AVC VIDEO SECURITY ON WIRELESS CHANNEL

Mrs, Rajashree N.Mandavgane[1] and Dr.N.G.Bawane[2]

[1]Nagpur University, B. D. College of Engineering, Sevagram Wardha, India

[2]Nagpur University, Professor, S.B.Jain Engineering college, Nagpur, India

ABSTRACT

The security of multimedia transmission is very important in today's life. It is a challenge to transfer the huge multimedia data mostly because of big file sizes and limited bit rates, which are still at a premium. Hence, the data to be sent has to be compressed. H.264/AVC is the best and practical solution available today to achieve this. If the data is made secure by good encryption after compression without changing the size of the compressed file, it is even better. This paper makes an attempt to achieve exactly this. If the data is encrypted after the compression, the software used for compression need not be changed. In this technique, use of selective encryption is applied without altering the compression software. Here, the data is first identified for I-frame which is selected for encryption. This selected data is then sliced and each slice data without slice header is encrypted using AES algorithm. After decoding the file, the frame can be seen to be distorted compared to the original one. When the video is decrypted with proper key, the video obtained which is the same as decoded without encryption.

KEYWORDS

H.264AVC, OFDM, AES, Selective encryption etc.

1. INTRODUCTION

Use of internet multimedia applications is increasing rapidly. Human life is very much dependant on internet which carries such multimedia data. Due to this, the multimedia data and its security while transmitting become very vital. The information to be sent for a large number of users and maintenance of security of the multimedia data in such cases is a big problem. There are some applications like video on demand, TV broadcasts which requires good security. Also the stored data is required to be transmitted reliably. There are many ways to secure this multimedia data. One of these is cryptography which is necessary when the data is transmitted over untrustworthy or lossy networks. When the sender and the receiver refer the same key the cryptography is called the symmetric key cryptography. Here AES (Advanced Encryption Standard) algorithm for symmetric key cryptography is used as one of the options for ensuring the security.

Following is some previous work referred to for achieving this. Considering the encryption before compression a method converting the yuv file to bitmap and then applied encryption to that binary data in [11] was shown. In [2], the input sequence of the YUV video is first compressed through H.264/AVC, then the I-frame is identified and finally, I-frame is partially encrypted using AES algorithm whereas in the proposed work, I-frame is sliced using FMO [Flexible Macroblock Ordering] and then the bits excluding slice header bits are encrypted using AES algornghm. In [4], selective encryption is performed on the I-frames and P-frames for both types of coding as CAVLC and CABAC along with compression which needs to modify the program for H.264 Codec. In [5], a new hierarchical Flexible Macroblock(MB) Ordering scheme

DOI : 10.5121/ijma.2016.8501

was proposed which also requires modification of the H.264 Codec program whereas in [1], a practical study of FMO for H.264/AVC was done.

This paper is organized as follows. Section 2 deals with discussion of basic features of the H.264 AVC. In Section 3, proposed encryption scheme along with the block diagram is given. In Section 4, results for the H.264/AVC are shown. In Section 5, conclusions are given.

2. H.264/AVC AND SELECTIVE ENCRYPTION

Until now a lot of literature has been published on H.264/AVC. It is a high performance video coding standard used in industry for compression. The H.264/AVC is described in a very lucid manner by [3] and [6]. In [9] and [10] H.264 is explained with all its input and output files. In AVC Codec software, the basic blocks are encoder and decoder. The encoder processes the frames in the units of MBs. So while considering the FMO the same unit is maintained for the slices of equal size. Three profiles are defined for the H.264/AVC which is baseline, main and extended. Each profile supports a set of functions. Here a baseline profile is considered for the experimentation as the potential application of the profile includes video telephony, videoconferencing and wireless communications. Two types of entropy coding are supported by the H.264 which are CAVLC and CABAC. A bit stream of baseline profile contains I-frames and P-frames only. P-frame depends upon the I-frame but the I-frame is independent. Modifying the slices of I-frame will automatically change the successive P-frames. This particular theme [2], is also used with the FMO and ASO for the distortion of the I slices. Baseline profile supports FMO and ASO (Arbitrary Slice Ordering).

Earlier, encryption was done over the entire data file, but the disadvantage of this approach is that, the software overheads were much more. It was then, that the researchers came up with an idea of selective encryption. Highly sensitive bits are selected from the file in such a way that the encryption time gets reduced and also the file can be distorted beyond recognition. This approach is now getting more prevalent as it saves time and efforts for both encryption and decryption.

3. PROPOSED SCHEME

In the proposed scheme, the original video is passed through the encoder. The Codec used is AVC. Then the bitstream is analyzed for the I-frame. It can be separated by the identifier as hex data 00 00 00 01 65. The identified I-frame is sliced using FMO. Here the dispersed FMO setting along with the 33MBs per slice and 2 slice groups are used. In AVC the slice is identified using the trace file. Following diagrams in figure1 and figure 2 show the theme of the proposed scheme.

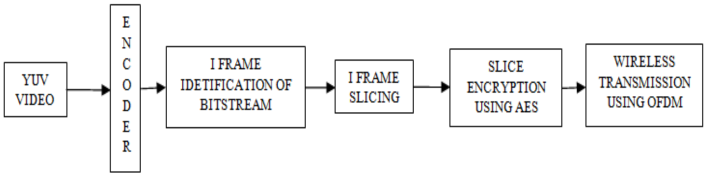

YUV VIDEO
ENCODER
I FRAME IDETIFICATION OF BITSTREAM
I FRAME SLICING
SLICE ENCRYPTION USING AES
WIRELESS TRANSMISSION USING OFDM

Figure 1. Encoding and Encryption of the Video

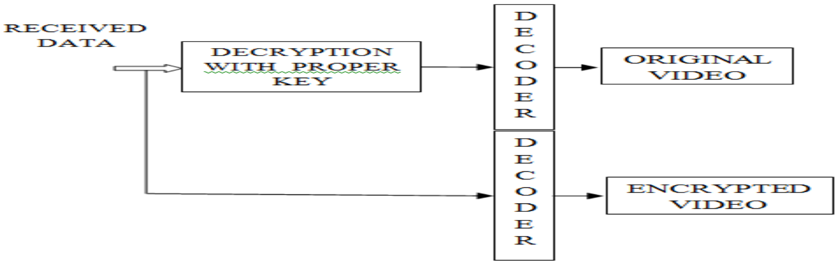


Figure 2. Decryption and Decoding of the Video

The MB organization without FMO and with FMO for different slices in AVC is obtained using trace file which gets matched with the settings for the encoder file of AVC. This organization is shown in Table 1 and Table 2 below. Different slices are fragmented into blocks of 16 bytes. These blocks are given as inputs to AES algorithm. For a specific key, these blocks are encrypted and the cipher text obtained for each block replaces the original 16 bytes block of the I-frame. Care is taken to see that, the slice header is excluded from being given as an input to AES. In AVC, any distortion in one slice has no effect on other undistorted slices.

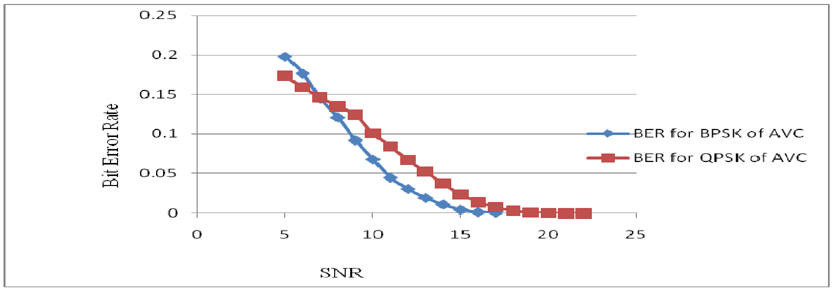


Figure 3. BER vs. SNR.

Table 1. Macroblock (MB) organization without FMO

SPS	PPS
SH of Slice 0	Slice 0 with 0 to 32 MBs
SH of Slice 1	Slice 1 with 33 to 65 MBs
SH of Slice 2	Slice 2 with 66 to 98 MBs

Table 2. Macroblock (MB) organization with FMO

SPS	PPS
SH of Slice 0	Slice 0 with first 33 even no. of MBs as 0,2,4….. to 64
SH of Slice 1	Slice 1 with remaining even no. of MBs as 66,68 .. to 98
SH of Slice 2	Slice 2 with first 33 odd no of MBs as 1,3,5……. to 65
SH of Slice 3	Slice 3 with remaining odd no. of MBs as 67,69 ….to 97

All the slices are encrypted and the encrypted file is passed through wireless channel using OFDM (orthogonal frequency division multiplexing). OFDM, which is a multicarrier system is used for wireless transmission applications and video broadcasting services. OFDM uses closely spaced orthogonal carriers that do not interfere with each other. OFDM with AWGN is used as a wireless channel. Different modulations such as [binary phase shift keying] BPSK and [quadrature phase shift keying] QPSK are applied for the data. The noise signal used is AWGN. Addition of the noise signal in the transmitted signal is gradually decreased so that the Signal to noise ratio [SNR] is increased. For the range of SNR from 5 dB to 25 dB the encrypted data is decrypted using the same key and their results are tabulated below as shown in Table 3. The graphs are plotted for the bit error rate [BER] vs SNR as shown in figure 3.

Table 3. SNR & Modulation for AVC.

AVC		
Foreman QCIF [10 frames]		
Parameters	BPSK	QPSK
SNR dB	5 to 25	5 to 25
Encoding Time	9.068 sec	9.068 sec
Encrypted Bits	14848	14848

The PSNR Y, U and V of encrypted video are measured with respect to original video and it is tabulated in Table 4 below. The part of the results from [4] are also shown here in Table 5 for the PSNR comparisons. Also frame wise encrypted video is shown in figure 5.

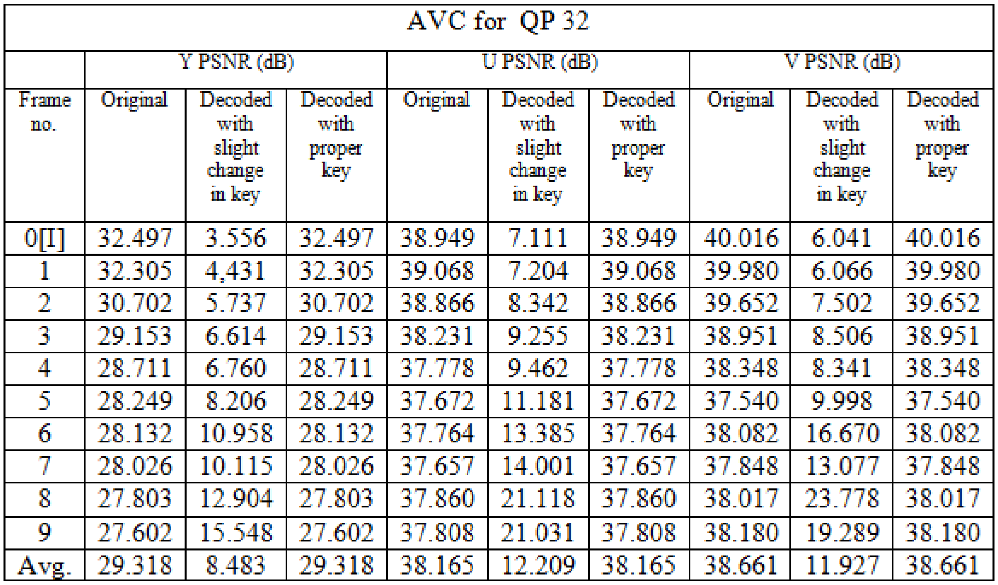
Table 4. PSNR for Original and Encrypted Video for AVC.

AVC for QP 32						
	Y PSNR (dB)		U PSNR (dB)		V PSNR (dB)	
Frame no.	Original	Encrypted	Original	Encrypted	Original	Encrypted
0[I]	32.497	6.226	38.949	7.25	40.016	5.574
1	32.305	4.411	39.068	7.193	39.980	6.058
2	30.702	5.295	38.866	7.824	39.652	6.671
3	29.153	6.315	38.231	8.641	38.951	7.506
4	28.711	6.825	37.778	9.463	38.348	8.342
5	28.249	7.853	37.672	10.370	37.540	9.313
6	28.132	11.180	37.764	13.888	38.082	10.320
7	28.026	11.973	37.657	15.285	37.848	12.029
8	27.803	12.879	37.860	22.123	38.017	17.648
9	27.602	13.089	37.808	21.711	38.180	14.893
Avg.	29.318	8.605	38.165	12.367	38.661	9.835

Table 5. PSNR Of I-Frame The Selective Encryption In [4]

AVC						
	Y PSNR (dB)		U PSNR (dB)		V PSNR (dB)	
QP	Original	SE in CAVLC	Original	SE in CAVLC	Original	SE in CAVLC
30	35.1	9.4	39.8	27.4	41.4	25.4
36	31.0	9.4	37.7	28.1	38.6	24.8

Table 6. PSNR for Original and Decoded Video with Proper Decryption Key and With Slight Change in Decryption Key



AVC for QP 32									
	Y PSNR (dB)			U PSNR (dB)			V PSNR (dB)		
Frame no.	Original	Decoded with slight change in key	Decoded with proper key	Original	Decoded with slight change in key	Decoded with proper key	Original	Decoded with slight change in key	Decoded with proper key
0[I]	32.497	3.556	32.497	38.949	7.111	38.949	40.016	6.041	40.016
1	32.305	4,431	32.305	39.068	7.204	39.068	39.980	6.066	39.980
2	30.702	5.737	30.702	38.866	8.342	38.866	39.652	7.502	39.652
3	29.153	6.614	29.153	38.231	9.255	38.231	38.951	8.506	38.951
4	28.711	6.760	28.711	37.778	9.462	37.778	38.348	8.341	38.348
5	28.249	8.206	28.249	37.672	11.181	37.672	37.540	9.998	37.540
6	28.132	10.958	28.132	37.764	13.385	37.764	38.082	16.670	38.082
7	28.026	10.115	28.026	37.657	14.001	37.657	37.848	13.077	37.848
8	27.803	12.904	27.803	37.860	21.118	37.860	38.017	23.778	38.017
9	27.602	15.548	27.602	37.808	21.031	37.808	38.180	19.289	38.180
Avg.	29.318	8.483	29.318	38.165	12.209	38.165	38.661	11.927	38.661

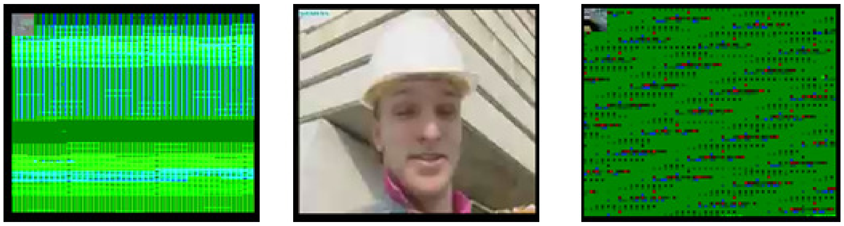
The video frames are also decoded with the change in the decryption key. Suppose a 16 byte encryption key is considered as below.

encr_key = [0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15].

For the same decryption key the resultant video is the same video as that can get decoded without encryption. But if the decryption key is slightly changed as below.

decr_key = [0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 05]

With the last byte is changed from 15 to 05 and remaining bytes are the same. The video is distorted. Both the frames are shown below in figure 4. Table 6 mentions the PSNR of decoded video with proper key and with slight change in key.

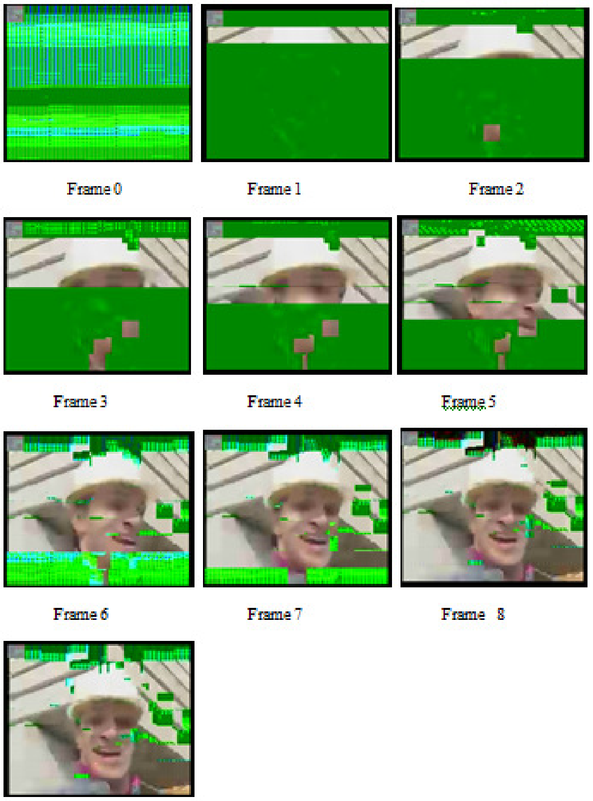


Decoded frame after encryption Decoded with proper key Decoded with slight change in key

Figure 4. Frames Decoded with Proper Decryption Key and with Slight Change in Decryption Key.

4. RESULT

In simulation, AWGN distorts the transmitted signal and it can be observed that for small SNR values, the BER is large. As the SNR is increased, the BER goes on reducing. Here it is observed that after the SNR value above 19 dB for BPSK, the bitstream is error free and gets decoded correctly and the bitstream is identical to that with bitstream decoded without encryption. Whereas BER above SNR 22 dB is zero in case of QPSK and the bitstream is error free. In the proposed method, Y PSNR in Table 4 is observed to be near about in the same range as in Table 5. But the U PSNR and V PSNR have been decreased as compared to Table 5. So it may be concluded that the encryption with the proposed method is more secured as compared to results in Table 5.



Frame 0 Frame 1 Frame 2

Frame 3 Frame 4 Frame 5

Frame 6 Frame 7 Frame 8

Frame 9

Figure 5. Frames After the I-Frame Encryption.

5. CONCLUSION

With an increase in the SNR value 22dB onwards as can be seen from the figure 3, as the bit error rate is zero the bitstream is the same as the original bitstream and gets decoded. The PSNR of this decoded bitstream is same as with the PSNR obtained for the bitstream without encryption. One more observation is that up to 4 to 5 frames the picture is unidentified if I frame is encrypted as seen from the figure 5. After that gradually the dependence of the other frames on the I-frame started decreasing. The frames are identified though they are blurred. So it can be concluded that if the number of I-frames are inserted at regular intervals of video frames, the security will also go on increasing. With respect to PSNR as mentioned in the result, the proposed method gives better security than the previous one.

REFERENCES

[1] Yves Dhondt, Peter Lambert, Stijn Notebaer &, Rik Van de Walle (2009) "Flexible Macroblock Ordering as a content adaptation tool in H.264/AVC" Proc of SPIE, Vol. 6015.

[2] M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan & B.B Zaidan (April 2010) "Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard" International Journal of Computer Theory and Engineering, Vol. 2, No. 2 pp. 223-229.

[3] Iain Richardson (2007) "An Overview of H.264 Advanced video coding" white paper.

[4] Zafar Shahid, Marc Chaumont & William Puech (May 2011) "Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames" IEEE Transactions on circuits and systems for video Technology vol. 21, no 5, pp. 565-576.

[5] Rong Luo & Bin Chen (Feb 2008) "A hierarchical scheme of flexible macroblock ordering for ROI based H.264/AVC video coding" ICACT, pp. 1579-1582.

[6] Iain E. Richardson(2008), The H.264 Advance Video Compression Standard, Wiley Second Edition.

[7] JSVM Software Manual, Version JSVM 9.19.14.

[8] H.264/14496-10 AVC Reference Software Manual May 2010.

[9] Mrs. R.N.mandavgane & Dr.N.G.Bawane(2013) "Appraisal of H.264 Codec" IJECSE vol. 2 , no.2 pp. 651-6

[10] Mrs. R.N.mandavgane & Dr.N.G.Bawane(2013) "Performance Evaluation of H.264 Codec" IJCA no.6 pp. 10-13

[11] Mrs. R.N.mandavgane & Dr.N.G.Bawane(2014) "Quality Assessment of Precodec Video Protection" IJARCSMS vol. 2, issue 1, pp. 264-268

AUTHORS

Mrs. Rajashree Nikhilesh Mandavgane received the B.E. degree in electronics and power engineering from Amravati University India, in 1987, and the M. Tech. in electronics engineering from the Visveswaraya regional college of engineering Nagpur, in 1994. In 1987, she joined the government polytechnic as a visiting lecturer at Amravati, in 1989 as a lecturer in Shegaon engineering college, Shegaon. Since December 1991, She has been with the B. D .College of Engineering, Svagram, where she was an lecturer, became an Associate Professor and currently as Head of the department of E&T. Her current research interests include digital electronics, and electronics. She is pursuing Ph. D. from Nagpur University. She is a Life Member of the Indian Society for Technical Education [ISTE] and the Institution of Engineer's

Dr. Narendra G. Bawane is a truly academician with active interest in Teaching and Research. He has total teaching experience of more than 25 years at graduate and Post-graduate level. He has completed his B.E. from Nagpur University in 1987 and M. Tech. in 1992 from IIT, New Delhi. He completed his Ph. D. in 2006 at VNIT, Nagpur.He has got more than 72 research papers to his credit in international and national Journals and Conferences. He is a reviewer of many reputed international Journals and member - programme committee of various international Conferences. He has worked in Government organization for several years and other reputed engineering colleges in the various capacities such as Head of Computer Science & Engineering, Electronics department, Dean

Autonomy etc. He was executive council member (Execom) and chair of SMC chapter of IEEE Bombay section which covers Maharashtra, MP, Chhattisgarh and Goa for year 2014-2015. He is active Execom member for year 2015-16.His areas of interest are Artificial Neural Network (ANN), Embedded system, Fuzzy logic system, Wavelet analysis, Hybrid intelligence, Image processing & Emotion in speech and facial recognition, Biomedical engineering etc. He is an Approved Ph. D. Supervisor in Electronics for Nagpur & Amravati Universities. He has guided 24 students at Postgraduate level. Total 06 candidates are pursuing Ph. D. under him in the field of Electronics and Electrical engineering. He is regularly invited by reputed organizations for expert talk. He has authored few books in the area of Microprocessor and Matlab Applications. He is senior member of IEEE and other professional societies such as CSI, ISTE. He strongly supports innovation and creativity in technical education. He is proud recipient of "Best Educationist Award 2012" conferred by International Institute of education and management, New Delhi.

.