J Real-Time Image Proc (2016) 12:473–482
DOI 10.1007/s11554-015-0509-3

SPECIAL ISSUE PAPER

Encryption algorithm for efficient transmission of HEVC media

Vasileios A. Memos · Kostas E. Psannis

Received: 14 January 2015 / Accepted: 8 May 2015 / Published online: 21 May 2015

Abstract Recently, H.265/MPEG-H or high efficiency video coding (HEVC) as it is well known, has been established as better compression standard due to reduction of about 50 % bit-rate for same video quality and less bandwidth consumption, compared to its predecessor H.264/MPEG-advanced video coding standard. Many algorithms have been proposed and developed for efficient and secure streaming of multimedia files. However, these methods do not meet all the requirements of effective and secure transmission over the internet. In this paper, we present a new encryption and transmission algorithm for efficient HEVC delivery. Experimental results demonstrate that our proposed algorithm is more secure and effective compared to previous algorithms used for H.264 standard and shows better overall performance.

Keywords H.264 · HEVC · Transmission · Encryption · AES algorithm

1 Introduction

H.265/MPEG-H or high efficiency video coding, known as HEVC, is the latest compression standard, which was officially approved in January 2013 [1], and became the successor of H.264/MPEG-4 or advanced video coding (AVC) standard [2]. The HEVC standard design has the features to be easily adaptable to about all the current existing H.264/MPEG-AVC applications, and emphasizes mainly on the capability of ultra-high-definition (UHD) video view [2] without much bandwidth consumption.

The basic achieve of the HEVC compression standard is the fact that it presents significantly better compression performance compared to the existing standards. Specifically, the HEVC standard causes about 50 % bit-rate reduction for about the same video quality, compared to H.264/MPEG-AVC standard [1, 3, 27]. In addition, it is designed to provide high-quality streaming multimedia, even on low-bandwidth networks, due to the fact that it consumes about half bandwidth less than H.264/MPEG-AVC. Therefore, the use of HEVC compression standard brings many benefits against compared to its predecessor H.264/MPEG-4 AVC standard [2, 4].

It is notable that HEVC standard presents specific complexity [4, 5, 28], and implementation [5], and it is being integrated into multimedia systems and protocols [6], while constitutes the current codec for resolutions beyond HDTV [7] for real-time streaming of video files [8]. Moreover, HEVC presents more effective rate–distortion (R–D) performance, using specific algorithms [9].

Due to the above features which established HEVC as the best compression standard, several researches focus on the development of security methods which can contribute to the protection of HEVC videos, while they are transmitted over the internet. Specifically, special encryption algorithms have been proposed for HEVC standard to protect the video sequence against cryptanalysis attacks by malicious users who use third-party tools and methods to crack and steal the transmitted video sequence.

In this paper, we present a new encryption algorithm for efficient secure transmission of video files compressed with HEVC standard. Our algorithm is based on known

V. A. Memos (✉) · K. E. Psannis
Department of Applied Informatics, University of Macedonia, 156 Egnatia Street, 54006 Thessaloniki, Greece
e-mail: tm0844@uom.edu.gr

K. E. Psannis
e-mail: kpsannis@uom.gr

algorithms proposed for previous compression standards, which we adapt properly so as to be applicable to the new standard.

The paper is organized as follows: In the "Related work" section, we present the related work of other researchers on video encryption area, both on HEVC standard and previous compression standards. In the "Proposed algorithm" section, we present and analyze our proposed algorithm for efficient encryption and transmission of video files, compressed with HEVC standard. "Experiments" section describes our methodology for the experiments we made upon the proposed algorithm, while "Experimental results" section includes the experimental results with comparative diagrams. "Conclusions and future work" section concludes the paper and indicates future research directions.

2 Related work

Multiple algorithms and schemes have been proposed for video encryption by many researchers, both in HEVC compression standard and in previous standards, such as H.264 and MPEG. Their main properties and limitations are presented in [10]. The authors make a series of comparisons to conclude that there is no method that can meet all the security requirements and thus, the suitable encryption algorithm for each video case depends on its confidentiality requirements.

A novel selective encryption scheme for secure transmission of video streams compressed with H.264/AVC standard is proposed in [11]. Simulation results demonstrate that its application implies PSNR degradations of about 25–30 dB when the ciphering key is unknown and thus, the video becomes unidentifiable. Another relative encryption algorithm especially for H.264/AVC format is proposed in [12] and its experimental results demonstrate much less important data encryption, better security, and high efficiency. Other selective encryption algorithms for image and videos compression standards: JPEG, JPEG2000, H.264/AVC, and H.265/HEVC are analyzed with cryptanalysis methods in [15].

In addition, encryption method and algorithm for Intra and Inter frames in MPEG videos are presented in [20]. According to the authors, highly private videos require encryption of all parts of the video, because all these are important in such cases. Thus, both Intra and Inter frames need to be encrypted. Another security scheme for MPEG video standard too is proposed in [21] and is based on AES-128 encryption algorithm. The difference here is that the authors choose and encrypt only the Intra frames of the video, because Inter frames are useless without knowing the corresponding Intra frames. This process saves 30–50 % of encryption/decryption time and does not affect the size of the encrypted stream.

A special study on the applicability and the encryption of H.264 video format including its scalable video coding (SVC) extension is presented in [13]. This survey is based on the latest results on video encryption methods which have been proposed. A scalable video encryption algorithm for H.264/SVC too is proposed in [14], which shows adequate performance and strength against cryptanalysis attacks, and it seems that it can be used in real-world applications. Moreover, possible bitstream elements, which can be used for HEVC compatible encryption, are described in [18], and ensure a good level of protection of the video information.

Finally, there are many encryption algorithms proposed exclusively for HEVC standard, based on selective encryption. Specifically, a new scheme based on selective encryption for HEVC is proposed in [16] and ensures transparent and sufficient encryption and protection against attacks. Moreover, this scheme allows fast encryption and decryption while preserving the format and length of the video stream. A new scheme for format compliant visual protection of HEVC using selective encryption too is proposed in [17], and offers a good level of protection with minimal use of computational requirements. Similar to this project, an efficient SE system for CABAC entropy coding of HEVC video standard is proposed in [19], which presents sufficient protection against cryptanalysis attacks, while making it proper for streaming on heterogeneous networks, due to the fact that bit-rate remains the same and the system requirements are minimal.

Although the new algorithms, which have been proposed exclusively for HEVC standard, present several advantages and are regarded to be effective solutions in protecting the video sequence, we merge two known algorithms proposed for previous standards [20, 21] and modify them properly so as to be integrated with HEVC standard, offering encryption and decryption time savings, while ensuring the protection level of the sequence against malicious users.

3 Proposed algorithm

Our proposed algorithm for efficient encryption and secure transmission is based on advanced encryption standard (AES), amendable to be adaptable to the new video compression standard, HEVC. AES was adopted by the U.S. government in 2002 and became the successor of the data encryption standard (DES) algorithm which was launched in 1977 [24]. This algorithm, known as Rijndael too, is a symmetric-key algorithm, fact which means that the same key is used for both encrypting and decrypting video files. Figure 1 depicts the encryption process of a video, using a

Fig. 1 The encryption process of a video file by using 256-AES key

256-bit key to our proposed cryptographic algorithm, which is described below.

J. Nehete et al. proposed a real-time MPEG video encryption algorithm using AES with key length of 128 bits (AES-128) [21]. In this paper, we adopt their proposed algorithm, making it amendable to AES-256 to ensure maximum security, due to the fact that larger key sizes use is more secure. Table 1 shows the required time to crack an encryption algorithm of a specific key size using brute force attack [25]. As it is clearly shown, the larger key sizes ensure more security, due to the fact that it is more time consuming to be cracked. Therefore, 256-bit key size of AES presents the maximum security level than other algorithms such as AES-128 or DES.

For some highly sensitive and important information, it is not always the best way to have a unique person in control of the key, and consequently, the security of the information. This problem is addressed by the development and use of secret sharing schemes, which allow keys to be shared among a group of people, with a predefined number of them needing to input their share in order to have access to the key [30]. Therefore, we introduce additionally a form of secret sharing scheme, Shamir's secret sharing (SSS) scheme, which is an encryption algorithm only for intra-frames and described analytically by Vijayalakshmi et al. for MPEG videos [20]. Specifically, SSS scheme is a cryptographic algorithm in which a secret is shared into *n* unique parts for equal number of participants, so as to be—some or all of them—necessary to reconstruct the original secret [20]. In our encryption algorithm for HEVC which is presented below, the embedded SSS algorithm is marked in italics.

Thus, using these two algorithms, we ensure the encryption of only I frames, because P and B frames are useless without knowing the corresponding I frames [21]. Moreover, researches have shown that the encryption of only I frames can save 30–50 % of encryption/decryption time and the size of encrypted stream does not change [21]. In the case of missing the secret key, the user's decoder will play quite different images from the original video, because of the fact that most of the image pixel values would have been changed [21].

Our proposed algorithm is formed as follows:

```
/*Proposed Encryption Algorithm for HEVC */
begin
open I-frame HEVC video file
create output file
/*Encryption Algorithm: For Intra frame */
for Each and Every DCT block
{
Step 1: Initialize nac = number of non-zero ACs
Step 2:
if (nac < 10 and nac > 5)
{
perform (4,5) secret sharing with
DC, AC1, . . . , AC3 as input and
store the result in DC, AC1, AC2, AC3, ACnac
}
if (nac < 20)
{
perform (8,9) secret sharing with
DC, AC1, . . . , AC7 as input and
store the result in DC, AC1, AC2, . . . , AC7, ACnac
}
if (nac > 20)
{
perform (12,13) secret sharing with
DC, AC1, . . . , AC11 as input and
store the result in DC, AC1, . . . , AC11, ACnac
}
}
while (not end of I-frame HEVC file)
{
read n bytes from input I-frame HEVC file in buffer
for each byte in buffer
{
if (collected sign bits == 256)
{
/*apply AES-256 encryption algorithm */
Rijndael(state,cipher_key)
{
key_expansion(cipher_key,expanded_key)
add_round_key(state,expaned_key)
/* Nr: Number of rounds,
Nc: No. of columns of state matrix */
for(i=1;i<Nr;i++)
Round(state,expaned_key + Nc*i)
Final_round(state,expanded_key+Nc*Nr)
}
put resulting sign bits in original place
}
}
write n bytes from buffer to output file
}
close input and output file
end
```

Table 1 The required time to crack an algorithm with respect to its key size

Key size	Time to crack
56-bit (DES)	399 s
128-bit (AES)	1.02×10^{18} years
192-bit (AES)	1.872×10^{37} years
256-bit (AES)	3.31×10^{56} years

4 Experiments

In this section, we conducted tests upon specific video sequences so as to indicate diagrammatically the effect of cryptographic algorithms on them. Specifically, we calculated the size and the encryption time of the used video sequences, after the application of the cryptographic algorithms: DES, AES-128, and AES-256 respectively. Then, we consider our recommendations for each case relative to the protection level they provide.

Table 2 indicates the test sequences, retrieved by JCT-VC main configuration common conditions [22], which we used to conduct the experiments. As shown in this Table and Table 3, the sequences differ from each other in terms of frame count, frame rate (fps), and bit rate (Mbps), and as a result of them, they have different sizes (MB) too.

Sequences used in the experiments are classified into five classes based on their resolution (class A, B1, B2, C, D). Class A sequences correspond to ultra-high definition (HD).

Sequences with a resolution of 2560 × 1600. Class B1 and B2 sequences correspond to full high-definition sequences with a resolution of 1920 × 1080. Class C and Class D sequences correspond to WVGA and WQVGA resolutions of 800 × 480 and 400 × 240, respectively.

For the experiments, Class A includes the Traffic, PeopleOnStreet, Nebuta, and SteamLocomotive sequences; Class B1 includes the Kimono, ParkScene sequences; Class B2 includes the Cactus, BQTerrace and BasketballDrive sequences; Class C includes the RaceHorses, BQMall, PartyScene and BasketballDrill sequences; and Class D includes the RaceHorses, BQSquare, BlowingBubbles and BasketballPass sequences.

For each Class (A, B1, B2, C, and D), we selected the maximum bitrate levels for the classes [22], as they are

Table 3 test classes and bit rates for HEVC

Class	Bit rate (Mbps)	MB/s
A	14	1.75
B1	6	0.75
B2	10	1.25
C	2	0.25
D	1.5	0.1875

Table 2 The sizes of each sequence of the test classes after encryption with DES, AES-128, and AES-256 algorithms for HEVC and H.264 standards

Class	Sequence name	Frame Count	Frame rate (fps)	Duration (s)	Original Size HEVC—(H.264) (MB)	Size after encryption with DES HEVC—(H.264) (MB)	Size after encryption with AES-128 HEVC—(H.264) (MB)	Size after encryption with AES-256 HEVC—(H.264) (MB)
A	Traffic	150	30	5	8.75 (24.31)	9.45 (26.25)	9.60 (26.67)	9.60 (26.67)
A	PeopleOnStreet	150	30	5	8.75 (24.31)	9.45 (26.25)	9.60 (26.67)	9.60 (26.67)
A	Nebuta	300	60	5	8.75 (24.31)	10.50 (29.17)	9.60 (26.67)	9.60 (26.67)
A	SteamLocomotive	300	60	5	8.75 (24.31)	10.50 (29.17)	9.60 (26.67)	9.60 (26.67)
B1	Kimono	240	24	10	7.50 (19.74)	8.40 (22.11)	7.68 (20.21)	7.68 (20.21)
B1	ParkScene	240	24	10	7.50 (19.74)	8.40 (22.11)	7.68 (20.21)	7.68 (20.21)
B2	Cactus	500	50	10	12.50 (32.89)	14.00 (36.84)	16.00 (42.10)	16.00 (42.10)
B2	BQTerrace	600	60	10	12.50 (32.89)	12.60 (33.15)	19.20 (50.52)	19.20 (50.52)
B2	BasketballDrive	500	50	10	12.50 (32.89)	14.00 (36.84)	16.00 (42.10)	16.00 (42.10)
C	RaceHorses	300	30	10	2.50 (5.68)	4.20 (9.54)	4.80 (10.91)	9.60 (21.81)
C	BQMall	600	60	10	2.50 (5.68)	4.20 (9.54)	9.60 (21.81)	19.20 (43.62)
C	PartyScene	500	50	10	2.50 (5.68)	3.50 (7.95)	8.00 (18.18)	16.00 (36.35)
C	BasketballDrill	500	50	10	2.50 (5.68)	3.50 (7.95)	8.00 (18.18)	16.00 (36.35)
D	RaceHorses	300	30	10	1.88 (3.91)	2.10 (4.38)	4.80 (10.01)	9.60 (20.02)
D	BQSquare	600	60	10	1.88 (3.91)	4.20 (8.76)	9.60 (20.02)	19.20 (40.04)
D	BlowingBubbles	500	50	10	1.88 (3.91)	3.50 (7.30)	8.00 (16.68)	16.00 (33.37)
D	BasketballPass	500	50	10	1.88 (3.91)	3.50 (7.30)	8.00 (16.68)	16.00 (33.37)

summarized in Table 3. This Table indicates also the transmission rate in MB per second for the ease of the following calculations.

For the calculation of the size of each video sequence, before and after encryption, we used the following general equation [23]:

$$\text{CipherText} = \text{PlainText} + \text{Block} - (\text{PlainText MOD Block}). \quad (1)$$

Thus, the above equation is modified as follows:

- For DES-56 encryption (56/8 = 7 blocks):

$$\text{CipherSequence} = \text{PlainSequence} + 7 - (\text{PlainSequence MOD } 7). \quad (2)$$

- For AES-128 encryption (128/8 = 16 blocks):

$$\text{CipherSequence} = \text{PlainSequence} + 16 - (\text{PlainSequence MOD } 16). \quad (3)$$

- For AES-256 encryption (256/8 = 32 blocks):

$$\text{CipherSequence} = \text{PlainSequence} + 32 - (\text{PlainSequence MOD } 32). \quad (4)$$

In addition, except of the above calculations upon HEVC standard, we present and compare the size of each sequence—before and after encryption—upon H.264 standard too. Based on the previous subjective video performance comparisons [26], Class A' sequences compressed in HEVC standard (4 K UHD) present an average 64 % bitrate reduction compared to H.264, Class B' (1080p) 62 %, Class C' (720p) 56 %, and Class D' (480p) 52 %, respectively.

Finally, a comparative analysis of the encryption speed of AES-128, AES-256, and DES algorithms for HEVC and H.264 standards is discussed in the next section and is based on Table 4, which indicates the amount of encrypted data (MB) every second after the application of DES, AES-128, and AES-256 algorithm, respectively [29].

Table 4 The encryption speed of every algorithm

Algorithm	Encryption speed (MB/s)
AES Rijndael (128-bit key)	61.01
AES Rijndael (256-bit key)	48.23
DES (56-bit key)	21.34

5 Experimental results

The results of the calculations of the previous section are presented in the Table 2. Figures 2, 3, 4, 5, and 6 depict diagrammatically the changes of the size of each sequence of each class after the encryption with DES, AES-128, and AES-256 algorithms in H.264 and HEVC compression standards, respectively. Specifically, Fig. 2 depicts these changes of the size of each sequence of Class A; Fig. 3 depicts these changes of the size of each sequence of Class B1; Fig. 4 depicts these changes of the size of each sequence of Class B2; Fig. 5 depicts these changes of the size of each sequence of Class C; Fig. 6 depicts these changes of the size of each sequence of Class D.

Based on these diagrams, we highly recommend AES-256 for Class A, B1, and B2, while for classes C and D, AES-128 security level could be more convenient if the security factor is not the priority, because of the fact that in these classes, AES-256 increase very much the size of the relative video sequences compared to AES-128. Table 2 indicates clearly the accurate sizes of each sequence before

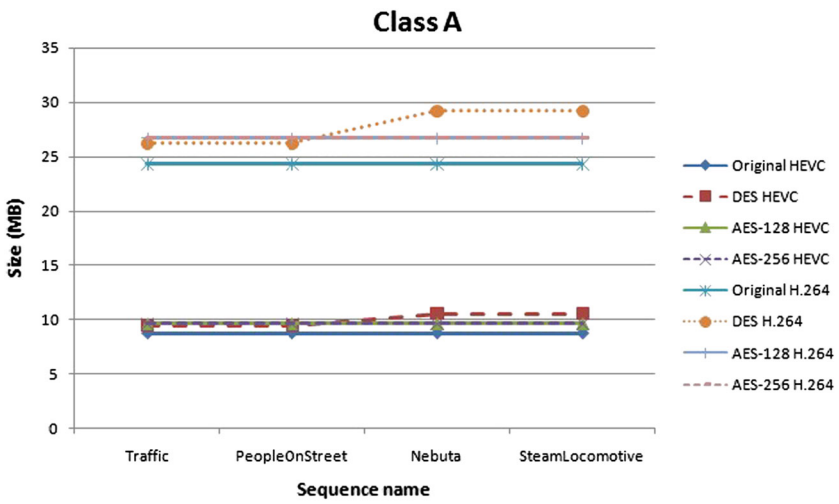

Fig. 2 The original size and the size after encryption with DES, AES-128, and AES-256 algorithms for the sequences of Class A

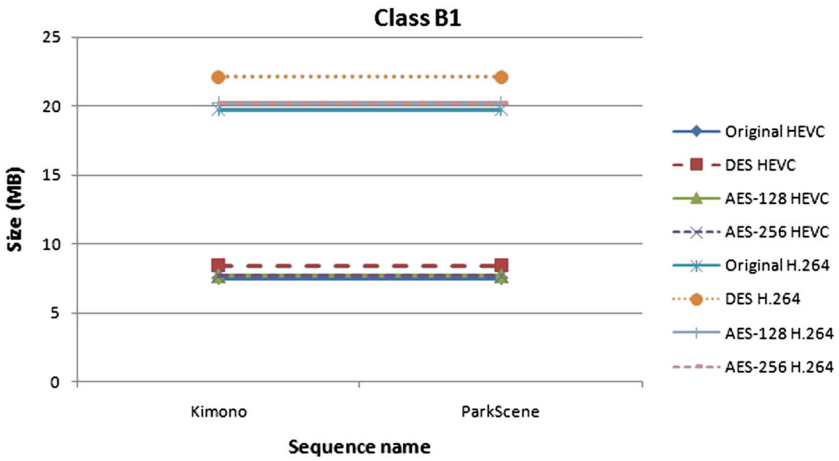

Fig. 3 The original size and the size after encryption with DES, AES-128, and AES-256 algorithms for the sequences of Class B1

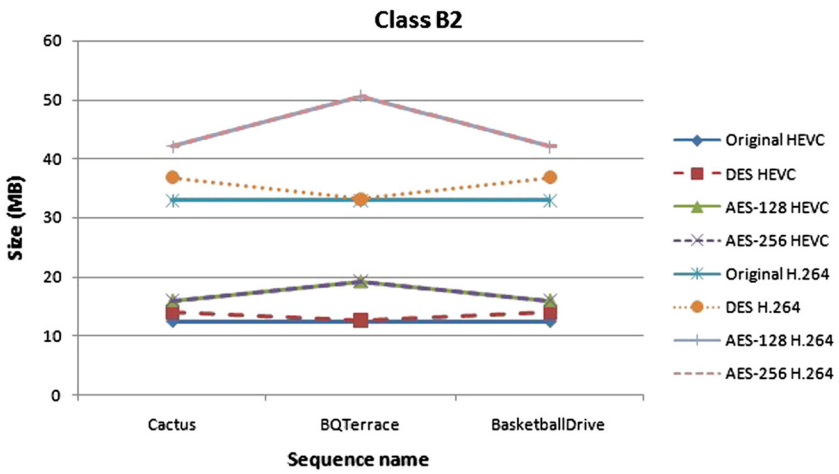

Fig. 4 The original size and the size after encryption with DES, AES-128, and AES-256 algorithms for the sequences of Class B2

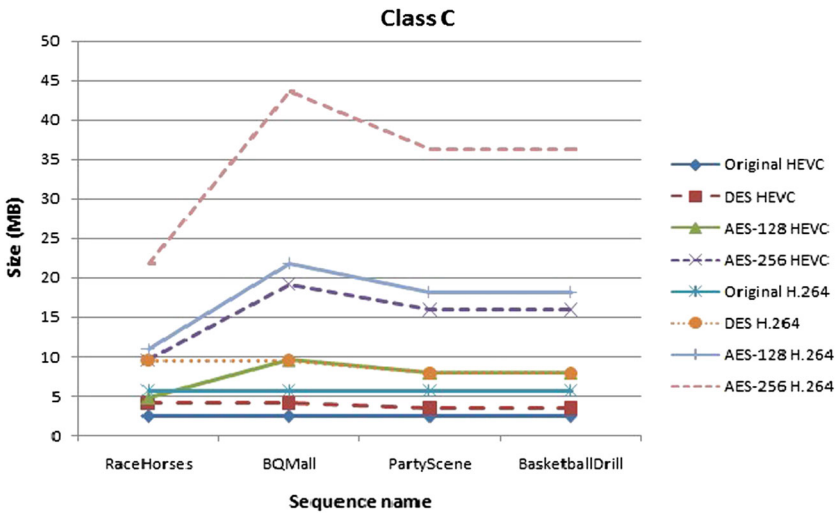

Fig. 5 The original size and the size after encryption with DES, AES-128, and AES-256 algorithms for the sequences of Class C

and after the application of DES, AES-128, and AES-256 algorithms for H.264 and HEVC format, respectively.

Generally, the AES-128 algorithm presents sufficient security level in some cases, but it is the fact that AES-256 maximize very much the security level. On the other hand, DES algorithm seems to be inconvenient and unsafe, because it is regarded easy to be cracked (Table 1), while some sequences increase their size more than the other two

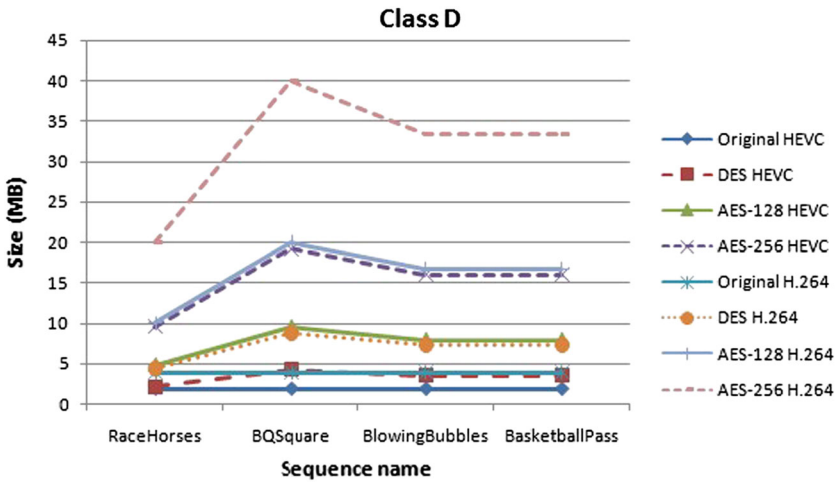

Fig. 6 The original size and the size after encryption with DES, AES-128, and AES-256 algorithms for the sequences of Class D

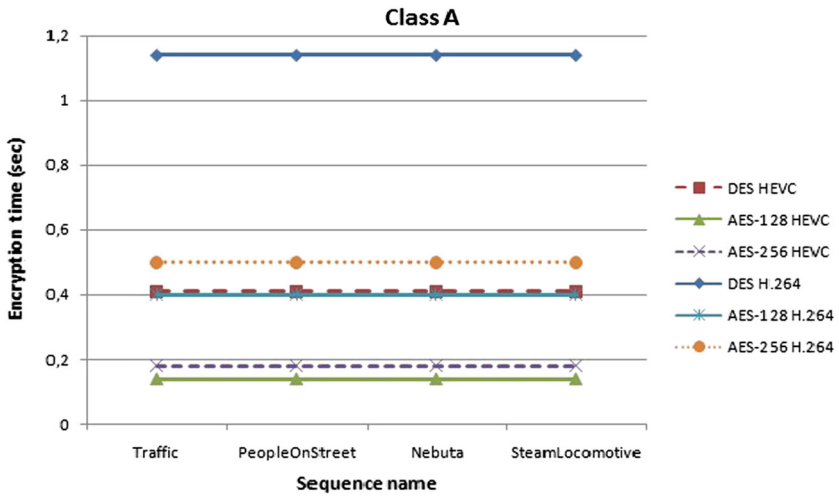

Fig. 7 The required encryption time of DES, AES-128, and AES-256 algorithms for the Class A sequences in HEVC and H.264 standard

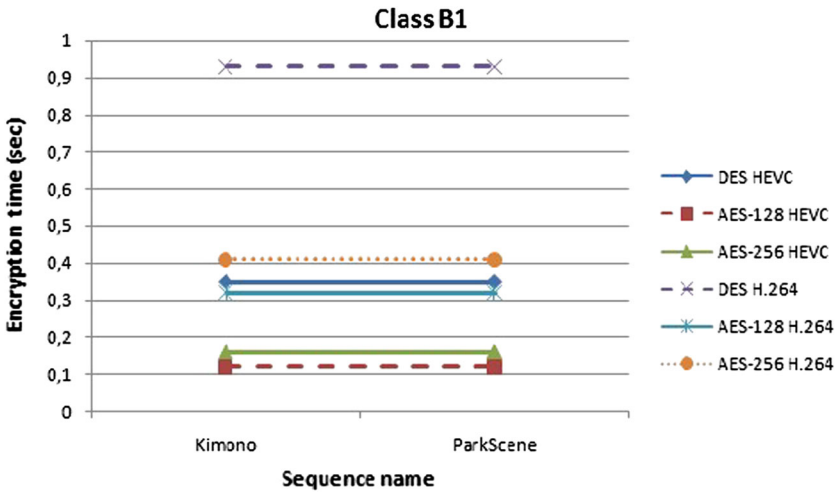

Fig. 8 The required encryption time of DES, AES-128, and AES-256 algorithms for the Class B1 sequences in HEVC and H.264 standard

algorithms, as it is shown diagramatically. Moreover, bandwidth savings thanks to HEVC are confirmed from the above diagrams, not only to the original video sequences, but also to their encrypted forms after the effect of the cryptographic mechanism of DES, AES-128, and AES-256 algorithms, compared to H.264 compression standard.

In addition, Figs. 7, 8, 9, 10, and 11 depict diagrammatically the required time for the sequences of each class

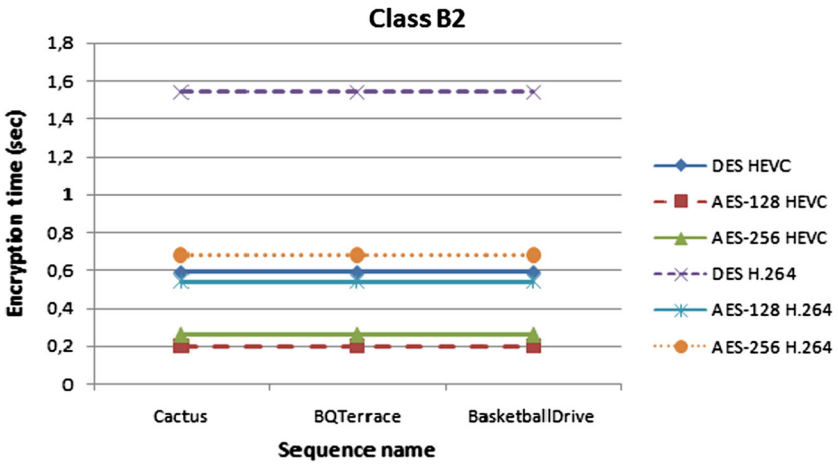

Fig. 9 The required encryption time of DES, AES-128, and AES-256 algorithms for the Class B2 sequences in HEVC and H.264 standard

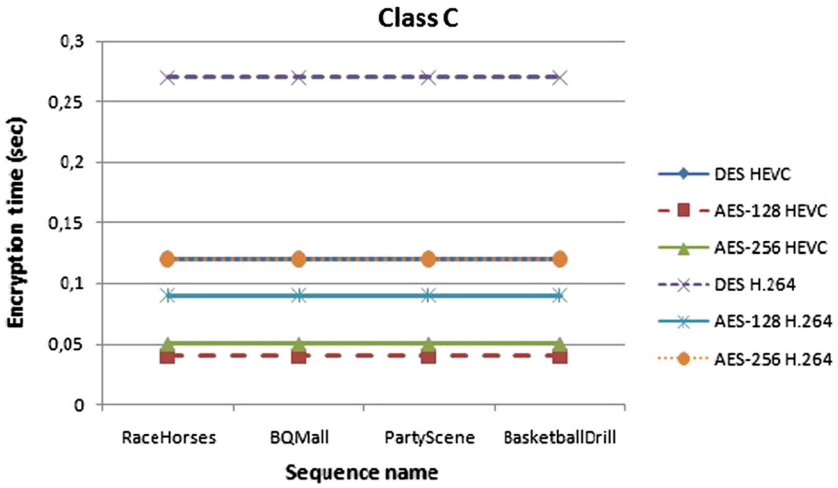

Fig. 10 The required encryption time of DES, AES-128, and AES-256 algorithms for the Class C sequences in HEVC and H.264 standard

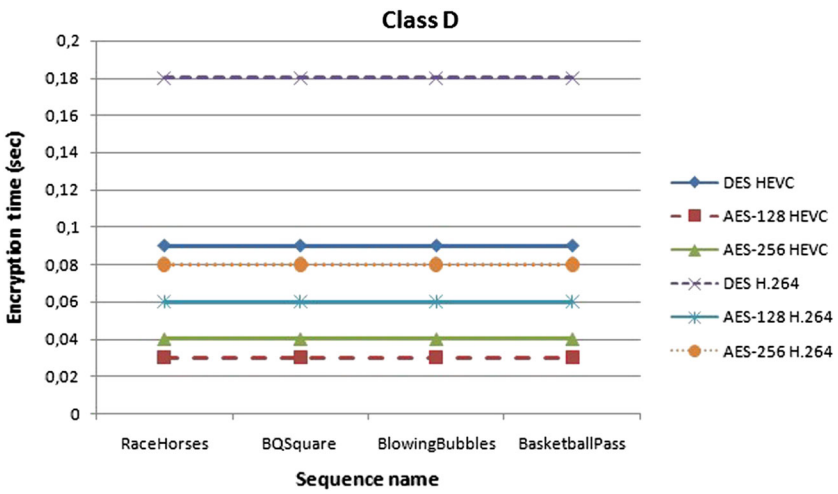

Fig. 11 The required encryption time of DES, AES-128, and AES-256 algorithms for the Class D sequences in HEVC and H.264 standard

after the application of DES, AES-128, and AES-256 algorithms in H.264 and HEVC format, respectively. Specifically, Fig. 7 depicts these required encryption times for the sequences of Class A in H.264 and HEVC compression standards, respectively; Fig. 8 depicts these required encryption times for the sequences of Class B1 in H.264 and HEVC compression standards, respectively; Fig. 9 depicts these required encryption times for the

sequences of Class B2 in H.264 and HEVC compression standards, respectively; Fig. 10 depicts these required encryption times for the sequences of Class C in H.264 and HEVC compression standards, respectively; Fig. 11 depicts these required encryption times for the sequences of Class D for H.264 and HEVC compression standards, respectively. The diagrams are the result of calculations based on Table 4.

According to these diagrams, AES-128 algorithm for HEVC standard is the fastest, as it requires the minimum possible time to encrypt the video sequences mentioned in the Table 2. Specifically, AES-128 needs 0.14, 0.12, 0.20, 0.04, and 0.03 s to encrypt each sequence of Class A, B1, B2, C, and D, respectively.

On the other hand, despite the fact that AES-256 is slower than AES-128 about 20.95 %, it offers a much better security level, as is depicted in Table 1. The corresponding encryption times for each sequence of Class A, B1, B2, C, and D are 0.18, 0.16, 0.26, 0.05, and 0.04 s, respectively.

Moreover, DES algorithm is presented very slow as it can encrypt only 21.34 MB per second and thus, it is about 2,26 times slower than AES-256 and 2,86 times than AES-128 algorithm, respectively.

Finally, the required encryption time for HEVC standard is much less than the corresponding time for H.264, due to the fact that HEVC presents bitrate reduction for all test classes compared to its previous compression standard, H.264 [26].

6 Conclusions and future work

A new encryption and transmission algorithm for efficient HEVC-media communications was presented. This algorithm merges two algorithms proposed for previous standards and it is modified so as to be amendable to the new video compression standard. A comparative analysis between DES, AES-128, and AES-256 was conducted to show which algorithm could be more convenient for the video sequences of each class A, B, C, and D compressed with HEVC. Experimental results show that despite the fact that AES-256 is slower than AES-128, it offers a much better security level and it is better for the classes A and B, due to bandwidth factor, while AES-128 seems to be sufficient to encrypt video of the classes C and D if the security factor is not the priority.

In addition, according to the comparative analysis of the last two recent compression standards, HEVC compression standard is shown to be better than H.264 using the same algorithms—DES, AES-128, and AES-256—for intra-frames encryption, because of the fact that it presents bandwidth savings and requires less time to be encrypted with relevant algorithms compared to H.264. Future work will include comparative analysis of the effectiveness of our algorithm with the other proposed algorithms for HEVC compression standard.

References

1. Sullivan, G.J., Ohm, J., Han, W.J., Wiegand, T.: Overview of the high efficiency video coding (HEVC) standard. IEEE Trans. Circuits Syst. Video Technol. **22**(12), 1649–1668 (2012)
2. Grois D., Marpe D., Mulayoff A., Itzhaky B., Hadar O.: Performance comparison of H.265/MPEG-HEVC, VP9, and H.264/MPEG-AVC encoders, 30th picture coding symposium (PCS) (2013)
3. 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. **22**(12), 1669–1684 (2012)
4. Vanne, J., Viitanen, M., Hamalainen, T.D., Hallapuro, A.: Comparative rate-distortion-complexity analysis of HEVC and AVC video codecs. IEEE Trans. Circuits Syst. Video Technol. **22**(12), 1885–1898 (2012)
5. Bossen, F., Bross, B., Suhring, K., Flynn, D.: HEVC Complexity and Implementation Analysis. IEEE Trans. Circuits Syst. Video Technol. **22**(12), 1685–1696 (2012)
6. Schierl, T., Hannuksela, M.M., Wang, Y.K., Wenger, S.: System layer integration of high efficiency video coding. IEEE Trans. Circuits Syst. Video Technol. **22**(12), 1871–1884 (2012)
7. Hanhart P., Rerabek M., De Simone F., Ebrahimi T.: Subjective quality evaluation of the upcoming HEVC video compression standard, applications of digital image processing XXXV. In: Proceedings of SPIE, vol. 8499 84990V (2012)
8. Nightingale J., Wang Q., Grecos C.: Benchmarking real-time HEVC streaming, real-time image and video processing. In: Proceedings of SPIE, vol. 8437 84370D-1 (2012)
9. Wang, S., Ma, S., Wang, S., Zhao, D., Gao, W.: Rate-GOP based rate control for high efficiency video coding. IEEE J. Sel. Top. Signal Process. **7**(6), 1101–1111 (2013)
10. Liu, F., Koenig, H.: A survey of video encryption algorithms. Comput Secur **29**(1), 3–15 (2010)
11. Bergeron C., Lamy-Bergot C.: Compliant selective encryption for H.264/AVC video streams. IEEE 7th workshop on multimedia signal processing (2005)
12. Saranya, P., Varalakshmi, L.M.: H.264 based Selective Video Encryption for Mobile Applications. Inter. J. Comput. Appl. **17**(4), 21–25 (2011)
13. Stütz, T., Uhl, A.: A Survey of H.264 AVC/SVC encryption. IEEE Trans. Circuits Syst. Video Technol. **22**(3), 325–339 (2012)
14. Jie G., Weidong Q., Chao D., Kefei C.: A scalable video encryption algorithm for H.264/SVC, In: Proceedings of the 2nd international conference on computer science and electronics engineering (ICCSEE) (2013)
15. Dubois L., Shahid Z., Puech W., Selective encryption of images and videos: from JPEG to H.265/HEVC through JPEG2000 and H.264/AVC, In: Progress in data encryption research, pp. 137–178, (2013)
16. Hofbauer H., Uhl A., Unterweger A.: Transparent encryption for HEVC Using bit-stream-based selective coefficient sign encryption, In: IEEE international conference on acoustics, Speech and Signal Processing (ICASSP), pp. 1986–1990 (2014)
17. Shahid, Z., Puech, W.: Visual protection of HEVC video by selective encryption of CABAC binstrings. IEEE Trans. Multimed. **16**, 24–36 (2013)

18. Van Wallendael G., Boho A., De Cock J., Munteanu A., Van de Walle R., "Encryption for High Efficiency Video Coding with Video Adaptation Capabilities", In: IEEE International Conference on Consumer Electronics (ICCE), pp. 31–32 (2013)
19. Shahid Z., Puech W.: Investigating the structure preserving encryption of high efficiency video coding (HEVC), In: Proceedings SPIE, real-time image and video processing, vol. 8656 (2013)
20. Vijayalakshmi, V., Varalakshmi, L.M., Sudha, G.F.: Efficient encryption of intra and inter frames in MPEG video. Recent trends in network security and applications communications in computer and information science, vol. 89, pp. 93–104. New York, Springer (2010)
21. Jayshri Nehete K., Bhagyalakshmi MB., Manjunath, Chaudhari S., Ramamohan TR, A real-time MPEG video encryption algorithm using AES", The national conference on communications (NCC), pp. 164–168 (2003)
22. Bossen F.: Common HM test conditions and software reference configurations," document JCTVC-L1100 of JCT-VC, Geneva, CH (2013)
23. How to calculate the size of encrypted data?. http://www.obviex.com/articles/CiphertextSize.pdf. Accessed 15 December 2014
24. Westlund, Harold, B.: NIST reports measurable success of advanced encryption standard. J. Res. Natl. Inst. Stand. Technol **107**(3), 307 (2002)
25. Arora M.: How secure is AES against brute force attacks?. http://www.eetimes.com/document.asp?doc_id=1279619. Accessed 15 December 2014
26. Tan T.K., Mrak M., Baroncini V., Ramzan N.: Report on HEVC compression performance verification testing. Joint Collab. Team Video Coding (JCT-VC) (2014)
27. Pourazad, M.T., Doutre, C., Azimi, M., Nasiopoulos, P.: HEVC: the new gold standard for video compression, how does HEVC compare with H.264/AVC? IEEE Consum. Electron. Mag. **1**(3), 36–46 (2012)
28. Lee A., Jun D., Kim J., Choi J.S., Kim J.: An efficient inter prediction mode decision method for fast motion estimation in high efficiency video coding, IEEE international conference on ICT convergence (ICTC), pp. 502–505 (2013)
29. Al Tamimi A. K.: Performance Analysis of data encryption algorithms. http://www.cse.wustl.edu/∼jain/cse567-06/ftp/encryption_perf/. Accessed 15 December 2014
30. Martin, R.: Introduction to secret sharing schemes. Computer Science Department, Rochester Institute of Technology, Rochester (2012)

Vasileios A. Memos is with the Department of Applied Informatics, School of Information Sciences, University of Macedonia, Greece. His main research interests include computer networks, wireless communications, cloud computing, network and computer security, cryptography, privacy and security software testing.

Kostas E. Psannis was born in Thessaloniki, Greece. Kostas received a degree in Physics from Aristotle University of Thessaloniki (Greece), and a Ph.D. degree from the Department of Electronic and Computer Engineering of Brunel University (UK). In the year 2001 to 2002, he was awarded the British Chevening scholarship sponsored by the Foreign & Commonwealth Office (FCO), British Government. He was awarded, in the year 2006, a research grant by IISF (Grant No. 2006.1.3.916). Since 2004, he has been a (Visiting) Assistant Professor in the Department of Applied Informatics, University of Macedonia, Greece, where currently he is an Assistant Professor (and Departmental LLP/Erasmus-Exchange Students Coordinator and Higher Education Mentor) in the Department of Applied Informatics, School of Information Sciences. He is also a joint Researcher in the Department of Scientific and Engineering Simulation, Graduate School of Engineering, Nagoya Institute of Technology, Japan. He has extensive research, development, and consulting experience in the area of telecommunications technologies. Since 1999, he has been participating in several R&D funded projects in the area of ICT (EU and JAPAN). Kostas Psannis was invited to speak on the EU-Japan Co-ordinated Call Preparatory meeting, Green and Content Centric Networking (CCN), organized by European Commission (EC) and National Institute of Information and Communications Technology (NICT)/ Ministry of Internal Affairs and Communications (MIC), Japan (in the context of the upcoming ICT Work Programme 2013) and International Telecommunication Union (ITU) SG13 meeting on DAN/CCN, July 2012, amongst other invited speakers. He has several publications in international Conferences, books chapters and peer-reviewed journals. His professional interests are Multimodal Data Communications Systems, Haptic Communication between Humans and Robots, Cloud Transmission/ Streaming/Synchronization, Future Media-Internet, Experiments on International Connections (E-ICONS) over TEIN3 (Pan-Asian), Science Information Network (SINET, Japan), GRNET (Greece)-Okeanos Cloud, and GEANT (European Union) dedicated high capacity connectivity. He is a member of IEEE. He is also member of the European Commission EURAXESS Links Japan, and member of the EU-JAPAN Centre for Industrial Cooperation.