HAL
open science

Privacy Protection in Real Time HEVC Standard Using Chaotic System

Mohammed Abu Taha, Wassim Hamidouche, Naty Sidaty, Marko Viitanen, Jarno Vanne, Safwan El Assad, Olivier Déforges

To cite this version:

Mohammed Abu Taha, Wassim Hamidouche, Naty Sidaty, Marko Viitanen, Jarno Vanne, et al.. Privacy Protection in Real Time HEVC Standard Using Chaotic System. Cryptography, 2020, 4 (2), pp.18. 10.3390/cryptography4020018 . hal-02880672

HAL Id: hal-02880672

https://hal.science/hal-02880672v1

Submitted on 29 Sep 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

cryptography

MDPI

Article

Privacy Protection in Real Time HEVC Standard Using Chaotic System †

Mohammed Abu Taha [1,*], Wassim Hamidouche [2,3], Naty Sidaty [2,3], Marko Viitanen [4], Jarno Vanne [4], Safwan El Assad [3,5] and Olivier Deforges [2,3]

1 College of Information Technology and Computer Engineering, Palestine Polytechnic University, Hebron PO BOX: 198, Palestine
2 Institut National des Sciences Appliquées de Rennes (INSA Rennes), 35708 Rennes CEDEX 7, France; wassim.hamidouche@insa-rennes.fr (W.H.); Naty.Sidaty@insa-rennes.fr (N.S.); olivier.deforges@insa-rennes.fr (O.D.)
3 Institut d'Électronique et de Télécommunication de Rennes (IETR), 35700 Rennes, France; Safwan.El-Assad@univ-nantes.fr
4 Faculty of Information Technology and Communication Sciences, Tampere University of Technology, 33720 Tampere, Finland; Marko.Viitanen@tut.fi (M.V.); jarno.vanne@tut.fi (J.V.)
5 Département Électronique et Technologies Numériques, Université de Nantes, 44300 Nantes, France
* Correspondence: m_abutaha@ppu.edu
† The paper is an extented version for our paper published in 26th European Signal Processing Conference (EUSIPCO 2018), Rome, Italy, 3–7 September 2018.

Received: 26 April 2020; Accepted: 18 June 2020; Published: 24 June 2020

Abstract: Video protection and access control have gathered steam over recent years. However, the most common methods encrypt the whole video bit stream as unique data without taking into account the structure of the compressed video. These full encryption solutions are time and power consuming and, thus, are not aligned with the real-time applications. In this paper, we propose a Selective Encryption (SE) solution for Region of Interest (ROI) security based on the tile concept in High Efficiency Video Coding (HEVC) standards and selective encryption of all sensitive parts in videos. The SE solution depends on a chaos-based stream cipher that encrypts a set of HEVC syntax elements normatively, that is, the bit stream can be decoded with a standard HEVC decoder, and a secret key is only required for ROI decryption. The proposed ROI encryption solution relies on the independent tile concept in HEVC that splits the video frame into independent rectangular areas. Tiles are used to pull out the ROI from the background and only the tiles figuring the ROI are encrypted. In inter coding, the independence of tiles is guaranteed by limiting the motion vectors of non-ROI to use only the unencrypted tiles in the reference frames. Experimental results have shown that the encryption solution performs secure video encryption in a real time context, with a diminutive bit rate and complexity overheads.

Keywords: selective encryption; Region of Interest (ROI); chaotic system

1. Introduction

High Efficiency Video Coding (HEVC) is the newest video coding standard issued by the Video Coding Experts Group (VCEG) and the ISO/IEC Moving Picture Experts Group (MPEG) [1]. The most important goal of the HEVC standardization efforts is to let 50% bitrate decrease for similar video quality [2], in contrast to its ancestor H.264/Advanced Video Coding (AVC) [3]. In the future, HEVC is expected to substitute the previous video coding standards in the trend applications, such as High Dynamic Range (HDR), Virtual Reality (VR), High Frame Rate (HFR), ultra high resolutions (4K and 8K), and so forth. In such applications, security and confidentiality of image and video content are of

fundamental importance for privacy protection. Thus, several studies have been committed to these goals in the last decade.

In general, the most regular approach for content protection is to encrypt the whole bit stream. In this method, the video bit stream is addressed as simple text data without taking into consideration the structure of the compressed video, and it is decodable only after the right decryption, although only some parts of the video are encrypted. This method limits the usage of the content to only users who have access rights to the encrypted parts. In addition, these algorithms are time and power consuming and not proper for real-time video applications mainly on mobile platforms. Consequently, Selective Encryption (SE) has emerged as a beneficial solution to these full encryption problems [4–7].

The main objective of SE is to decrease the amount of information to encrypt while keeping an adequate level of security. Thus, only the most sensitive information in the bit-stream is encrypted. In this work, we concentrate on SE that only hides the Region of Interest in the video (human faces, personal data, etc.) and retains the background of the video as is. In our approach, the HEVC frames is first divided into independent rectangular sections called tiles [8] and then only the tiles relating to the ROI are encrypted.

The proposed work encrypts a group of HEVC parameters encompassing Motion Vector Differences (MVD), Motion Vector (MV) signs, Transform Coefficient (TC), TC signs, as given in Reference [9]. Moreover, we propose a format-compliant encryption algorithm of the luma and chroma Intra Prediction Modes (IPM). The proposed SE solution relies on the chaos-based stream cipher which based on a chaotic keystream generator published in References [10,11]. It includes a set of HEVC coding restrictions to deny the encryption propagation out of the ROI under an Inter coding configuration. The encryption and decryption operations are endorsed in practice by implementing them in the real-time *Kvazaar* HEVC [12] encoder and the *OpenHEVC* decoder [13], respectively.

The rest of this paper is organized as follows—Section 2 presents the background related to the HEVC standard and selective video encryption. The proposed selective encryption of IPM and ROI encryption in HEVC are investigated in Sections 3 and 4, respectively. Performance evaluations and associated discussion are given in Section 5. Finally, Section 6 concludes the paper and gives some perspectives for the future work.

2. Related Works

2.1. HEVC Standard

The emerging tools, defined in the HEVC standard, involve larger coding blocks, quad-tree block partitioning, more precise Intra and Inter predictions, optimized entropy coding, and the new in-loop Sample Adaptive Offset (SAO) filter. The HEVC video frame is divided into square Coding Tree Unit (CTU) of fixed size, from 16×16 up to 64×64 pixels. Each CTU can be recursively divided through a quad-tree partitioning method to Coding Unit (CU). In YUV color representation, the CUs consist of three Coding Block (CB), one for luma and two for chroma. The decision between intra or inter prediction is carried out at the CU level. CUs are predicted in intra mode from reconstructed neighbouring samples in the same slice. For I (Intra coded) slices, only intra prediction mode is used, whereas intra or inter prediction modes can be used in P and B slices [1,14]. In this section, we focus on three HEVC characteristics—entropy coding, Intra prediction mode, and parallelization approaches.

2.1.1. HEVC Entropy Coding

HEVC coding model identifies Context-Adaptive Binary Arithmetic Coding (CABAC) for entropy coding. The CABAC technique is composed of three main tasks—binarization, context modeling, and arithmetic coding [15]. These three functions are shown in Figure 1. The binarization function transform the syntax elements to binary symbols (bin). Five binarization methods are identified in HEVC—Unary (U), Truncated Unary (TU), Fixed Length (FL), Truncated Rice code with an adaptive context p (TRp), and the kth-order Exp-Golomb (EGk) codes. Subsequently, the context modeling

updates the probabilities of bins and, finally, the arithmetic coding compresses the bins into bits corresponding to the estimated probabilities. The arithmetic coding can be performed with context coding or with bypass coding. The first mode makes use of the estimated probabilities of syntax elements whereas the second one considers each bin with an equal probability of 0.5.

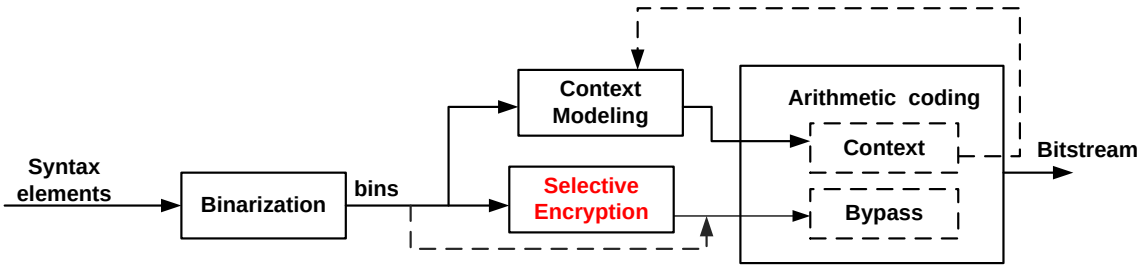


Figure 1. Main functions of CABAC engine.

2.1.2. Intra Prediction Modes

The HEVC encoder permits higher coding efficiency partly by offering 35 IPMs. These modes consist of one Planar (mode 0), one DC (mode 1), and 33 Angular modes (modes 2–34). For an effective coding of the 35 IPMs, a shortlist of the three Most Probable Mode (MPM) is defined in HEVC specifications. This list is derived from the IPMs of the neighbouring blocks and other fixed IPM. Three syntax elements are used to signal the IPM for a luma Prediction Block (PB) in the bitstream. As shown in Table 1, the first flag signals if the MPM are used, the second flag determines the first MPM, and the third flag references which one of the two last MPM is selected. Therefore, MPM0, MPM1, and MPM2 are coded by 2, 3, and 3 bits, respectively. The first bit in red color is coded using a CABAC context while other bins are bypass coded. The residual 32 modes out the MPM list are coded by a FL code with 5-bin that are bypass coded. In HEVC, an adaptive scanning method of TCs is utilized for the block of sizes of 4×4 and 8×8 to gain from the statistical distribution of the active coefficients in 2-D transform blocks. For modes (6-14), vertical scan is used, horizontal scan for modes (22-30), and diagonal scan for the rest of the modes. The chroma IPMs are derived from the luma IPMs if the Derived flag is set to 1. Otherwise, the chroma IPMs are then encoded by three bits [1,16]. Table 2 shows the derivation process of the chroma IPMs. If the derived chroma intra mode is congruent to the initial chroma intra mode, then the Intra angular mode (i.e., mode-34) is used for the chroma, otherwise, the derived one is used.

Table 1. High Efficiency Video Coding (HEVC) coding solution for Intra Prediction Modes (IPMs), where the first bit is coded using a CABAC context.

Number of bits	Code	Coded Mode
2	10	IPM0
3	110	IPM1
3	111	IPM2
6	000000 ⋮ 011111	32 remaining IPMs

Table 2. Derivation process of the chroma IPMs.

Chroma IPM	Luma IPM			
	0	**26**	**10**	**1**
Planar (mode 0)	34	0	0	0
Angular (mode 26)	26	34	26	26
Angular (mode 10)	10	10	34	10
DC (mode 1)	1	1	1	34
Derived (luma mode)	0	26	10	1

2.1.3. Tiles in HEVC

HEVC standard defines a new parallelization concept called Tiles [15,17,18] for parallel encoding/decoding of a single picture. The input frame can be divided into various tiles each of them comprises an integer number of an individually decodable Coding Tree Block (CTB). The number of tiles and the location of their boundaries can be defined consistently for the entire sequence or changed from picture to picture. Besides, the CABAC context is set at the starting of each tile. Tiles allow a flexible classification of CTU. in addition, tiles provide a favored correlation of pixels and a excellent coding efficiency over slices as they do not have a header information.

2.2. Selective Video Encryption

Nowadays, a set of encryption algorithms has been devoted for HEVC videos. Shahid et al. [19] introduced a joint compression and SE solution that lies on CABAC bin strings. Hamidouche et al [9,20] published a selective chaos-based crypto-compression system for HEVC and its scalable extension Scalable High efficiency Video Coding (SHVC) [21]. Boyadjis et al. [22] presented an extended SE solution for H.264/AVC and HEVC streams. It solves the main security issues of SE: the security of contents concern to the amount of information leak over a secured video. The contribution in Reference [22] handles both numerical and visual enhancements of the encryption performance concerning some state-of-the-art solutions.

Many studies have recognized the encryption of ROI in the video content. Peng et al. [23] offered an encryption proposal for human faces in H.264/AVC video. This solution is based on Flexible Macroblock Ordering (FMO) and chaos. Dufaux et al. [24] presented an efficient methodology to encrypt ROI using code stream-domain encryption. Research in Reference [25] facilitated rectangular region privacy by de-recognising faces. These approaches ensure that face recognition software cannot reliably recognize de-identified faces, even though part of the facial details are protected. In Reference [26], the writer examined the privacy protection in H.264/Scalable Video Coding (SVC) [27]. This solution tracks face areas (ROI) first and then encrypts them in the transform domain by scrambling the sign of the non-zero TCs at all SVC layers.

All of these studies do not take into account the specific HEVC tiles representations. In addition, no solution has investigated the Luma and Chroma IPMs encryption performances. This is the first study that handles the encryption of Luma and Chroma IPMs in HEVC standards. In the following sections, we present our proposed solution based on IPMs and chaos-based encryption systems as well as the ROI encryption implementation in HEVC encoder.

3. Proposed Video Encryption System

3.1. Intra Prediction Parameters Encryption

In HEVC standard, there are three scanning orders of the quantized TCs. The scanning order is obtained for Intra blocks from the IPM. The proposed research encrypts the IPM with keeping the original scanning order of the modes (the order before encryption). This solution makes the IPM encryption format-compliant with HEVC, that is, decodable with any standard HEVC decoder.

Distinct from the encryption of other syntax elements, the encryption of the IPMs is processed before the entropy coding and, thus, may reduce Rate-Distortion (RD) performance.

The proposed encryption of IPMs is performed as depicted in Algorithm 1. First, the IPM items are classified into three sets: $Set_VER \in \{6, 7, 8, 9, 10, 11, , 12, 13, 14\}$, $Set_HOR \in \{22, 23, 24, 25, 26\,27, 28, 29, 30\}$, and $Set_DIA \in \{0, 1, 2, 3, 4, 5, 15, 16, 17, 18, 19, 20, 21, 31, 32, 33, 34\}$. Each set includes the prediction modes that have the same scanning direction *(horizontal, vertical, or diagonal)*. The encryption process is performed using a circular shift operation. Each IPM, in a specific set, is shifted according to a key stream bits. The stream values, required to the encryption process, are generated by a key-stream generator based on chaos. Then, a new IPM position is inferred inside the same set. The chroma IPMs are derived from the luma IPMs according to Table 2. The derivation process of the chroma IPMs must depend on the encrypted luma IPMs to guarantee format-compliant encryption.

Algorithm 1 Encryption of IPMs.

Input: *Intra Prediction Mode* **IPM**
Output: *Encrypted Intra Prediction Mode* **E_IPM**

```
Set_VER ∈ {6, 7, 8, 9, 10, 11, 12, 13, 14}
Set_HOR ∈ {22, 23, 24, 25, 26, 27, 28, 29, 30}
Set_DIA ∈ {0, 1, 2, 3, 4, 5, 15, 16, 17, 18, 19, 20, 21, 31, 32, 33, 34}
Call chaotic generator to produce bit steam K
if IPM > 5 And IPM < 15 then
    E_IPM=Circular shift(Set_VER, IPM, K)
else if IPM > 21 And IPM < 31 then
    E_IPM=Circular shift(Set_HOR, IPM, K)
else
    E_IPM=Circular shift(Set_DIA, IPM, K)
end if
```

3.2. CABAC Level Encryption

The proposed encryption solution is realized at the CABAC bin string level for a set of sensitive HEVC parameters including MVs, MV signs, TCs, and TC signs. These syntax elements are processed as illustrated in Figure 1. Selectively encrypted HEVC bitstreams are format compliant and accomplish the real-time requirements.

3.3. Encryption System Based on Chaos

Our encryption system relies on chaos, which is a state of dynamical systems whose apparently-random states of disorder and irregularities are often governed by deterministic laws that are highly sensitive to initial conditions. For a particular syntax element, the key-stream generator will generate the required key streams needed to get the ciphering data. The key stream generator is fostered from our previous work [10,11]. The internal state, which involves the main cryptographic complexity of the system, is consists by two third-order recursive filters. The first recursive cell contains a discrete Skew tent map and the second one contains a discrete piecewise linear chaotic map. These chaotic maps are performed as non-linear filters. A new initial vector IV value is produced in each keystream generator call. This value allows to produce a different key stream sequence on each generator call. The detailed structure and the cryptographic security analysis of the key stream generator is elaborated in Reference [10]. The scheme of our key stream generator based on a chaotic map is depicted in Figure 2. The proposed system use the chaos based stream cipher to encrypt the sensitive bits in the frame. This encryption algorithm, as mentioned, relies on an efficient chaotic generator that uses two chaotic recursive filters, a technique of disturbance and chaotic multiplexing. This is a kind of stream cipher encryption. Indeed synchronous stream cipher based on a chaotic generator have been used. The sender and the receiver needs the shared secrete key to operate the

chaos based generator in order to produce the key-streams used in the encryption and the decryption process the structure of this encryption system is figured out in Figure 3. The equations of the *Discrete* Skew Tent and *Discrete* PWLCM maps are respectively given by [10]:
Discrete Skew Tent Map:

$$X_s[n] = \begin{cases} \left\lceil 2^N \times \frac{X_s[n-1]}{P1} \right\rceil & \text{if } 0 < X_s[n-1] < P1 \\ 2^N - 1 & \text{if } X_s[n-1] = P1 \\ \left\lceil 2^N \times \frac{2^N - X_s[n-1]}{2^N - P1} \right\rceil & \text{if } P1 < X_s[n-1] < 2^N \end{cases} . \quad (1)$$

Discrete PWLCM map:

$$X_p[n] = \begin{cases} \left\lceil 2^N \times \frac{X_p[n-1]}{P2} \right\rceil & \text{if } 0 < X_p[n-1] \leq P2 \\ \left\lceil 2^N \times \frac{X_p[n-1] - P2}{2^{N-1} - P2} \right\rceil & \text{if } P2 < X_p[n-1] \leq 2^{N-1} \\ \left\lceil 2^N \times \frac{2^N - P2 - X_p[n-1]}{2^{N-1} - P2} \right\rceil & \text{if } 2^{N-1} < X_p[n-1] \leq 2^N - P2 \\ \left\lceil 2^N \times \frac{2^N - X_p[n-1]}{P2} \right\rceil & \text{if } 2^N - P2 < X_p[n-1] \leq 2^N - 1 \\ 2^N - 1 - P2 & \textit{otherwise} \end{cases} . \quad (2)$$

The values produced $X_s[n], X_p[n]$ by the recursive cells in the `internal state` are entered to the `output function`. Then, the output sequence $Xg(n)$ is obtained using a chaotic multiplexing controlled by the chaotic sequence $Xth = X1_s(n-1) \oplus X1_p(n-1)$ and by a threshold $Th = 2^{N-1}$, as shown in and Equation (3), or by xoring $X1_s$ and $X1_p$ as clarified in Equation (4).

$$Xg(n) = \begin{cases} X_s(n), & \text{if } 0 < Xth \leq Th \\ X_p(n), & \text{otherwise} \end{cases} \quad (3)$$

$$Xg(n) = X_s(n) \oplus X_p(n). \quad (4)$$

To evaluate the statistical performances of the keystream produced, we also use one of the most popular test for investigating the randomness of binary data, namely the NIST statistical test [28]. This test is a statistical package that consists of 188 tests and sub-tests that were proposed to assess the randomness of arbitrarily long binary sequences. These tests focus on a variety of different types of non-randomness that could exist in a sequence. We generated 100 different binary sequences, each with a different secret key, and 31,250 samples (corresponding to 1 million bits); we used the NIST test on all of these entities. For each test, a set of 100 P_value is produced and a sequence passes a test whenever the $P_value \geq \alpha = 0.01$, where α is the level of significance of the test. A value of $\alpha = 0.01$ means that 1% of the 100 sequences are expected to fail. The proportion of sequences passing a test is equal to the number of $P_value \geq \alpha$ divided by 100. In Figure Figure 4 we present the obtained proportion versus test for delay 1. As we can see, all the 188 tests and sub-tests pass the NIST. Notice that the minimum pass rate for each statistical test, with the exception of the random excursion variant test, is approximately= equal to 0.960150 for 100 binary sequences. The minimum pass rate for the random

excursion variant test is approximately 0.952091 for a sample size =62 binary sequences. Our algorithm passed all the NIST tests as shown in Table 3.

The encryption of syntax elements at the CABAC level, including MV differences, MV signs, TCs, and TC signs, is given by the the following formula:

$$C_i = P_i \oplus X_i, \tag{5}$$

where P_i refers to the syntax elements, C_i the encrypted syntax elements and X_i the key stream bits. In addition, the encryption of the luma and chroma IPMs is carried out as follows:

Let N be the number of items in the vector $V = [\mathrm{IPM}_1, \mathrm{IPM}_2, \cdots, \mathrm{IPM}_N]$, $V \in \mathbb{Z}^N$, X_i the key stream bits generated by key-stream generator, and j the index of the IPM to encrypt in the vector V. The new value, IPM_{encr}, produced for the current IPM of index j is given as follows:

$$\mathrm{IPM}_{encr} = V[(j + X_i) \mod N]. \tag{6}$$

The decryption algorithm is performed by inverse operations of (5) and (6). Finally, the secret key that is used to initialize the chaotic generator must be shared between the encoder and the decoder.

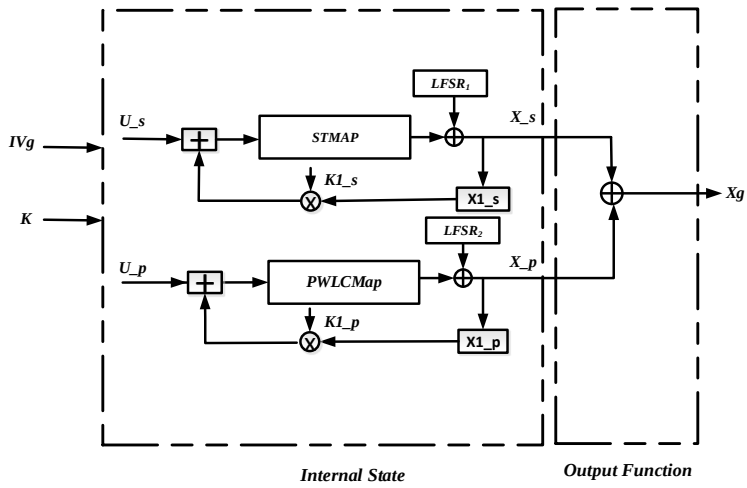


Figure 2. General structure of chaos based generator.

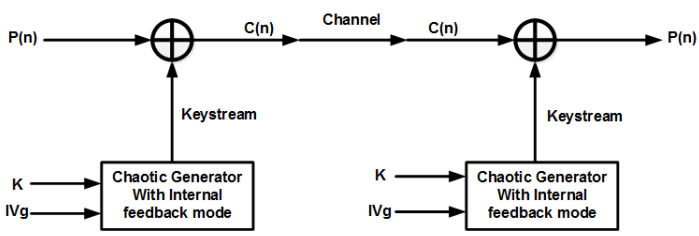


Figure 3. Stream cipher encryption.decryption structure.

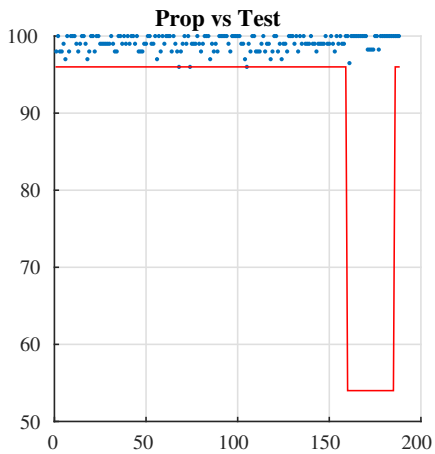


Figure 4. NIST Test with delay 1.

Table 3. Nist Test values with delay 1.

Test	*P*_Value	Proportion
Frequency test	0.637	100.000
Block-frequency test	0.956	98.000
Cumulative-sums test	0.715	99.500
Runs test	0.720	98.000
Longest-run test	0.055	98.000
Rank test	0.554	99.000
FFT test	0.109	100.000
nonperiodic-templates	0.546	98.973
overlapping-templates	0.2256	99.000
universal	0.994	99.000
approximty entropie	0.575	99.000
random-excursions	0.428	97.581
random-excursions-variant	0.428	98.925
serial test	0.519	99.000
linear-complexity	0.740	98.000

4. ROI Encryption Implementation in HEVC Codec

4.1. ROI Encryption System Based on Tiles

The presented ROI encryption is based on the tile concept inserted in HEVC. This technique divides the video image into various rectangles with integer number of blocks, where Intra prediction and entropy coding dependencies are cracked at the tile borders. The proposal encrypts only the tiles comprising the ROI, while the non ROI tiles stay clear (not encrypted). A group of most sensitive HEVC parameters, including MVs, MV signs, TCs, and TC signs, after that, they are encrypted at the CABAC bin string level to decrease the visual quality of the ROI. This is done in format compliant with HEVC and with a constant bitrate of the encrypted videos. In addition to these four parameters, we implemented the HEVC format compliant encryption of IPMs, which may come with a slight raise in the bit rate.

4.2. Encryption Propagation in Inter Video Coding

The merge mode in HEVC deduces *MVs* from a list of spatial neighbouring and temporal candidates. Referring to these candidates can broadcast encryption from the encrypted tiles to the background, when the ROI is not correctly decrypted. Thus, we force the temporal candidates of the background tiles to be inside the background region in the reference frame. In order to prevent the

propagation of encryption outside the ROI tile, two non-normative encoding constraints are used in the *Kvazaar* encoder (as shown in Figure 5):

1. The *MVs* of the predicted block are restricted to point only to the co-located tile of the reference frame.
2. The in-loop filters are disabled across the tile boundaries.

These two constraints tend to have a negative influence on RD performance, depending on the resolution, tiling configuration, and the video content. However, they ensure a safe interpolation process at the tile boundaries.

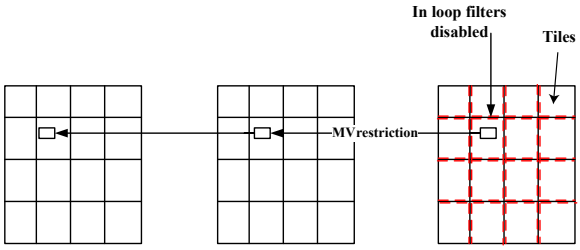


Figure 5. MVs and in-loop filter restrictions.

5. Results and Discussion

5.1. Experiments

The proposed SE encryption solution is implemented in the HEVC test Model (HM) version 16.7 [29] and tested using All Intra (AI) and Random Access (RA) coding configurations. The ROI-based encryption and decryption algorithms are integrated in the *Kvazaar* HEVC real time encoder and *OpenHEVC* decoder, respectively. In this experiment, Nine video sequences from different classes and categories were used. These videos, of 10 s duration each (except *PeopleOnStreet* of 5 s), taken from HEVC common test conditions [16], are listed in Table 4. They are jointly encoded and encrypted, in both Intra and Inter coding configurations, at four Quantization Parameter (QP)s, where $QP\ values \in \{22, 27, 32, 37\}$. The encrypted videos are encoded with two uniform tiling configurations—4×3 (i.e., four horizontal by three vertical repartition) and 4×4. The same encoder configuration, without tiles and encryption, is used as a reference. The processor used in these experiments has 32-bit 4-core Intel Core i5 processor, running at 2.60 GHz with 16 GB of main memory. The operating system is Ubuntu 14.04 Trusty Linux distribution.

Table 4. Benchmarks of video sequences used in the experiment.

Sequence	Class	Resolution	Frame Rate
PeopleOnStreet	A	2560×1600	30
Kimono	B	1920×1080	24
ParkScene	B	1920×1080	24
BasketballDrive	B	1920×1080	50
Cactus	B	1920×1080	50
BQTerrace	B	1920×1080	60
Vidyo1	E	1280×720	60
Vidyo3	E	1280×720	60
Vidyo4	E	1280×720	60

In the following, we elaborate in detail the performance of the proposed encryption system. It is noteworthy that two HEVC platforms are used in this study (HM and *Kvazaar* /*OpenHEVC*). The first one is the selective encryption (whole frame), which is performed under the HM encoder/decoder. Several objective measurements have been applied—Peak Signal-to-Noise Ratio (PSNR), Structural SIMilarity (SSIM), IPMs Bjøntegaard Delta Bit Rate (BD-BR) [30] evaluations. The second one is the

ROI-based encryption that is implemented using *Kvazaar* encoder/*OpenHEVC* decoder and other metrics to assess the encryption that has been used—complexity evaluation, BD-BR with PSNR and SSIM.

5.2. Objective Measurements

5.2.1. Video Quality Metrics

PSNR and the SSIM are applied to validate the quality of the encrypted videos. The quality of the video after encryption gives an indication of the level of the visual content and, thus, the encryption solution consistency. The results of these two metrics, using original and encrypted ROI solutions, are given in Tables 5 and 6. The average PSNR inside the ROI, for all encrypted sequences, still below 11.2 dB and the SSIM values are below 0.22. According to quality concepts, the obtained results give a strong indication that the video quality is degraded very much. In addition, despite the diversity of QP, video quality is degraded at different bit-rates. Furthermore, the known plain-text attack is impracticable.

Table 5. Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity (SSIM) values of original and encrypted videos encoded by *Kvazaar* (QP = 22).

Sequence	Original		Encrypted ROI	
	PSNR	SSIM	PSNR	SSIM
PeopleOnStreet	42.7	0.92	11.1	0.22
Kimono1	42.1	0.95	9.8	0.22
ParkScene	42.2	0.90	10.76	0.21
Cactus	42.4	0.93	10.3	0.21
BQTerrace	41.7	0.90	10.7	0.22
BasketballDrive	41.4	0.95	10.0	0.22
Vidyo1	45.3	0.91	11.2	0.20
Vidyo3	44.5	0.93	10.8	0.20
Vidyo4	44.7	0.90	11.0	0.21

Table 6. PSNR and SSIM for three sequences encoded by HM with various QP.

Sequence	QP	Original-PSNR			SE-PSNR			Original-SSIM			SE-SSIM		
		Y	U	V	Y	U	V	Y	U	V	Y	U	V
BasketballDrive (B)	22	42.1	43.5	44.9	10.2	10.8	11.1	0.92	0.94	0.94	0.21	0.22	0.24
	27	41.3	42.2	43.6	10.1	10.7	11.0	0.89	0.91	0.93	0.2	0.21	0.21
	32	37.5	38.8	39.1	9.8	10.5	10.9	0.76	0.72	0.88	0.16	0.18	0.22
	37	36.7	37.9	38.1	8.1	8.9	10.1	0.74	0.78	0.81	012	0.16	0.18
Kimono1 (B)	22	43.7	44.1	45.1	9.5	10.1	10.3	0.96	0.96	0.99	0.17	0.18	0.19
	27	42.3	42.9	43.1	9.1	10.0	10.1	0.95	0.98	0.98	0.17	0.17	0.19
	32	38.8	38.9	39.9	8.5	9.9	10.3	0.82	0.83	0.88	0.14	0.16	0.18
	37	37.8	38.6	38.9	7.5	8.4	9.9	0.77	0.78	0.80	0.12	0.14	0.17
PeopleOnStreet (A)	22	38.6	41.4	43.4	10.2	10.6	11.3	0.95	0.95	0.97	0.19	0.19	0.22
	27	38.3	39.8	41.2	9.5	9.9	10.3	0.91	0.93	0.94	0.17	0.20	0.22
	32	37.0	38.1	40.6	8.9	9.3	10.1	0.88	0.90	0.92	0.18	0.19	0.21
	37	35.4	37.6	38.9	8.1	9.0	9.8	0.78	0.83	0.88	0.15	0.15	0.19

In Table 7, we provide a comparison in terms of **psnr,ssim!** (**psnr,ssim!**) objective metrics, between the proposed encryption solution and state-of-the-art encryption research examples. Our SE solution has a lower PSNR value compared to Reference [5] with fewer SSIM values than those given in References [5,22]. Furthermore, we applied PSNR and SSIM matrices, depicted in Tables 8 and 9, for two different encryption levels—(TC, TC signs, MV, MV signs) and (TC, TC signs, MV, MV signs, IPMs) in AI and RA coding configurations. When we put both encryption levels together the

encryption is powerful and also the results show the impact of quality degradation of IPMs encryption on the video sequences.

Table 7. Comparative evaluation, using weighted PSNR and SSIM for three sequences encoded by HM at (QP = 32).

Sequence	Wallendael et al. [5]		Boyadjis et al. [22]		Proposed SE	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
BasketballDrive	11.4	0.40	10.4	0.43	**9.9**	**0.17**
Kimono1	10.1	0.32	**6.6**	0.27	8.9	**0.14**
Vidyo1	12.9	0.61	11.2	0.55	**10.1**	**0.18**

Table 8. Average PSNR (Y) values in dB of the three video classes encoded by HM (QP = 22).

Class	Main Intra		Random Access	
	TC, TCs, MV and MVs	All	TC, TCs, MV and MVs	All
B	11.1	**10.2**	10.4	**10.2**
D	9.3	**8.9**	8.7	**8.4**
E	10.2	**9.6**	9.7	**9.1**

Table 9. Average SSIM values of the three video classes encoded by HM used (QP = 22).

Class	Main Intra		Random Access	
	TC, TCs, MV and MVs	All	TC, TCs, MV and MVs	All
B	0.33	**0.25**	0.30	**0.21**
D	0.26	**0.20**	0.23	**0.18**
E	0.22	**0.19**	0.20	**0.17**

5.2.2. BD-BR Rate Evaluation

We consider the BD-BR metric [30], which indicates the differences between two bit-rate-PSNR curves.

The process of the encoding is carried out for both cases of coding Inter and Intra considering 4×4 and 4×3 tile repartitions, taking into account the limitations with MVs and the in-loop filters disabling across the tile edges. In Tables 10 and 11 we provide the magnitude of RD losses with Intra and Inter coding configurations of the two tiles configurations. As we noticed, the overhead in the bit rate range of 2% and 18.23% comes from the restrictions of the MVs depending on the coding configuration (Inter and Intra), video content and number of tiles within the frame.

The BD-BR loss for 4×4 tiles repartition in Inter coding is larger than the loss in Intra coding configuration and extends to 12.33% and 5.36%, respectively. The BD-BR loss for 4×3 tiles repartition is less than the loss for 4×4 tiles in both coding configurations. For example, the loss in BD-BR of *Parkscene* (1920×1080) video sequence with 4×3 and 4×4 tiles with Inter coding configuration is around 8.55% and 9.81%, respectively. This variation in loss is comes from the limitations related to tile coding: the in-loop filtering disabling across tiles and the restrictions on MVs in the higher number of tiles configuration (4×4). While, using Intra coding configurations the BD-BR loss is remains minimal and it doesn't transcend 4.13% and 5.16%, respectively. For example the BD-BR loss for *PeopleOnStreet* (2560×1600) video sequence is 5.01% and 3.11% in Inter coding and 3.55%, 2.04% in Intra coding configuration. The restrictions in coding slightly reduce the BD-BR efficiency and this is due to the nature of video sequence content and resolution.

The IPMs encryption makes a Little bit-rate increase, The expense of increase is more in Inter coding configurations wherase in Intra blocks are less frequent than in Intra configuration. Figure 6 shows the RD performance using the average bit-rate variation between two bit-rate-wPSNR (weighted PSNR calculated after the right decryption) curves for *BasketballDrive* video sequence with and without encryption. As depicted in Figure 6, the IPMs encryption conducts to a minimal BD-BR loss.

Table 10. BD-rate and complexity of the proposed encryption solution in Intra and Inter coding. Nine video sequences, encoded by Kvazaar (4 × 4 tile configuration), are used.

Resolution	Sequence	Intra Coding (4 × 4 Tiles)			Inter Coding (4 × 4 Tiles)		
		Bit Rate Loss (%)	Complexity Increase (%)		Bit Rate Loss (%)	Complexity Increase (%)	
		BD-Rate	Encoding	Decoding	BD-Rate	Encoding	Decoding
2560 × 1600	*PeopleOnStreet*	3.67	3.05	1.87	5.13	3.27	2.88
1920 × 1080	*Kimono1*	5.16	3.16	1.21	13.19	3.87	1.96
	ParkScene	4.09	2.34	1.13	9.81	3.08	1.89
	Cactus	5.43	2.82	2.02	7.65	3.96	2.19
	BQTerrace	7.18	2.19	1.67	18.23	3.54	1.93
	BasketballDrive	6.34	3.16	2.15	17.11	3.78	2.44
1280 × 720	*Vidyo1*	4.21	2.13	1.32	13.87	2.60	1.91
	Vidyo3	6.17	2.31	1.41	10.08	2.98	2.07
	Vidyo4	6.01	2.25	1.48	15.91	2.71	1.88
Average		5.36	2.60	1.58	12.33	3.31	2.12

Table 11. BD-rate and complexity of the proposed encryption system in Intra and Inter coding. Nine video sequences, encoded by *Kvazaar* (4 × 3 tile configuration), are used.

Resolution	Sequence	Intra Coding (4 × 3 Tiles)			Inter Coding (4 × 3 Tiles)		
		Bit Rate Loss (%)	Complexity Increase (%)		Bit Rate Loss (%)	Complexity Increase (%)	
		BD-Rate	Encoding	Decoding	BD-Rate	Encoding	Decoding
2560 × 1600	*PeopleOnStreet*	2.14	2.11	1.12	3.42	2.16	1.71
1920 × 1080	*Kimono1*	4.13	2.13	1.01	11.65	2.48	1.63
	ParkScene	3.68	1.98	1.06	8.55	2.18	1.12
	Cactus	3.14	1.68	1.22	5.12	2.56	1.67
	BQTerrace	4.32	1.67	1.10	12.56	2.14	1.73
	BasketballDrive	4.74	1.36	1.17	13.49	2.68	1.41
1280 × 720	*Vidyo1*	2.08	1.43	1.15	9.19	1.93	1.43
	Vidyo3	4.65	1.21	1.08	7.81	1.68	1.47
	Vidyo4	4.79	1.64	1.33	11.02	1.98	1.39
Average		3.74	1.69	1.13	9.20	2.19	1.50

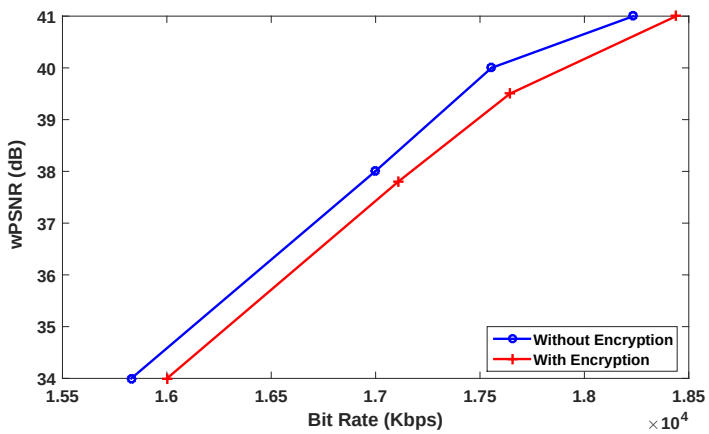


Figure 6. Rate distortion for proposed IPMs encryption for *BasketballDrive* video sequence encoded by HM.

5.2.3. Encryption Quality

Encryption Quality (EQ) is a measure of the difference between the frequency of repetition for each gray level using encryption and without using it. The maximum EQ value is calculated using the following two equations, as given in [31], see Appendix A:

$$EQ = \frac{\sum_{i=0}^{255} |o_i(P) - o_i(C)|}{256}, \tag{7}$$

where $o_i(C)$ are the observed occurrence for the gray level i in the encrypted frame C, and $o_i(P)$ are the observed occurrences of the same gray level i in the plain frame P.

$$EQ_{max} = \frac{510 \times L \times W}{256^2}, \tag{8}$$

where L and W are the hight and the width of the gray frame.

The larger the EQ value, the better the encryption security is. The maximum EQ value of a given video frame of *Kimono1*, *PeopleOnStreet* and *Vidyo1* sequences are equal to 16,136, 31,875 and 7171, respectively [32]. In Table 12 we provide the EQ value. The results indicate that the EQ values of our encryption solution with two video sequences (*Kimono1* and *PeopleOnStreet*) are higher compared to results given by EQ [32]. This enhancements is brought by the IPM encryption that not examined in [32].

Table 12. The EQ for proposed SE and the state of the art [32] (QP = 22) encoded by HM.

Sequence	EQ in [32]	EQ of Proposed SE
Kimono1	8996	**10192**
PeopleOnStreet	14884	**18965**
Vidyo1	–	**4288**
Vidyo3	–	**4319**
Vidyo4	–	**4380**

5.3. Entropy Analysis

The Information entropy is the probability of occurrence for each symbol in the video frame [33]. the value of the entropy should be 8 for the truly random frame. Table 13 shows that the probability of the occurrence of each encrypted block in the encrypted video frame number 15 by the proposed chaos-based SE scheme is near to the theoretical value 8. This indicates that the proposed scheme is secure and robust against the entropy attack.

Table 13. Entropy of frame number 30 for different video sequences.

Sequence	Information Entropy
PeopleOnStreet	7.10
Kimono	7.23
ParkScene	7.50
BasketballDrive	7.44
Cactus	7.35
BQTerrace	7.21
Vidyo1	7.01
Vidyo3	7.34
Vidyo4	7.21

5.3.1. Key Security

From the generated sequences, it is impossible to find the secret key; this is because of the structure of the chaotic generator which also includes a `chaotic switching`. The knowledge of part of the secret key is not very useful for an attacker because of the intrinsic property of the chaotic signal, which is extremely sensitive to the secret key. The size of the secret key, formed by all the initial conditions and by all the parameters of the system, varies from `299 bits`, with delay = 1, to `555 bits`, with delay = 3. This means that the brute force attack is impracticable.

5.3.2. Visual Analysis

Visual encryption investigation is applied to assess the unrecognizable level of the videos after encryption. Encrypted video is marked as of top level of visual security if the deformity of the

encrypted video is too messy to be realized. We applied the Edge Differential Ratio (EDR) which evaluates the edges variations between the original and the encrypted images, with RA encoding configuration [34], using the Laplacian of Gaussian method [35]. The proposed encryption method is highly efficient when the edges of the encrypted frames are not remarkable. The EDR is calculated as:

$$EDR = \frac{\sum_{i=0}^{h-1} \sum_{j=0}^{w-1} |P_E(i,j) - C_E(i,j)|}{\sum_{i=0}^{h-1} \sum_{j=0}^{w-1} |P_E(i,j) + C_E(i,j)|}, \tag{9}$$

where P_E and C_E are the edge detected binary matrix for the plain and cipher frame, respectively. Figure 7 illustrates the visual impact of the proposed solution on the frame content. Figure 7b shows the distortion on visual content quality of the frame. Edges in the encrypted frame (Figure 7d) are completely affected compared to edges in the original frames (Figure 7c).

The common step for identifying and tracking the ROI in the video is to split the HEVC frame into tiles where all ROI are included in ROI tiles and the background in separated non ROI tiles [36]. In Figure 8, the tiles that include a human face represent the ROI tiles and the other tiles represent the background tiles. The proposed encryption solution performs a selective encryption of ROI tiles by encrypting the most sensitive HEVC syntax elements to decrease the visual quality of the ROI as described in Sections 3 and 4. Based on this figure, we can observe that the proposed encryption solution decreases the quality of the ROI zone while the background remains clean even in inter coding configuration. Videos decoded and decrypted with the correct key are illustrated on the right side while being decoded without decryption on the left side.

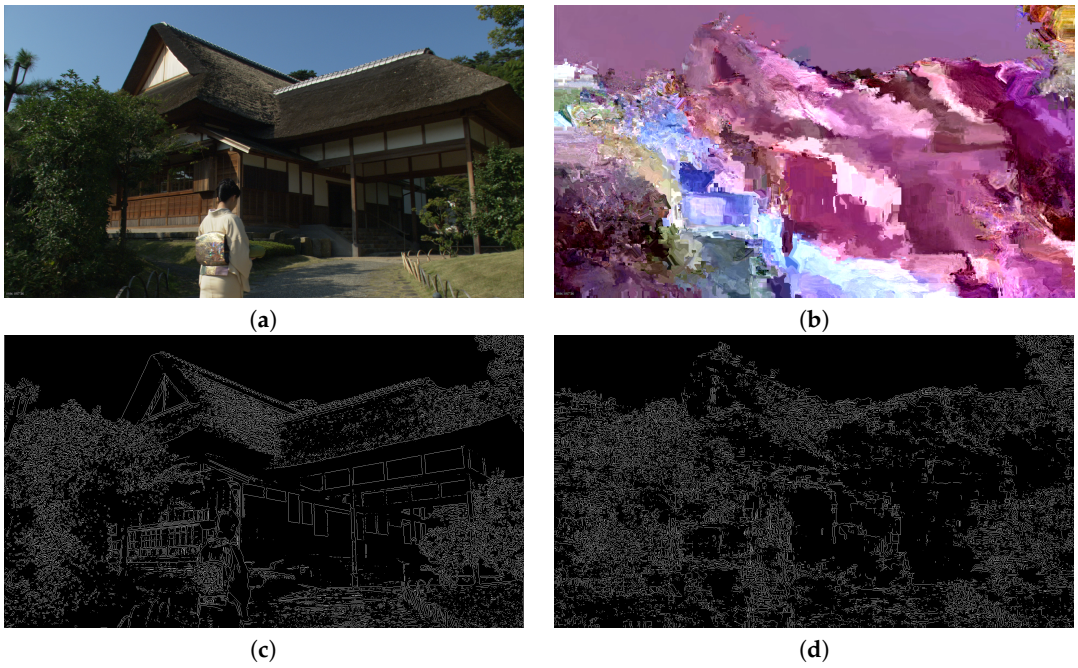


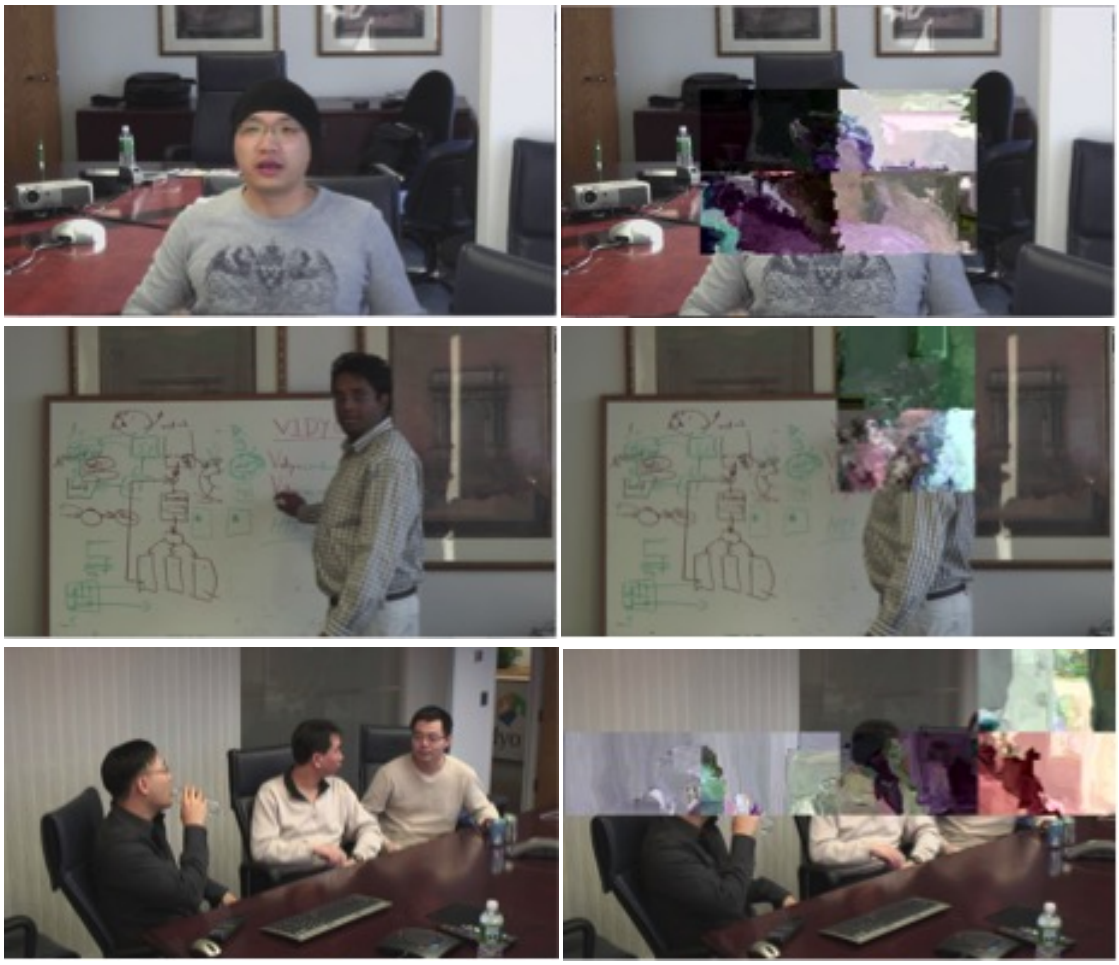
Figure 7. The edges of frame # 184 in Kimono1 video sequence encoded by HM. (**a**) Original frame without encryption; (**b**) Encrypted frame; (**c**) The edges of original frame; (**d**) The edges of encrypted frame.

The proposed real time selective solution performs a secure protection of privacy in the HEVC video content with a little overhead in bit rate and coding complexity. Traditional algorithms are more complex and require a longer time for execution, which is not suitable for real time applications such as live TV. The proposed system aims to gain a deep understanding of video data security of multimedia technologies and to provide security for real time video applications using selective encryption for HEVC. Although suggested in a number of specific cases, selective encryption could be much more widely used in consumer electronic applications ranging from mobile multimedia terminals

through digital cameras. Furthermore, this solution can be used in free space optical communication applications. In Table 14, we made a comparative study with other selective encryption solutions. Our algorithm encrypts most sensitive parameters in an HEVC in format compliant manner.

Table 14. Comparison with other encrypting techniques.

Algorithm	Encrypted Elements	Format Compliant	Bit Increase	Encryption Algorithm
Xu [37]	IPM, MVDs, T1s, signs of the NZ coefficients	yes	no	Chaos
Abomhara [38]	I frame	no	no	AES
Shahid [19]	T1s, NZ level	yes	no	AES
Fei [23]	IPM, MVD, Signs of residual	yes	yes	Chaos
Sung [39]	Motion vector	yes	yes	RC4
Wei [40]	NALUs	yes	yes	RC4
Wang [41]	IPM, MVD, Quantization coefficients	yes	yes	Hash and AES
Shuli [42]	IPM, MVDs, Signs of residual, delta QP	yes	yes	Chaos and AES
Proposed algorithm	IPM, MV,MVS,TC,TCS	yes	IPM	Chaos



(**a**) (**b**)

Figure 8. Frame #10 of different HEVC videos, encrypted with the proposed ROI encryption: (**a**) Correctly decrypted videos. (**b**) ROI-Encrypted videos.

5.4. Subjective Evaluations

The subjective experiment was performed in the IETR laboratory psychovisual room, and was aligned with the `ITU-R BT.500-13` Recommendation [43]. In this evaluation we used a display screen Full HD 32 inch Samsung *UN32J5003* to view the sequences of videos. In this experiment, fifteen observers, 10 men and 5 women took part in this test, with an age between 20 and 40 years. All the subjects were tested for color blindness and visual acuity depending on Ishihara and Snellen charts, respectively, and have a visual acuity of 10/10 in both eyes with or without correction, as figured

out in [44]. We considered five video sequences from Table 4 (*FourPeople*, *Kimono1*, *BasketballDrive*, *BQSquare*, *Cactus*). The selective encryption and encoding is applied by using an HM(`16.7`) encoder with RA encoding. The selective encryption is performed in two levels—(TC, TC signs, MV, MV signs) and All (TC, TC signs, MV, MV signs, IPM). Finally, these coding configurations come with 40 encrypted video sequences, with various QP and resolutions.

5.4.1. Design and Procedure

The Double Stimulus Continuous Quality Scale (DSCQS) method [43] has been applied in our subjective quality evaluation experiment. Each encrypted video was showed twice to the observer as long as its original version. The observers will judge the visibility degree of the content of the encrypted videos numerically. That means, each participant should specify a visibility score to each of the 40 test videos, concerning to a rating scale, ranging from 1—meaning the video content is *Completely Invisible*—to 5—which means that the video content is *Clearly Visible*. After each test condition, a devoted Graphical User Interface (GUI) is shown on the screen for about 9 s during which the observer gives and then confirms their judgement. The videos were shuffled in such an order that two consecutive sequences must be from various configuration categories in order to remove the observer's memory effects.

5.4.2. Data Processing

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 (10).

$$MOS_{jk} = \frac{1}{N}\sum_{i=1}^{N} s_{ijk}, \tag{10}$$

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.

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%. This is given by Equation (11). Scores respecting the experiment conditions must be contained in the interval $[MOS_{jk} - IC_{jk}, MOS_{jk} + IC_{jk}]$.

$$IC_{jk} = 1.95\frac{\delta_{jk}}{\sqrt{N}}, \quad \delta_{jk} = \sqrt{\sum_{i=1}^{N}\frac{(s_{ijk} - MOS_{jk})}{N}}. \tag{11}$$

5.4.3. Subjective Scores

The subjective results scores of all participants, collected through the dedicated GUI, have been used for the perceptual encryption measurement. Figure 9 illustrates the MOS for two encryption configurations, four video sequences coded with the HM software at QP22 in RA configuration. Subjects scores range generally between *(barely visible)* and *(completely invisible)* for the first encryption scheme. This indicates that the visibility of the human is considerably decreased by the impact of our proposed SE solution. Indeed, the obtained results indicate that the content of the video is invisible. Furthermore, subjects attempt to guess the type of video context without the ability to see any detail of the presented video. We noticed a Little variation on MOS, relying on the video content and the used QP. The impact of IPM encryption is powerful on the content visibility. Indeed, the main observers scores steered to *Completely Invisible* when the IPM encryption has been added to the first encryption level (scheme). The subjects can barely see a few parts of the video (without ability to decide the general context of the shown video). Results depend strongly on the video classes and video contents have a strong impact. *BQSquare* (Classe D) and *Cactus* are completely invisible to all subjects, with $MOS \simeq 1$, and very few variations depending on the used QP. Moreover, *BasketballDrive* shows low visibility

scores due to its strong movement character. Curves of this video were dramatically reduced when we added the IPMS encryption.

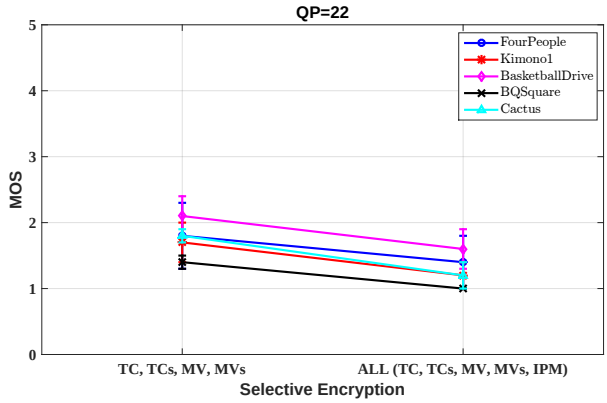


Figure 9. Subjects visibility scores including 95% confidence intervals for (QP = 22), the video sequences are encoded by HM.

5.4.4. Statistical Analysis

The Analyse of Variance (ANOVA) [45] was used to perform statistical study. In fact, ANOVA permits us to examine if the variance in visibility scores comes from the intended variation of experimental variables (i.e., QP, Class, Encrypted Scheme and Content), or just as a result of chance. Table 15 implies that only the 'Encryption Scheme' parameter has an important impact on the subject's scores with P-value < 0.0001 (a factor is considered influencing if the P-value < 0.05).

Table 15. ANOVA on the whole dataset, Df: number of degree-of-freedom and F-value: Fisher test.

Source	DF	F-Value	*P*-Value
Class	2	1.0121	0.4001
Content	4	0.9871	0.5501
QP	3	0.1281	0.128
SE Scheme	1	97.754	<0.0001

5.5. Complexity Evaluations

Table 10 reports the complexity overhead of encryptions for 4×4 and 4×3 tile configurations on our 2.6 GHz Core i5 processor, respectively. For 4×4 tile configuration, the average encoding time slows down by 2.6% in Intra coding and 3.3% in Inter coding. The respective decoding times are 1.6% and 2.1% higher. Changing the tile configuration to 4×3 decreases respective complexity overheads to 2.2% and 1.6% for encoding and 1.5% and 1.1% for decoding. These results confirm that the proposed SE solution can be performed without noticeable complexity performance compromises. This is especially important in embedded and mobile devices that have restricted processing power, as we can notice in Figures 10 and 11.

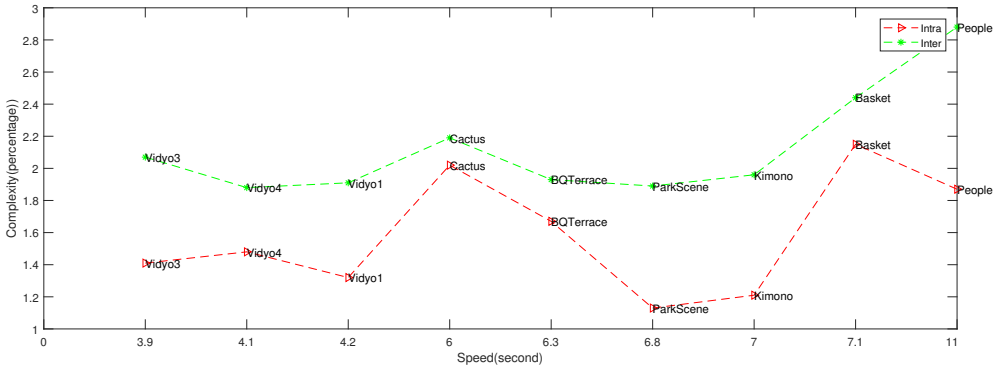


Figure 10. Decoding time vs. complexity overhead for 9 video sequences.

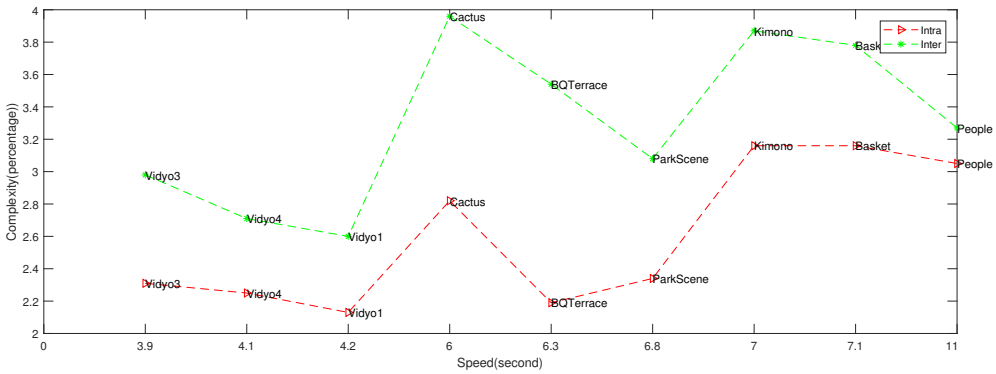


Figure 11. Encoding time vs. complexity overhead for 9 video sequences.

6. Conclusions

This paper proposed a selective encryption solution that protects privacy by encrypting merely the ROI in the HEVC video content and selective encryption of the whole sensitive parts in videos. The ROI is extracted through an independent HEVC tile concept. The ROI encryption is based on chaos-based generator and it is performed at the CABAC bin string level for the most sensitive HEVC parameters, including motion vectors, transform coefficients, and intra prediction modes. The format compliant encryption of IPM has been also investigated in this paper which introduces a slight bitrate increase. The encrypted bit stream can be decoded with a standard HEVC decoder and a privacy key is only needed for the decryption. However, there is some bit rate overhead in the HEVC encoding process in order to prevent the propagation of the encryption outside the ROI. The proposed encryption and decryption algorithms were integrated into HM reference software in order to validate their conformance with the HEVC standard. Respectively, their diminutive impact on coding speed was verified as a part of the real-time *Kvazaar* HEVC encoder and *OpenHEVC* decoder. Objective rate-distortion-complexity examinations indicated that the proposed solution performs a secure protection of privacy in the HEVC video content with a little overhead in bit rate and coding complexity. It also prevents unexpected behaviour of the decoder.

Author Contributions: Conceptualization, M.A.T. and W.H.; Methodology W.H.; Software, N.S.; Validation, M.A.T., J.V. and M.V.; Formal analysis, M.A.T.; Investigation, S.E.A.; Resources, S.E.A.; Data curation, M.A.T.; Writing—original draft preparation, M.A.T.; Writing—review and editing, M.A.T.; Visualization, M.A.T.; Supervision, W.H.; Project administration, M.A.T.; Funding acquisition, O.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research funded by the European Celtic-Plus project 4KREPROSYS—4K ultraHD TV wireless REmote PROduction SYStems and Academy of Finland.

Acknowledgments: This work is supported by the European Celtic-Plus project 4KREPROSYS—4K ultraHD TV wireless REmote PROduction SYStems and Academy of Finland (decision number 301820).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

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

1. The worst case of the original frame relating to the encryption solution is at low entropy configuration. The whole image has the same color, as an example all pixels are black or blue. Thus, the total number of occurrences of the pixel Z_1 in the original frame P is $H_{Z_1}(P) = h \times w$, where $Z_1 \in \{0, 255\}$. In addition, 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 method should generate 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 (7), we derive the maximum EQ (EQ_{max}) as follows:

$$\mathrm{EQ}_{max} = \frac{|\frac{h \times w}{256} - h \times w| + |\frac{h \times w}{256} - 0| \times 255}{256} \tag{A1}$$

Since, h and w are positive integer, then:

$$EQ_{max} = \frac{510 \times h \times w}{256^2} \tag{A2}$$

References

1. Sullivan, G.J.; Ohm, J.R.; Han, W.J.; Wiegand, T. Overview of the High Efficiency Video Coding (HEVC) Standard. *IEEE Trans. Circuits Syst. Video Technol.* **2012**, *22*, 1649–1668. [CrossRef]
2. Ohm, J.R.; Sullivan, G.J.; Schwarz, H.; Tan, T.K.; Wiegand, T. Comparison of the Coding Efficiency of Video Coding Standards— Including High Efficiency Video Coding (HEVC). *IEEE Trans. Circuits Syst. Video Technol.* **2012**, *22*, 1669–1684. [CrossRef]
3. 1: Advanced Video Coding for Generic Audiovisual Services, ITU-T Rec. Available online: https://www.itu.int/rec/T-REC-H.264-201906-I/en (accessed on 6 January 2020).
4. Shahid, Z.; Puech, W. Visual Protection of HEVC Video by Selective Encryption of CABAC Binstrings. *IEEE Trans. Multimed.* **2014**, *16*, 24–36. [CrossRef]
5. 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.* **2013**, *59*, 634–642. [CrossRef]
6. Shifa, A.; Asghar, M.N.; Noor, S.; Gohar, N.; Fleury, M. Lightweight Cipher for H. 264 Videos in the Internet of Multimedia Things with Encryption Space Ratio Diagnostics. *Sensors* **2019**, *19*, 1228. [CrossRef]
7. Chung, Y.; Lee, S.; Jeon, T.; Park, D. Fast video encryption using the H. 264 error propagation property for smart mobile devices. *Sensors* **2015**, *15*, 7953–7968. [CrossRef]
8. Misra, K.; Segall, A.; Horowitz, M.; Xu, S.; Fuldseth, A.; Zhou, M. An Overview of Tiles in HEVC. *IEEE J. Sel. Top. Signal Process.* **2013**, *7*, 969–977. [CrossRef]
9. Hamidouche, W.; Farajallah, M.; Sidaty, N.; Assad, S.E.; Deforges, O. Real-time Selective Video Encryption based on the Chaos System in Scalable HEVC Extension. *Signal Process. Image Commun.* **2017**, *58*, 73–86. [CrossRef]
10. Taha, M.A.; El Assad, S.; Queudet, A.; Déforges, O. Design and Efficient Implementation of a Chaos-based Stream Cipher. *Int. J. Internet Technol. Secured Trans.* **2017**, *7*, 89–114. [CrossRef]
11. Taha, M.A.; El Assad, S.; Jallouli, O.; Queudet, A.; Déforges, O. Design of a Pseudo-Chaotic Number Generator as a Random Number Generator. In Proceedings of the 11th International Conference on Communications, Bucharest, Romania, 21 October 2016; pp. 401–404.
12. Kvazaar. Kvazaar HEVC Encoder. Available online: https://github.com/ultravideo/kvazaar (accessed on 4 December 2019).

13. openHEVC. HEVC Decoder. Available online: http://openhevc.insa-rennes.fr (accessed on 5 December 2019).
14. Lainema, J.; Bossen, F.; Han, W.J.; Min, J.; Ugur, K. Intra Coding of the HEVC Standard. *IEEE Trans. Circuits Syst. Video Technol.* **2012**, *22*, 1792–1801. [CrossRef]
15. Sze, V.; Budagavi, M.; Sullivan, G.J. High Efficiency Video Coding (HEVC). In *Integrated Circuit and Systems, Algorithms and Architectures*; Springer: Berlin, Germany, 2014.
16. Bossen, F.; Bross, B.; Suhring, K.; Flynn, D. HEVC Complexity and Implementation Analysis. *IEEE Trans. Circuits Syst. Video Technol.* **2012**, *22*, 1685–1696. [CrossRef]
17. Chi, C.C.; Alvarez-Mesa, M.; Juurlink, B.; Clare, G.; Henry, F.; Pateux, S.; Schierl, T. Parallel Scalability and Efficiency of HEVC Parallelization Approaches. *IEEE Trans. Circuits Syst. Video Technol.* **2012**, *22*, 1827–1838.
18. Ryu, E.K.; Nam, J.H.; Lee, S.O.; Jo, H.H.; Sim, D.G. Sample Adaptive Offset Parallelism in HEVC. In *Multimedia and Ubiquitous Engineering*; Springer: Berlin, Germany, 2013; pp. 1113–1119.
19. Shahid, Z.; Chaumont, M.; Puech, W. Fast Protection of H. 264/AVC by Selective Encryption of CAVLC and CABAC for I and P Frames. *IEEE Trans. Circuits Syst. Video Technol.* **2011**, *21*, 565–576. [CrossRef]
20. Hamidouche, W.; Farajallah, M.; Raulet, M.; Deforges, O.; El Assad, S. Selective video Encryption using Chaotic System in the SHVC Extension. In Proceedings of the 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brisbane, QLD, Australia, 19–24 April 2015; pp. 1762–1766.
21. Boyce, J.M.; Ye, Y.; Chen, J.; Ramasubramonian, A.K. Overview of SHVC: Scalable Extensions of the High Efficiency Video Coding Standard. *IEEE Trans. Circuits Syst. Video Technol.* **2016**, *26*, 20–34. [CrossRef]
22. Boyadjis, B.; Bergeron, C.; Pesquet-Popescu, B.; Dufaux, F. Extended Selective Encryption of H. 264/AVC (CABAC) and HEVC Encoded Video Streams. *IEEE Trans. Circuits Syst. Video Technol.* **2015**, 1–15. [CrossRef]
23. Peng, F.; Zhu, X.W.; Long, M. An ROI Privacy Protection Scheme for H. 264 Video based on FMO and Chaos. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1688–1699. [CrossRef]
24. Dufaux, F.; Ebrahimi, T. Scrambling for Privacy Protection in Video Surveillance Systems. *IEEE Trans. Circuits Syst. Video Technol.* **2008**, *18*, 1168–1174. [CrossRef]
25. Newton, E.M.; Sweeney, L.; Malin, B. Preserving Privacy by De-identifying Face Images. *IEEE Trans. Knowl. Data Eng.* **2005**, *17*, 232–243. [CrossRef]
26. Sohn, H.; AnzaKu, E.T.; De Neve, W.; Ro, Y.M.; Plataniotis, K.N. Privacy Protection in Video Surveillance Systems using Scalable Video Coding. In Proceedings of the Sixth IEEE International Conference on Advanced Video and Signal Based Surveillance, Genova, Italy, 2–4 September 2009; pp. 424–429.
27. Schwarz, H.; Marpe, D.; Wiegand, T. Overview of the Scalable Video Coding Extension of the H.264/AVC Standard. *IEEE Trans. Circuits Syst. Video Technol.* **2007**, *17*, 1103–1120. [CrossRef]
28. Elaine, B.; John, K. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012.
29. Institute, F.H.H. Reference Software Model (hm). Available online: https://mpeg.chiariglione.org/tags/hm (accessed on 10 October 2019).
30. Bjøntegaard, G. VCEG-M33: Calculation of Average PSNR Differences Between RD-Curves. Available online: https://www.mathworks.com/matlabcentral/mlc-downloads/downloads/submissions/41749/versions/1/previews/bjontegaard2.m/index.html (accessed on 3 January 2020).
31. Ahmed, H.E.d.H.; Kalash, H.M.; Allah, O.F. Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images. In Proceedings of the 2007 International Conference on Electrical Engineering, Lahore, Pakistan, 11–12 April 2007; pp. 1–7.
32. Farajallah, M. Chaos based Crypto and Joint Crypto-Compression Systems for Images and Videos. Ph.D. Thesis, University of Nantes, Nantes, France, 2015.
33. Sallam, A.I.; El-Rabaie, E.S.M.; Faragallah, O.S. Efficient HEVC selective stream encryption using chaotic logistic map. *Multimed. Syst.* **2018**, *24*, 419–437. [CrossRef]
34. Taneja, N.; Raman, B.; Gupta, I. Selective Image Encryption in Fractional Wavelet Domain. *AEU-Int. J. Electron. Commun.* **2011**, *65*, 338–344. [CrossRef]
35. Joshi, R.L.; Fischer, T.R. Comparison of Generalized Gaussian and Laplacian Modeling in DCT Image Coding. *IEEE Signal Process. Lett.* **1995**, *2*, 81–82. [CrossRef]
36. Qi, M.; Chen, X.; Jiang, J.; Zhan, S. Face Protection of H. 264 video based on Detecting and Tracking. In Proceedings of the 8th International Conference on Electronic Measurement and Instruments, Xi'an, China, 16–18 August 2007; pp. 2–172.

37. Xu, H.; Tong, X.; Meng, X. An efficient chaos pseudo-random number generator applied to video encryption. *Optik* **2016**, *127*, 9305–9319. [CrossRef]
38. Abomhara, M.; Zakaria, O.; Khalifa, O.O.; Zaidan, A.; Zaidan, B. Enhancing Selective Encryption for H. 264/AVCUsing Advanced Encryption Standard. *Int. J. Comput. Electr. Eng.* **2010**, *2*, 223. [CrossRef]
39. Hong, S.S.; Han, M.M. The study of selective encryption of motion vector based on the S-Box for the security improvement in the process of video. *Multimed. Tools Appl.* **2014**, *71*, 1577–1597. [CrossRef]
40. Wei, Z.; Wu, Y.; Ding, X.; Deng, R.H. A scalable and format-compliant encryption scheme for H. 264/SVC bitstreams. *Signal Process. Image Commun.* **2012**, *27*, 1011–1024. [CrossRef]
41. Wang, X.; Zheng, N.; Tian, L. Hash key-based video encryption scheme for H. 264/AVC. *Signal Process. Image Commun.* **2010**, *25*, 427–437. [CrossRef]
42. Cheng, S.; Wang, L.; Ao, N.; Han, Q. A Selective Video Encryption Scheme Based on Coding Characteristics. *Symmetry* **2020**, *12*, 332. [CrossRef]
43. ITU Radiocommunication Assembly. *Methodology for the Subjective Assessment of the Quality of Television Pictures*; International Telecommunication Union: Geneva, Switzerland, 2003.
44. Sidaty, N.; Hamidouche, W.; Deforges, O. A New Perceptual Assessment Methodology for Selective HEVC Video Encryption. In Proceedings of the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, USA, 5–9 March 2017.
45. Gamst, G.; Meyers, L.S.; Guarino, A. *Analysis of Vvariance Designs: A Conceptual and Computational Approach with SPSS and SAS*; Cambridge University Press: Cambridge, UK, 2008.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).