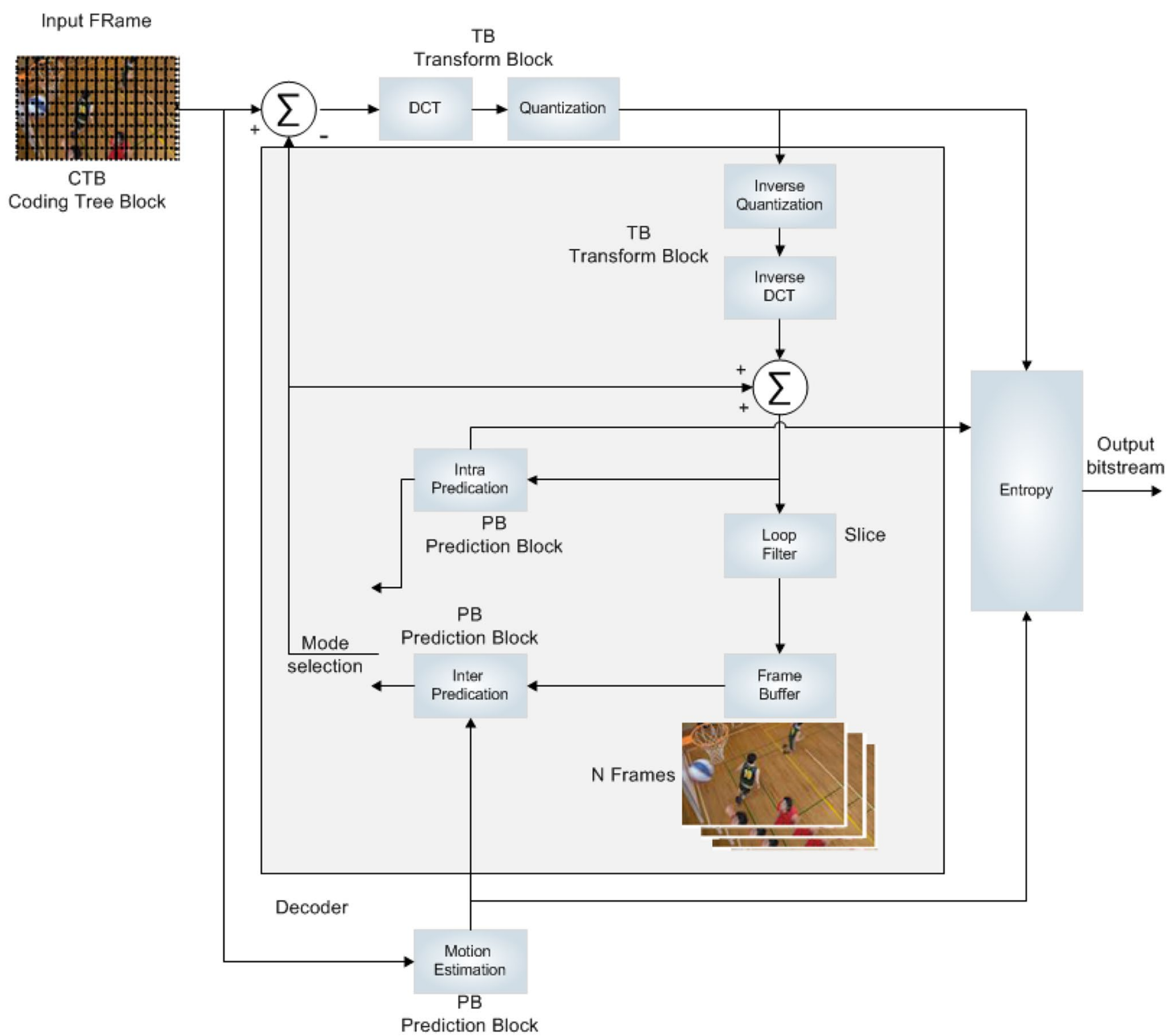



Fig. 1 The HEVC hybrid video coding structure [12]

prediction mode, the CU is predicted from its reconstructed neighboring CUs in the same slice. Figure 2 shows that the HEVC intra prediction has 35 modes containing DC mode, planar mode, and 33 angular modes. The intra prediction mode from 2 to 18 is defined as horizontal mode because of the source of the prediction in the horizontal direction while the intra prediction mode from 19 to 34 is defined as vertical mode because of the source of the prediction in the vertical direction. In the HEVC intra prediction, the size of the prediction block is variable from 4 × 4 to 32 × 32. The intra prediction reference for the prediction block (PB) is formed from the reconstructed neighboring blocks in the double length in the horizontal or vertical directions [13].

In the inter prediction, the previous reconstructed pictures are used as a reference for motion compensation. The difference between a picture and its successor in the video sequence is generated by the displacement between block based areas in the successive pictures during the video coding process. The inter prediction in the HEVC is carried out on the prediction block (PB) level and is defined as motion compensated prediction (MCP). The motion information (motion vector) of the current PB can represent the displacement between the current PB and its location in the reference sample picture [13].

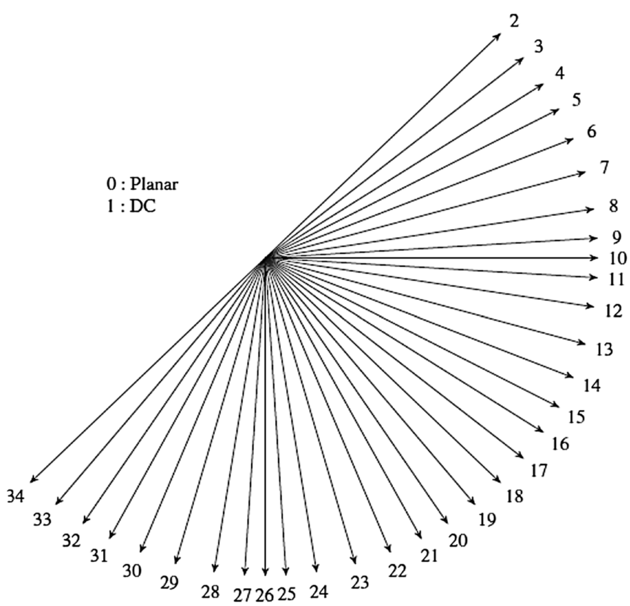



**Fig. 2** HEVC intra prediction modes [13]

Figure 3, introduced the inter picture prediction concept in the HEVC stander. The motion vector ($\Delta x$, $\Delta y$) represents the displacement between the position of the block in the previous reference picture and the position of the block in the current picture where $\Delta x$ represents the horizontal displacement and $\Delta y$ represents the vertical displacement. The previously coded pictures are defined as a reference picture and indicated by reference index $\Delta t$. The combination of the motion vector and the reference index is called the motion data. There are two types of the inter prediction defined as uni-prediction and bi-prediction [12]. In the bi-prediction, two groups of motion data ($\Delta x_0$, $\Delta y_0$, $\Delta t_0$) and ($\Delta x_1$, $\Delta y_1$, $\Delta t_1$) are combined together to produce the final motion compensated prediction for the current picture. The previously coded pictures in the bi-prediction are saved in two separate lists called list 0 and list 1.

The entropy process encodes a group of symbols that represents the video sequence into a compressed bit stream to be transmitted or stored. The HEVC video coding uses the context-based adaptive binary arithmetic coding (CABAC) for the entropy process [14]. The CABAC is a type of entropy coding that is presented in the previous video coding H.264/AVC. In the H.264/AVC, although the CABAC introduces high video coding efficiency, it has a problem with the parallel processing concept and hence restricts its throughput. In HEVC video coding, the CABAC entropy coding provides the parallel processing concept to enhance the throughput.

Figure 4, shows the block diagram of the CABAC that is used in the entropy coding in the HEVC. The binarization process is used to convert the non-binary values to binary values called bins that represent the syntax elements. The

**Fig. 3** inter prediction concept in HEVC [12]

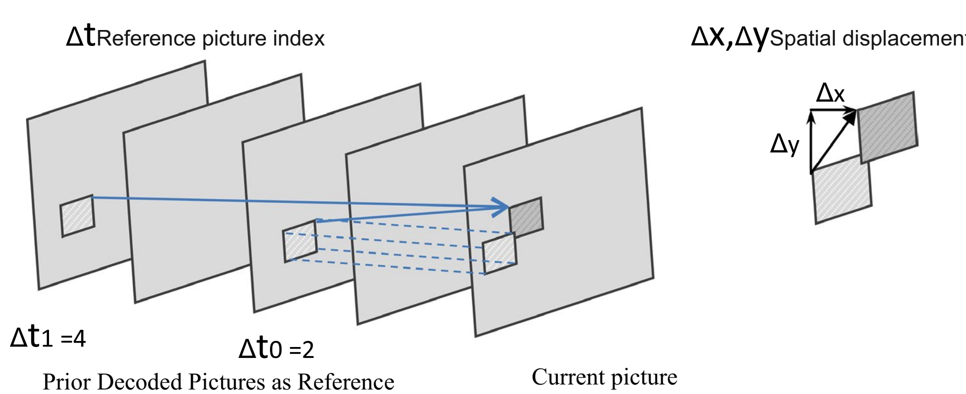
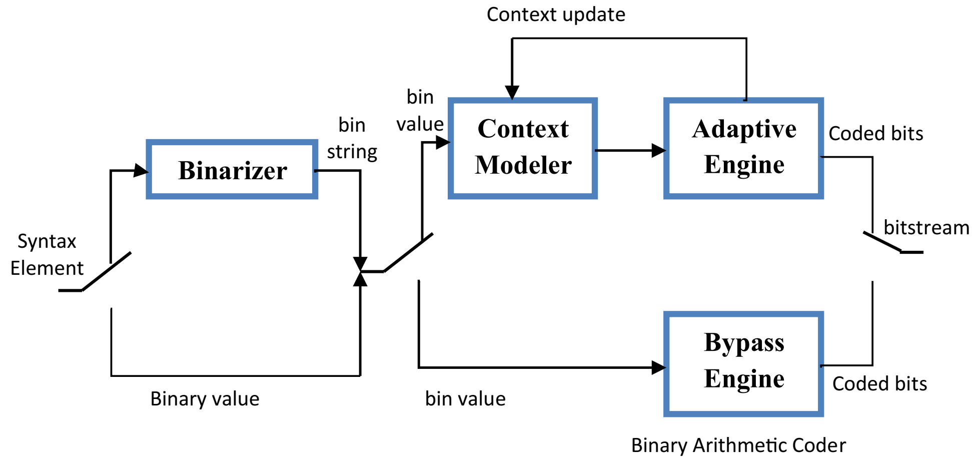


**Fig. 4** HEVC CABAC entropy coding block diagram [14]




bypass model presents a non-adaptive regular arithmetic coding with fixed settings depends on bin position that is used for coding the DCT coefficients signs and MVD signs that are existed randomly. In this model, the bins values are signaled directly to the output bitstream. The adaptive coding engine model is utilized for coding the most frequently observed bins [14].

There are two kinds of video encryption schemes as follows:

- Perceptual or transparent encryption that provides the ability to view the video in low quality while preventing the unauthorized user from accessing the video in high quality. This kind is utilized in pay-per-view applications.
- Sufficient encryption that provides the ability of visual distortion for the video content and preventing the unauthorized user from viewing the video.

In [15], Hofbauer et al. proposed an HEVC SE scheme that based on flipping the AC DCT coefficients sign bits in the luminance channel randomly based on a specified percentage p of signs in the bit stream. This scheme performs fast video encryption/decryption with video format compliance guarantee.

In [16], Tew et al. enhanced the Hofbauer et al. [15] scheme by encrypting the transform skip signal, AC DCT coefficients and MVD sign bins based on hash function.

In [17], Shahid and Puech introduced an HEVC SE technique that depends on encrypting the truncated rice binstrings of the quantized transform coefficients (QTCs) by AES in cipher feedback mode (CFB) [18]. The context of the binstrings of the truncated rice code of the QTCs should be remaining unchanged to provide the video format compliance and provide the same bit-rate with little processing power.

In [19], Glenn et al. proposed an HEVC SE technique that depends on encrypting particular syntax elements like reference picture set (RPS), QP information, Inter information (reference picture indices, MVD), Residual information, Deblocking filter and SAO parameters. The syntax elements have been encrypted by the AES that means the encoder and the decoder have the same Key. At the encoder side, the AES algorithm generates pseudo-random bits based on the shared encryption key then perform XOR between the syntax element that is selected to be encrypted and the pseudo-random bits resulting in the encrypted bits in the video bitstream. At the decoder side, the AES algorithm generates pseudo-random bits based on the shared encryption key then perform XOR operation between the encrypted bits and the pseudo-random bits resulting in the original bits.

## 3 The proposed encryption method

### 3.1 chaotic systems

The chaos theory is the basic mathematical concept of the chaotic cryptography. Chaotic systems have several significant features that provide a tradeoff between high security and computational complexity power [20]. The rapid chaotic system has the following properties:

- Deterministic: the chaotic system has mathematical equations to control their behavior.
- Sensitive to the initial conditions and parameters: any simple change in the initial conditions or parameters of the chaotic system results in rapid and uncorrelated change in the chaotic map.
- The ergodicity: the map path will pass through all the partitioned regions of the state space.

One of the simplest chaotic-based encryption systems is the CLM [21]. The CLM is defined in Eq. 1.

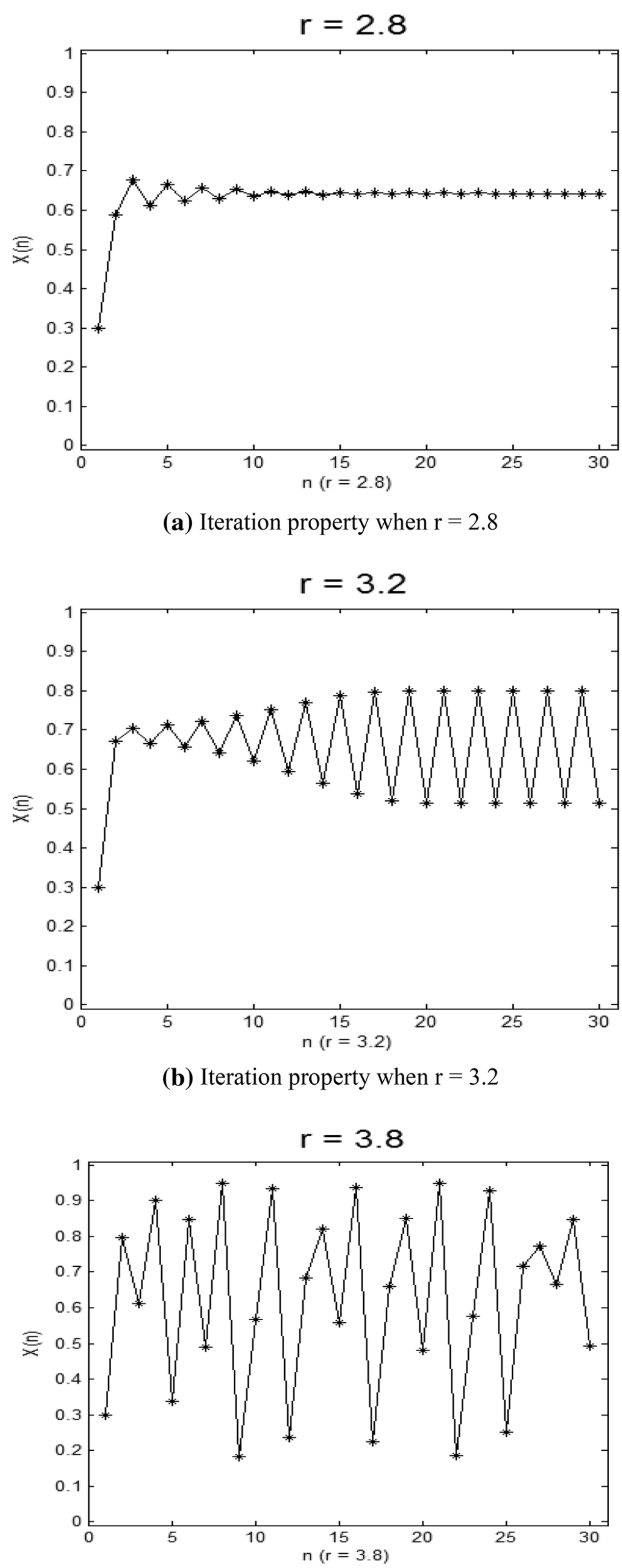
$$X_{n+1} = rX_n (1 - X_n) \tag{1}$$

where $X_n$ takes values from 0 to 1. The parameter $r$ is a positive constant and takes values from 1 to 4. The $r$ value defines the chaotic logistic map behavior.

A MATLAB program is used to simulate the CLM map in Eq. 1. Let the initial value $X_0 = 0.3$ and loop iteration = 100,000. Figure 5 shows the behavior of the CLM with respect to the various values of parameter $r$.

Figure 5a shows that when $r \in [0, 3]$, the CLM gives the same results after several iterations without any chaotic behavior. Figure 5b shows that when $r \in [3, 3.57]$, the CLM gives a periodic shape with the same peak points. Figure 5c shows that when $r \in [3.57, 4]$, the CLM gives the chaotic behavior with different peak points. Figure 6 shows the bifurcation diagram of the CLM.

- For $r \in [0, 3.57]$, the points concentrate on several values and could not be used for video cryptosystem.
- For $r \in [3.57, 4]$, the logistic map exhibits chaotic behavior, and ensure the sensitive to the initial conditions and parameters property.
- For $r \in [0, 3.57]$, the points concentrate on several values and could not be used for video cryptosystem.
- For $r \in [3.57, 4]$, the logistic map exhibits chaotic behavior, and ensure the sensitive to the initial conditions and parameters property.




**(a)** Iteration property when r = 2.8

**(b)** Iteration property when r = 3.2

**(c)** Iteration property when r = 3.8

**Fig. 5** Analysis of logistic map [21]

### 3.2 The proposed CLM-based HEVC SE scheme

The proposed CLM-based HEVC SE scheme based on encrypting the sign bins of the DCT coefficients and the MVD in the CABAC entropy process by using the CLM-based encryption [20, 21]. The proposed CLM-based HEVC SE scheme provides the encrypted bitsteam in a format compliance manner and at the same bit rate compared to the original data. The CLM-based encryption provides a minimum computational complexity overhead that helps in minimizing the encryption/decryption time in the encoding/decoding process. Figure 7 shows the block diagram of the proposed CLM-based HEVC SE scheme.

The proposed selective encryption for HEVC algorithm is described in the following steps:

1. Generating random value of $r$ parameter of the chaotic logistic map using a given secret key. The $r$ value should be between 3.57 and 4.
2. Generating the pseudo-random bits by using the chaotic logistic map encryption system in the previous step.
3. The DCT coefficient sign bit is XORed with a random bit generated in the previous step.
4. The MVD sign bit is XORed with a random bit generated in step 2.

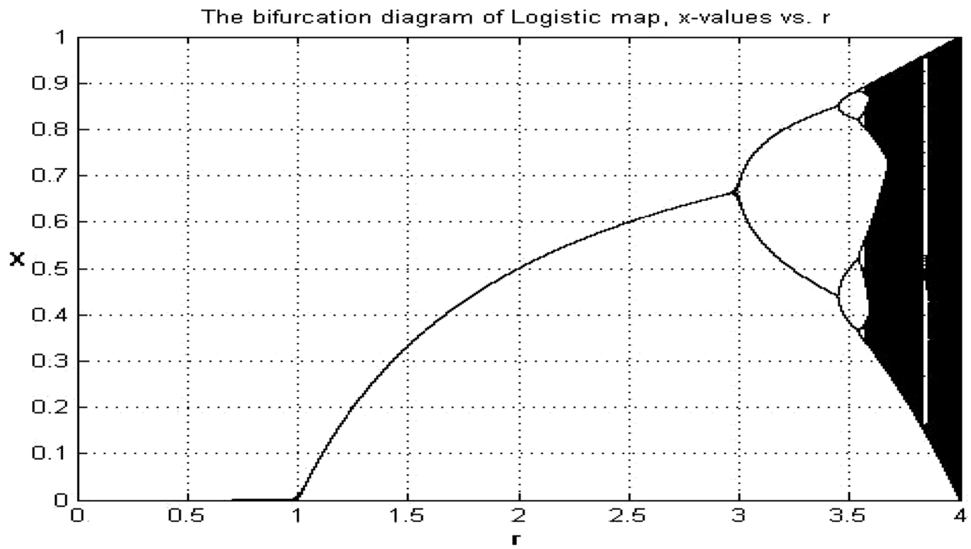



**Fig. 6** Bifurcation diagram of the CLM $r \in [0, 4]$ [21]

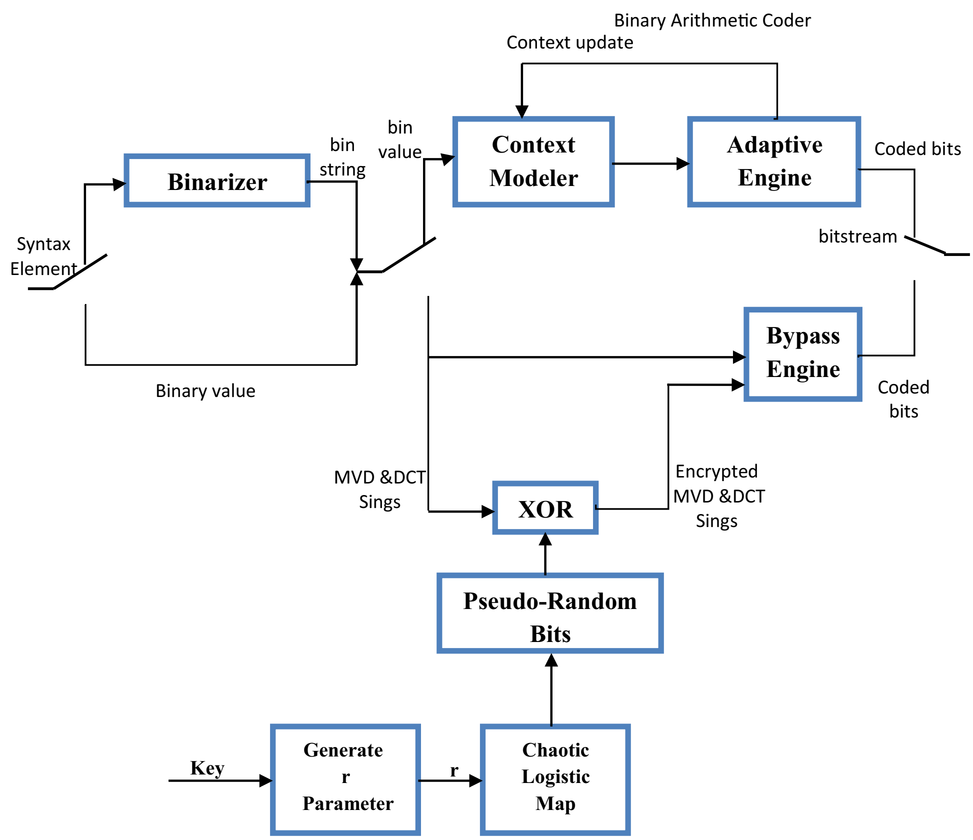



**Fig. 7** The proposed selective encryption for HEVC block diagram

Hofbauer et al. [15] and Tew et al. [16] encrypt only the AC DCT coefficients sign bits and keep the DC coefficients sign bits without encryption. But the proposed CLM-based HEVC SE encrypts all the AC and DC coefficients signs that results in more visual scrambling for the video contents and provides more security.

Shahid and Puech [17] and Glenn et al. [19] use the 128-bit AES to encrypt the HEVC bitstream that results in delay in the encoding/decoding processes. But the proposed CLM-based HEVC SE uses the CLM that achieve a high level of security with lower complexity and minimum the delay in the encoding/decoding processes.

## 4 Performance study

Table 1 shows the comparison analysis between the proposed CLM-Based HEVC SE and the previous related HEVC SE schemes.

From Table 1 the proposed CLM-based HEVC SE performs the lowest computational time in the sufficient encryption type. To prove that, the next subsection will provide the performance comparison study for the proposed CLM-based HEVC SE scheme, the Glenn HEVC SE scheme [19] and the Shahid HEVC SE scheme [17].

There are many objective video quality metrics like the bjontegaard delta (BD) bitrate, the peak signal-to-noise ratio (PSNR) and SSIM metrics that can be used to analyse the performance of various video coding techniques. The PSNR is widely used because of its simplicity but it does not contain any property of the human visual system (HVS). The SSIM is defined for measuring the components of the luminance similarity, the contrast similarity and the structural similarity [22]. This section describes test experiments to measure the scrambling performance and the encoding time between the proposed CLM-based HEVC SE scheme and the Glenn HEVC SE scheme [19]. The proposed CLM-based HEVC SE scheme, the Glenn HEVC SE scheme [19] and the Shahid HEVC SE scheme [17] are implemented by applying the encryption on the HM16.0 reference software [23].

The methodology of the experimental results is described as follows:

1. Encoding the video test sequence that shown in Table 2 by the original HM16.0 reference software without encryption to generate the original video stream.
2. Encoding the video test sequence that are in Table 2 by the modified version of the HM16.0 reference software by applying AES to encrypt the DCT and MVD sign bits to generate the encrypted video stream of Glenn HEVC SE scheme [19].
3. Encoding the video test sequence that are in Table 2 by the modified version of the HM16.0 reference software by applying the proposed CLM-based HEVC SE scheme to encrypt the DCT and MVD sign bits to generate the encrypted video stream of the proposed CLM-based HEVC SE scheme.
4. Compare the average encoding time per each frame between the proposed CLM-based HEVC SE scheme and the Glenn HEVC SE scheme and the Shahid HEVC SE scheme.
5. Compare the bjontegaard delta (BD) bitrate, the average PSNR and SSIM between the encrypted video stream generated from the proposed CLM-based HEVC SE scheme and the Glenn HEVC SE scheme with reference to the original video stream.

The machine that is utilized in the implementation has the following specifications; CPU speed 3.4 GHz core i7, physical RAM size 6 GB and hard disk size 500 GB. The encoding parameters are described in Table 3. These experiments use the MSU video measurement tool to measure the PSNR and SSIM metrics [26].

### 4.1 Encoding time experimental results

The Table 4 illustrates the measurement of the average encoding time for one frame in seconds of the proposed CLM-based HEVC SE scheme, the Glenn HEVC SE [19] and the Shahid HEVC SE [17] for the video sequence dataset in Table 2.

**Table 1** Comparison analysis between the proposed CLM-based HEVC SE and the previous HEVC SE schemes

| Encryption schema | Encryption types | Encryption domain | Encryption algorithm | Format compliance | Compression dependent | Low complexity |
|---|---|---|---|---|---|---|
| The proposed CLM-based HEVC SE | Sufficient encryption | DCT coeff signs + MVD signs | Stream cipher (chaotic logistic map + XOR) | Yes | Yes | Yes |
| Glenn HEVC SE [19] | Sufficient encryption | DCT coeff signs + MVD signs | Stream cipher (AES + XOR) | Yes | Yes | No |
| Shahid HEVC SE [17] | Sufficient encryption | DCT coeff signs + MVD signs + DCT coeff_abs_level remaining suffix | Block cipher (AES-CFB) | Yes | Yes | No |
| Hofbauer HEVC SE [15] | Perceptual encryption | AC DCT coeff signs | Stream cipher permutation | Yes | XOR No | Yes |
| Yiqi Tew HEVC SE [16] | Perceptual encryption | AC DCT coeff signs + transform skip signal | Stream cipher permutation | Pseudo-random Bits yes | Yes | Yes |

**Table 2** Performance study video sequences [24, 25]

| Frame sequence | Resolution | Frame per second (fps) |
|---|---|---|
|  Bosphorus | 3840 × 2160 | 120 |
|  Jockey | 1920 × 1080 | 120 |
|  FourPeople | 1280 × 720 | 60 |
|  Mobcal | 720 × 576 | 25 |
|  Forest | 320 × 240 | 30 |

**Table 3** Encoding parameters values

| Parameter | Value |
|---|---|
| Profile | Main |
| Configuration | Low delay for real time applications |
| Group of picture (GOP) | Four frames consists of one I frame followed by Three B Frames |
| Quantization parameter (QP) | 22-27-32-37 |

The experimental results show that the proposed CLM-based HEVC SE scheme has encoding time lower than the encoding time of the Glenn HEVC SE scheme [19] and lower than the Shahid HEVC SE. Table 4 showed that the proposed CLM-based HEVC SE scheme saved the average frame encoding time from 4 s for the low-resolution video (320 × 240) to 17 s for the high-resolution video (3840 × 2160) than the Glenn HEVC SE scheme [19]. This saving in the encoding time is due to using the chaotic logistic map encryption algorithm, which is low complex than using the AES to generate the pseudo random bit based on a shared key which used to encrypt the sign bits of the DTC coefficients and the MVD. Also, the proposed CLM-based HEVC SE scheme saved the average frame encoding time from 11.5 s for the low-resolution video (320 × 240) to 1429 s for the high-resolution video (3840 × 2160) than the Shahid HEVC SE scheme [17]. This saving in the encoding time is due to using the chaotic logistic map encryption algorithm, which is low computational time, instead of using the AES–CFB encryption algorithm. The Shahid HEVC SE scheme [17] does not meet the real-time constraint because it consumes a lot of time for preparing the plaintext blocks and converting the non-dyadic encryption space to dyadic encryption space in the encryption process.

**Table 4** Average encoding time per frame in seconds for the proposed, Glenn HEVC SE and the Shahid HEVC SE techniques

| Video Sequence | Technique | | |
|---|---|---|---|
| | The proposed CLM-based HEVC SE | Glenn HEVC SE [19] | Shahid HEVC SE [17] |
| Bosphorus | 910 | 927 | 2339 |
| Jockey | 295 | 309 | 510 |
| FourPeople | 125 | 140 | 253 |
| Mobcal | 53 | 60 | 216 |
| Forest | 15 | 19 | 26.5 |

### 4.2 Bjontegaard delta (BD) bitrate, PSNR and SSIM experimental results

The bjontegaard delta (BD) bitrate is used to evaluate the compression efficiency of the HEVC video after the encryption process [27]. It computes the average PSNR and the delta bit rate between two curves with different rate-distortion. The PSNR and the SSIM metrics are used to compare the visual degradation between the encrypted and the original video stream. These metrics indicate how much video quality is lost due to the encryption process.

Tables 5, 6 illustrate the measurement of the average PSNR and SSIM of the proposed CLM-based HEVC SE scheme and the Glenn HEVC SE [19] for the video sequence dataset in Table 2. Table 7 illustrates the measurement of the BD bitrate for the proposed CLM-based HEVC SE scheme and the Glenn HEVC SE [19] for the video sequence dataset in Table 2.

Tables 8, 9 illustrate the measurement of the average PSNR and SSIM for the proposed CLM-based HEVC SE scheme and the Glenn HEVC SE scheme [19] for the Four

**Table 5** Average PSNR for the proposed and the Glenn HEVC SE encryption techniques

| Video sequence | Technique | |
|---|---|---|
| | The proposed CLM-based HEVC SE | Glenn HEVC SE [19] |
| Bosphorus | 11.74 | 10.92 |
| Jockey | 12.73 | 10.67 |
| FourPeople | 8.25 | 9.46 |
| Mobcal | 7.89 | 8.21 |
| Forest | 4.57 | 5.43 |

**Table 6** Average SSIM for the proposed and the Glenn HEVC SE encryption techniques

| Video sequence | Technique | |
|---|---|---|
| | The proposed CLM-based HEVC SE | Glenn HEVC SE [19] |
| Bosphorus | 0.34 | 0.217 |
| Jockey | 0.029 | 0.045 |
| FourPeople | 0.011 | 0.146 |
| Mobcal | 0.233 | 0.154 |
| Forest | 0.081 | 0.073 |

**Table 7** Bjontegaard-delta Bit-rate for the proposed and the Glenn HEVC SE encryption techniques

| Video sequence | Technique | |
|---|---|---|
| | The proposed CLM-based HEVC SE | Glenn HEVC SE [19] |
| Bosphorus | 0.00 | 0.00 |
| Jockey | 0.00 | 0.00 |
| FourPeople | 0.00 | 0.00 |
| Mobcal | 0.00 | 0.00 |
| Forest | 0.00 | 0.00 |

People video sequence with resolution of $1280 \times 720$ at different QP values and their corresponding encryption results are shown in Figs. 8, 9.

The proposed CLM-based HEVC SE scheme has visual distortion with a slight difference of that is generated by the Glenn HEVC SE scheme [19]. Also, the CLM-based HEVC SE has no impact on the HEVC compression efficiency, as the Glenn HEVC SE.

Tables 5 and 8 showed that the encrypted video generated by the proposed CLM-based HEVC SE scheme has lower average PSNR than the average PSNR of the encrypted video that is generated by the Glenn HEVC SE scheme [19] by 0.8 dB. Tables 6, 9 showed that the encrypted video that is generated by the proposed CLM-based HEVC SE scheme has average SSIM higher than the average SSIM of the encrypted video that is generated by the Glenn HEVC SE scheme [19] by 0.015.

**Table 8** Average PSNR of both the proposed CLM-based HEVC SE scheme and the Glenn HEVC SE scheme [19] for FourPeople video sequence at different QP values

| QP | Technique | |
|---|---|---|
| | The proposed CLM-based HEVC SE | Glenn HEVC SE [19] |
| 22 | 7.12 | 9.41 |
| 27 | 7.63 | 10.37 |
| 32 | 8.25 | 9.46 |
| 37 | 7.79 | 9.74 |

**Table 9** Average SSIM of both the proposed CLM-based HEVC SE scheme and the Glenn HEVC SE scheme [19] for Four People video sequence

| OP | Technique | |
|---|---|---|
| | The proposed CLM-based HEVC SE | Glenn HEVC SE [19] |
| 22 | 0.088 | 0.016 |
| 27 | 0.05 | 0.018 |
| 32 | 0.011 | 0.146 |
| 37 | 0.059 | 0.127 |

Table 7 showed that the Bjontegaard-Delta bit-rate values both of the CLM-based HEVC SE and Glenn HEVC SE are zero. That means the both schemes preserve the bit rate after encryption process and there is no impact on the HEVC video compression efficiency. The saving of the same bit rate is due to the encryption of the bypass syntax elements of the MVD and DCT coefficient signs that provide motion scrambling and texture deformation. These syntax elements are represented as one bit (zero or one) in the original video and after the encryption process, they also are represented as one bit. So both of the CLM-based HEVC SE and Glenn HEVC SE have no compression efficiency overhead cost.

## 5 Security analysis

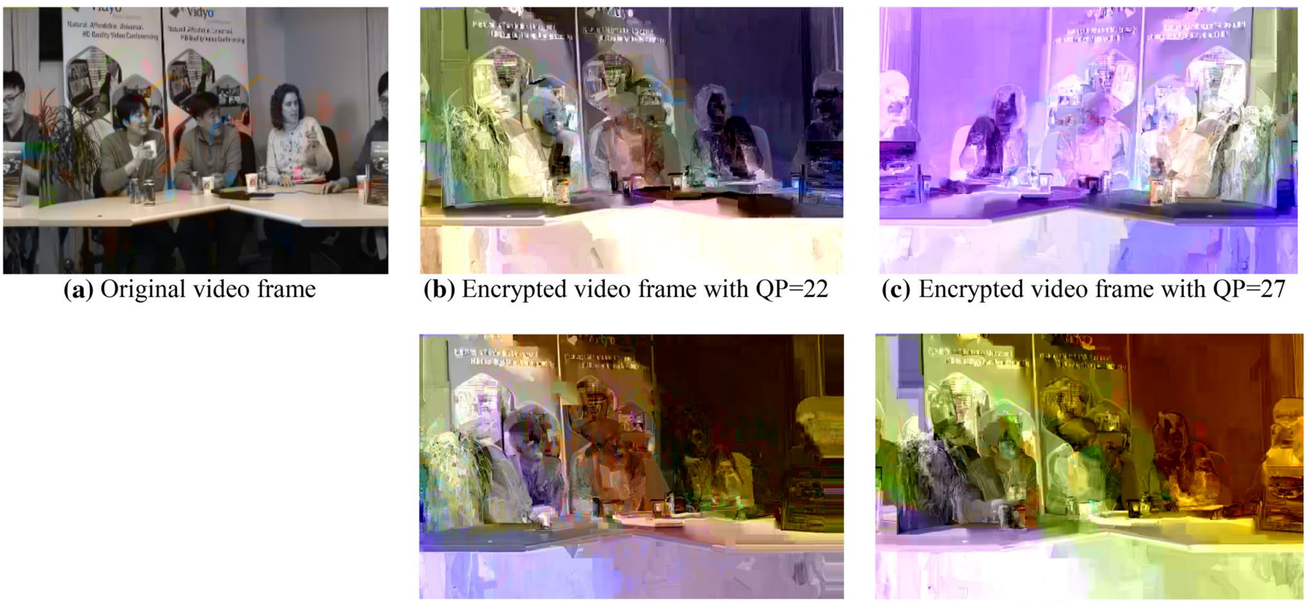
This section presents the security analysis of the proposed CLM-based HEVC SE scheme like key space analysis, statistical analysis, and sensitivity analysis to ensure the

A- Original Fourpepole Video Frame.

B- Encrypted Fourpepole Video Frame By Glenn HEVC SE Scheme [19]

C- Encrypted Fourpepole Video Frame By The Proposed CLM-Based HEVC SE Scheme

**Fig. 8** Encryption Of fourpeople video frame using the proposed CLM-Based HEVC SE scheme and The Glenn HEVC SE scheme [19]



**(a)** Original video frame
**(b)** Encrypted video frame with QP=22
**(c)** Encrypted video frame with QP=27
**(d)** Encrypted video frame with QP=32
**(e)** Encrypted video frame with QP=37

**Fig. 9** Encryption Of Fourpeople video frame using the proposed CLM-Based HEVC SE scheme at different QP

security and the robustness of the proposed CLM-based HEVC SE scheme against the most common attacks.

### 5.1 Key space analysis

To prevent the brute force attack, large key space should be used [27]. The proposed CLM-based HEVC SE scheme uses CLM which has sensitive initial condition that is calculated from the secret key with 256-bit length. The key space size of the proposed CLM-based HEVC SE scheme is $2^{256}$ which is very large and provides good robustness against the brute force attack.

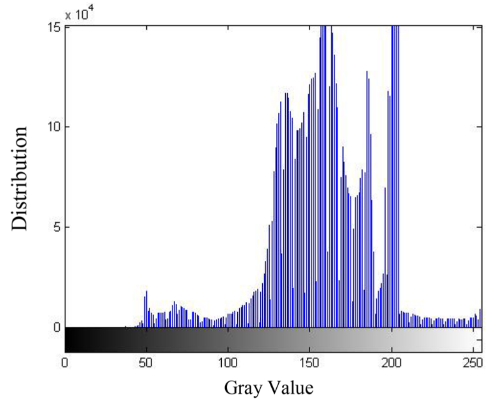
### 5.2 Statistical analysis

To prove that the proposed CLM-based HEVC SE scheme is robust, statistical analysis have been performed by using the histogram and correlations coefficient analysis.

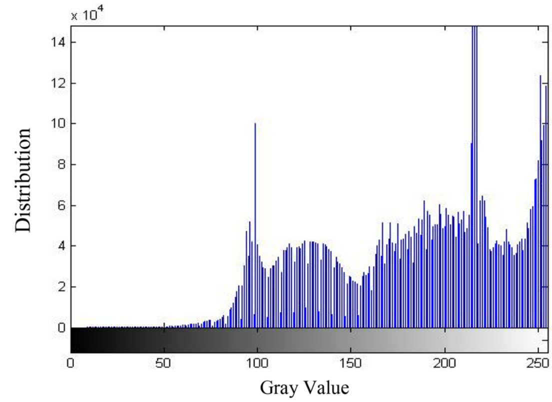
#### *5.2.1 Histograms analysis*

The histogram analysis is a graphical representation of pixels distribution in video frame for each color intensity level [28].

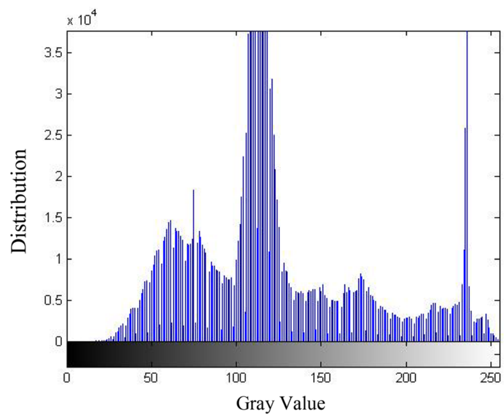
Figure 10 shows the histogram of the original and the encrypted video frame number 10 using the proposed CLM-based HEVC SE scheme for the video sequences in Table 2.



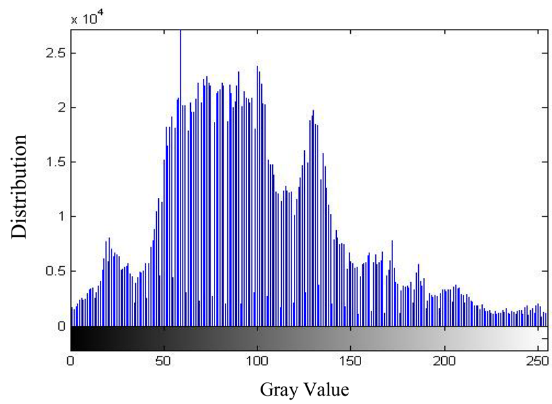

**(a)** Histogram of original video Frame # 10 of the Bosphorus with resolution 3840x2160 video sequence



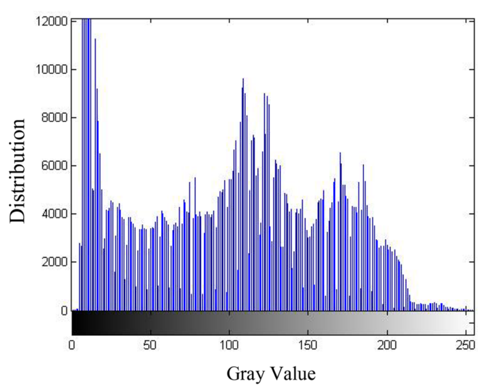

**(b)** Histogram of encrypted video Frame # 10 of the Bosphorus with resolution 3840x2160 video sequence



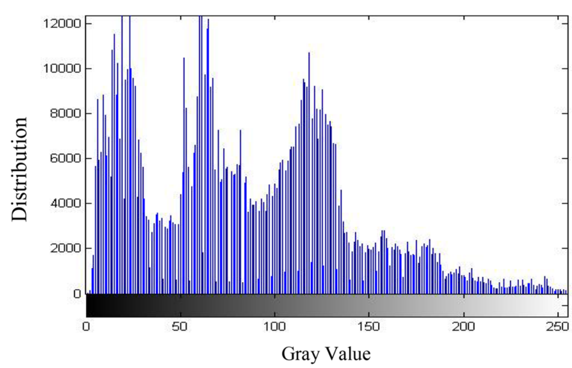

**(c)** Histogram of original video Frame # 10 of the Jockey with resolution 1920x1080 video sequence




**(d)** Histogram of encrypted video Frame # 10 of the Jockey with resolution 1920x1080 video sequence

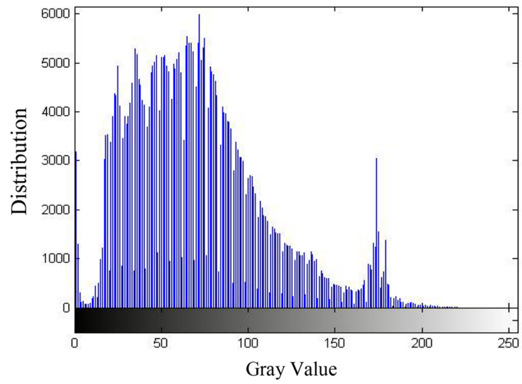



**(e)** Histogram of original video Frame # 10 of the FourePeople with resolution 1280x720 video sequence

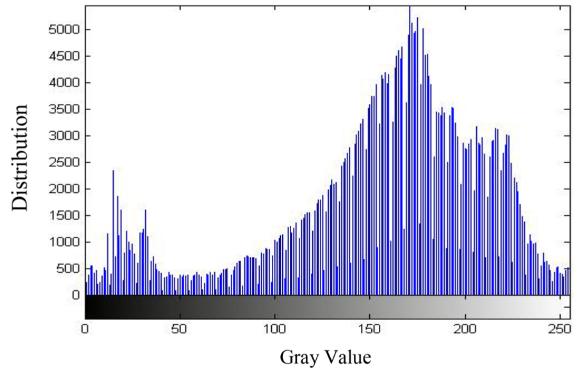



**(f)** Histogram of encrypted video Frame # 10 of the FourePeople with resolution 1280x720 video sequence

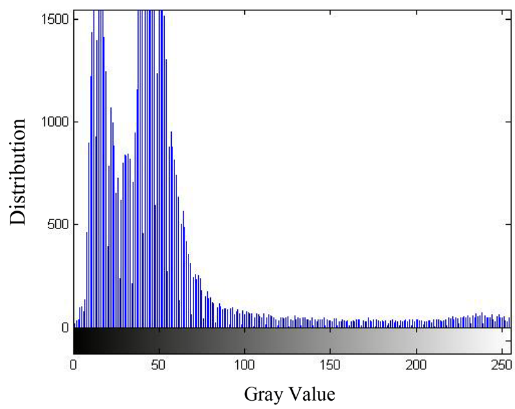
**Fig. 10** Histogram analysis of the original and encrypted of video frame # 10 of the video sequences In Table 1 using the proposed CLM-based HEVC SE scheme



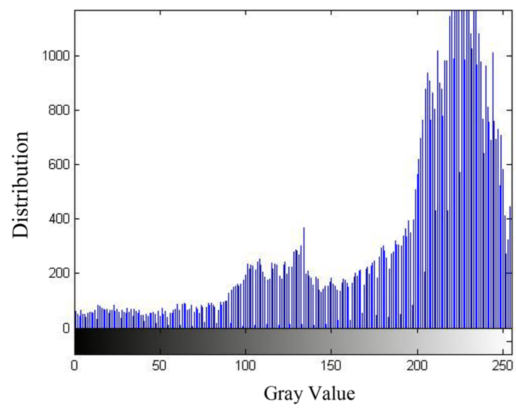

**(g)** Histogram of original video Frame # 10 of the Mobcal with resolution 720x576 video sequence




**(h)** Histogram of encrypted video Frame # 10 of the Mobcal with resolution 720x576 video sequence




**(i)** Histogram of original video Frame # 10 of the Forest with resolution 320x240 video sequence




**(j)** Histogram of encrypted video Frame # 10 of the Forest with resolution 320x240 video sequence

**Fig. 10** (continued)

### *5.2.2 Correlation coefficient analysis*

Correlation coefficient analysis measures the linear dependence between two adjacent pixels in the same image or two corresponding pixels in different images at the same position [29]. The correlation coefficient r can be estimated as:

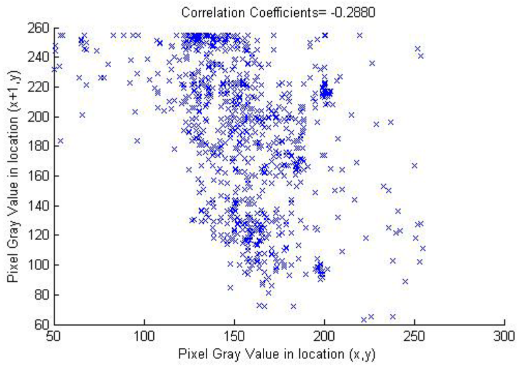
$$r(x,y)=\frac{\sum_i (x_i-x_m)(y_i-y_m)}{\sqrt{\sum_i (x_i-x_m)^2}\sqrt{\sum_i (y_i-y_m)^2}} \tag{2}$$

where, $x_i$ is intensity value of first pixel in position $i$ and $x_m$ is the mean intensity value of first pixel in position $i$. $y_i$ is intensity value of second pixel in position $i$ and $y_m$ is the mean intensity value of second pixel in position $i$. The correlation coefficient has the following values:

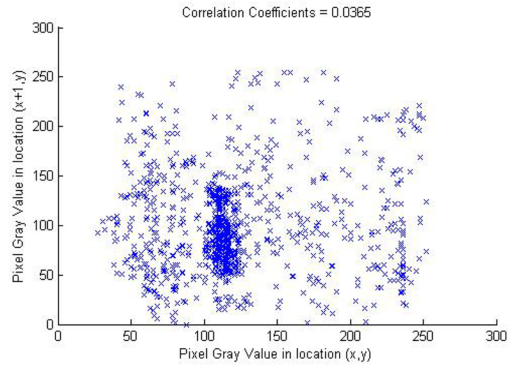
- $r = 1$: the two frames are identical.
- $r = 0$: the two frames are uncorrelated.
- $r = -1$: the two frames are anti-correlated.

For testing the correlation coefficient analysis of the proposed CLM-based HEVC SE scheme, the following steps are performed:

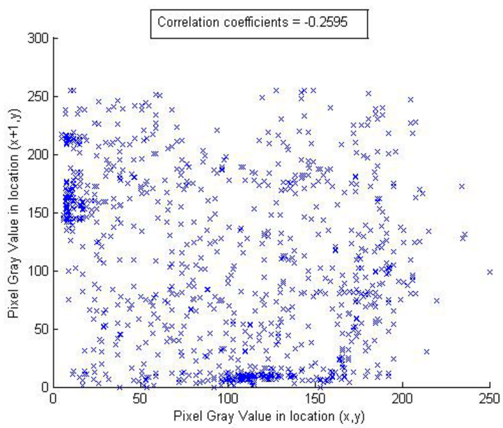
- Select random 1000 pixels from the original video frame #10 from FourPeople video sequence.



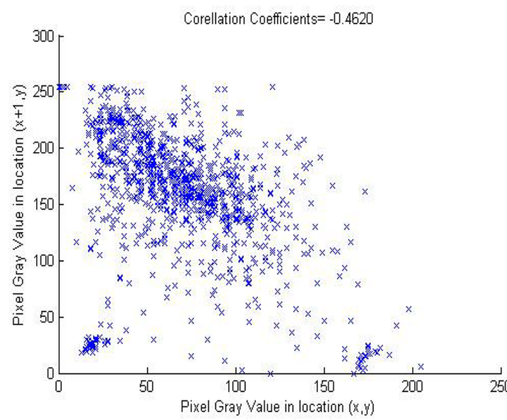

**(a)** Bosphorus with resolution 3840x2160 video sequence



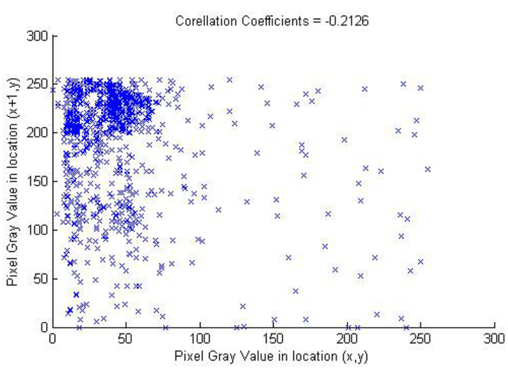

**(b)** Jockey with resolution 1920x1080 video sequence




**(c)** FourePeople with resolution 1280x720 video sequence




**(d)** Mobcal with resolution 720x576 video sequence




**(e)** Forest with resolution 320x240 video sequence

**Fig. 11** Correlation distribution between the horizontally pixels in encrypted/original video frame #10 from video sequences in Table 2 using the proposed CLM-based HEVC SE scheme

- Select the corresponding 1000 pixels from the encrypted video frame #10 from FourPeople video sequence at the same positions.
- Calculate the correlation coefficient for the 1000 pixels using the formula in Eq. (2).

Figure 11 shows the correlation distribution among 1000 horizontal pixels in original video frame #10 from video sequences in Table 2 and their correspondent pixels in the encrypted frame for the proposed CLM-based HEVC SE scheme. Table 10 shows the correlation coefficients among the encrypted and the original frame #10 in

**Table 10** Correlation coefficients among the original and the encrypted frame #10 of the video sequences in Table 2 using the proposed CLM-based HEVC SE scheme

| Direction of the corresponding pixels | Bosphorus | Jockey | FourPeople | Mobcal | Forest |
|---|---|---|---|---|---|
| Horizontal | – 0.2880 | 0.0365 | – 0.2595 | – 0.4020 | – 0.2126 |
| Vertical | – 0.2998 | 0.0304 | – 0.2341 | – 0.4082 | – 0.2557 |
| Diagonal | – 0.3376 | 0.0994 | – 0.2222 | – 0.4104 | – 0.2533 |

**Table 11** The encryption quality of the proposed CLM-based HEVC SE scheme for the first 5 frames of the Fourpepole video sequences in Table 2 at different QP values

| QP | Frame # | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| 22 | 6882 | 6864 | 6819 | 6788 | 6745 |
| 27 | 7128 | 7116 | 7127 | 7129 | 7112 |
| 32 | 7431 | 7439 | 7446 | 7434 | 7435 |
| 37 | 8287 | 8249 | 8204 | 8199 | 8173 |

**Table 12** The encryption quality of the proposed CLM-based HEVC SE scheme for the first 5 frames of the video sequences in Table 2 at different resolutions

| QP | Frame # | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Bosphorus | 92,329 | 92,470 | 92,510 | 92,553 | 92,624 |
| Jockey | 12,764 | 12,762 | 12,759 | 12,766 | 12,956 |
| FourPeople | 7431 | 7439 | 7446 | 7434 | 7435 |
| Mobcal | 6624 | 6644 | 6643 | 6641 | 6643 |
| Forest | 1494 | 1496 | 1499 | 1502 | 1506 |

the horizontal, vertical and diagonal directions. It is clear from Fig. 11 and Table 10 that there is the low correlation between the pixels in the encrypted frame and the original frame in all directions.

### 5.3 Encryption quality analysis

The video encryption quantity (EQ) estimates the average difference between the occurrence of each pixel gray level in encrypted and original video frames [30].

The video encryption quantity (EQ) is computed using the following equation:

$$\text{Encryption Quality} = \frac{\sum_{L=0}^{255} \left| H_L(F') - H_L(F) \right|}{256} \tag{3}$$

where $F'$ is encrypted video frame, $F$ is original video frame and $H_L$ is the occurrence of each gray level $L$ for encrypted/original video frame. Table 11 shows the encryption quality of the proposed CLM-based HEVC SE scheme for the first 5 encrypted frames of the FourPepole video sequence at different QP values and illustrates that the encryption quality increases with QP. Also, Table 12 shows the encryption quality of the proposed CLM-based HEVC SE scheme for the first 5 encrypted frames of the video sequences in Table 2 at different resolutions values and illustrates that the encryption quality increases with QP.

### 5.4 Key sensitivity analysis

The proposed CLM-based HEVC SE scheme should have the high key sensitivity that means the encrypted video cannot be decrypted correctly with tiny changes in the secret key that used in the encryption process. The key sensitivity of

**(a)** Original image

**(b)** Encrypted image with key "18446744073709551610"

**(c)** Encrypted image with key "08446744073709551610"

**Fig. 12** Key sensitivity analysis of the proposed CLM-based HEVC SE scheme

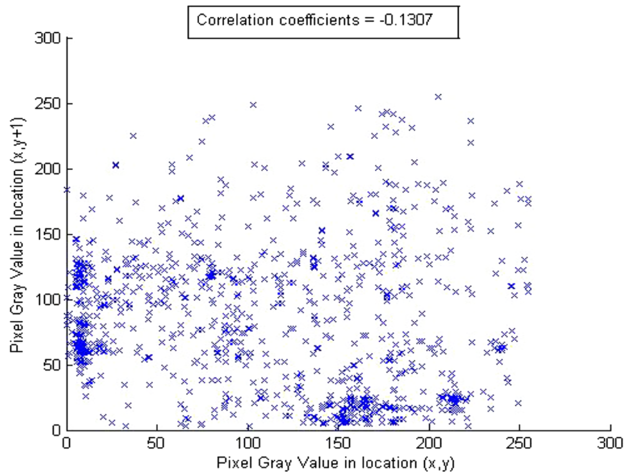



**Fig. 13** Correlation coefficients between the two different encrypted video frames obtained in Fig. 12b, c using the proposed CLM-based HEVC SE scheme

the proposed CLM-based HEVC SE scheme guarantees the robustness against brute-force attack.

For testing the key sensitivity of the proposed CLM-based HEVC SE scheme, the following steps are performed:

a) An original video frame #10 from the FourPeople video sequence in Fig. 12a is encrypted by the proposed CLM-based HEVC SE scheme using the secret key "18446744073709551610" and resulted in the encrypted video frame as shown in Fig. 12.

**Table 13** Correlation coefficients among the original and the encrypted frame #10 of the video sequences in Table 2 using the proposed CLM-based HEVC SE scheme

| | Bosphorus | Jockey | FourPeople | Mobcal | Forest |
|---|---|---|---|---|---|
| EDR | 0.89 | 0.93 | 0.91 | 0.82 | 0.87 |

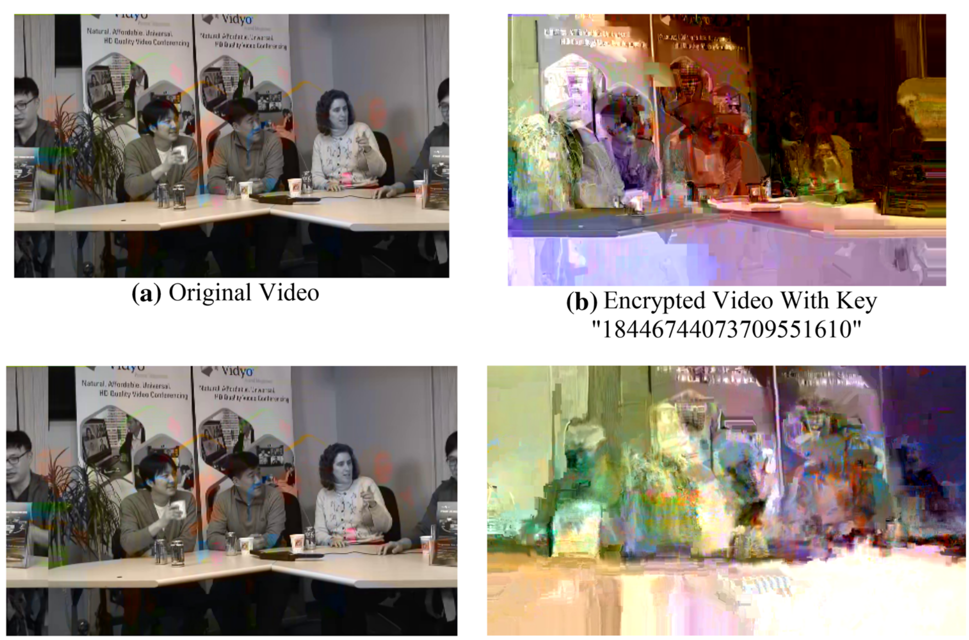
b) An original video frame #10 from the FourPeople video sequence in Fig. 12a is encrypted by the proposed CLM-based HEVC SE scheme using different secret key "08446744073709551610" (the most significant bit is changed in the secret key) and resulted in the encrypted frame video as shown in Fig. 12c.

Figure 12 shows that there are different versions of the encrypted video frames that generated with different encryption keys using the proposed CLM-based HEVC SE scheme. To ensure the difference between the two encrypted video frames in Fig. 12b, c, the correlation between the corresponding pixels at the same position in the two encrypted video frames is calculated and shown in Fig. 13.

Figure 13 shows that there is a small correlation between the two encrypted video frames although these have been encrypted using two similar secret keys with only one change the most significant bit. So the proposed CLM-based HEVC SE scheme ensures high sensitivity with respect to slightly change in the secret key.

Moreover, in Fig. 14, we have shown the results of some attempts to decrypt an encrypted video with slightly different secret keys than the one used for the encryption of

**Fig. 14** The decrypted video effect on the key sensitive for the CLM-based HEVC SE scheme




**(a)** Original Video

**(b)** Encrypted Video With Key "18446744073709551610"

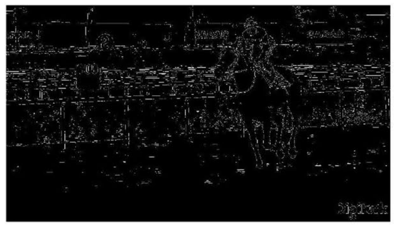
**(c)** Decrypted image with key "18446744073709551610"

**(d)** Decrypted image with key "08446744073709551610"

**Fig. 15** Laplacian of Gaussian edge detection for the original and encrypted video frame #10 for the video sequences in Table 2

**(a)** Original Bosphorus with resolution 3840x2160 video sequence

**(b)** Encrypted Bosphorus with resolution 3840x2160 video sequence

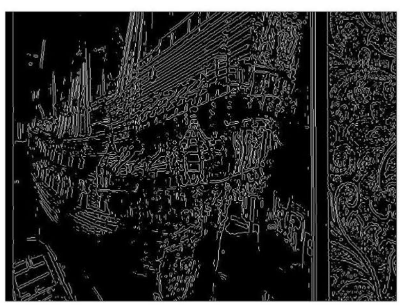


**(c)** Original Jockey with resolution 1920x1080 video sequence

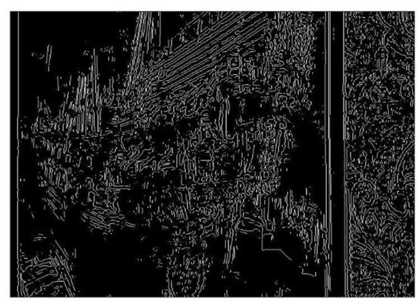
**(d)** Encrypted Jockey with resolution 1920x1080 video sequence

**(e)** Original FourePeople with resolution 1280x720 video sequence

**(f)** Encrypted FourePeople with resolution 1280x720 video sequence



**(g)** Original Mobcal with resolution 720x576 video sequence



**(h)** Encrypted Mobcal with resolution 720x576 video sequence

**(i)** Original Forest with resolution 320x240 video sequence

**(j)** Encrypted Forest with resolution 320x240 video sequence

**Table 14** Correlation coefficients among the original and the encrypted frame #10 of the Four People video sequences using the proposed CLM-based HEVC SE scheme

| | Bosphorus | Jockey | FourPeople | Mobcal | Forest |
|---|---|---|---|---|---|
| H(m) | 7.332 | 7.460 | 7.563 | 7.471 | 7.192 |

the original image. Particularly, in Fig. 14a, b respectively, the original image and the encrypted image produced using the secret key "18446744073709551610" (in ASCII) are shown whereas in Fig. 14c, d respectively, the videos after the decryption of the encrypted video (shown in Fig. 14b with the secret keys "18446744073709551610" (in ASCII) and "08446744073709551610" (in ASCII). It is clear that the decryption with a slightly different key fails completely and hence the proposed CLM-based HEVC SE is highly key sensitive.

### 5.5 Edges detection protection

The proposed CLM-based HEVC SE scheme should protect the frames edges information from the attacks. The visual distortion for the encrypted video frame using the proposed CLM-based HEVC SE scheme can be measured by the edge differential ratio (EDR) as [31]:

$$\mathrm{EDR} = \frac{\sum_{i,j=1}^{N} \left| H(i,j) - \overline{H}(i,j) \right|}{\sum_{i,j=1}^{N} \left| H(i,j) + \overline{H}(i,j) \right|} \tag{4}$$

where $H(i,j)$, $\overline{H}(i,j)$ the pixel values in the detected edges within the binary version for the original and encrypted video frames. Table 13 shows that the EDR between the original and the encrypted video frame #10 from video sequences in Table 2 is closed to 1 that ensures that the original and encrypted video frames are different. Figure 15 shows the Laplacian of Gaussian edge detection for the original and encrypted video frames.

### 5.6 Information entropy analysis

The Information entropy is the probability of occurrence for each symbol in the video frame [32].

The entropy can be defied as:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad \text{bits,} \tag{5}$$

where $H(m)$ denotes the entropy of $m$ and $p(m_i)$ denotes the probability of occurrence of symbol $m_i$ in $m$.

Because the pixel is 8 bits in the gray scale frame, the value of the entropy should be 8 for the truly random frame.

Table 14 shows that the probability of the occurrence of each encrypted block in the encrypted video frame #10 by the proposed CLM-based HEVC SE scheme is computed according to Eq. 5 and is near to the theoretical value 8. This means the proposed CLM-based HEVC SE scheme is secure and robust against the entropy attack.

## 6 Conclusion

This paper presents an overview of the HEVC video coding structure and introduces the CABAC entropy coding block diagram. It also presents an efficient CLM-based HEVC SE scheme that used the low computational complexity CLM to encrypt the DCT coefficients sign bits and the MVD sign bits. The CLM-based HEVC SE encrypts these syntax elements because any modification of the sign bin (one bit) has no effect on the HEVC video format compliance and the HEVC bit rate. A comparison between the proposed CLM-based HEVC SE scheme and the Glenn HEVC SE is presented. The experimental results showed that the proposed CLM-based HEVC SE scheme saves the average frame encoding time from 4 s for the low resolution video (320 × 240) to 17 s for the high resolution video (3840 × 2160) with remaining of the near visual distortion of the encrypted video stream by Glenn HEVC SE as seen with slight difference PSNR and SSIM values. The security analysis of the proposed CLM-based HEVC SE scheme is inspected using security performance indicators like key space analysis, encryption quality analysis, statistical analysis and sensitivity analysis. The security analysis experimental results ensure and prove the robustness and superiority of the proposed CLM-based HEVC SE scheme with respect to most attacks.

## References


1. Wang, M., Ngan, K.N., Xu, L.: Efficient H.264/AVC video coding with adaptive transforms. IEEE Trans. Multimedia **16**(4), 933–946 (2014)
2. Souza, D., Ilic, A., Roma, N., Sousa, L.: GHEVC: an efficient HEVC decoder for graphics processing units. IEEE Trans. Multimedia **19**(3), 459–474 (2017)
3. Asghar, M., Kousar, R., Majid, H., Fleury, M.: Transparent encryption with scalable video communication: lower-latency, CABAC-based schemes. J. Vis. Commun. Image Represent **45**(1), 122–136 (2017)
4. Grois, D., Marpea, D., Nguyena, T., Hadarb, O.: Performance comparison of H.265/MPEG-HEVC, VP9, and H.264/MPEG-AVC encoders. Proceedings of SPIE 9217, Applications of Digital Image Processing XXXVII (2014)

5. Misra, K., Segall, A., Horowitz, M., Shilin, X., Fuldseth, A., Zhou, M.: An overview of tiles in HEVC. IEEE J. Select. Top. Signal Process. **7**(6), 969–977 (2013)
6. Richardson, I.E.: The H.264 advanced video compression standard. Wiley Publishing, Hoboken (2010)
7. Gao, M., Fan, X., Zhao, D., Gao, W.: An enhanced entropy coding scheme for HEVC. Signal Process. Image Commun. **44**(1), 108–123 (2016)
8. Vanne, J., Viitanen, M., Hamalainen, T.: Efficient mode decision schemes for HEVC inter prediction. IEEE Trans. Circuits Syst. Video Technol. **24**(9), 1579–1593 (2014)
9. Ma, X., Zeng, W., Yang, L., Zou, D., Jin, H.: Lossless ROI privacy protection of H.264/AVC compressed surveillance videos. IEEE Transac. Emerg. Top. Comput. **4**(3), 349–363 (2016)
10. Liu, F., Koenig, H.: A survey of video encryption algorithms. J. Comput. Security **19**(1), 3–15 (2010)
11. Tew, Y., Wong, K.S.: An overview of information hiding in H.264/AVC compressed video. IEEE Trans. Circuits Syst. Video Technol. **24**(2), 305–319 (2014)
12. Sze, V., Budagavi, M., Sullivan, G.J.: High Efficiency Video Coding (HEVC). International Publishing Switzerland, Springer (2014)
13. Lin, J.L., Chen, Y.W., Huang, Y.W., Lei, S.M.: Motion vector coding in the HEVC standard. IEEE J. Select. Top. Signal Process. **7**(6), 957–968 (2013)
14. Bossen, F., Bross, B., Suhring, K., Flynn, D.: HEVC complexity and implementation analysis. IEEE Trans. Circuits Syst. Video Technol. **22**(12), 1685–1696 (2012)
15. Hofbauer, H., Unterweger, A., Uhl, A,: Transparent encryption for HEVC using bit-stream-based selective coefficient sign encryption. Proc. IEEE Int. Conf. Acoust Speech Signal Process. (ICASSP), May 2014, pp. 1986–1990
16. Tew, Y., Minemura, K., Wong, K.: HEVC selective encryption using transform skip signal and sign bin. Proc. APSIPA Annual Summit Conf. 2015, December 2015, pp. 963–970
17. Shahid, Z., Puech, W.: Visual protection of HEVC video by selective encryption of CABAC binstrings. IEEE Trans. Multimedia **16**(1), 24–36 (2014)
18. NIST: Advanced encryption standard (AES), pp. 197. FIPS Publication (2001)
19. Van Wallendael, G., Boho, A., De Cock, J., Munteanu, A., Van de Walle, R.: Encryption for high efficiency video coding with video adaptation capabilities. IEEE Trans. Consum. Electron. **59**(3), 634–642 (2013)
20. http://www.physics.sfsu.edu/~mstevens/chaos/chaos.htm. Accessed 1 June 2016
21. Hamidouche, W., Farajallah, M., Ould-Sidaty, N., El Assad, S., Déforges, O.: Real-time selective video encryption based on the chaos system in scalable HEVC extension. Signal Process. Image Commun. **58**(1), 73–86 (2017)
22. Goswami, K., Lee, J., Kim, B.: Fast Algorithm For The High Efficiency Video Coding (HEVC) encoder using texture analysis. Inf. Sci. **364**(1), 72–90 (2016)
23. Fraunhofer Heinrich Hertz Institute: High Efficiency Video Coding: HEVC software repository. 2015. https://hevc.hhi.fraunhofer.de
24. https://media.xiph.org/. Accessed 1 June 2016
25. http://ultravideo.cs.tut.fi/#testsequences. Accessed 1 June 2016
26. MSU Graphics and Media Lab, Video Group, MSU codecs. http://www.compression.ru/video/. Accessed 1 June 2016
27. Bjontegaard, G.: Calculation of average PSNR differences between RD-curves. Document VCEG-M33 of ITU-T Video Coding Experts Group (VCEG); Apr. 2001
28. Osama, S., Allah, F., Afifi, A.: Optical color image cryptosystem using chaotic baker mapping based-double random phase encoding. Int. J. Opt. Quant. Electron. **49**(3), 1–28 (2017)
29. Ahmad, J., Ahmed, F.: Efficiency analysis and security evaluation of image encryption schemes. Int. J. Video Image Process. Netw. Security **12**(04), 18–31 (2012)
30. Kaur, A., Kaur, L., Gupta, S.: Image recognition using coefficient of correlation and structural SIMilarity index in uncontrolled environment. Int. J. Comput. Appl. **59**(5), 32–39 (2012)
31. Jolfaei, A., Mirghadri, A.: A new approach to measure quality of image encryption. Int. J. Comput. Netw. Security **2**(8), 38–43 (2010)
32. http://www.mathworks.com/help/images/ref/edge.html. Accessed 1 June 2016