# Experimental Analysis of two Encryption Schemes for Security of Video Streaming

**Rajashree Mandavgane, Narendra Bawane**

***Abstract*: With an exponential growth of multimedia and high speed internet, many relevant services and software are available for common person. Out of which, one of the applications is that common man wants to send multimedia data on internet. H.264 codec is used to compress this data by the systems. But data on the internet can be hacked, pirated or tampered with. Hence some security is required for multimedia data. In this paper, two schemes are provided for securing the video streaming after compression. One is with the proposed algorithm and the other with the standard algorithm(AES). In the second scheme, FMO is applied to bitstream which adds error resilience to the data. Both the schemes are applied selectively to I frame only of AVC/SVC. Performance is evaluated by finding PSNR for quality measurement.Alsooverheadbitandencodingtimearecompared. Security is discussed for some attacks. After considering the results for PSNR and discussion for other parameters, it is concluded that the second encryption scheme is much better as compared to the firstone.***

***Index Terms*: Bitstream, Encryption, FMO, H.264AVC/SVC, Security.***

## I. INTRODUCTION

This, due to fast growth of network bandwidth, improved compression techniques and advanced delivery technology, media communication over wireless networks, is rapidly increasing. Demand for multimedia services is increasing exponentially. Multimedia is distributed over open and generallyinsecurechannel.Piracyofsensitivedataisanother threat. Hence secure delivery of multimedia has become an important and critical concern. An attempt has been made to secure multimedia stream in thisproject.

For secure transmission of the data, it is protected before transmission. Primary solution for protecting the data is the encryption. Earlier, entire data was encrypted but nowadays selective and only sensitive parts are encrypted.

**Revised Manuscript Received on May 24, 2019.**

**Mrs. RajashreeMandavgane**, Electronics Engineering, Nagpur University, Nagpur, India.

**Dr. NarendraBawane**, Principal, Nagpur University Jhulelal Institute of Technology, Nagpur, India..

Surveyofencryptiontechniquesisdonein[1],[2]and[3]. Accordingly encryption algorithms are classified as pre compression, post compression and compression integrated encryptions. Preferred technology for compression is h.264 video codec. This is open source, free of charge with encoding & decoding programs supplied by the manufacturers. Hence, extra security is required.

In encryption before compression, Shi and Bhargava presented the VEA and its improved version RVEA in [6] whichencryptsmotionvectorswithPandBframes.Selective encryption using wavelet transform and DCT transform are proposed by W. Zeng and S. Lei in [7]. Both the schemesare found to be less secure for chosen plain text attacks.Manyresearchers have proposed different algorithms based obitplane encryption, bit level image encryption, permutation of pixels lying in the region of interests, SCANmethodology etc. P and B frames are also used instead of I frame in one of the methods ofencryption.

In encryption integrated compression, intra prediction mode encryption, inter prediction mode encryption, motion vector encryption, sign encryption of motion vector, Ex-Golomb code encryption for motion vector, secret transform, DCT coefficient encryption, secret scan order, entropy coding encryption are proposed in different research papers. Researchers tried encryption with single parameters as well as more than one parameters. In this category of encryption almost all the parameters are considered. Result obtained are also visually similar in almost all the schemes.

InencryptionaftercompressionencoderencodesYUVvideo and result is a bitstream. This bitstream have two different format as NALU and as per annexure B [8], dependent upon the encoder programming. Researcher considered different parameters of the bitstream for encryrpion. Depending on which parameter is used for encrytrpion, there are NALU encryption,containerformat,partial/selectiveencryption.M. Abomhara et al. in [9] presented the new scheme for partial encryption. Paper claims for low bit overhead and low computational complexity but does not give anyexplainationobout security issue. Some more schemes such as a selective encryption for RTP payload Equal to 101,103 and 104which are I frame, SPS and PPs respectively is proposed in [10]. Selective encryptionalgorithm used in encryption after compression are more suitable from the security point of view. This is because, already after compression there is no

any correlation between plaintext and compressed text. This compressed text if further encrypted; it will be very difficult forattackerstoattacksonthisciphertext.Henceinthispaper video is encrypted after compression.

## II. TWO DIFFERENTSCHEMES

In this paper, two different schemes are applied for encrypting the video before transmission.

### A. First ProposedScheme

In H.264AVC, baseline profile is considered for programming. Baseline profile encodes the video with only I and P frames. Algorithm is applied to only I frames selectively. All the ensuing frames are dependent on the I-frame. Hence, encrypting the I-frame affects the P frames following it. InIframes, all the Macro block softhe frames are encoded using intra prediction whereas in P frames some Macroblocks are coded using[a] interprediction.

The algorithm used for encryption before compression in [4 considered for encryption after compression. The only differenceinstepsofalgorithmisthattheextrastepofIframe separation is inserted. I frame is identified in the bitstream after encryption using the hex code 65. Fig 1 shows the proposed scheme where as Fig 2 shows the flowchart for the proposed algorithm of I frame encryption respectively. The algorithm is applied to AVC and SVC. When the encrypted videoisdecoded,itisobservedthattheIframeinAVCandI and one P frame in SVC are missing as shown in bar chart in Fig 3 and 4 respectively.

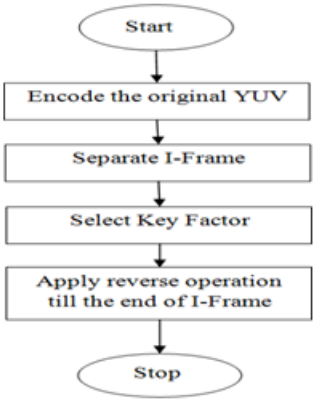



Fig. 1 Proposed scheme for I frame encryption

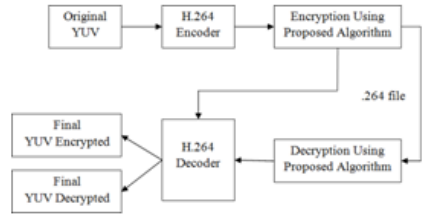
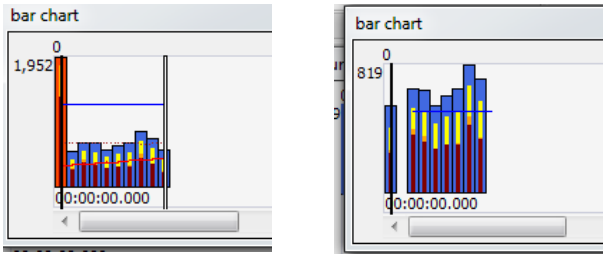



Fig. 2 Flowchart of proposed algorithm for I frame encryption




(b)

Fig. 4 Bar chart of (a) decoded (b) encrypted video for 10 frames (SVC)

### B. Second ProposedScheme

Infirstscheme,theproposedalgorithmusedwasnotmuch complex and keys were not that strong enough too. Selecting AES as a standard algorithm is a good option. Instead of reducingthekeylengthandcomplexityofthealgorithm,here number of bits to be encrypted is reduced by selecting the I-frameforencryption.FramesareencodedbyapplyingFMO as error resilient tool. Fig.5 and Fig. 6 show the theme of the proposed scheme [5]. In the proposed scheme, the original video is passed through the encoder. The bitstream is analyzedfortheI-frame.Thedatafollowing0000000165is identified as I frame data. The identified I-frame is sliced using FMO. The algorithm for the above scheme is shown below in flowchart fig. 7. Fig. 8 shows the bar chart for encoded and encrypted video of AVC. The colour of I frame getschangedduetoencryption.SchemeappliedtoSVCgives only the single frame as in Fig. 9 after encryption as SVC is more complex thanAVC.

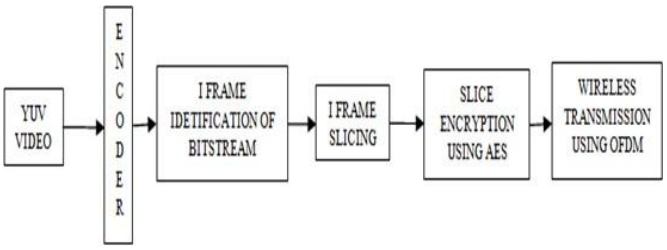
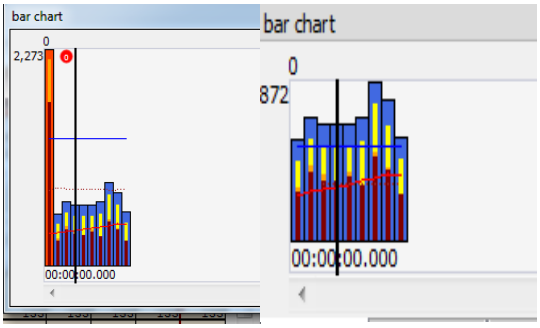



Fig. 5 Encoding and Encryption of Video




(a) (b)

Fig. 3 Bar chart of (a) decoded (b) encrypted video for 10 frames (AVC)

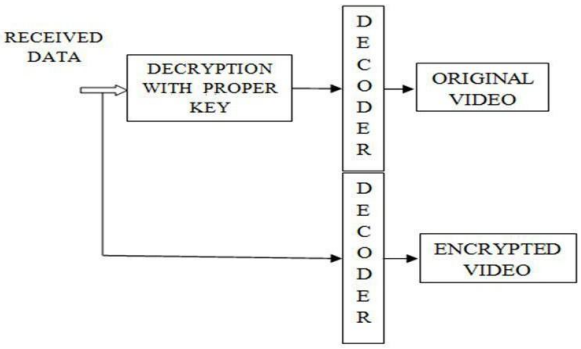
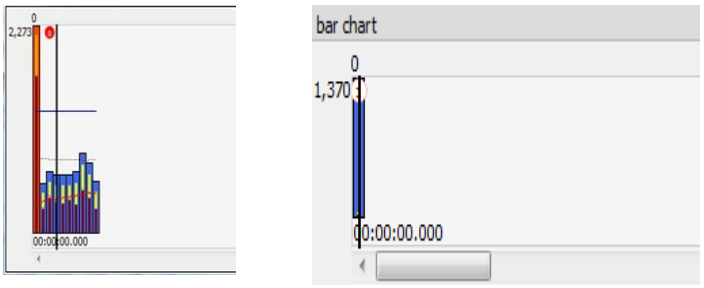



Fig. 6 Decoding and Decryption of Video



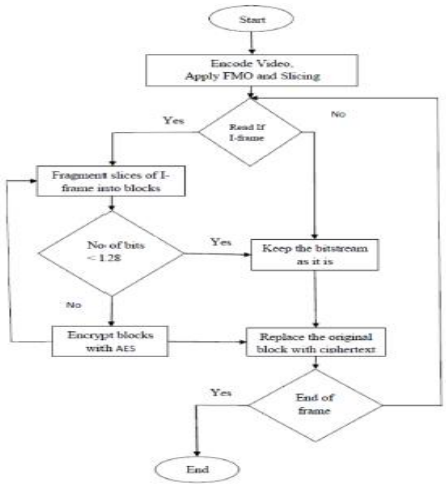




Fig. 7 Flowchart for I Frame Encryption

b. (b)

Fig. 8 Bar chart of (a) encoded (b) encrypted video for 10 frames (AVC)

Fig. 9 Bar chart of encrypted video(SVC)

## III. COMPARATIVEANALYSIS

Two approaches are studied which encrypt the video of YUV sequence foreman with QCIF format after compression. This section describes the outcome of the performance comparison which include PSNR, key factor analyses, overhead bit, required encryption time.

### A. PSNRComparison

The percentage decrease in PSNRs between video decrypted with wrong key and the decoded video is calculated. For comparison of two schemes, the PSNRs are shownintable1.Fromthistable,itisseenthatthepercentage decrease in Y,U and V PSNR for the decrypted video with wrong key in first scheme is less as compared to second scheme.

TABLE I
DECREASE IN PSNRS FORAVC

| Sr. No. | Percentage decrease in Y PSNR | | Percentage decrease in U PSNR | | Percentage decrease in V PSNR | |
|---|---|---|---|---|---|---|
| | I scheme | II scheme | I scheme | II scheme | I scheme | II scheme |
| 0[I] | -- | 89.06 | -- | 81.74 | -- | 84.90 |
| 1[P] | 65.34 | 86.28 | 30.32 | 81.56 | 32.35 | 84.83 |
| 2[P] | -- | 81.31 | -- | 78.54 | -- | 81.08 |
| 3[P] | 65.00 | 77.31 | 30.20 | 75.80 | 31.71 | 78.16 |
| 4[P] | 65.06 | 76.46 | 30.29 | 74.95 | 31.43 | 78.25 |
| 5[P] | 64.85 | 70.95 | 30.01 | 70.32 | 30.57 | 73.37 |
| 6[P] | 65.07 | 61.05 | 29.98 | 64.56 | 30.48 | 56.23 |
| 7[P] | 65.18 | 63.91 | 29.93 | 62.82 | 30.07 | 65.45 |
| 8[P] | 65.23 | 53.59 | 29.63 | 44.22 | 29.81 | 37.45 |
| 9[P] | 65.17 | 43.67 | 29.28 | 44.37 | 30 | 49.48 |
| Avg. | 65.11 | 71.07 | 29.96 | 68.01 | 30.80 | 69.15 |

### B. Encoding Time Analysis

Percentageincreaseintimetogetthecipher textis0.75%in firstproposedschemeandthatofinsecondproposedscheme is 38%. Increase in time to get cipher text is more in second case as compared to the firstscheme

### C. Overhead BitAnalysis

Theincreaseinnumberofbitsintheprocessofencryption is called overhead bit. In both proposed schemes. the encryption process is applied to bitstream after encoding, so extra bits are not getting generated. Hence there is no any calculation for overhead bits. Bits with and without encryption aresame

### D. Security Analysis

It is not easy to determine the security of encryption scheme.Thefactorswhichdecidethesecurityarethecostof breaking the cipher should be greater than the actual cost involvedinprocessandthetimerequiredtobreakthecipher should exceed information lifetime. It is discussed for the followingattacks.

1) **Cipher Text only Attacks**: In this attack, the attacker has a knowledge of only cipher text and he has to check the key by only brute force. In case of second proposed scheme as the key length is 128 bit long, applying brute force for getting the key requires very large amount oftime.

2) **KnownplaintextAttacks**:Inthisattack,attackerhas some additional knowledge other than cipher text. He also knowsplaintextandalgorithm.Butbecausethekeylengthis 128 bit long, again it is not that easy to break thekey.

## IV. CONCLUSIONS

In this paper, performance comparison of two different proposedschemesisinvestigated.WithrespecttoPSNR,itis concluded that the video in first scheme can be more easily guessed than the second proposed scheme. Considering case of encoding time ofsecond scheme, it can be stated that although the time requiredis more for converting plaintext to cipher text, security of the scheme is more as compared to the first scheme. In both theschemes,noextrabitsgetgenerated.Henceboththeschemes are free from overhead. After discussion of some security checkattacks,itisevidentthatthesecondproposedschemeis strongerwithrespecttosecurityascomparedtofirstproposed scheme.

## REFERENCES


1. K. John Singh and R. Manimegalai, "A Survey on Joint Compression and Encryption Techniques for Video Data" Journal of Computer Science, ISSN 1549-3636, 8 (5): pp.731-736,2012.
2. Jolly Shah and Dr. VikasSaxena, "Video Encryption: A Survey", International Journal of Computer Science Issues, Vol. 8, Issue 2, pp. 525-534, March2011.
3. Thomas Stutz and Andreas Uhl, "A Survey of H.264 AVC/SVC Encryption", Technical Report 2010-10, Technical Report2010.
4. Mrs. Rajashree N. Mandavgane and Dr. N.G.Bawane, "Quality Assessment of Precodec Video Protection", International Journal of Advance Research in Computer Science and Management Studies, (IJARCSMS), Volume 2, Issue 1, pp. 264-268, ISSN: 2321-7782 (Online) January2014.
5. Mrs. Rajashree N. Mandavgane and Dr. N.G.Bawane, "AVC VIDEO SECURITY ON WIRELESS CHANNEL", The international journal of multimedia & its applications, (IJMA), VOL.8, NO.5, and DOI: 10.5121/ijma.2016.8501,pp.1-8,October.
6. C. Shi, S. Y.Wang, and B. Bhargava, "MPEG video encryption in real-time using secret key cryptography", Proceedings of the International Conference on Parallel and Distributed Processing TechniquesandApplications(PDPTA"99),LasVegas,Nev,USA,pp. 191– 201, June-July 1999.
7. M. W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video", IEEE Transactions on Multimedia, vol. 5, no. 1, pp. 118–129,2003.
8. ITU-T H.264. Advanced video coding for generic audiovisual services, November2007.
9. M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan& B.B Zaidan "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, April2010.
10. WeiHuang,WenqingFanandTingtingZhang,"ASelectiveEncryption Scheme for H.264/AVC Video Coding", Informatics in Control, Automation and Robotics, Volume 2, LNEE 133, pp.317–32.


## AUTHORS PROFILE

Mrs. RajashreeNikhileshMandavgane 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 VisveswarayaregionalcollegeofengineeringNagpur, in 1994. she served as an lecturer, associate professor and head of the department.. Her current research interestsincludedigitalelectronicsandelectronics. She is pursuing Ph. D. from Nagpur University. She is a life member of the ISTE and IE.

Dr.NarendraG.Bawane,isatrulyacademicianwith 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 Hehasgotmorethan72researchpaperstohiscredit in international and national Journals and Conferences. He is a reviewer of many reputed international Journals and member - programmecommittee of various international Conferences. He has worked in Government organization for several years and other reputedengineering colleges in the various capacities such as Head of Computer Science &Engineering,Electronicsdepartment,DeanAutonomyetc.Hewasexecutive 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 year2015-16. 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&AmravatiUniversities.Hehasguided24studentsatPostgraduate 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.