Computers, Materials & Continua
DOI:10.32604/cmc.2022.019151
Article

Tech Science Press

Utilization of HEVC ChaCha20-Based Selective Encryption for Secure Telehealth Video Conferencing

Osama S. Faragallah[1,*], Ahmed I. Sallam[2] and Hala S. El-sayed[3]

[1]Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
[2]Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt
[3]Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Shebin El-Kom, 32511, Egypt
[*]Corresponding Author: Osama S. Faragallah. Email: o.salah@tu.edu.sa
Received: 03 April 2021; Accepted: 04 May 2021

Abstract: Coronavirus (COVID-19) is a contagious disease that causes exceptional effect on healthcare organizations worldwide with dangerous impact on medical services within the hospitals. Because of the fast spread of COVID-19, the healthcare facilities could be a big source of disease infection. So, healthcare video consultations should be used to decrease face-to-face communication between clinician and patients. Healthcare video consultations may be beneficial for some COVID-19 conditions and reduce the need for face-to-face contact with a potentially positive patient without symptoms. These conditions are like top clinicians who provide remote consultations to develop treatment methodology and follow-up remotely, patients who consult about COVID-19, and those who have mild symptoms suggestive of the COVID-19 virus. Video consultations are a supplement to, and not a substitute for, telephone consultations. It may also form part of a broader COVID-19 distance care strategy that contains computerized screening, separation of possibly infectious patients within medical services, and computerized video-intensive observing of their intensive care that helps reduce mixing. Nowadays, the spread of the COVID-19 virus helps to expand the use of video healthcare consultations because it helps to exchange experiences and remote medical consultations, save costs and health procedures used to cope with the pandemic of the COVID-19 virus, and monitor the progress of treatment plans, moment by moment from a distance with precision, clarity and ease. From this perspective, this paper introduces a high-efficiency video coding (HEVC) ChaCha20-based selective encryption (SE) scheme for secure healthcare video Consultations. The proposed HEVC ChaCha20-based SE scheme uses the ChaCha20 for encrypting the sign bits of the Discrete Cosine Transform (DCT) and Motion Vector Difference (MVD) in the HEVC entropy phase. The main achievement of HEVC ChaCha20-based SE scheme is encrypting the most sensitive video bits with keeping low delay time, fixed bit rate of the HEVC, and format compliance. Experimental tests guarantee that the proposed HEVC ChaCha20-based SE scheme can ensure the confidentiality of

the healthcare video consultations which has become easy to transmit through the internet.

Keywords: Telehealth; HEVC; cahcha20; video conferencing

1 Introduction

Healthcare video consultations are the exchange of healthcare data from a site to another site via video conferencing to enhance the health of patients. The appearance of COVID-19 virus created extraordinary challenges for delivery of healthcare services, and there is a need to increase the use of video consultations to assist persons who want routine care, and keep beneficiaries with slight symptoms in their homes while keeping access to the healthcare they need. Reducing community increase of COVID-19, in addition to reducing the contact to other patients and doctors will slow COVID-19 spread. The fast spread of the virus has reintroduced and re-established the Telemedicine technology [1] and video consultations [2] technologies for remaining the healthcare without growing the danger of possible contact between patients and doctors.

The earlier patient sorting, before arriving in the emergency department, becomes an essential strategy for health care regulator. Healthcare video consultations are beneficial to self-quarantine and helps doctors and patients communication using mobiles or websites [3]. Healthcare video consultations are the exchange of healthcare data from a site to another site via videoconferencing to enhance the health of patients. In addition, with the appearance of COVID-19, there is a need to increase the use of video consultations to assist persons who want routine care, and keep beneficiaries with slight symptoms in their homes while keeping access to the healthcare they need. Reducing community increase of COVID-19, in addition to reducing the contact to other patients and doctors will slow COVID-19 spread [4]. The next components are involved in the healthcare video consultation [5]:

- The healthcare video consultation is via a videoconferencing platform.
- Healthcare video data is transferred electronically between patient and healthcare professional in real time manner.
- The doctors make clinical skills to provide healthcare and feedback to both the specialist and the patient.
- Video coding removes the redundancy and unimportant video data to reduce the video size. The video coding consists of the following processes:
- The video encoder: transfers the video in its original format to the compressed format.
- The video decoder: it is a reverse process of the video decoder that transfers video in its compressed to the original format.

The video can display a set of 30 pictures that called frames per second. The video coding can remove many redundant data that can be found in the consecutive frames. The International Standardization Organization and the International Telecommunications Union co-operate together and formed team for developing the most recent video coding standards like H.264 and HEVC [5].

The ITU-T and ISO/IEC have developed the H.264 in 2003 to improve the video transmission through the internet because it gives better video compression efficiency than the other old video coding standard. There are many applications that can use the H264 standard like HD TV broadcasting through the internet and real time Video conferencing applications [6].

Recently, ITU-T and ISO/IEC have developed the HEVC to enhance the efficiency of the video coding process. It decreased the compressed video bit rate about 50% less than the video bit rate that is compressed by the H.264 [6]. Due to the rapid increase of the real time video applications through the internet, the video security has become very interesting topic for research. Video security depends on encryption that achieves the video data confidentiality and protects the video data from unauthorized attacks [7].

At last years, the rapid development of the digital video coding technique results in large video applications, like High Definition (HD)/Full HD/Ultra HD video contents, video-conferencing and Healthcare video consultations through the internet. Because of the large size of the raw digital video, it should be stored or transmitted in a compressed format. The video compression is the technique of decreasing the bit rate of the digital video signal by eliminating the redundancy and removing the unimportant elements [7]. Many video compression standards were implemented to convert the large bits of the raw digital video to a compact format with a small number of bits [7].

Nowadays many organizations in the medical, commercial, and military fields use the internet to distribute their multimedia applications like Healthcare video consultations. So the multimedia security plays an important role in protecting the multimedia contents against the unauthorized attacks [7]. Naive Encryption Algorithm (NEA) is simple technique for video encryption process. It employs standard encryption for video data [8]. The disadvantages of the NEA technique are:

- Encryption process cost that is utilized for HD videos.
- Inappropriate for making another process like watermarking on the encrypted video bits after the encryption process.

Because of NEA disadvantages, researchers thought in another effective technique that is called video selective encryption. The selective encryption technique encrypts the high sensitivity bits in the video that ensures the following criteria [8–10]:

- Tunability: The video encryption technique should be dynamic and flexible.
- Visual degradation: The video encryption technique should destroy the visualization of the video.
- Security: The video encryption technique should ensure the confidentiality of the video.
- Encryption ratio: The video encryption technique should improve video encryption ratio.
- Compression friendliness: The video encryption technique enhances video compressing efficiency.
- Format compliance: The video encryption technique must use standard coding technique for decoding the encrypted video.

Many of the video selective encryption techniques use the encryption standard algorithms like AES and DES for encrypting the most sensitive video bits. The contribution of the HEVC selective encryption technique is to encrypt the sensitive bits of the video with low delay time, keeping the bit rate of the HEVC and format compliance [9].

The main aim of this paper is to present an efficient Healthcare video consultations using selective encryption technique. The paper project proposes an efficient selective encryption technique for the most recent video coding standard HEVC that can be used in the real-time healthcare video consultations [10]. The proposed technique will ensure the confidentiality of the healthcare video consultations which has become easy to transmit through the internet. With the spread of COVID-19, there is an essential need for the use of video consultations to assist patients

in their houses while keeping access to the healthcare they need. Decreasing public meetings of COVID-19 will slow COVID-19 spread [4].

This rest of paper is sectioned as follows. Section 2 explains and presents the previous related HEVC SE encryption schemes. Section 3 presents the proposed HEVC ChaCha20-based SE scheme for health video consultations. Section 4 compares the performance of the proposed HEVC ChaCha20-based SE scheme and HEVC SE method in [11] and illustrates the analysis of the security for the proposed HEVC ChaCha20-based SE scheme. Section 5 presents the main conclusions of the paper.

2 HEVC SE Schemes

This paper aims to develop a selective encryption algorithm for the most recent video coding standards (HEVC) [12]. This part briefly overviews and provides the necessary background and preliminaries of the proposal. The security of healthcare video consultation is very interesting challenge to protect the video consultation content from attacks while storing or during transmission through the internet [13,14]. The below discussion will give review for the most popular video encryption techniques [15].

Naive algorithm is a method for encrypting the entire video bit stream using standard encryption algorithms. This algorithm is not suitable to be used for video with large size be because it is very slow and its computational overhead will be unacceptable especially for real-time video applications [16]. In [17], a secure MPEG (SECMPEG) has been proposed by Meyer and Gadegast as a selective video encryption technique for MPEG-1. The SECMPEG algorithm performs encryption for the headers of sequence and slice layers, extra I-frames blocks DCT coefficients, entire I/P/B-frames blocks, and the whole MPEG-1. In [18], the authors presented a secure real-time MPEG compressed video that uses the DES encryption to encrypt only the MPEG video I-frame, the sequence header and the IOS end code. In [11], the authors proposed a HEVC encryption technique that uses the AES-128 encryption algorithm for producing pseudo-random bits and performed XOR with some selective sensitive HEVC bits. In [19], the authors proposed a fast MPEG video encryption algorithm (VEA). The MPEG VEA divided the video stream into portions. Each portion is divided into odd list, and even list. The even list is encrypted and XOR with the odd list streams. In [20], the authors presented a selective encryption algorithm for H.264 transcoder to encrypt the transform coefficient and motion vector sign bits. The encryption algorithm can be adaptive depends on the application characteristics. For applications like TV on mobile phone and real time applications that do not need high quality, sign bits encryption would be more appropriate. In [21], the authors proposed an H.264 selective video encryption scheme that uses the AES-128 in OFB mode for encrypting the DCs and some of the ACs coefficients. In [22], the authors presented an H.264/AVC chaotic based selective encryption algorithm to encrypt parameters in context based adaptive variable length coding (CAVLC) mode by using multiple Rényi chaotic maps. It preserves the video format compliance with providing sufficient protection. In [23], the authors introduced an H.264/SVC scalable and format compliant encryption scheme. This scheme is used to protect the scalable video coding and to keep its format compliant. It encrypts the video coding layer in the base layer of the SVC. In [24], the authors proposed an HEVC transparent selective encryption by the encryption of DCT sign bits of AC coefficients for HEVC video coding standard. In [25], the authors introduced an HEVC selective encryption scheme that modifies the scheme in [24] by the encryption of DCT sign bits of AC coefficients and transform skip bits for HEVC. In [26], the authors introduced an HEVC Visual

Protection scheme that utilizes the AES-128 in CFB mode to encrypt the DCT truncated rice binstrings in the entropy stage of the HEVC video coding standard.

3 HEVC SE Schemes

The ChaCha20 is a 256-bit stream cipher algorithm that is developed by Daniel J. Bernstein for guaranteeing high-security performance [27]. ChaCha20 uses the block method through similar key and consecutively growing block counter parameters. After that ChaCha20 generates the keystream by writing the numbers in little-endian order. Then the keystream is XORed with a plain text to generate the cipher text [28,29]. The ChaCha20 algorithm shown in Fig. 1 depends on the Quarter-Round operation depicted in Fig. 2 that represents the core round algorithm and defined by Eqs. (1)–(4) as [30]:

$$W = W + X; \quad Z = Z \oplus W; \quad Z = (Z) \lll 16 \tag{1}$$

$$Y = Y + Z; \quad Y = X \oplus Y; \quad X = (X) \lll 12 \tag{2}$$

$$W = W + X; \quad Z = Z \oplus W; \quad Z = (Z) \lll 8 \tag{3}$$

$$Y = Y + Z; \quad X = X \oplus Y; \quad X = (X) \lll 7 \tag{4}$$

Fig. 3 presents the block diagram for the proposed ChaCha20-based HEVC SE technique that is used in the healthcare video consultation. The proposed ChaCha20-based HEVC SE uses the low complexity ChaCha20 encryption algorithm to encrypt the bits in the bypass mode in the entropy process of the HEVC coding standard to ensure the video format compliance [24,25]. These bits include the sign bits of the DCT coefficients and MVD, the DCT remaining absolute value suffixes, MVD absolute value suffixes, and dQP sign bits [26].

Algorithm 1 : ChaCha20	
Inputs :	Cipher Key K
	Counter C
	Nonce N
	Plain text P
Outputs : Cipher text E	
B ← [K,C,N]	
B" ← B	
For i = 0 To 10 do	
Q-Round (B0, B4, B8, B12)	
Q-Round (B1, B5, B9, B13)	
Q-Round (B2, B6, B10, B14)	
Q-Round (B3, B7, B11, B15)	
Q-Round (B0, B5, B10, B15)	
Q-Round (B1, B6, B11, B12)	
Q-Round (B2, B7, B8, B13)	
Q-Round (B3, B4, B9, B14)	
End For	
B ← B + B"	
E ← B ⊕ P	
Return E	

Figure 1: ChaCha20 algorithm

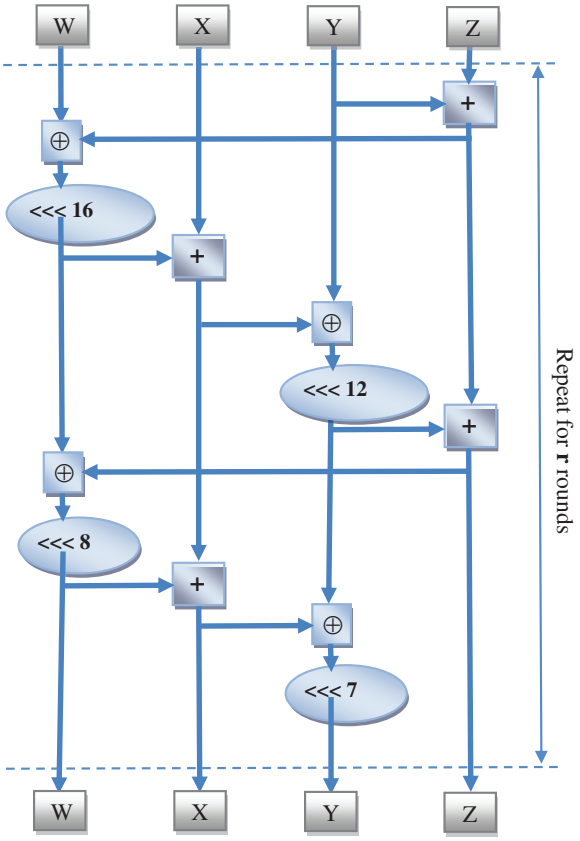

Figure 2: The block diagram for quarter-round operation

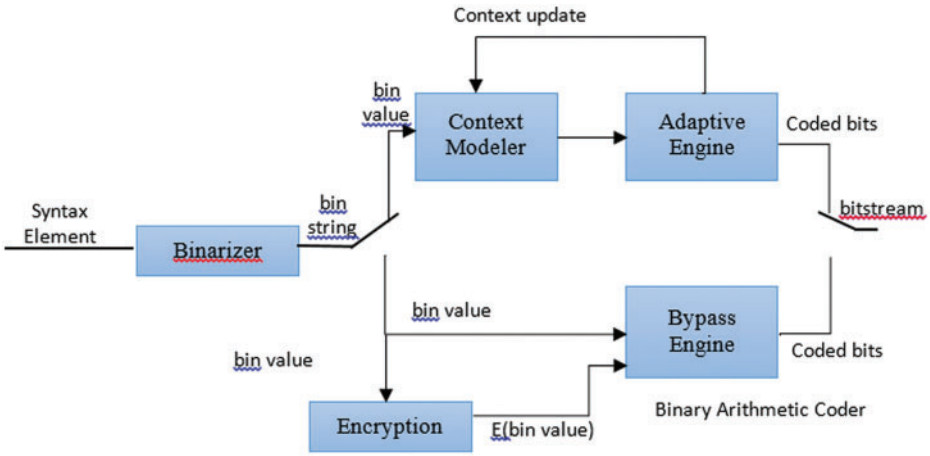

Figure 3: Block diagram of the proposed technique

The proposed HEVC ChaCha20-based SE scheme shown in Fig. 3 can be described as follows:

- The ChaCha20 encryption algorithm with key K is used to generate a pseudo-random Bits S which can be represented using Eq. (5) as:

$$S = ChaCha20(K) \tag{5}$$

- The S is XORed with each binarized syntax element for generating the encrypted syntax elements.

4 Performance Study

Due to the rapid increase of video applications through the internet, the video security has been a challenged topic to preserve the confidentiality and integrity of multimedia contents against the hackers. The paper presents a HEVC ChaCha20-based SE scheme for healthcare video consultation that is based on the latest video coding standard HEVC. The proposed HEVC ChaCha20-based SE scheme should have the features of keeping video format compliance and fixed video bit rate. The proposed HEVC ChaCha20-based SE scheme for healthcare video consultation will be developed using selective encryption algorithm on the HM16.0 reference software that is used as research tool for implementing the HEVC. The research methodology can be defined as follows:

(a) Use the HM16.0 to produce the original HEVC bitstream without encryption for the video dataset that defined in Tab. 1.
(b) Use the HM16.0 to produce the encrypted HEVC bitstream by applying standard encryption algorithms like AES encryption algorithm encryption for the video dataset that defined in Tab. 1.
(c) Use the HM16.0 to produce the encrypted HEVC bitstream by applying ChaCha20 encryption algorithm encryption for the video dataset that defined in Tab. 1.
(d) Compare the complexity between the proposed and the previous related work techniques.
(e) Use the MSU Tool to evaluate the PSNR and SSIM between the videos generated from the proposed and the previous related work techniques [31–33].
(f) Introduce the security analysis for the proposed techniques to guarantee the strength of the proposed HEVC ChaCha20-based SE scheme for healthcare video consultation against the unauthorized attacks for the video dataset that defined in Tab. 1.

Table 1: Videos Dataset [34]

Name	Resolution	Frequency (frame per second)
PeopleOnStreet	2560 × 1600	60
BasketballDrive	1920 × 1080	60
PartyScene	832 × 480	60
Mobile	253 × 288	60

4.1 PSNR and SSIM Analysis

Tabs. 2 and 3 give the mean PSNR and SSIM of the proposed HEVC ChaCha20-based SE method in [11] for the PeopleOnStreet at different QP values. Tab. 2 illustrates that the proposed ChaCha20-based HEVC SE scheme generates encrypted videos with lower PSNR values than

their corresponding encrypted videos that generated by HEVC SE scheme in [11] at different QP values. These results confirm and ensure the efficiency of the proposed ChaCha20-based HEVC SE scheme over HEVC SE scheme in [11] at different QP values. Tab. 3 provides that the proposed ChaCha20-based HEVC SE scheme generates encrypted video with lower SSIM values than their corresponding encrypted videos that generated by HEVC SE scheme in [11] at different QP values. These results again confirm and guarantee the efficiency of the proposed ChaCha20-based HEVC SE scheme over HEVC SE scheme in [11] at different QP values. Fig. 4 shows the results of encrypting the PeopleOnStreet at different QP values.

Table 2: Mean PSNR at various values of QP

QP values	Original	The proposed ChaCha20-based HEVC SE	Glenn HEVC SE in [11]
40	29.56	9.34	12.89
24	41.08	9.05	13.1
8	53.6	9.147	12.79

Table 3: Mean SSIM at various values of QP

QP values	Original	The proposed ChaCha20-based HEVC SE	Glenn HEVC SE in [11]
40	0.984477	0.105398	0.345
24	0.998825	0.198378	0.314
8	0.999934	0.244854	0.269

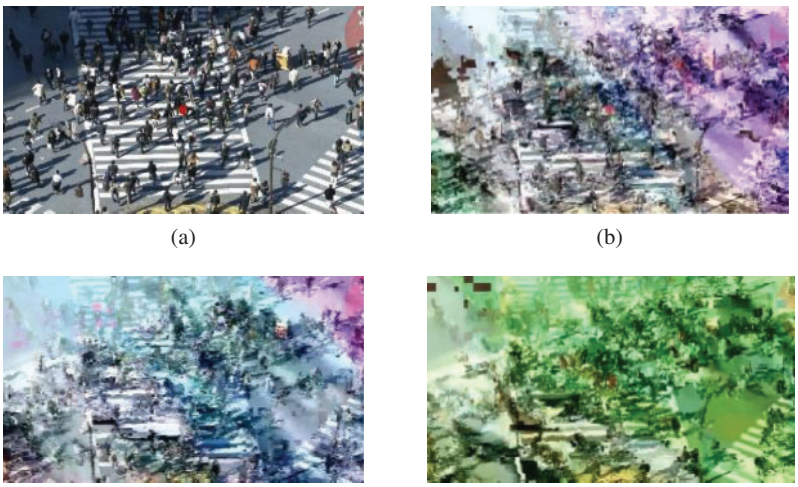

Figure 4: Encryption results of PeopleOnStreet video at vatious QP values (a) Original PeopleOnStreet video frame (b) Encrypted video at QP = 40 (c) Encrypted video at QP = 24 (d) Encrypted video at QP = 8

4.2 Histograms Test

Fig. 5 presents the histogram results for frame #50 of the compressed PeopleOnStreet plain-video and ciphervideo using the suggested HEVC ChaCha20-based SE scheme at various values

of QP. The achieved results indicate that the histograms for frame #50 of the of the compressed PeopleOnStreet ciphervideo are completely distinguishable from the histogram for frame #50 of the of the compressed PeopleOnStreet plainvideo at various QP values.

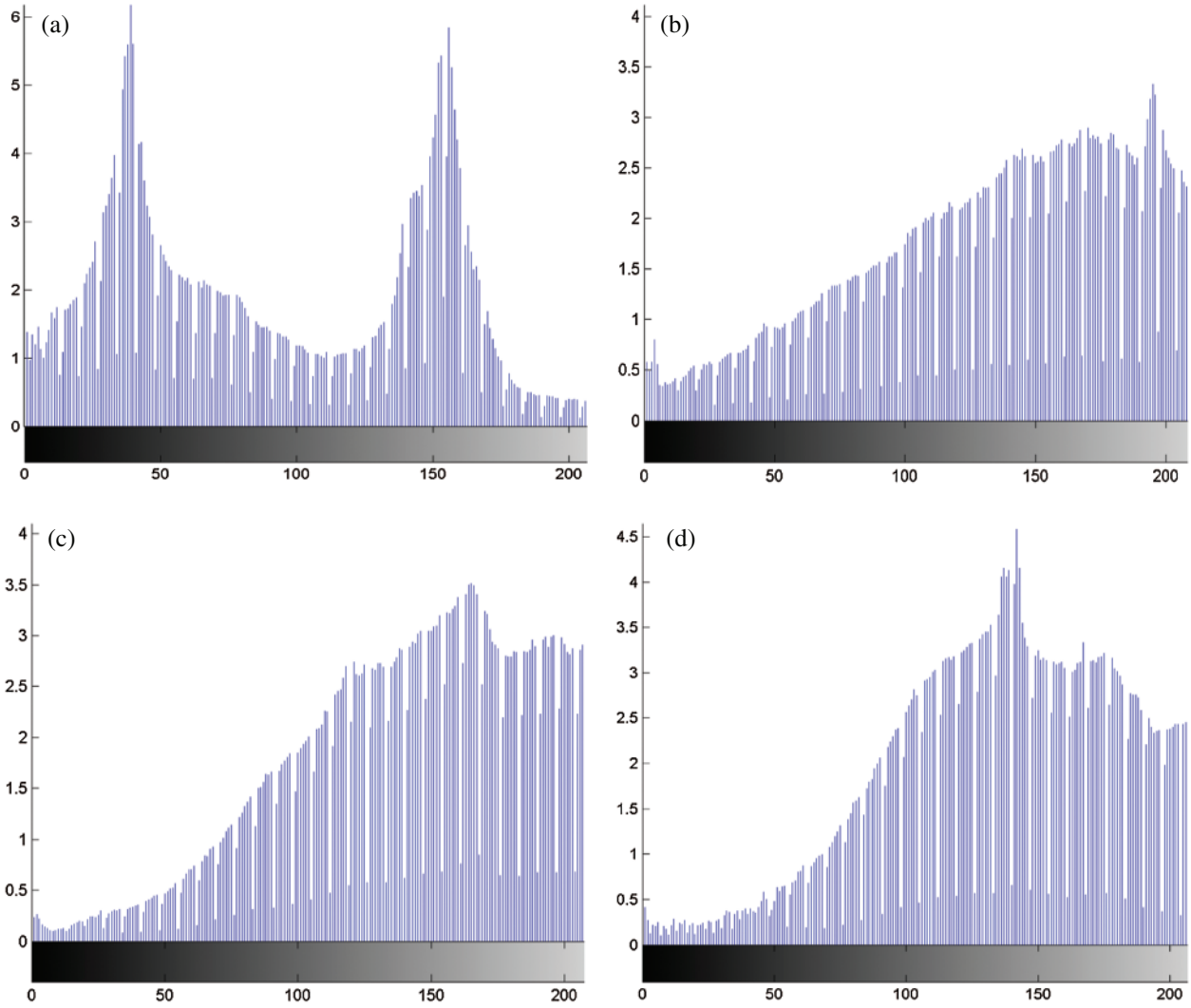

Figure 5: Histogram results of PeopleOnStreet video frame #50 at various QP values (a) Original PeopleOnStreet frame #50 histogram (b) Encrypted frame histogram at QP = 40 (c) Encrypted frame histogram at QP = 24 (d) Encrypted frame histogram at QP = 8

4.3 Correlation Coefficient Analysis

Tab. 4 and Fig. 6 show the histogram correlation coefficients results of the proposed HEVC ChaCha20-based SE scheme for tested videos in Tab. 1. From the achieved results shown in Fig. 5 and Tab. 4, it is obvious that the proposed HEVC ChaCha20-based SE scheme has small values of correlation coefficients in horizontal, vertical, and diagonal directions that ensures acceptable

video visual distortion which in turn can guarantee the confidentiality of the proposed HEVC ChaCha20-based SE scheme for real time health video consultations.

Table 4: Correlation coefficients outcomes of the proposed HEVC ChaCha20-based SE scheme for the tested videos given in Tab. 1

Direction	Mobile	PartyScene	BasketballDrive	PeopleOnStreet
Horizontal	0.29989	0.20983	0.55381	−0.01745
Vertical	0.26864	0.27012	0.51921	−0.094264
Diagonal	0.30769	0.23155	0.53213	−0.1176

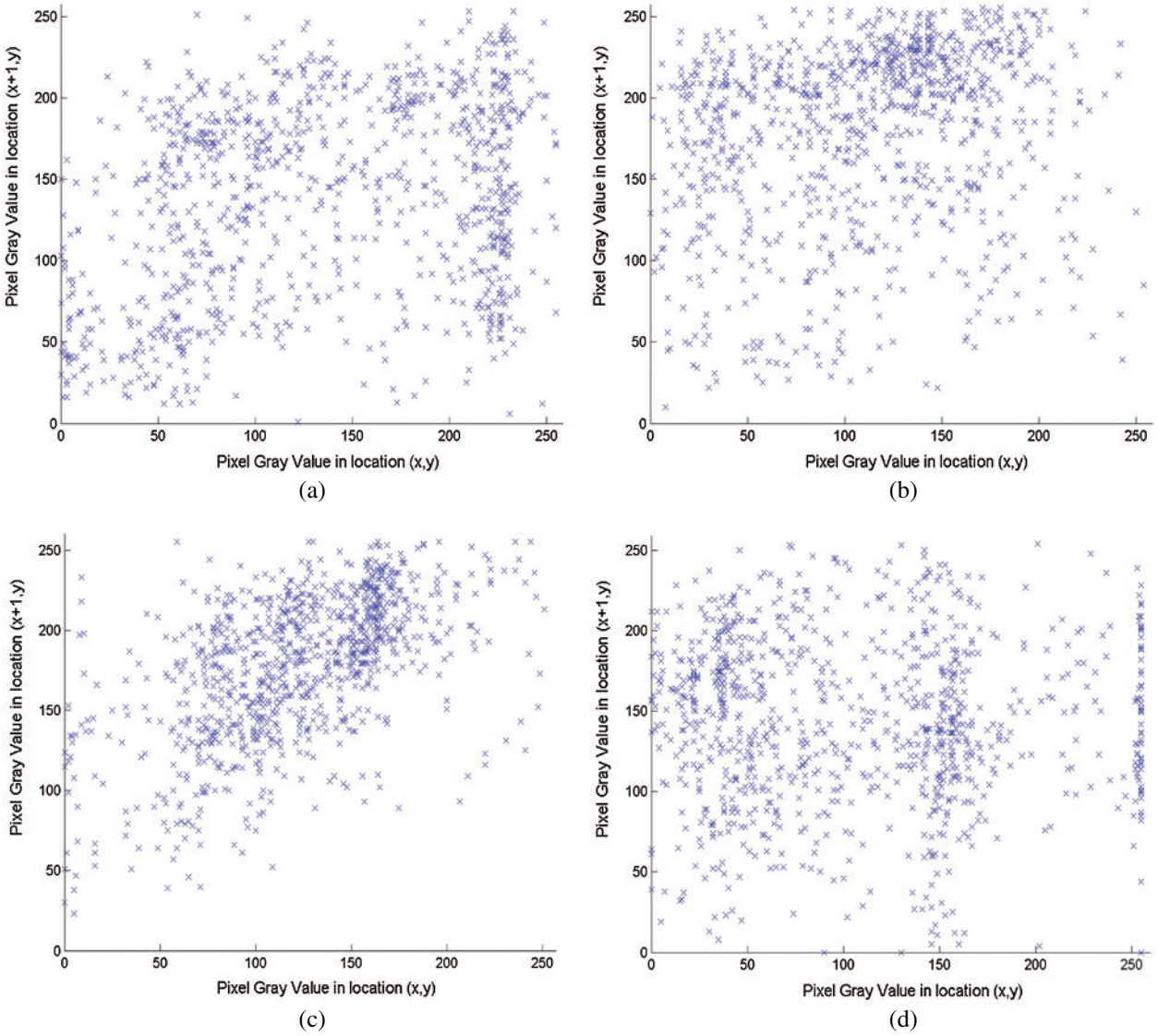

Figure 6: Correlation coefficients outcomes of the proposed HEVC ChaCha20-based SE scheme for the tested videos given in Tab. 1. (a) Mobile (b) PartyScene (c) BasketballDrive (d) PeopleOn-Street sequence

4.4 Encryption Quality (EQ) Analysis

Tab. 5 gives the encryption quality (EQ) results of the proposed HEVC ChaCha20-based SE scheme for tested videos shown in Tab. 1 at various QP values.

The achieved EQ results given in Tab. 5 prove that the proposed HEVC ChaCha20-based SE scheme has high encryption quality (EQ) values for all tested videos in Tab. 1 at various QP values that can provide acceptable video visual distortion which again in turn can guarantee the confidentiality of the proposed HEVC ChaCha20-based SE scheme for real time health video consultations.

Table 5: EQ results of the proposed HEVC ChaCha20-based SE scheme for tested videos given in Tab. 1 at various QP values

QP	HEVC stream			
	Mobile	PartyScene	BasketballDrive	PeopleOnStreet
40	659.47	4090.4	19964	29659
24	816.48	4505.5	11524	38186
8	644.67	1760.8	17324	33890

4.5 Edges Detection Protection

Tab. 6 and Fig. 7 show the EDR results of the proposed ChaCha20-based HEVC SE scheme for plain/cipher video frame #50 of all tested videos in Tab. 1. The achieved EDR results in Tab. 6 and Fig. 7 prove that Lack of similarity for plain/cipher video frame #50 of all tested videos in Tab. 1, and this can guarantee the efficiency of the proposed ChaCha20-based HEVC SE scheme for real time health video consultations.

Table 6: EDR results of the proposed HEVC ChaCha20-based SE scheme for frame #50 of all tested videos given in Tab. 1

HEVC stream	Mobile	PartyScene	BasketballDrive	PeopleOnStreet
EDR	0.8939	0.8695	0.8906	0.8573

4.6 Information Entropy Test

The information entropy results of the proposed HEVC ChaCha20-based SE scheme for video frame #50 of all tested videos are presented in Tab. 7. The achieved results demonstrate that the proposed HEVC ChaCha20-based SE scheme has information entropy values closed to 8 for video frame #50 of all tested videos in Tab. 1 which ensure providing acceptable video visual distortion and in turn can guarantee the immunity of the proposed HEVC ChaCha20-based SE scheme with respect to entropy attack.

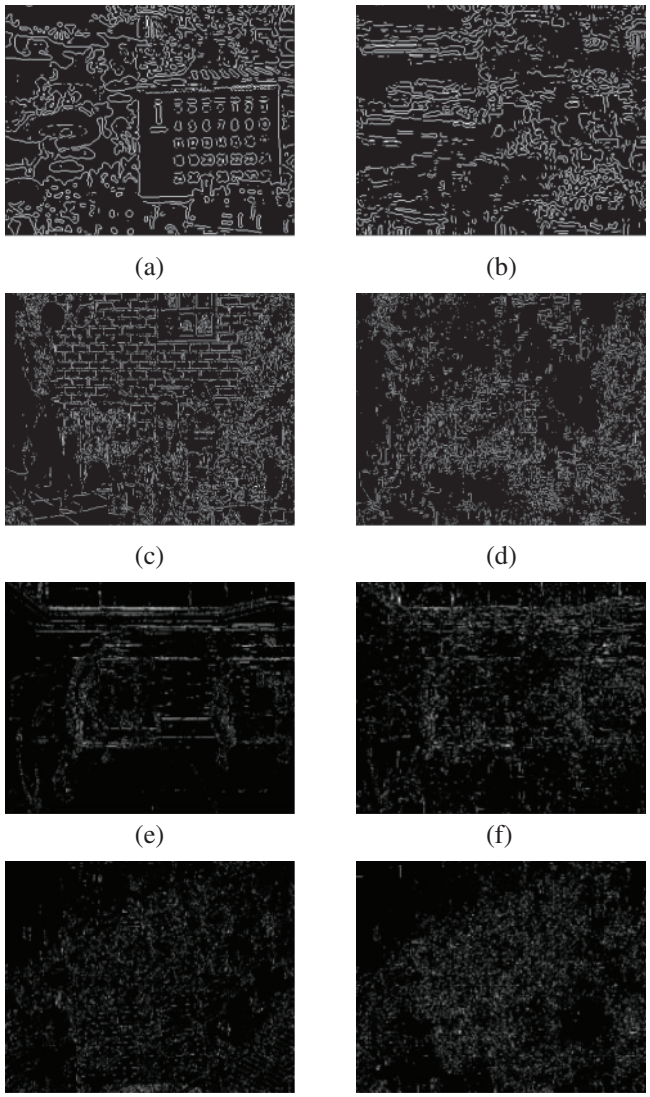

Figure 7: Laplacian of Gaussian EDR of the proposed HEVC ChaCha20-based SE scheme for frame #50 of all tested videos given in Tab. 1. (a) Original mobile (b) Encrypted mobile (c) Original PartyScene (d) Encrypted PartyScene (e) Original BasketballDrive (f) Encrypted BasketballDrive (g) Original PeopleOnStreet (h) Encrypted PeopleOnStreet

Table 7: Information entropy of the proposed HEVC ChaCha20-based SE scheme for frame #50 of all tested videos given in Tab. 1

HEVC stream	Mobile	PartyScene	BasketballDrive	PeopleOnStreet
Entropy	7.5398	7.191	6.613	7.5998

5 Conclusions

This paper focuses on protecting the confidentiality of the most recent digital video coding which is the HEVC that is used in the most new healthcare video consultation applications. The main contribution of this paper is to develop an efficient HEVC ChaCha20-based SE scheme with the features of keeping the video format compliance, same bit rate, and security with low computational complexity constraints to be used in video consultation real-time applications. The proposed HEVC ChaCha20-based SE scheme preserves the format compliance by encrypting some HEVC syntax elements that any modifications on them will have no impact on keeping features like low delay time, fixed bit rate of the HEVC, and format compliance. The HEVC ChaCha20-based SE scheme uses the ChaCha20 for encrypting the MVD sign bits and the DCT coefficients in HEVC entropy phase. The main contribution of HEVC ChaCha20-based SE scheme is using ChaCha20 to encrypt the most sensitive bits of the video that maintains and keeps low delay time, fixed bit rate of the HEVC, and format compliance. Also, the proposed HEVC ChaCha20-based SE scheme for health video consultations is compared with Glenn et al. HEVC SE scheme. The comparison illustrates that the HEVC ChaCha20-based SE scheme for health video consultations decreases the encoding time for low resolution and high resolution videos by 2 and 23 s respectively. Also, the security analysis shows that the HEVC ChaCha20-based SE scheme for health video consultations has an acceptable HEVC visual distortion that keep the confidentiality of the real time video consultations against almost attacks.

Acknowledgement: The authors would like to thank the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/08), Taif University, Taif, Saudi Arabia for supporting this research work.

Funding Statement: This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/08), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Doshi, Y. Platt, J. R. Dressen, B. K. Mathews and J. C. Siy, "Keep calm and log on: Telemedicine for COVID-19 pandemic response," *Journal of Hospital Medicine*, vol. 15, pp. 302–304, 2020.

[2] D. Kobayashi, T. Otsubo and Y. Imanaka, "The effect of centralization of health care services on travel time and its equality," *Health Policy*, vol. 119, no. 3, pp. 298–306, 2015.

[3] Y. L. Basta, K. Tytgat, H. H. Greuter, J. H. J. Klinkenbijl, P. Fockens *et al.,* "Organizing and implementing a multidisciplinary fast track oncology clinic," *International Journal for Quality in Health Care*, vol. 29, no. 7, pp. 966–971, 2017.

[4] T. Greenhalgh, J. Wherton, S. Shaw and C. Morrison, "Video consultations for COVID-19," *BMJ*, vol. 368 m998, pp. 1–2, 2020.

[5] J. G. Zamora, J. L. Alave, D. F. Corvino and A. Fernandez, "Videoconferences of infectious diseases: An educational tool that transcends borders. A useful tool also for the current COVID-19 pandemic," *Le Infezioni in Medicina*, vol. 28, no. 2, pp. 135–138, 2020.

[6] A. Sallam, E. EL-Rabaie and O. S. Faragallah, "Performance study of HEVC and H.264 video coding standards," *Menoufia Journal of Electronic Engineering Research*, vol. 27, no. 1, pp. 237–259, 2018.

[7] D. Galiano, A. Del Barrio, G. Botella and D. Cuesta, "Efficient embedding and retrieval of information for high-resolution videos coded with HEVC," *Computers & Electrical Engineering*, vol. 81, no. 12, pp. 106541, 2020.

[8] A. Sallam, E. EL-Rabaie and O. S. Faragallah, "HEVC selective encryption using RC6 block cipher technique," *IEEE Transactions on Multimedia*, vol. 20, no. 7, pp. 1636–1644, 2018.
[9] F. Peng, X. Zhang, Z. Lin and Min Lon, "A tunable selective encryption scheme for H.265/HEVC based on chroma IPM and coefficient scrambling," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 8, pp. 2765–2780, 2020.
[10] M. Asghar, R. Kousar, H. Majid and M. Fleury, "Transparent encryption with scalable video communication: Lower-latency, CABAC-based schemes," *Journal of Visual Communication and Image Representation*, vol. 45, no. 1, pp. 122–136, 2017.
[11] G. Wallendael, A. Boho, J. Cock, A. Munteanu and R. Walle, "Encryption for high efficiency video coding with video adaptation capabilities," *IEEE Transactions on Consumer Electronics*, vol. 59, no. 3, pp. 634–642, 2013.
[12] Fraunhofer Heinrich Hertz Institute, "High efficiency video coding: HEVC software repository," 2015. [Online]. Available: https://hevc.hhi.fraunhofer.de, Access Date: 1/6/2020.
[13] A. Bovik, *Hand Book of Image and Video Processing. Chapter 6*. San Diego, CA: Elsevier Academic Press, 2005.
[14] A. Sallam, E. EL-Rabaie and O. S. Faragallah, "Comparative study of video compression techniques," *Menoufia Journal of Electronic Engineering Research*, vol. 27, no. 1, pp. 1–32, 2018.
[15] M. Abomhara, O. Zakaria and O. O. Khalifa, "An overview of video encryption techniques," *International Journal of Computer Theory and Engineering*, vol. 2, no. 1, pp. 103–110, 2010.
[16] A. Babatunde, R. Jimoh, O. Abikoye and B. Isiaka, "Survey of video encryption algorithms," *Journal of Informatics & Communication Technology*, vol. 5, no. 1, pp. 65–80, 2017.
[17] A. Sallam, E. EL-Rabaie and O. S. Faragallah, "CABAC-based selective encryption for HEVC using RC6 in different operation modes," *Journal of Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28395–28416, 2018.
[18] G. Spanos and T. Maples, "Security for real-time MPEG compressed video in distributed multimedia applications," in *Conf. on Computers and Communications*, Scottsdale, AZ, USA, pp. 72–78, 1996.
[19] C. Shi and B. Bhargava, "A fast MPEG video encryption algorithm," in *Proc. of the 6th Int. Multimedia Conf.*, Bristol, UK, 1998.
[20] M. Nithin, L. Damien and R. David, "A novel secure H.264 transcoder using selective encryption," in *Proc. of the IEEE Int. Conf. on Image Processing*, San Antonio, TX, USA, pp. 85–88, 2007.
[21] W. Yajun, C. Mian and T. Feng, "Design of a new selective video encryption scheme based on H.264," in *Proc. of the Int. Conf. on Computational Intelligence and Security*, Harbin, China, pp. 1–5, 2007.
[22] O. Lui and K. Wong, "Chaos-based selective encryption for H.264/AVC," *Systems and Software*, vol. 86, no. 12, pp. 3183–3192, 2013.
[23] Z. Wei, Y. Wub, X. Ding and R. Deng, "A scalable and format-compliant encryption scheme for H.264/SVC bitstreams," *Signal Processing: Image Communication*, vol. 27, no. 9, pp. 1011–1024, 2012.
[24] H. Hofbauer, A. Unterweger and A. Uhl, "Transparent encryption for HEVC using bit-stream-based selective coefficient sign encryption," in *Proceedings of IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Florence, Italy, pp. 1986–1990, 2014.
[25] Y. Tew, K. Minemura and K. Wong, "HEVC selective encryption using transform skip signal and sign bin," in *Proc. of APSIPA Annual Summit and Conf.*, Hong Kong, China, pp. 963–970, 2015.
[26] Z. Shahid and W. Puech, "Visual protection of HEVC video by selective encryption of CABAC binstrings," *IEEE Transactions on Multimedia*, vol. 16, no. 1, pp. 24–36, 2014.
[27] D. J. Bernstein, "ChaCha, a variant of Salsa20," in *Workshop Record of SASC 2008: The State of the Art of Stream Ciphers*, Lausanne, Switzerland, pp. 1–6, 2008.
[28] J. P. Aumasson, S. Fischer, S. Khazaei, W. Meier and C. Rechberger, "New features of latin dances: Analysis of Salsa, ChaCha, and Rumba," in *Fast Software Encryption. LNCS*, K. Nyberg, (Eds.), vol. 5086. Lausanne, Switzerland, Springer, pp. 470–488, 2008.
[29] A. Langleyand, W. Chang, N. Mavrogiannopoulos, J. Strombergson and S. Josefsson, "ChaCha20-poly1305 cipher suites for transport layer security (TLS)," in *Internet Requests for Comments RFC 7905*, Internet Engineering Task Force (IETF), pp. 1–8, 2016. https://datatracker.ietf.org/doc/html/rfc7905.

[30] F. De Santis, A. Schauer and G. Sigl, "ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications," in *Design, Automation & Test in Europe Conf. & Exhibition*, Lausanne, Switzerland, pp. 692–697, 2017.

[31] MSU Graphics and Media Lab, "Video group, MSU codecs," 2020. [Online]. Available: www.compression.ru/video/, Access Date: 1/6/2020.

[32] A. Sallam, E. EL-Rabaie and O. S. Faragallah, "Efficient HEVC selective stream encryption using chaotic logistic map," *Journal of Multimedia Systems*, vol. 24, no. 4, pp. 419–437, 2017.

[33] O. S. Faragallah, A. A.Afifi, H. S. El-sayed, M. A. AlZain, J. F. Al-Amri *et al.,* "Efficient HEVC integrity verification scheme for multimedia cybersecurity applications," *IEEE Access*, vol. 8, pp. 154112–154135, 2020.

[34] Xiph.org video test media, "MJPEG tools," [Online]. Available: https://media.xiph.org/video/derf/, Access Date: 1/6/2020.