Real-Time Selective Video Encryption based on the Chaos System in Scalable HEVC Extension

Wassim Hamidouche, Mousa Farajallah, Naty Ould-Sidaty, Safwan El Assad, Olivier Déforges

Real-Time Selective Video Encryption based on the Chaos System in Scalable HEVC Extension

Wassim Hamidouche[a], Mousa Farajallah[b,], Naty Sidaty[a], Safwan El Assad[c], Olivier Deforges[a]

[a]*IETR/INSA of Rennes, Rennes, France*
[b]*College of Information Technology and Computer Engineering - Palestine Polytechnic University- Hebron - Palestine*
[c]*IETR Ecole polytech- University of Nantes-Rue Christian Pauc-44306 Nantes cedex 3-France*

Abstract

In this paper we propose a real-time selective video encryption solution in the scalable extension of High Efficiency Video Coding (HEVC) standard, referred to as SHVC. The proposed scheme encrypts a set of sensitive SHVC parameters with a minimum delay and complexity overheads. The encryption process is performed at the CABAC binstring level and fulfils both constant bitrate and format compliant video encryption requirements. In addition, it preserves all SHVC functionalities, including bitstream extraction for mid-network adaptation and error resilience.
We compare the performance of three selective SHVC encryption schemes: the first scheme encrypts only the lowest SHVC layer, the second encrypts all layers and the last scheme encrypts only the highest layer. The performance of the proposed schemes is assessed over different video encryption criteria, at different scalability configurations and various High Definition (HD) video sequences. Experimental results showed that encrypt only the lowest layer or all layers enables a high security level, while encrypting only the highest layer leads to a perceptual encryption solution, by slightly decreasing the highest layer quality. Moreover, the processing complexity of the proposed solution is assessed in the context of a real-time SHVC decoder. The complexity overhead remains low and does not exceed 6% of the real-time decoding of SHVC video sequences.

Keywords: Selective video encryption, joint crypto-compression solution, HEVC, scalable HEVC, chaotic generator, perceptual security, subjective quality assessment.

1. Introduction

The new video coding standard High Efficiency Video Coding (HEVC) [1], finalized in January 2013 [2], enables up to 50% gain in terms of subjective video quality with respect to the H.264/AVC (Advanced Video Coding) high profile [3]. The scalable extension of HEVC (SHVC), adopted in October 2014, under two profiles (Scalable Main and Scalable Main 10), defines tools to enable fidelity (SNR), spatial, bit depth and color gamut scalability [4, 5]. The SHVC extension takes advantage of the spatial correlation between different video representations in order to improve the rate distortion coding performance by around 15%-30% [6] compared to the simulcast coding configuration. The SHVC bitstream is granular which enables the end-user to decode a set of layers that reach the requested video quality and fulfil user requirements in terms of bandwidth, display, computing and energy capabilities. In the upcoming years, the HEVC standard and its scalable extension SHVC are expected to be progressively deployed by the industry in order to offer new services with the perspective of replacing previous video compression standards, such as AVC [7] and its scalable extension SVC (Scalable Video Coding) [8]. On the other hand, security and confidentiality of multimedia contents have become a challenging research topic. They have been widely investigated in the last

decade by using standard cryptography [9–11], and chaos-based cryptography [12, 13]. Indeed, a variety of chaos-based crypto-systems have been investigated and most of them are based on the structure of Fridrich, which is based on the traditional confusion-diffusion architecture proposed by Shannon. Compared with traditional cryptography, the chaos-based cryptography is more flexible, more modular and easier to implement, which makes it more suitable for large-scale data encryption, such as images and video sequences.

2. Context and Motivations

In this section we give a brief description of both SHVC extension and chaos-based generator followed by the motivations of this work.

2.1. SHVC Extension

The SHVC extension has been defined to provide spatial, fidelity, bit depth and color scalability with a simple and efficient coding architecture [4, 5]. All technologies defined in the HEVC standard are used in SHVC including quadtree-based block partitioning, large transform and prediction blocks, accurate intra/inter predictions, in-loop sample adaptive offset filter and highly adaptive entropy coding [1]. Moreover, the HEVC standard uses the concept of dQP to adapt the QP value at the coding unit level for visual quality optimization and rate control. The SHVC

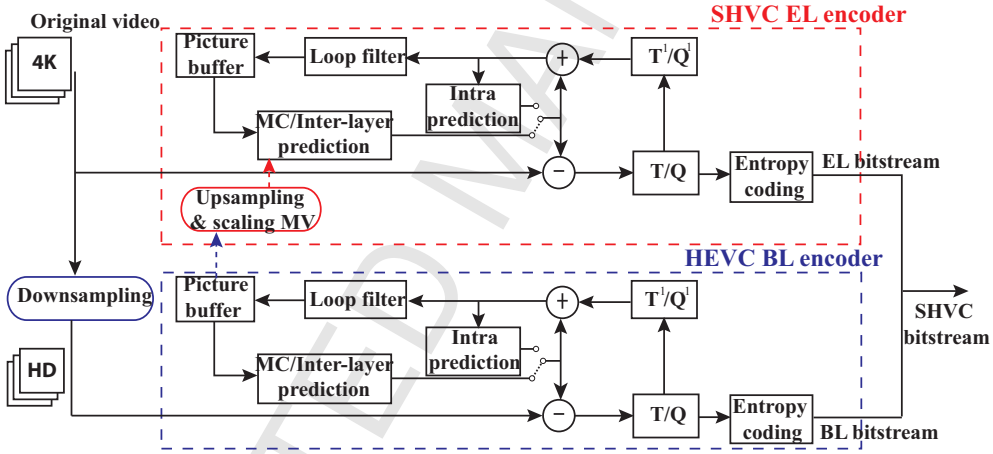


Figure 1. Block diagram of the SHVC encoder, where encoding two scalability layers are encoder [5]

extension adopts an inter-layer prediction to take advantage of spatial correlation and improve the rate-distortion performance compared to independent encoding of the layers. The SHVC encoder consists of L HEVC encoders, one encoder to encode each layer with L the number of layers: one Base Layer (BL) and $L-1$ Enhancement Layers (EL). In the case of spatial scalability, the BL HEVC encoder encodes a down-sampled version of the original video and feeds the first EL encoder with the decoded picture and its MVs. The enhancement layer encoder encodes a higher resolution video with using the decoded picture from the lower layer as an additional reference picture. The inter-layer reference picture is up-sampled and its MVs up-scaled to match with the resolution of the EL layer being decoded. Figure 1 shows an example of the SHVC encoder encoding two layers in a spatial scalability configuration. In the case of SNR scalability, the encoding process remains unchanged except that the picture used for inter-layer prediction is used without being up-sampled and its MVs up-scaled. The CABAC engine defined in HEVC remains unchanged in SHVC. The SHVC encoder has one independent CABAC engine per layer (see Figure 1). The CABAC engine at each layer consists of three main functions: binarization, context modeling and arithmetic coding [14]. First, the binarization step converts syntax elements to binary symbols (bin). Second, the context modeling updates the probabilities of bins, and finally the arithmetic coding compresses the bins into bits according to the estimated probabilities. Five binarization methods are used in HEVC, namely Unary (U), Truncated Unary (TU), Fixed Length (FL), Truncated

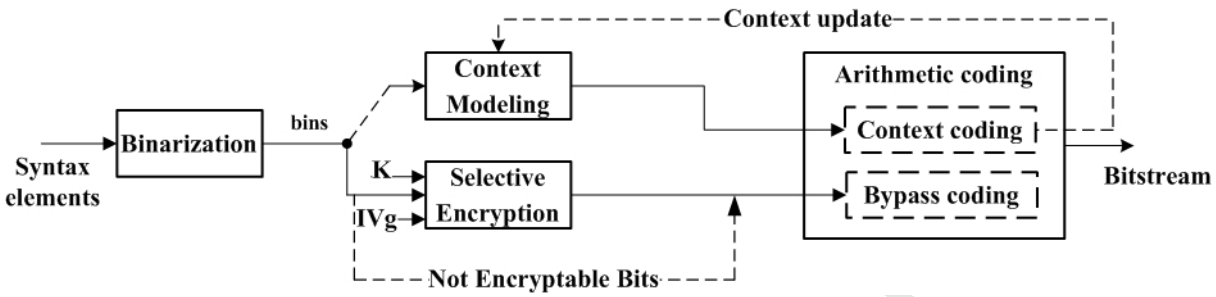


Figure 2. Three main functions in the CABAC

Rice Code with context p (TRp) and Kth Order Exp-Golomb Code(EGk). The U code represents an unsigned integer Y with a binstring of length $Y + 1$ composed of Y 1-bins followed by one 0-bin. The TU code is defined with the largest possible value of the syntax element $cMax$ ($0 \leq Y \leq cMax$). When the syntax element value $Y < cMax$, the TU is equivalent to U code, otherwise Y is represented by a binstring of $cMax$ 1-bins. The FL code represents a syntax element Y with its binary representation of length $\lceil \log_2(cMax + 1) \rceil$ with $\lceil x \rceil$ is smallest integer greater than or equal to x. The TRp code is a concatenation of a quotient $q = \lfloor Y/2^p \rfloor$ (with $\lfloor x \rfloor$ being the largest integer less than or equal to x) and a remainder $r = Y - q2^p$. The quotient q is first represented by the TU code as a prefix concatenated with a suffix r represented by the FL code of length p. The EGk code is also a concatenation of prefix and suffix. The prefix part of the EGk code is the U representation of $l(Y) = \lfloor \log_2(\frac{Y}{2^k} + 1) \rfloor$. The suffix part is the FL code of $Y + 2^k(1 - 2^{l(Y)})$ with $cMax = k + l(Y)$.

The arithmetic coder can be performed either by an estimated probability of a syntax element (context coded) or by considering equal probability of 0.5 (bypass coded). The three main functions of the CABAC at each SHVC layer are illustrated in Figure 2. The CABAC engine at each SHVC layer is initialized at the start of each frame and then the frame of each layer is encapsulated in an independent slice.

2.2. Robust and Fast Chaotic Generator

The performance in terms of robustness and speed of any chaos-based cryptosystem depends greatly on the used chaotic generator. Moreover, the generated sequences must exhibit good cryptographic properties. We use an enhanced version (fast and secure) of our chaotic generator (without delays) published in El Assad and Noura patent [15]. It should be noted that the proposed joint selective encryption can be used with any secure and fast classical or chaos-based generator to obtain similar results [16, 17].

Indeed, to the best of our knowledge, practically, most chaotic generators of the literature, in which they combine two chaotic maps are robust against statistical and known attacks. The main difference between them is how is the degree of robustness (described until now by the complexity of their structures) and their computational performance.

As illustrated in Figure 3, the chaotic generator consists of two discrete chaotic maps, namely the Skew Tent Map (STM), given by equation (6) and the Piece-wise Linear Chaotic Map (PWLCM), specified by equation (7), where P_1 and P_2 are the control parameters which range from 1 to $2^N - 1$ and $2^{N-1} - 1$, respectively, with $N = 32$ is the used finite precision of the calculus. n represents the discrete time variable and $X_1[n]$ and $X_2[n]$ vary between 1 and $2^N - 1$. U_p and U_s each of 32 bits length come from an Initial Vector (IVg) produced by a pseudo random generator and are used to set $X_1[n-1]$ and $X_2[n-1]$, respectively at $n = 0$. Each chaotic map includes a technique of perturbation based on a Linear Feedback Shift Register (LFSR). The outputs of the two disturbed maps are added or xored depending on whether the two values are equal or not, respectively.

The used chaos-based generator is described in the following four steps:

1. First, the secret key K, composed of 6 initials parameters, is used as an input of the chaotic generator. These initial parameters are U_p, U_s, $X_1[0]$, $X_2[0]$, P_1, P_2, Q_1 and Q_2. P_1 , P_2 are control parameters in the range $[1, 2^N - 1]$ and $[1, 2^{N-1} - 1]$ respectively. Q_1 and Q_2 are perturbing signals produced by the linear feedback shift registers (LFSRs).

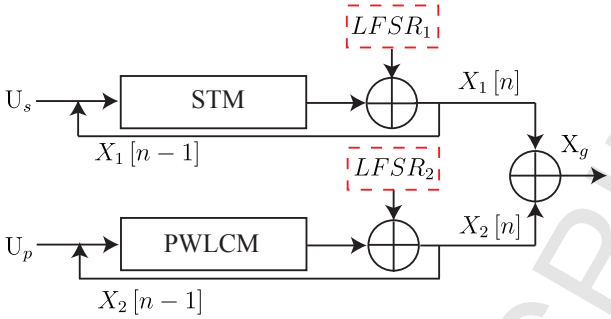


Figure 3. Block diagram of the used chaotic sequence generator

2. The Us and Up values are extracted from the 64-bit IVg, $U_s = lsb(IVg)$ and $U_p = msb(IVg)$. Notice that Us and Up are used only in the first iteration of random values creations. This will increase the complexity of the system and prevents the recurrent random samples productions.
3. The creation of first random sample value is performed as in Equations (1) and (2).

$$X_1[1] = STM\{mod[U_s + X_1[0], 2^N], P1\} \oplus Q_1 \tag{1}$$

$$X_2[1] = PWLCM\{mod[U_p + X_2[0], 2^N], P2\} \oplus Q_2 \tag{2}$$

4. The generation process of the remainder random sequences is done in the same manner as in previous without including the U_s and U_p values (see Equations (3) and (4))

$$X_1[n] = STM\{mod[(X_1[n-1], 2^N], P_1\} \oplus Q_1 \tag{3}$$

$$X_2[n] = PWLCM\{mod[X_2[n-1], 2^N], P_2\} \oplus Q_2 \tag{4}$$

5. The final random value $X_g(n)$ is produced by xoring the $X_1(n)$ and $X_2(n)$ as follows:

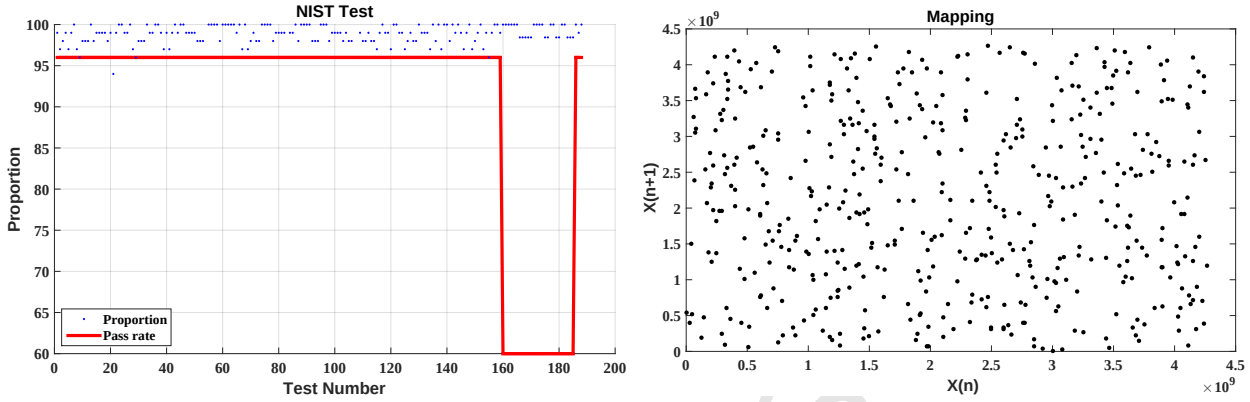
$$X_g[n] = X_1[n] \oplus X_2[n] \tag{5}$$

The used chaotic generator illustrated in Figure 3 enables the following features:

1. Cryptographically secure: First, as we can see in Figure 4(a), the produced sequences have passed the 188 statistical tests defined by the National Institute of Standards and Technology (NIST) [18]. We have performed the NIST test (a battery of 188 tests) on 100 sequences, each contacting one million bits. In Figure 4 (a), we show the obtained proportion value of sequences passing a test, versus the index of the test (from 1 to 188). As we can see, the produced sequence have passed the 188 tests :
   Second, the mapping of Figure 4(b) (curve [X(n+1), X(n)]) shows that the generated sequences are unpredictable. Moreover, the size of the secret key is equal to 169 bits and the length of the generated trajectories (orbits) are very long.
2. Fast encryption: the generator can reach a bitrate of 1180 Mbit/s on Core-i5-4300M CPU running at 2.6 GHz and Ubuntu 14.04, 64-bit operating system.
3. Strong non-linearity compared to the main stream ciphers of the literature (eStream) [19]. As shown in Figure 4(b), the trajectory of the proposed chaos-based generator looks as messy. This means that an attacker can not retrieve any useful information from the output and thus a cipher text attack is infeasible.

The proposed chaotic generator produces completely different output sequences when it is initialized with a different IVg and the same secret key.

$$X_1[n] = \begin{cases} \left\lfloor \frac{2^N \times X_1[n-1]}{P_1} \right\rfloor & \text{if } 0 < X_1[n-1] < P_1 \\ 2^N - 1 & \text{if } X_1[n-1] = P_1 \\ \left\lfloor \frac{2^N \times (2^N - X_1[n-1])}{2^N - P_1} \right\rfloor & \text{if } P_1 < X_1[n-1] < 2^N \end{cases} \tag{6}$$



(a) NIST tests (b) Mapping

Figure 4. Robustness and specification of the proposed chaos-based generator

$$X_2[n] = \begin{cases} \left\lfloor \frac{2^N \times X_2[n-1]}{P_2} \right\rfloor & \text{if } 0 < X_2[n-1] < P_2 \\ \left\lfloor \frac{2^N \times (X_2[n-1]-P_2)}{2^{N-1}-P_2} \right\rfloor & \text{if } P_2 < X_2[n-1] < 2^{N-1} \\ \left\lfloor \frac{2^N \times (2^N - X_2[n-1]-P_2)}{2^{N-1}-P_2} \right\rfloor & \text{if } 2^{N-1} \leq X_2[n-1] < 2^N - P_2 \\ \left\lfloor \frac{2^N \times (2^N - X_2[n-1])}{P_2} \right\rfloor & \text{if } 2^N - P_2 \leq X_2[n-1] < 2^N - 1 \\ 2^N - 1 & \text{if } 2^N - 1 \leq X_2[n-1] \end{cases} \tag{7}$$

2.3. Related Work

The most straightforward method to secure video contents is to encrypt the whole file by using standard encryption algorithms such as Advanced Encryption Standard (AES) [20]. This method called Naive Encryption Algorithm (NEA) treats the video bitstream as text data without considering the structure of the compressed video [10]. However, NEA suffers from several drawbacks. First, the encryption/decryption process becomes time and energy consuming (computationally costly) for large-scale data, especially video at high resolution and high bitrate. Therefore, NEA may not be suitable for real-time video streaming applications, which have rigid restrictions on delay and energy on mobile devices. Second, the NEA prevents untrusted middle-box[1] in the network from performing post-processing operations on the encrypted video bitstream such as transcoding and watermarking. Third, the NEA solution applied on the scalable video bitstream does not preserve the bitstream features such as sub-stream extraction for network adaptation and error resilience [11].

Selective video encryption has emerged as an effective alternative to NEA [11, 21, 22]. Selective video encryption considers the coding structure of the video bitstream and encrypts only the most sensitive information in the video bitstream, in the following, some research are discussed:

- Authors in [21] studied the impact, in terms of both video quality and bitrate, of encrypting different HEVC parameters (ie. syntax elements). The encryption of a set of parameters including Transform Coefficients (TCs), TC sign, Motion Vector (MV) difference, MV difference sign and delta Quantization Parameter (dQP) enables a high degradation of the video quality with a slight increase in bitrate.

- Shahid et al. [22] proposed a selective encryption solution for the HEVC video at a constant bitrate. The proposed solution encrypts a set of HEVC syntax elements including TCs, TC sign, MVs difference and MV sign. The encryption is performed at the level of the Context-Adaptive Binary Arithmetic Coding (CABAC) binstring (i.e., after the binarization process of the CABAC). The binarization of the TCs is performed in the

[1] Untrusted middle-box refers to the middle-box that does not hold the secret key used to encrypt the video.

HEVC draft 6 [2] through a combination of Truncated Rice code with an adaptive context p (TRp) and kth-order Exp-Golomb (EGk) code with $k = 0$ (EG0).

- Authors in [22] proposed an algorithm to encrypt the suffix of only TCs that do not impact the adaptive parameter p after encryption. Thus, this algorithm fulfills constant bitrate and format compliant encryption requirements. Moreover, the AES algorithm is used, in Cipher Feedback (CFB) mode, to encrypt the HEVC syntax elements. Therefore, the authors in [22] proposed an algorithm to transform non-dyadic Encryption Space (ES) to dyadic a ES to prepare the plaintext for AES-CFB encryption, dyadic space represented by a number of bits and should be multiple of 2. However, in some cases, the last bit suffix can not be encrypted (non-dyadic ES).

- The encryption of Region of Interest (ROI) has been investigated by the authors in [23] based on the tiles repartition in HEVC [1] through both selective and naive encryption of the tiles within the ROI.

- Authors in [24] proposed an encryption framework that offers full protection to the SVC bitstream while providing necessary transparency to perform secure mid-network adaptation. The whole SVC bitstream is encrypted using the AES encryption algorithm in block cipher mode, except the syntax elements containing information required to perform the adaptation. This clear (non-encrypted) information is also used to generate the Initial Vector (IV) of the AES encryption algorithm.

- In [25] authors showed the performance of a selective[3] encryption solution of the SVC bitstream with respect to the conventional standardized encryption solution: Secure Real-time Transport Protocol (SRTP). The selective encryption solution enables a significant gain in terms of both processing complexity and end-to-end delay: since no encryption/decryption is required for network adaptation and only partial information is encrypted/decrypted by the end-users. However, the selective encryption solution introduces a slight bitrate overhead mainly related to the transmission of the IVs required to initialize the AES algorithm to cope with issues related to error and synchronization.

2.4. Motivations and Contributions

In this paper we investigate a real-time selective encryption for the SHVC coded video. Our main motivation is to design an encryption solution with the four following features: a) format compliant, b) constant bitrate, c) secure with low delay and low complexity, d) maintain SHVC scalability features, including granularity with the capability of accessing to different quality representations of the video content.

In this paper we propose an encryption solution that encrypts, in format compliant and constant bitrate, a set of SHVC parameters including TCs, TC sign, MV difference, MV difference sign and dQP sign. The encryption process is performed at the level of the CABAC binstring. We also propose a new algorithmic solution that determines the encryptable bins after the binarization of the TCs in TRp and EG-k ($k = p + 1$) codes while satisfying constant bitrate and format compliant requirements. The proposed encryption solution uses a chaotic encryption system [15, 26]. Chaotic-based encryption systems are more flexible and modular, and thus are suitable for large-scale data encryption [27]. Moreover, the chaotic generator used as stream cipher enables the encryption and decryption the SHVC syntax elements on the fly, without additional delay and memory usage.
We investigate three SHVC encryption schemes. The first scheme encrypts only the lowest layer (SHVC-BL), the second scheme encrypts all SHVC layers (SHVC-All) while the third scheme encrypts only the highest SHVC layer (SHVC-EL). The performance of the proposed schemes has been assessed in different scalability configurations: fidelity (SNR) and spatial at two ratios 2x and 1.5x. The first scheme, encrypting only the lowest layer, enables a high security level on all layers. In fact, the inter-layer predictions, used in the SHVC extension, propagate the encryption from the encrypted base layer (BL) into all Enhancement Layers (EL). Moreover, this scheme encrypts on average less than 8% of the whole SHVC bitstream. This low encryption space is proportional to the resolution of the encrypted BL which is lower than the resolution of the EL especially in spatial scalability. The scheme encrypting

[2] The binarization of the residual has been changed in the HEVC standard.
[3] Selective encryption scheme refers in [25] to the encryption of either only the base layer or encrypting only Intra coded pictures in both layers.

only the highest layer enables a perceptual (transparent) encryption where the base layer remains clear and the quality of the EL is decreased below the quality of the BL. Regarding computational complexity, the proposed schemes were assessed in the context of a real-time SHVC decoder. The decryption of the BL in the first scheme (SE-SHVC-BL) introduces on average less than 3% additional complexity, while decrypting all layers introduces less than 6% of the whole decoding time of HD resolution video. We also show that the complexity overhead remains similar when using the AES encryption algorithm in stream cipher mode. Table 1 compares the SE-SHVC-BL and SE-SHVC-EL encryption schemes with the state of the art on different video encryption criteria. The SE-SHVC-BL and SE-SHVC-EL enable secured and perceptual video encryption, respectively; and can be applied on different SHVC scalability configurations: temporal, spatial, fidelity, bit depth and color gamut. With respect to transcoding capability, the SE-HEVC-BL scheme is robust to transcoding of all ELs while the SE-HEVC-EL encryption scheme is robust to BL transcoding. In fact, the ELs can be transcoded since they are not encrypted. On the other hand, SE-HEVC-EL is robust to BL transcoding since the BL is not encrypted, the transcoding can be performed on the BL. It should be noted that when the BL is transcoded it can not be used to decode the enhancement layer without drift errors. Finally, the SE-HEVC-EL encryption scheme can also be applied to the single layer HEVC standard corresponding to simulcast and single layer HEVC configurations.
The rest of this paper is organized as follows. The proposed selective SHVC encryption schemes are described in section 3. The performance of the proposed encryption schemes is assessed and discussed in section 4. Finally, section 5 concludes this paper.

3. Proposed SHVC Selective Encryption Schemes

The proposed solution encrypts the SHVC bitstream in three different configurations (here known as schemes). The first scheme encrypts only the bitstream of the BL (SE-SHVC-BL). This scheme will also affect the quality of the ELs since the decoded BL picture and its MVs are used as a reference for the inter-layer predictions of the EL encoders. The second scheme (SE-SHVC-All) encrypts the bitstream of all SHVC layers. Therefore, these two schemes will achieve a high security level of encryption since in addition to the encryption of the BL, all ELs are implicitly or explicitly encrypted in schemes SE-SHVC-BL and SE-SHVC-All, respectively. The third scheme (SE-SHVC-EL) encrypts only the highest EL. Thus, the lower quality of the video remains clear and only end-users holding the secret key can visual a higher quality of the video. The encryption solution encrypting each layer is similar and is described in the next sections.

3.1. Encryption Parameters

The proposed encryption solution is SHVC format compliant and does not affect the compression ratio of the SHVC encoder. Therefore, only syntax elements binarized in FL code and then bypass coded can be safely encrypted. The selective encryption is performed after the binarization process in the CABAC as illustrated in Figure 2.
The CABAC uses the EG1 code for the binarization of MV differences the binarized values are then bypassed. Thus, the suffix part of MV difference is encrypted without impacting the compression ratio or violate the format compliance requirement, regarding the compression ratio, in the bypass mode each bit have the same probability which means flipping zero to one does not affect the compression ratio. Regarding the format compliance remember that the suffix of the EG1 is binarized using FL code which means the flipping bits will be a valid representation of the suffix part of the EG1. As an example, assume that on of the MV difference is 7, then using EG1, the prefix part is 110 and the suffix part is 001 while the whole code-word is 110001, now the prefix part is the U representation of $l(7)$ and one bit change will crash the decoder, while the suffix part is given by a FL code, as a result flipping 001 to one of the 000,001,010,011,100,101,110,111 values is a valid representation of the FL code and so is a format compliant encryption.

The sign of MV difference is also encrypted since it is binarized in FL code with $cMax = 1$ and bypassed, again, bypass mode assign the same probability for zero as well as for one which mean changing zero to one or vice versa will never affect the compression ratio. Moreover, since the MV difference sign is binarized in FL code with $cMax = 1$, flipping zero to one or vice versa will keep it in the same format which means a format compliant value.
The absolute value of the dQP is context coded so its encryption will affect its probability and the compression ratio.

SE schemes	Format compliance	Constant bitrate	Encryption algorithm	Encryption domain	Robust to transcoding	Video standard	Support scalability
Li et al. [28]	No	Yes	Leak Extraction (Stream cipher)	NAL	No	H.264/SVC	Yes
Carrillo et al. [29]	Yes	No	Pseudo random pixel permutation	Pixel	Yes	Independent	ROI
Wallendael et al. [30]	Yes	No	AES as stream cipher	Transform	No	HEVC	No
Shahid et al. [22]	Yes	Yes	AES (block cipher)	Binstrings	No	HEVC	No
SE-SHVC-BL	Yes	Yes	Chaotic (stream cipher)	Binstrings	Yes for ELs	SHVC	Yes
SE-SHVC-EL	Yes	Yes	Chaotic (stream cipher)	Binstrings	Yes for BL	HEVC & SHVC	Yes

Table 1. Comparison between the proposed encryption schemes (SE-SHVC-BL and SE-SHVC-EL) and the state of the art methods.

We propose in this paper to encrypt only the dQP sign which is bypassed in the SHVC CABAC and binarized in FL code with $cMax = 1$.

Concerning the TCs, they are bypassed and binarized with a combination of TRp with $p \in \{0, 1, 2, 3, 4\}$ and EGk codes ($k = p + 1$). The suffix of the EGk code can be safely encrypted, while encryption of the TRp suffix is not format compliant since its encryption can affect the p parameter value and consequently the compression ratio. In this paper we propose an algorithm enabling to accurately determine of the bins of the TRp suffix that can be encrypted without changing the p before and after all possible values of the TRp suffix. The p parameter value is updated after the binarization of each TC depending on its absolute value $| \omega |$ as follows:

Algorithm 1 Update the p parameter in TRp code

if ($| \omega | > 3 \times 2^p$) **then**
  $p = min(p + 1, 4)$
end if

where p is initialized to 0 at the start of each transform sub-block.
The absolute value of TC (it is represented in this study as ω) is composed of the base level (it is represented in this study as *baseLevel*) plus the remaining part (it is represented in this study as ϕ). $| \omega | = baseLevel + \phi$. The value of the *baseLevel* is computed based on the value ω with $baseLevel \in \{1, 2, 3\}$ for $\omega \neq 0$. The base level value is first signalled in the bitstream with specific syntax elements and then only the remaining part ϕ different from 0 is binarized in TRp and EGk codes. Algorithm 2 provides the positions (from the least significant bin) of the encryptable bins in the TRp suffix.

In the case where base level is equal to 1, the whole suffix can be encrypted since the ϕ value plus 1 (*baseLevel*) never exceeds the threshold to update p for all possible suffix values ($\phi + 1 \leq 3 \times 2^p$). In the following part we discuss the encryption configurations provided in Table 2 for base level different from 1. Table 2 provides the encryptable bins in the suffix of the TC binarized in TRp code with $p = 3$. The threshold computed by Algorithm 1 to update the parameter $p = 3$ is equal to 24 (3×2^p). When the ϕ value is less than 16 or greater than 23, the three bins of the suffix can be safely encrypted since in these cases the TC value ($| \omega |$) remains less or greater than 24 for all possible suffix values. When the ϕ value is less than 20 (and greater than 15) only the first two bins of the suffix can be encrypted. This is because encrypting the third bin can increase the value of the TC $| \omega |$ to be greater than the threshold value and then update the p parameter while the initial value $| \omega |$ does not. In the case where the ϕ value is equal to 22 or 23 along while the base level is equal to 2, the suffix can not be encrypted since changing one bin in the suffix brings the value of the TC $| \omega |$ on the other side of the threshold. In all other configurations provided in Table 2 only the

Algorithm 2 Encryptable bins in the TRp suffix of TCs ω.

Require: Basic Level **baselevel**
Require: cRice parameter **cRP**
Require: Coefficient **coef**
Ensure: Encryptable Bins

if (**baselevel** == 1) **then**
  The whole suffix is encryptable.
else if (**cRP** == 1) **then**
  if (**baselevel** == 2 AND (**coef** == 4 OR **coef** == 5)) **then**
    No encryption.
  else
    The whole suffix is encryptable.
  end if
else if (**cRP** == 2) **then**
  if (**coef** $\leq$ 7 OR **coef** $\geq$ 12) **then**
    The whole suffix is encryptable.
  else if (**baselevel** == 2 AND (**coef** == 10 OR **coef** == 11)) **then**
    No encryption.
  else
    The first bin of the suffix is encryptable.
  end if
else if (**cRP** == 3) **then**
  if (**coef** $\leq$ 15 OR **coef** $\geq$ 24) **then**
    The whole suffix is encryptable.
  else if (**coef** $\leq$ 19) **then**
    The first two bins of the suffix are encryptable.
  else if (**baselevel** == 2 AND (**coef** == 22 OR **coef** == 23)) **then**
    No encryption.
  else
    The first bin of the suffix is encryptable.
  end if
else if (**cRP** == 4) **then**
  if (**coef** $\leq$ 31 OR **coef** $\geq$ 48) **then**
    The whole suffix is encryptable.
  else if (**coef** $\leq$ 39) **then**
    The first three bins of the suffix are encryptable.
  else if (**coef** $\leq$ 43) **then**
    The first two bins of the suffix are encryptable.
  else if (**baselevel** == 2 AND (**coef** == 46 OR **coef** == 47)) **then**
    No encryption.
  else
    The first bin of the suffix is encryptable.
  end if
end if

first bin of the suffix can be safely encrypted. Therefore, Algorithm 2 enables the format-compliant encryption of all possible bins in the suffix of the TCs binarized in TRp code, aiming to maximize the encryption space.

Finally, the sign of the TC is encrypted. Table 3 summarizes the encrypted parameters in the proposed selective

ϕ	*baseLevel*		Preffix	Suffix
	2	3		
	ω			
14	16	17	10	**110**
15	17	18	10	**111**
16	18	19	110	0**00**
17	19	20	110	0**01**
18	20	21	110	0**10**
19	21	22	110	0**11**
20	22	23	110	10**0**
21	23	24	110	10**1**
22	24	-	110	110
22	-	25	110	11**0**
23	25	-	110	111
23	-	26	110	11**1**
24	26	27	1110	**000**

Table 2. Encryptible bins in bold font of the TC suffix binarized in TRp code with $p = 3$ and $\omega = baseLevel + \phi$

Syntax elements	Binarization	Encrypted part
MV dif.	EG1	Suffix
MV dif. sign	FL	1 bin
TCs	TRp and EGk	EGk suffix and TRp suffix as in Alg. 2
TC sign	FL	1 bin
dQP sign	FL	1 bin

Table 3. Encrypted syntax elements in the proposed SHVC selective encryption solution, all theses syntax elements are bypass coded

encryption solution.

3.2. Chaotic-based Encryption System

The principle of the encryption system is illustrated in Figure 5. The encryption process is carried out syntax element by syntax element using a simple xor and addition operations:

$$c_i = s_i \oplus (x_i + c_{i-1}) \tag{8}$$

where s_i is the encryptable bin of one syntax element (plain), c_{i-1} is the encrypted bin of the previous syntax element. The previous encrypted value is used to transfer the diffusion effect from one encrypted parameter to the other plain ones, and x_i is the generated bits from the chaotic generator (dynamic key). To encrypt the first syntax element, c_{i-1} with $i = 0$ is set to IV ($c_{-1} = IV$). The confusion effect is obtained by mixing the plain parameters with the key stream while the diffusion effect is obtained by using the previous ciphered parameters c_{i-1}.
In case that the addition operation has an overflow, the result is truncated since the addition operation in the both encryption and the decryption parts are exactly the same.

It must be noted that the chaotic generator at each iteration (call) generates a key stream of 32 bits. We add an extra layer on the top of the chaotic generator to manage returning a specific number of bits k ($0 \leq k \leq 32$) equal to the number of bits required to encrypt each syntax element (ie. length of s_i in bits). This layer manages an internal

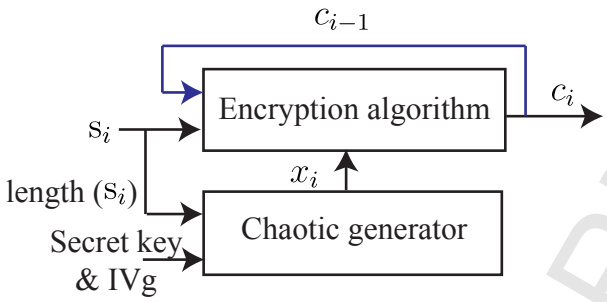


Figure 5. Encryption system using the stream cipher chaotic generator

buffer that stores the key stream of 32 bits and calls the chaotic generator to fill its internal buffer when it is empty or the number of requested bits is higher than the remaining bits within the buffer. On the decoder side, the decryption is performed by an inverse operation as follows:

$$s_i = c_i \oplus (x_i + c_{i-1}) \tag{9}$$

3.3. End-to-End Synchronization

Synchronization between the encoder and the decoder is a challenging issue when the selective encryption is used with a stream cipher system. Moreover, the encryption must be robust to packet losses (i.e., enable re-synchronization of the decryption even after packet loss occurs in the network). Therefore, the joint compression/encryption system should be carefully designed to enable a secure encryption while preserving all SHVC features including sub-stream extraction and error resilience; and also by minimizing the bitrate overhead.

To preserve all SHVC functionalities, the dependencies of the chaotic generator follow the SHVC coding dependencies including temporal dependency (inter prediction) between frames of the same layer and dependency between SHVC layers (inter-layer prediction). We consider one independent chaotic generator for each SHVC layer, where each generator will produce the dynamic key (x_i) used to encrypt the syntax elements of the corresponding SHVC layer. This enables an independent encryption and decryption of the L SHVC layers. Moreover, the L different secret key must be shared between the encoder and the decoder decoding the L video layers. This solution enables access rights per service brought by a specific set of SHVC layers (HD, UDH, High Dynamic Range, High Frame Rate etc.). Each chaotic generator is re-initialized with the same secret key and a new IVg at each new Clean Random Access (CRA) frame [31]. This enables a safe sub-stream extraction with a correct decryption of the BL and the corresponding ELs event when previous frames are not extracted and decoded. The IVg is a pseudo random sequence of 64 bits carried our at the start of each CRA frame either at the bitstream level as Supplemental Enhancement Information (SEI) or at the transport level by the used transport protocol (RTP, MPEG-TS, DASH). Authors in [32] proposed a solution to use attributes of Real-time Transport Protocol (RTP) as an IV and thus avoids additional bitrate overhead. In [24], the non-encrypted information in the video bitstream is used to generate the Initial Vector (IV) of the AES encryption algorithm without additional overhead.

Figure 10 illustrates the structure of the encrypted SHVC bitstream with two layers using SE-SHVC-All encryption scheme. The Video Parameter Set (VPS) header contains information related to the whole video then the Sequence Parameter Set (SPS) and Picture Parameter Set (PPS) headers containing information of the BL are signalled followed by the first BL slice. The SPS and PPS headers of the EL are signalled before the first EL slice. The encrypted data at both the BL and EL slices using the SE-SHVC-All scheme are highlighted by red segments referring to a partial encryption. Therefore, the proposed selective encryption schemes do not encrypt the video headers including slice headers, information that is usually used for mid-network adaptation.

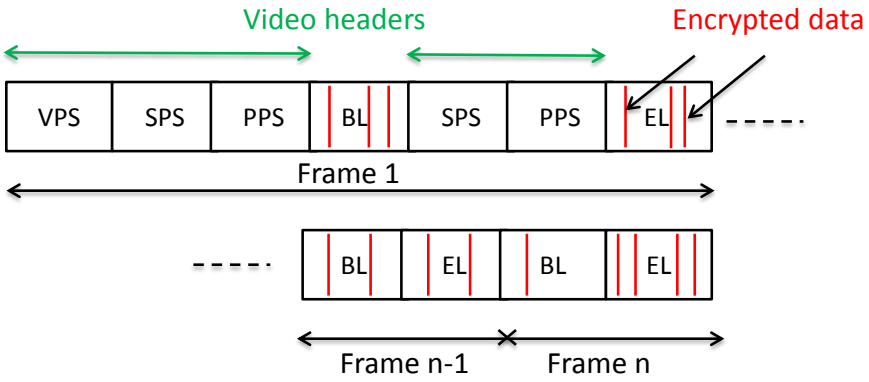


Figure 6. Structure of the encrypted SHVC bitstream with two layers using SE-SHVC-All encryption scheme

4. Results and Discussions

4.1. Experimental Design

The proposed encryption schemes were implemented in the Scalable Reference software Model (SHM) encoder version 4.1 [33]. The decryption algorithms were implemented under the optimized [4] SHVC decoder *OpenHEVC* [34]. This allows assessment of the complexity overhead of the decryption process in the context of the real-time SHVC decoder. We consider the common SHVC test conditions [35]. The configuration of the test video sequences is provided in Table 4. These video sequences are encoded in low delay P configuration (I frame followed by P frames), two layers ($L = 2$) and three scalability configurations: two spatial configurations with ratios 2x, 1.5x and one fidelity (SNR) configuration. We consider three QP configurations EL QP is $QP_{EL} \in \{22, 26, 34\}$ and the corresponding BL QP is equal to the QP_{EL} in spatial scalability configurations and $QP_{BL} \in \{26, 30, 38\}$ in SNR scalability. We use both Peak Signal to Noise Ration (PSNR) and the Structural SIMilarity (SSIM) criteria to assess the quality of the decoded video.

Class	Sequences	Resolution	Frame rate (Hz)	duration (s)
B	*Kimono*	1920x1080	24	10
	ParkScene		24	10
	Cactus		50	10
	BasketBallDrive		50	10
	BQTerrace		60	10
A	*Traffic*	2560x1600	30	5
	PeopleOnStreet		30	5

Table 4. Video sequences considered in the experiments.

4.2. Objective Quality and Encryption Space

Table 5 gives an average performance in terms of PSNR Y, SSIM and ES of the three proposed encryption schemes for video classes A and B at one particular EL QP configuration (QP_{EL}=22). We can notice that encryption schemes SE-SHVC-BL and SE-SHVC-All, encrypting only the BL and both layers respectively, drastically decrease the objective quality of the video sequences by decreasing their average PSNR Y values to below 10 dB and their average SSIM values to below 0.2, in all scalability configurations. The encryption scheme SE-SHVC-BL considerably decreases the objective quality of both layers since the inter-layer prediction used in the SHVC extension propagates

[4] Optimized software refers in this paper to a code-source written in Single Instruction Multiple Data (SIMD) operations.

errors, introduced by encryption, from the encrypted BL to the clear (non-encrypted) EL. In fact, the EL decoder uses reconstructed samples of the BL picture as a reference for inter-layer prediction and also uses the encrypted BL MVs in the inter-layer merge mode[5]. We can also notice that the SE-SHVC-All encryption scheme enables a further decrease in the objective quality of the SHVC video by 0.1 dB to 0.2 dB with respect to the SE-HEVC-BL encryption scheme.
On the other hand, the SE-SHVC-EL encryption scheme encrypting only the EL slightly decreases the objective quality of the EL video. This is because most of the information is predicted from the clear BL while only details (difference between BL and EL) of the video are encoded and encrypted at the EL.
The ES of the SE-SHVC-BL remains on average less than 8% of the whole SHVC video bitstream including BL and EL. This low ES is obtained thanks to the selective encryption where only the most sensitive syntax elements are encrypted and also because the size of the BL bitstream is lower than the size of the non-encrypted EL particularly in spatial scalability configurations. The encryption space in the ES-HEVC-EL encryption scheme is around 11% of the whole SHVC video bitstream and encryption of both layers with SE-SHVC-All encryption scheme increases the ES to 16% on average.
The PSNR Y, SSIM and ES performance of the three considered schemes in all scalability configurations is provided in Table 6 for the 1080p50 *Cactus* video sequence at different QP configurations. We can notice that the three proposed encryption schemes decrease the objective quality of the video to the same low quality level whatever the QP values and the corresponding initial quality of the video. However, the ES slightly decreases with high QP values in the SE-SHVC-All encryption scheme since less syntax elements are present at low bitrate configuration. Moreover, for the SE-SHVC-BL and SE-SHVC-EL encryption schemes the ES depends not only on the QP but also on the scalability configuration which changes the resolution of the BL and the correlation degree between the two layers (related to the video sequence, the scalability configuration and the QP used at each layer).
Table 7 shows the BL and EL PSNR of the three color components (Y, U and V) of the 1600p30 *Traffic* video sequence encrypted with the SE-SHVC-BL encryption scheme at different scalability and QP configurations. This Table shows that the SE-SHVC-BL encryption scheme decreases the PSNR of both layers to the same level in different QP and scalability configurations. The PSNR of the BL and EL is decreased to around 8.5 dB for the luminance Y component and 13 dB and 15 dB for the U and V color components, respectively.
Table 8 gives the ES repartition between the different encrypted SHVC syntax elements in the three proposed encryption schemes for the *Traffic* video sequence in two QP configurations. In the two bitrate configurations, the TC sign represents the most encrypted syntax element with more than 85% and 73% in high and low bitrate configurations, respectively for the SE-SHVC-All encryption scheme. The proportion of the TC sign is higher than the TC since most of the TC values ω lower than the base level (*baseLevel*) and different from zero are not binarized (remaining part ϕ is equal to 0) while their sign is signalled. Moreover, for the TCs binarized in TRp code, the proposed Algorithm 2 may reduce the number of encrypted bins in the TRp suffix. We can also notice that proportions of the MVs difference sign and the MVs difference slightly increase at low bitrate configuration mostly at the expense of TC sign and TCs syntax elements which are reduced at high QP value (low bitrate). The ES repartition in encryption schemes SE-SHVC-BL and SE-SHVC-EL shows that scalability configuration also impacts the ES repartition mostly caused by the resolution of the BL and the correlation between these two layers. Finally, the dQP sign represents less than 1% and 2% of the encrypted syntax elements in SE-SHVC-All scheme at high and low bitrate configurations, respectively.

4.2.1.1 Histogram analysis
To resist against an important statistical attack, the histogram of the encrypted frame should be uniformly distributed as much as possible and different from the original frame. Figure 7 shows the histogram of the frame #8 of the *PeopleOnStreet* video sequence at QP_{EL}=22 in SNR scalability for the three proposed selective encryption schemes. In Figures 7b and 7c relating the frames encrypted with encryption schemes SH-SHVC-BL and SE-SHVC-All, respectively, the histograms are distributed in a manner close to the pseudo-random distribution and are completely different from the original one. This result together with previous statistical analysis results leads to the robustness of the proposed schemes to the statistical and visual analysis attacks.

[5]Merge mode in the SHVC inter-layer prediction uses the MVs from the BL for motion compensation.

Class	Sca.	QP_{BL} -QP_{EL}	No encryption		SE-SHVC-BL			SE-SHVC-All			SE-SHVC-EL		
			PSNR	SSIM	PSNR	SSIM	ES	PSNR	SSIM	ES	PSNR	SSIM	ES
A	SNR	26-22	41.12	0.95	8.28	0.16	7.27	8.25	0.13	15.06	23.69	0.69	7.79
	2x	22-22	41.3	0.95	9.04	0.14	5.62	8.96	0.1	16.61	17.72	0.48	10.98
	HEVC	.-22	41.25	0.95	-	-	-	-	-	-	8.55	0.1	17.83
B	SNR	26-22	39.54	0.91	9.18	0.18	6.23	9.13	0.15	15.72	25.77	0.69	9.49
	2x	22-22	39.6	0.91	9.82	0.19	4.11	9.66	0.14	17	18.65	0.42	12.89
	1.5x		39.57	0.91	9.11	0.18	6.31	9.03	0.15	16.41	21.97	0.6	10.1
	HEVC	.-22	39.6	0.91	-	-	-	-	-	-	9.29	0.14	18.27

Table 5. Video quality (PSNR Y and SSIM) and ES of the three proposed SHVC encryption schemes

QP_{BL}-QP_{EL}	Sca.	No encryption		SE-SHVC-BL			SE-SHVC-All			SE-SHVC-EL		
		PSNR	SSIM	PSNR	SSIM	ES	PSNR	SSIM	ES	PSNR	SSIM	ES
26-22	SNR	38.65	0.9	8.69	0.19	4.97	8.65	0.16	14.99	24.68	0.7	10
22-22	2x	38.68	0.9	8.72	0.2	3.38	8.63	0.14	16.39	17.5	0.47	13.01
	1.5x	38.66	0.9	9.27	0.21	5.23	9.17	0.16	15.6	20.25	0.6	10.37
.-22	HEVC	38.68	0.9	-	-	-	-	-	-	9.04	0.14	16.91
30-26	SNR	37.09	0.87	8.78	0.25	6.86	8.73	0.21	14.16	23.25	0.66	7.3
26-26	2x	37.16	0.88	8.99	0.27	4.92	8.83	0.18	15.61	17.79	0.49	10.69
	1.5x	37.10	0.88	8.68	0.2	7.28	8.67	0.17	14.64	21.76	0.64	7.36
.-26	HEVC	37.15	0.88	-	-	-	-	-	-	8.81	0.2	16.66
38-34	SNR	33.66	0.82	7.75	0.29	6.66	7.75	0.27	12.41	24.51	0.69	5.74
34-34	2x	33.78	0.82	8.28	0.23	4.69	8.28	0.2	13.63	19.73	0.55	8.93
	1.5x	33.66	0.82	9.61	0.25	6.69	9.59	0.24	12.58	22.97	0.66	5.61
.-34	HEVC	33.92	0.83	-	-	-	-	-	-	8.31	0.26	14.69

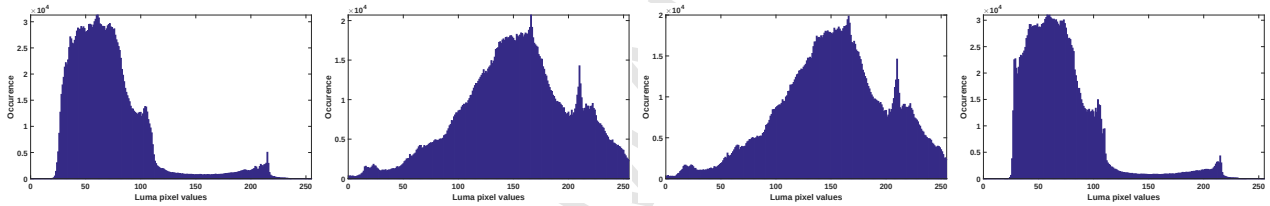
Table 6. Video quality and ES of the three proposed SHVC encryption schemes for the 1080p50 *Cactus* video sequence

QP_{BL}-QP_{EL}	Sca.	BL PSNR (dB)						EL PSNR (dB)					
		No encryption			SE-SHVC-BL			No encryption			SE-SHVC-BL		
		Y	U	V	Y	U	V	Y	U	V	Y	U	V
26-22	SNR	39.46	39.98	42.45	8.29	12.78	14.12	41.6	41.46	43.86	8.08	13.53	14.62
22-22	2x	40.77	42.42	44.25	8.78	13.96	14.42	41.67	41.50	43.96	9.44	12.49	14.61
.-22	HEVC	-	-	-	-	-	-	41.69	41.52	44.05	8.39	13.19	14.66
30-26	SNR	37.37	38.87	41.3	8.96	12.36	13.7	39.31	39.85	42.24	8.4	14.01	19.92
26-26	2x	38.04	40.55	42.51	8.46	15.68	17.15	39.41	39.91	42.32	9.21	16.97	17.54
.-26	HEVC	-	-	-	-	-	-	39.46	39.98	42.45	8.29	12.78	14.12
38-34	SNR	33.06	36.92	39.28	8.36	14.52	20.29	34.96	37.47	39.83	8.4	14.01	19.92
34-34	2x	32.98	37.46	39.76	9.11	16.36	18.11	35.06	37.5	39.84	8.84	14.03	14.83
.-34	HEVC	-	-	-	-	-	-	35.23	37.66	40	8.08	16.41	19.68

Table 7. BL and EL PSNR of the $Traffic$ video sequence in different scalability and QP configurations: SE-SHVC-BL encryption scheme

Syntax element	QP_{EL}	SE-SHVC-BL		SE-SHVC-All		SE-SHVC-EL		
		SNR	2x	SNR	2x	SNR	2x	HEVC
MV diff.	22	2	0.68	3.15	2.88	1.15	2.2	3.22
MV diff. sign		3.45	1.75	6.61	6.91	3.15	5.1	6.36
TCs		3.66	3.01	3.67	3.4	0.01	0.38	7.39
TC sign		34.53	24.17	85.74	86.28	51.2	62.06	82.52
dQP sign		0.33	0.11	0.81	0.55	0.48	0.44	0.49
Sum		43.98	29.73	100	100	56.01	70.26	100
Bitrate (Mbit/s)		12.6	9.4	28.66	31.63	16.05	22.22	29.03
MV diff.	34	5.67	2.73	9.59	9.27	3.91	6.53	7.62
MV diff. sign		5.94	4.33	12.06	13.48	6.11	9.14	9.37
TCs		2.94	1.76	2.94	1.79	0	0.02	6.39
TC sign		44.89	32.75	73.56	74.05	28.66	41.3	75.53
dQP sign		0.86	0.31	1.83	1.39	0.96	1.07	1.07
Sum		60.32	41.90	100	100	39.67	58.09	100
Bitrate (Mbit/s)		1.8	1.25	2.99	3	1.18	1.74	3.28

Table 8. Repartition of the encrypted SHVC syntax elements in the three proposed schemes for $Traffic$ video sequence



(a) Original (b) SE-SHVC-BL (c) SE-SHVC-All (d) SE-SHVC-EL

Figure 7. Histograms of frame #8 *Kimono* video sequence in the three encryption schemes with SNR scalability and QP_{EL}=22

4.2.1.2 Edge differential ratio

Edge Differential Ratio (EDR) evaluates the edge differences between the original and the encrypted video sequences [36, 37]. As the edges are not longer clear the encryption solution is secure. To produce the edges of both frames (original and encrypted ones) the Laplacian of Gaussian method is used. The EDR is calculated as follows:

$$EDR = \frac{\sum_{i=0}^{h-1}\sum_{j=0}^{w-1}|P(i,j) - C(i,j)|}{\sum_{i=0}^{h-1}\sum_{j=0}^{w-1}|P(i,j) + C(i,j)|} \quad (10)$$

Where P and C are the bit value in the edge detected binary matrix for the plain-frame (non-encrypted) and the ciphered-frame, respectively.

Table 9 presents the average evaluation results of the EDR for the three proposed schemes. It is clear that the average EDR values are close to 1, which ensure that the proposed encryption schemes SE-SHVC-BL and SE-SHVC-All have high ability to hide the edges of the encrypted frames. Figure 8 shows the edges of frame #8 of *Kimono* video sequences. It confirms the results provided in Table 9. In fact, the structural information of the encrypted frame by schemes SE-SHVC-BL and SE-SHVC-All are completely hidden and become useless for the attacker.

4.3. Visual Quality

Figure 9 shows the visual quality of *BasketballDrive* video sequence frame #9 encrypted by schemes SE-SHVC-BL and SE-SHVC-EL. We can notice that scheme SE-SHVC-BL encrypting only the BL also affects the visual quality of the EL. The inter-layer prediction using the decoded BL picture and its MVs propagates the errors to the EL. However, by using the SE-SHVC-EL, the BL remains clear and the quality of the EL is slightly decreased compared

Video	Sca.	SE-SHVC-BL	SE-SHVC-All	SE-SHVC-EL
Kimono	SNR	0.95	0.95	0.78
	2x	0.96	0.95	0.88
	1.5x	0.96	0.95	0.78
	HEVC	-	-	0.95
People-OnStreet	SNR	0.93	0.93	0.54
	2x	0.93	0.92	0.81
	HEVC	-	-	0.92

Table 9. Edge differential ratio for *Kimono* and *PeopleOnStreet* video sequences at QP_{EL}=22

(a) Original (b) SE-SHVC-BL (c) SE-SHVC-All (d) SE-SHVC-EL

Figure 8. Illustration of the Edges of frame #8 *Kimono* video sequence in the three encryption schemes with SNR scalability and QP_{EL}=22

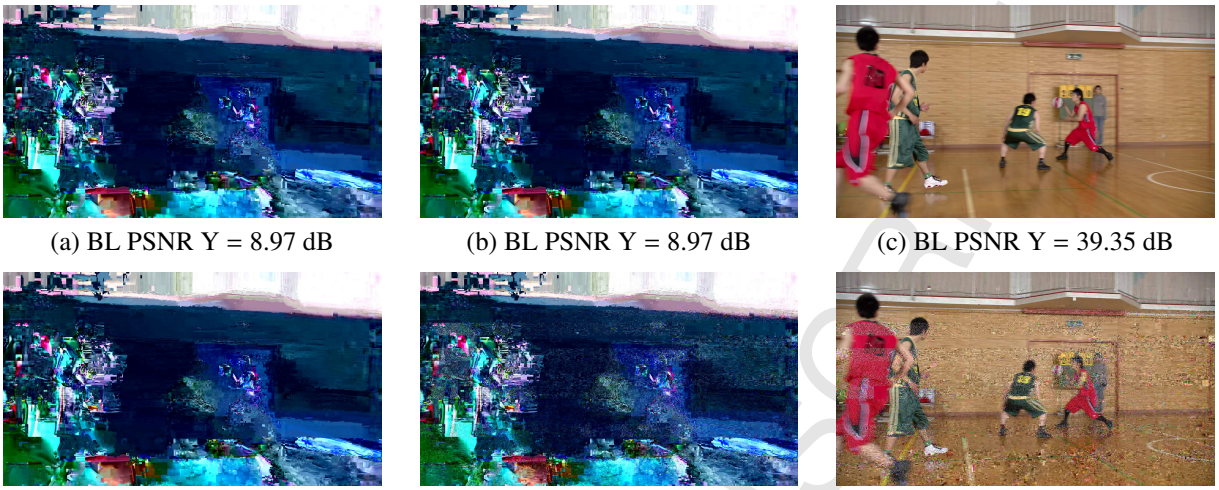
to the SE-SHVC-BL scheme. This is because most of the information is predicted from the base layer and only details (encrypted data) are encoded at the level of the EL. We can notice that the proposed SE-SHVC-EL encryption scheme leads to a perceptual (transparent) encryption solution by decreasing the visual quality of the EL layer below the quality of the BL while the EL video is still recognized. However, the encryption scheme SE-SHVC-BL enables a more secure encryption solution by drastically decreasing the visual quality of all layers. Additional analysis on the security parameters of these three proposed selective encryption schemes are investigated in the next section.

4.4. Subjective Quality Assessment

In order to evaluate, subjectively, the robustness of the proposed real time selective encryption method, we have performed a set of subjective encryption tests. They consist in evaluating the degree of perceptibility of visual content in the encrypted videos. Different configurations (perceptual schemes) and quality levels (different QPs) have been studied in this tests campaign. In this subjective quality assessment, the Double Stimulus Continuous Quality Scale (DSCQS) method was used [38]. Each encrypted video was presented twice to participants accompanied by its reference version (original). Participants were asked to numerically quantify the degree of content visibility of the encrypted videos. In other words, each participant must assign a visibility score to each of the 12 test videos, according to a rating scale: video content is *completely invisible* 1, *Barley visible* 2, *Slightly visible* 3, *visible* 4 and *clearly visible* 5 [39]. At the end of each test condition, a dedicated Graphical User Interface (GUI) is displayed on the screen for about 10 seconds during which the observer gives and then con-firms its judgement. At the beginning of the experiment, additional sequences were introduced in order to stabilise the opinion of the observers (these sequences will not be taken into account for the final data processing). To eliminate the memory effect, video sequences were mixed in such a way that two successive sequences must be from different categories, sequences and quality levels.
The first step in the results analysis is to calculate the average score of Mean Opinion Score (MOS) for each video used in the experience. This average is given by equation 11.

$$MOS_{jk} = \frac{1}{N}\sum_{i=1}^{N} s_{ijk} \tag{11}$$

where s_{ijk} is the score of participant i for degree of visibility j of the sequence k and N is the number of observers.



(a) BL PSNR Y = 8.97 dB (b) BL PSNR Y = 8.97 dB (c) BL PSNR Y = 39.35 dB

(d) EL PSNR Y = 8.98 dB (e) EL PSNR Y = 8.88 dB (f) EL PSNR Y= 17.59 dB

Figure 9. Visual quality of frame #9 of the *BasketballDrive* video sequence in SNR scalability configuration (a) (d) SE-SHVC-BL, (b) (e) SE-SHVC-ALL and (c) (f) SE-SHVC-EL)

In order to better evaluate the reliability of the obtained results, it is advisable to associate for each MOS score a confidence interval, usually at 95%.

Figure10 illustrates the MOS for four considered videos encrypted with the SE-BL-SHVC encryption scheme at three QP configurations. We can notice that the subject scores are between 1 and 2 which refer to *completely invisible* and *barely visible* qualities for the four videos at three different bitrates. Moreover, the confidential intervals for all video remain low and do not exceeds 2. The 2 point in the rating scale means that subjects can scarcely see a few things of the video (without being able to recognize the global context of the presented video). These subjective results confirm the high security level of the SE-BL-SHVC scheme to drastically decrease the video quality which convenient for secure applications.

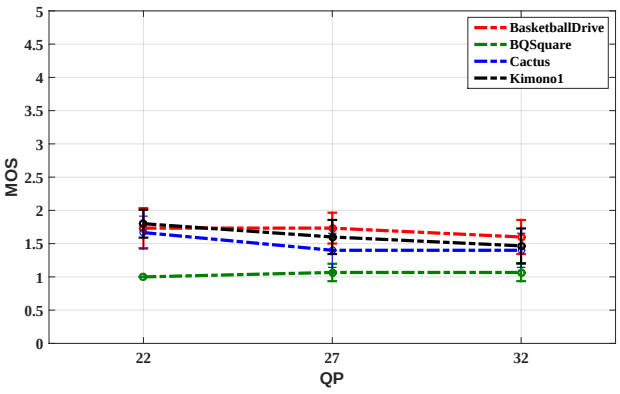


Figure 10. Subjects visibility scores including 95% confidence intervals

4.5. Security Analysis

4.5.1 Encryption Quality

The difference between the frequency of occurrence for each byte before and after encryption is called Encryption Quality (EQ). It calculates the average frequency difference between all possible bytes in the original and the encrypted video frames. The EQ is defined as follows [40]:

$$EQ = \frac{\sum_{Z=0}^{255} |H_Z(C) - H_Z(P)|}{256} \tag{12}$$

where $H_Z(C)$ is the total number of occurrences for the byte Z in the ciphered frame C, and $H_Z(P)$ is the total number of occurrences of the same byte Z in the original frame P.
Therefore, the higher the EQ value is, the more secure is the encryption solution. Table 10 presents the EQ of the three proposed encryption schemes at different scalability configurations for *Kimono* and *PeopleOnStreet* video sequences. The presented values are the average EQ over encrypted frames of these two video sequences. The EQ does not have a relative point for comparison. We propose a derivation from Equation 12 to find the maximum value of the EQ noted EQ_{max}:

$$EQ_{max} = \frac{510 \times h \times w}{256^2} \tag{13}$$

where h and w are the height and the width of the gray video frame, respectively. The derivation of Equation (13) from Equation (12) is detailed in Appendix 5.
The maximum EQ values of *Kimono* and *PeopleOnStreet* video sequences computed by Equation (13) are equal to 16136.7 and 31875, respectively. We can notice from Table 10 that encryption schemes SE-SHVC-BL and SE-SHVC-All reach on average a higher EQ then half the maximum EQ in all scalability configurations and for both video sequences. However, the encryption scheme SE-SHVC-EL performs low EQ, which corresponds to features of the perceptual video encryption target. Figure 11 gives more information on the EQ at each frame by the Cumulative Distribution Function (CDF) of the EQ for *Kimono* (a) and *PeopleOnStreet* (b) video sequences. We can notice that all frames of the *Kimono* and *PeopleOnStreet* video sequences have an EQ higher than 38.69% and 41.08% of the maximum EQ, respectively. On the other hand, all frames of these two video sequences have an EQ lower than 70.44% and 57.69% of the maximum EQ, respectively.

Video	Sca.	SE-SHVC-BL	SE-SHVC-All	SE-SHVC-EL
Kimono	SNR	9025	8996	684
	2x	7651	7675	1101
	1.5x	9895	9900	571
	HEVC	-	-	9355
People-OnStreet	SNR	14833	14884	3355
	2x	14528	14739	5161
	HEVC	-	-	14129

Table 10. Encryption Quality for *Kimono* and *PeopleOnStreet* video sequences at QP_{EL}=22

4.5.2 Key Sensitivity Test

Key sensitivity is extremely crucial for any encryption algorithm. It has a high security level relative to key sensitivity attacks if a slight change in the secret key produces a completely different ciphered image [41]. The testing scenario of key sensitivity is as follows: we have an original frame P and two secret keys are different in one bit related to the least significant bit in the key (K_1 and K_2). First, P is encrypted using K_1 to obtain the ciphered frame $C1$. Then the same frame P is encrypted using K_2 to obtain $C2$. Security parameters used to measure the resistance of any proposed cryptosystem for this attack are: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity

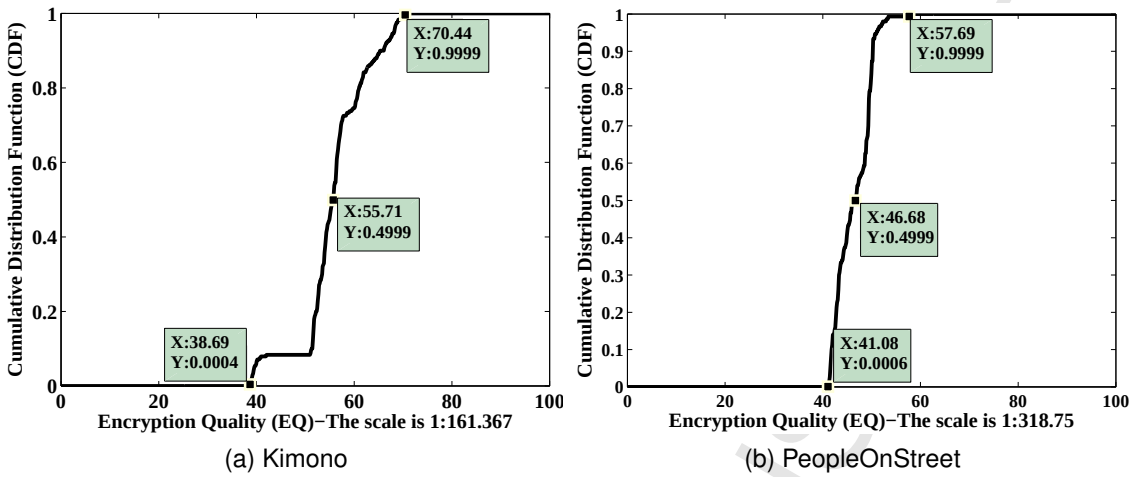


Figure 11. Cumulative Distribution Function (CDF) of the EQ for *Kimono* and *PeopleOnStreet* video sequences in SNR scalability, QP_{EL}=22 and SE-SHVC-BL encryption scheme

(UACI), they are given by the following equations, respectively [42, 43]:

$$NPCR = \frac{1}{h \times w} \times \sum_{i=1}^{h} \sum_{j=1}^{w} D_{i,j} \times 100\% \tag{14}$$

where

$$D_{i,j} = \begin{cases} 0, & \text{if} \quad C1_{i,j} = C2_{i,j} \\ 1, & \text{if} \quad C1_{i,j} \neq C2_{i,j} \end{cases} \tag{15}$$

$$UACI = \frac{1}{h \times w \times 255} \times \sum_{i=1}^{h} \sum_{j=1}^{w} |C1_{i,j} - C2_{i,j}| \times 100\% \tag{16}$$

The above tests are usually used to measure the resistance of a full encryption cryptosystem against the differential attacks introduced by Eli Biham and Adi Shamir [44].

Sca.	*Kimono*		*PeopleOnStreet*	
	UACI	NPCR	UACI	NPCR
SNR	31.74	97.02	35.36	98.29
2x	36.75	98.98	39.34	98.37
HEVC	34.87	98.44	36.06	97.76

Table 11. Average performance of Key sensitivity attack over all frames of *Kimono* and *PeopleOnStreet* video sequences: SE-SHVC-BL, QP_{EL}=22

The optimal values of NPCR and UACI are 99.58% and 33.46%, respectively [42]. Although the proposed encryption solution is selective, the presented UACI and NPCR values in Table 11 for encryption scheme SE-SHVC-BL are close to optimal. Moreover, the average Hamming distance between the two encrypted frames are 49.69 and 50.87 for *Kimono* and *PeopleOnStreet*, respectively. These HD values are too close to the optimal value of 50%. Finally, all experiments indicate that the proposed cryptosystems are sensitive to the one bit change in the secret key.

4.5.3 Error Concealment Attacks

One of the scenarios used to accomplish this type of attack is performed by replacing all encrypted bits with zeros. Table 12 presents the average PSNR and SSIM values over the whole frames of Kimono and *PeopleOnStreet* video sequences after replacing all encrypted bits by zeros for the BL.

	Sca.	*Kimono*		*PeopleOnStreet*	
		No enc.	Rep. by 0	No enc.	Rep. by 0
PSNR (dB)	SNR	41.55	7.82	40.64	9.2
	2x	41.63	7.87	40.92	9.05
	1.5x	41.51	8.47	-	-
	HEVC	41.66	8.75	40.8	9.01
SSIM	SNR	0.93	0.17	0.95	0.17
	2x	0.93	0.24	0.95	0.16
	1.5x	0.93	0.2	-	-
	HEVC	0.92	0.2	0.95	0.09

Table 12. Average PSNR and SSIM for replacing encrypted bits by zero: QP_{EL}=22, SE-SHVC-BL

It is clear from Table 12, that after replacing all encryptable bits with zero, the PSNR and SSIM values remain low and far from the correct decoded and decrypted sequences. These results contend the robustness of the proposed schemes against this scenario of the known plain-text attacks.

4.5.4 Brute Force Attack

It breaks the cryptosystem by trying a large number of possible keys until the correct one is found. In the worst case, all possible keys in key space are tested [45], [46].
Encryption of MVD and residual signs was classified by [47] to be secure selective encryption algorithms. In our proposed cryptosystem extra parameters such as the sign of dQP together with suffixes of the MVD and residuals increase the complexity of brute force attack.

4.6. Complexity Evaluation

In this section we assess the computational complexity of the encryption schemes in the context of a real-time SHVC decoder. We use a computer fitted with an Intel Core i5 processor running at 2.5 GHz.
Table 13 gives the Decoding Time (DT) and Complexity Overhead (CO) of the three encryption schemes using both chaotic and AES[6] encryption systems for the 1080p50 *Cactus* video sequence at different QP configurations. We can notice the high CO at high bitrate configuration (QP_{EL}=22) with respect to low bitrate configuration (QP_{EL}=34). This is mainly caused by the encryption of more syntax elements, including the complexity introduced by Algorithm 2 to safely encrypt the TCs, which increase in number at a high bitrate. The encryption scheme SE-SHVC-BL enables the lowest CO since only syntax elements of the BL are encrypted; and more especially in spatial scalability configurations where the resolution of the BL is lower than the EL resolution. On the other hand, the CO using either chaotic or AES encryption systems remains low in the context of real-time SHVC decoder and varies between 0% to 5% according to the bitrate, the scalability configuration and the used encryption scheme. This CO performance is obtained thanks to the low ES of the proposed selective encryption solution where less than 17% of the whole video size is encrypted. The maximum bitrate in Table 8 of the encryptable bits for the high resolution 1600p30 *Traffic* video sequence are 31.63 Mbit/s and 28.66 Mbit/s in 2x and SNR scalability configurations, respectively, with encryption scheme SE-SHVC-All at high bitrate (QP_{EL}=22). These bitrates remain very low with respect to the Chaotic and AES generators bitrates which are equal to 823.9 Mbit/s and 888 Mbit/s [7], respectively. This not only decreases the complexity of the encryption/decryption, which is inconvenient for battery-operated devices, but also decreases the end-to-end delay for live and real-time video streaming applications.

[6] AES system is used here in stream cipher mode (counter mode) for complexity comparison purposes with respect to the chaotic system
[7] This performance is obtained on a Core-i5-4300M CPU @ 2.6 GHz, using the Cryptopp [48] implementation of the AES encryption algorithm

QP_{BL}-QP_{EL}	Sca.	DT	SE-SHVC-BL				SE-SHVC-All				SE-SHVC-EL			
			Chaotic		AES		Chaotic		AES		Chaotic		AES	
			DT	CO	DT	CO	DT	CO	DT	CO	DT	CO	DT	CO
26-22	SNR	19.25	19.88	3.27	19.71	2.38	20.01	3.94	20.02	4	19.88	3.27	19.97	3.74
22-22	2x	17.30	17.58	1.16	17.53	1.32	17.91	3.52	17.95	3.75	17.92	3.58	17.84	3.12
	1.5x	18.74	19.19	2.4	19.20	2.45	19.37	3.36	19.48	3.94	19.19	2.4	19.33	3.14
.-22	HEVC	13.53	-	-	-	-	-	-	-	-	14.24	5.2	14.06	3.9
30-26	SNR	12.19	12.57	3.11	12.28	0.73	12.32	1.06	12.38	1.55	12.35	1.31	12.67	3.93
26-26	2x	10.02	10.10	0.79	10.57	5.48	10.32	2.99	10.33	3.09	10.23	2.09	10.31	2.89
	1.5x	11.35	11.73	3.34	11.79	3.87	11.71	3.17	12	5.72	11.59	2.11	11.63	2.46
.-26	HEVC	7.14	-	-	-	-	-	-	-	-	7.24	1.4	7.27	1.82
38-34	SNR	7.63	7.73	1.31	8	4.84	7.99	4.71	7.69	0.78	7.63	0	7.76	1.7
34-34	2x	6.09	6.09	0	6.2	1.8	6.28	3.11	6.18	1.47	6.13	0.65	6.34	4.1
	1.5x	7.1	7.22	1.69	7.25	2.11	7.18	1.12	7.32	3.09	7.27	2.39	7.48	5.35
.-34	HEVC	4.07	-	-	-	-	-	-	-	-	4.13	1.47	4.18	2.7

Table 13. Decoding Time (DT) in second and Complexity Overhead (CO) in % of the three proposed SE solutions for the *Cactus* video sequence in different scalability and QP configurations

5. Conclusion

In this paper we have proposed a selective video encryption solution based on the chaotic system in the scalable HEVC extension. The chaos-based stream system used is more robust and faster than the traditional stream ciphers. The proposed selective encryption (SE) solution encrypts the most sensitive syntax elements in the scalable HEVC (SHVC) bitstream at the CABAC binstring level. This encryption solution is an SHVC format compliant and does not impact the SHVC compression ratio. The encryption is applied on the SHVC bitstream in three different configurations: encryption of only the Base Layer (BL), encryption of all layers and encryption of only the highest Element Layer (EL) resulting in three encryption schemes SE-SHVC-BL, SE-SHVC-All and SE-SHVC-EL, respectively. Experimental results have shown that the first two schemes enable a high security level by drastically decreasing the visual quality of the video while the third scheme performs perceptual video encryption. The three schemes preserve all SHVC functionalities, including bitstream extraction and error resilience. This process enables the untrusted middle-box to perform network adaptation on the bitstream and further decrease the end-to-end delay. The ES of SE-SHVC-BL scheme remains low and does not exceed 8% of the whole SHVC bitstream and this scheme also passes all security encryption tests. In terms of computational complexity, the SE-SHVC-BL encryption scheme introduces a low complexity overhead, which remains lower than 3% of the whole SHVC decoding time of High Definition video sequences at high bitrate.

Acknowledgment

This work is supported by the European Celtic-Plus project 4KREPROSYS - 4K ultraHD TV wireless REmote PRODuction SYStems, 2015-2017.

A. Appendix 1: Maximum Encryption Quality (EQ)

The maximum value of the EQ is derived based on the following two assumptions:

1. The worst case of the original frame regarding to the encryption algorithm is at low entropy configuration. This means that the whole image has the same color, as an example all pixels are black or blue. Therefore, the total number of occurrences of the pixel Z_1 in the original frame P is $H_{Z_1}(P) = h \times w$, where $Z_1 \in \{0, 255\}$. Moreover, the total number of occurrences of the pixel Z_2 (Z_2 is any pixel except Z_1) in the original (no encrypted) frame P is $H_{Z_2}(P) = 0$, where $Z_2 \in \{0, 255\}$ and $Z_2 \neq Z_1$.

2. The most secure algorithm should produce a ciphered frame in which all pixels are randomly distributed. Therefore, the total number of occurrences of any pixel Z in the ciphered frame is $H_Z(C) = \frac{h \times w}{256}$, where $Z \in \{0, 255\}$.

Based on these two assumptions and using Equation (12), we derive the maximum EQ (EQ_{max}) as follows:

$$EQ_{max} = \frac{|\frac{h \times w}{256} - h \times w| + |\frac{h \times w}{256} - 0| \times 255}{256} \tag{17}$$

Since, h and w are positive integer, then:

$$EQ_{max} = \frac{510 \times h \times w}{256^2} \tag{18}$$

References

[1] G. J. Sullivan, J. R. Ohm, W. J. Han, T. Wiegand, Overview of the high efficiency video coding standard, IEEE Transactions on Circuits and Systems for Video Technology (TCSVT) 22 (2012) 1648–1667.

[2] High Efficiency Video Coding, in: Rec. ITU-T H.265 and ISO/IEC 23008-2, Sapporo, JP, 2013.

[3] J. R. Ohm, G. J. Sullivan, H. Schwarz, T. K. Tan, T. Wiegand, Comparaison of the Coding Efficiency of Video Coding standards including High Efficiency Video coding (HEVC), IEEE TCSVT 22 (2012) 1858–1870.

[4] G. J. Sullivan, J. M. Boyce, Y. Chen, J. R. Ohm, A. Vetro, Standardized Extensions of High Efficiency Video Coding (HEVC), IEEE Journal of Selected Topics in Signal Processing 7 (6) (2013) 1001–1016.

[5] J. Chen, J. Boyce, M. H. Y. Ye, G. J. Sullivan, Y. K. Wang, HEVC Scalable Extensions (SHVC) Draft Text 7, in: Document JCTVCR100, Sapporo, JP, 2014.

[6] V. Seregin, Y. H. T. D. Chuang, D. K. Kwon, F. L. Leannec, AHG Report: SHVC software, in: Document JCTVC-L0011, Geneva, Switzerland, 2013.

[7] T. Wiegand, G. J. Sullivan, G. Bjontegaard, A. Luthra, Overview of the H.264/AVC Video Coding Standard, IEEE TCSVT 13 (7) (2003) 560–576.

[8] H. Schwarz, D. Marpe, T. Wiegand, Overview of the Scalable Video Coding Extension of the H.264/AVC Standard, IEEE TCSVT 17 (9) (2007) 1103–1120.

[9] I. Agi, L. Gong, An Empirical Study of Secure MPEG Video Transmissions, in: Network and Distributed System Security, 1996, pp. 201–210.

[10] L. Qiao, K. Nahrstedt, Comparaison of MPEG Encryption Algorithms, Data Security in Image Communication and Networking 22 (1998) 437–448.

[11] T. Stutz, A. Uhl, A Survey of H.264 AVC/SVC Encryption, IEEE TCSVT 22 (3) (2003) 325–339.

[12] S. E. Assad, M. Farajallah, A New chaos-based image encryption system, ELSEVIER Journal on Signal Processing: Image Communication.

[13] M. Farajallah, S. E. Assad, O. Deforges, Fast and Secure Chaos-based Cryptosystem for Images, International Journal of Bifurcation and Chaos (IJBC).

[14] V. Sze, M. Budagavi, High Throughput CABAC Entropy Coding in HEVC, IEEE TCSVT 22 (2012) 1778–1791.

[15] S. El Assad, H. Noura, Generator of Chaotic Sequences and Corresponding Generating System, uS Patent 8,781,116 (Jul. 15 2014).

[16] C. Manifavas, G. Hatzivasilis, K. Fysarakis, Y. Papaefstathiou, A survey of lightweight stream ciphers for embedded systems, Security and Communication Networks 9 (10) (2016) 1226–1246.

[17] M. A. Taha, S. El Assad, A. Queudet, O. Déforges, Design and efficient implementation of a chaos-based stream cipher, International Journal of Internet Technology and Secured Transactions (2017) paper–IJITST_161464.

[18] R. Andrew, S. Juan, N. James, S. Miles, B. Elaine, A statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Tech. rep., DTIC Document (2001).

[19] S. Teo, K. K. Wong, H. Bartlett, L. Simpson, E. Dawson, Algebraic analysis of Trivium-like ciphers, in: Twelfth Australasian Information Security Conference, 2014, pp. 77–81.

[20] FIPS-197-Advanced Encryption Standard (AES), in: National Institute of Standards and Technology, 2001.

[21] G. Van Wallendael, A. Boho, J. De Cock, A. Munteanu, R. Van de Walle, Encryption for high efficiency video coding with video adaptation capabilities, IEEE Transactions on Consumer Electronics 59 (3) (2013) 634–642.

[22] Z. Shahid, W. Puech, Visual Protection of HEVC Video by Selective Encryption of CABAC Binstrings, IEEE Transactions on Multimedia 16 (2014) 24 – 36.

[23] M. Farajallah, W. Hamidouche, O. Dforges, S. E. Assad, ROI encryption for the HEVC coded video contents, in: IEEE International Conference on Image Processing (ICIP),, Barchalona, Spain, 2015, pp. 3096–3100.

[24] H. K. Arachchi, X. Perramon, S. Dogan, A. M. Kondoz, Adaptation-aware Encryption of Scalable H.264/AVC Video for Content Security, ELSEVIER Journal on Signal Processing: Image Communication 24 (6) (2009) 468–483.

[25] H. Hellwagner, R. Kuschnig, T. Stütz, A. Uhl, Efficient In-Network Adaptation of Encrypted H.264/SVC Content, ELSEVIER Journal on Signal Processing: Image Communication 24 (9) (2009) 740–758.

[26] J. Fridrich, Symmetric Ciphers based on Two-Dimensional Chaotic Maps, International World Scientific Journal on Bifurcation and Chaos 8 (06) (1998) 1259–1284.

[27] M. Farajallah, Z. Fawaz, S. E. Assad, O. Dforges, Efficient Image Encryption and Authentication Scheme Based on Chaotic Sequences, in: International Conference on Emerging Security Information, Systems and Technologies, Barchalona, Spain, 2013, pp. 150–155.

[28] C. Li, X. Zhou, Y. Zhong, NAL Level Encryption for Scalable Video Coding, Advances in Multimedia Information Processing (PCM) 5353 (2008) 496–505.

[29] P. Carrillo, H. Kalva, S. Magliveras, Compression Independent Reversible Encryption for Privacy in Video Surveillance, EURASIP Journal on Information Security 2009 (5) (2009) 1–13.
[30] G. V. Wallendael, A. Boho, J. D. Cock, A. Munteanu, R. V. de Walle, Encryption for High Efficiency Video Coding with Video Adaptation Capabilities, IEEE Transactions on Consumer Electronics 59 (2013) 634 – 642.
[31] R. S. et al., Overview of HEVC High-Level Syntax and Reference Picture Management, IEEE TCSVT 22 (2012) 1969–1684.
[32] B. Boyadjis, C. Bergeron, S. Lecompte, Auto-Synchronized Selective Encryption of Video Contents for an Improved Transmission Robustness over Error-prone Channels, in: IEEE ICIP, 2015.
[33] SHVC Reference software model (SHM), in: https://hevc.hhi.fraunhofer.de/svn/svn_SHVCSoftware/.
[34] W. Hamidouche, M. Raulet, O. Deforges, 4K Real-Time and Parallel Software Video Decoder for Multi-layer HEVC Extensions, IEEE Transactions on Circuits and Systems for Video Technology (TCSVT) 26 (1) (2016) 169 – 180.
[35] V. Seregin, Y. He, Common SHM test conditions and software reference configurations, in: document JCTVC-O1009, Geneva, Switzerland, 2013.
[36] N. Taneja, B. Raman, I. Gupta, Selective Image Encryption in Fractional Wavelet Domain, AEU-International Journal of Electronics and Communications 65 (4) (2011) 338–344.
[37] N. Taneja, B. Raman, I. Gupta, Chaos Based Partial Encryption of SPIHT Compressed Images, International Journal of Wavelets, Multiresolution and Information Processing 9 (02) (2011) 317–331.
[38] I.-R. B.-. Recommendation, Methodology for the subjective assessment of the quality of television picture, Geneva.
[39] N. Sidaty, W. Hamidouche, O. Deforges, Subjective evaluation methodology for selective encryption, EEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2017).
[40] H. E. H. Ahmed, H. M. Kalash, O. Allah, Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images, in: International Conference on Electrical Engineering (ICEE), 2007, pp. 1–7. doi:10.1109/ICEE.2007.4287293.
[41] N. K. Pareek, V. Patidar, K. K. Sud, Diffusion Substitution based Gray Image Encryption Scheme, Digital Signal Processing 23 (3) (2013) 894–901.
[42] W. Yue, N. J. P, A. Sos, NPCR and UACI randomness tests for image encryption, Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT) (2011) 31–38.
[43] F. Maleki, A. Mohades, S. M. Hashemi, M. E. Shiri, An Image Encryption System by Cellular Automata with Memory, in: Third International Conference on Availability, Reliability and Security, IEEE, 2008, pp. 1266–1271.
[44] E. Biham, A. Shamir, Differential cryptanalysis of des-like cryptosystems, Journal of CRYPTOLOGY 4 (1) (1991) 3–72.
[45] S. Singh, The code book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Random House Digital, Inc., 2011.
[46] S. Bruce, Applied Cryptography: Protocols, Algorithms, and Source Code in C, ISBN 0-471-12845-7, John Wiley & Sons, Second Edition, 1996.
[47] A. Said, Measuring the Strength of Partial Encryption Schemes, in: IEEE International Conference on Image Processing (ICIP), Vol. 2, 2005, pp. II–1126–9. doi:10.1109/ICIP.2005.1530258.
[48] Cryptopp: C++ software encryption library, in: http://www.cryptopp.com.

Wassim Hamidouche received the Engineering Degree in Computer Science from the University of Sciences and Technologies of Algiers, Algeria, in 2006 and the Master Degree in Electrical Engineering from the University of Poitiers, France, in 2007. He received Ph. D. Degree in Signal and Image Processing from the University of Poitiers, France in 2010. From 2011 to 2012 he has been a Research Engineer with Canon Research Centre, Rennes, France, where he worked on video compression standard High Efficiency Video Coding (HEVC) and its scalable extension SHVC. Since 2013 he has been a research engineer with the IETR laboratory, IMAGE group, Rennes, France. His research interests focus on efficient real time and parallel architectures for the new generation video coding standard, multimedia transmission over heterogeneous networks, and multimedia content security. Since 2015 he has been an associate professor at INSA Rennes.

Mousa Farajallah received his bachelor degree in electrical and computer engineering from Palestine Polytechnic University, Palestine 2006, master degree in electronics and computer engineering from Alquds university in Jerusalem, Palestine, in 2010. He did a pre-Phd courses in cryptography in Saarland university, Germany, in 2012. and finally the PhD in INSA Rennes and IETR Lab at LUMAN university (NANTES University) since September 2012 to 2015. His PhD topic is crypto-compression system for image and video. From 2015 to 2016, he is assistant professor at Palestine Polytechnic University (PPU) teaches cryptography for master students and information security for bachelor. Currently, he is the head of the Computer Engineering and Security Department at PPU. His research interests are in the area of cryptography, security issues of image and video He serves on the program committee of ISTP workshop in conjunction with ICITST, International Journal of Bifurcation and Chaos and reviewer for many other international journals.

Naty Sidaty received the Engineer and Master degrees in telecommunications and electronics from the National Engineering School of Tunis, Tunisia 2010, and Limoges University, France 2011, respectively. He received the PhD degree in signal and image processing from the University of Poitiers in 2015. He is currently a postdoctoral research at IETR Lab/INSA of Rennes, France. His research interests include Visual Attention Modeling, Video Quality Assessment (SDR and HDR), Video Security (HEVC Perceptual Encryption) and New Coding Tools (HEVC, JEM).

Olivier Déforges is a professor at National Institute of Applied Sciences of Rennes (INSA). He received a Ph.D. degree in image processing in 1995. In 1996, he joined the Department of Electronic Engineering at the INSA of Rennes, Scientific and Technical University. He is a member of the Institute of Electronics and Telecommunications of Rennes (IETR), UMR CNRS 6164 and leads the IMAGE team of the IETR laboratory (40 peoples). O. Déforges authored more than 130 technical papers. His principal research interests are image and video lossy and lossless compression, image understanding, fast prototyping, and parallel architectures. O. Déforges has also been involved the ISO MPEG standardization group since 2007.

Safwan El Assad received his PhD degree in electrical engineering from the University of Lille 1, France in 1987. His doctoral thesis was on electromagnetic compatibility. He joined the University of Nantes, France in September 1987, where he is now an Associate Professor. From 1988 to 1996, his main area of research was in radar imaging, remote sensing, signal and images processing. From 1996 until 2002, he developed topics in digital communications, adaptive equalization for digital channels by neural network, and e-learning. His current research area is focus on chaos-based information hiding and security including: Chaos-based crypto and crypto-compression systems for images and videos; chaos-based watermarking and steganography systems. He has supervised 11 PhDs (Current 3) and 23 Master students. He worked on 4 European projects and he published (as an author, co-author) more than 150 papers in refereed international journals and conference proceedings, as well as books and 3 patents.

Highlights

- We proposed a real-time selective and format complaint video encryption solution in the scalable extension of (HEVC) standard.
- The proposed solution is preserving all scalability functionalities.
- We derived the optimal value of the encryption quality security measurement.
- The encryption process is performed at the CABAC binstring level and fulfils both constant bitrate and format compliant video encryption requirements