iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** III **Month of publication:** March 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Comparative Study of Video Encryption Techniques for HEVC

Sagar. S. Hade[1], Sonal. K. Jagtap[2]
Department of E&TC University of Pune,India.

Abstract— Study of different Encryption techniques focuses on newly video codec which is high efficiency video codec (HEVC). It focused on the different recent methods of video protection. Development of HEVC standard is main target of researchers now a day.in this paper survey summarizes the latest research results of protection of HEVC video codec as well as we also compare the different protection approach of H264/AVC Video codec. Digital video transmission on unauthorized channel needs some protection to avoid the unwanted attacks on multimedia content. Data hiding in such encrypted domain without decryption also preserves the confidentiality of the content.so, the encryption of such a large multimedia is very much cumbersome for that reason we summarize and analyses selective encryption scheme used on video content. Comparison and analysis of different encryption domain gives some concrete conclusion about the guaranteed protection. The main objective of video encryption is video should be in format compliance after applying encryption algorithm.it allows to play video even after encryption so transmission of such format compliance encrypted video has less memory requirement.
Keywords— H.264; Multimedia security; HEVC; Entropy coding; CABAC;

I. INTRODUCTION

Security is one of the most important task in the network and internet applications.Due to the rapid growth in the transmission techniques network bandwidth plays a crucial role.transmission efficiency is intemperately depends on the network bandwidth.to achieve security in data transmission use of the technique like encryption is essential to achieve sufficient security of the data. In multimedia data transmission there is large number of data to be encrypted.In video processing we have to deal with large number of data in such case encryption of such a large data is not mandatory all the time.encryption of particular selected data reduce the computation in greater extends and result is less computation time and transmission time.there are different type of compression technique now a most widely used video compression technique is AVC/H.264 it provides less computational complexity. now there is HEVC(High Efficiency Video Coding)newly emerging slandered introduce since past few years it provides better compression efficiency than existing AVC/H.264.HEVC can compress a video to about half the bit rate of H.264/MPEG-4 AVC without sacrificing its frame resolution and picture quality.HEVC supports different mode of operation in low delay mode I frame followed by a number of P frame.particularly low delay mode is used for real time application which includes online gaming and video conferencing, In another mode of random access we can access any part of the frame randomly.feature of accessing random part of frame provides better compression and suitable for most of data storage application it allows 20% reduction in bit-rate[1]. Nowadays transmission of multimedia through unauthorized channel increases in greater extent such a digital content can be easily modify,edit and copy.Selective Encryption(SE)is used to restrict the access of video to the particular authenticated user,in SE some part of video bit-stream encrypt using one of the mode of Advance Encryption Standard(AES)[1]. Data encryption can be used for either wat in whole as well as selective part encryption .proper designing of encryption technique allows advance functionality like conditional access of some portion of data[2].While encrypting video content format compliance of video is most important and challenging task.Arithmetic coding is very sensitive to change in a single bit can affect format compliance of video bit-stream,so before encryption conversion of bit-stream to Binstring always guarantees for same format[1].While encryption of video data it is necessary to examine video coding standard with their functionality. The rest of the paper is organized as follows.In section II,overview of HEVC compression technique and context adaptive binary arithmetic coding(CABAC),in section III describes feature for video encryption,in IV we discribes security issue of video encryption, in section V we take survey on different Encryption technique and in section VI we compare different approach of protection of video content.Section VII contains concluding remarks about review.

II. OVERVIEW OF HEVC/ H.265 AND ITS ARITHMETIC CODING

In HEVC codec structure Each picture is split into different rectangle block, with the exact block partitioning being conveyed to the decoder. The first frame of a video is coded using only intrapicture prediction.in intraprediction frame is coded independently which not depends on past or future frame. For all remaining frame of a sequence or between random access

points, interpicture coding modes are used for most blocks. The encoding process for interpicture prediction consists of the difference between reference frame and current frame and calculate residual data this data gives the motion vectors(MV)of the consecutive frames and this data applied for predicting the samples of each block. The encoder and decoder generate identical interpicture prediction signals by applying motion compensation (MC) using the MV and mode decision data[3].

The residual data which is nothing but difference between reference frame and current frame of the video,Then this deta is transformed by a linear spatial transform. The transform coefficients are then,quantized, scaled, and entropy coded, then transmitted together with the prediction information.in HEVC copression technique context based binary adaptive coding(CABAC)is used as a entropy coding[3].CABAC encoding consist of three stages.

A. Binarization
B. Context Modeling
C. Binary arithmetic coding

In binarization process input element which may quantized transform coefficients,motion vector component or any other nonbinary syntax element of video converted into binary form and create binstring from video bitstream.There are different code trees to convert bitstream into binstring like the unary code,the truncated unary code, the truncated rice code, exponential golumb code ,the fixed length code characteristics of syntax element decides the which code or combination of code going to use.then bins pass to the context modeling stage it distributes the bins according to probability of occurrence of each bin.and finally using binary arithmetic coding use to code the symbol[4].

III. FEATURES FOR VIDEO ENCRYPTION

Multimedia data content the lots of raw data encryption of such a data is very slow. Selective encryption is a technique to save computational time, conversion speed and system overhead. This technique provides quick security by only encrypting a selected portion of a bit stream. Selective encryption is helpful for the multimedia content like images, video content and audio content. In most of application where confidential data has to send over unauthorized transmission channel SE provides better visual protection.

We need to define a set of evaluation criteria that will help evaluating and comparing selective encryption algorithms. Some criteria listed below are gathered from the literature which classified as shown in Fig.1.

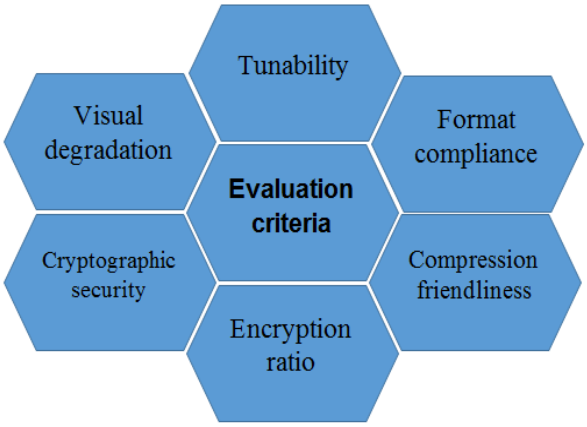


Fig.1: Evalution criteria of selective encryption.

A. Tunability (T)

In different encryption algorithms the encrypted part and encryption parameters changes dynamically according to the multimedia data. This property limits the application range of the Algorithm. It could be very desirable to be able to dynamically define the encrypted part and the encryption parameters with respect to different applications scenarios and requirements[5].

B. Visual degradation (VD)

This criterion measures the perceptual distortion of encrypted video with respect to the plain video. It assumes that the cipher

video can be decoded and viewed without decryption. This assumption is not satisfied for all existing algorithms. In some applications, it could be required to achieve enough visual degradation, so that an attacker would still understand the content but desire to pay to access the unencrypted content[5].

C. Cryptographic security (CS)

Most of the research works on selective encryption evaluate the security level based only on visual degradation. The visual degradation achieved is very high, but the security of the algorithm is very fragile. The cryptographic security should rely on the encryption key[5].

D. Encryption ratio (ER)

This criterion measures the ratio between the size of the encrypted part and the whole multimedia data size. Encryption ratio can minimized by using selective encryption[5].

E. *Compression friendliness (CF)*

A selective encryption algorithm is considered compression friendly if it has no or very little impact on data compression efficiency. Encryption algorithms impact data compressibility or introduce additional data that is necessary for decryption. It is desirable that this impact remains limited.

F. Format compliance (FC)

The encrypted bitstream should be compliant with the compressor. Any standard decoder should be able to decode the encrypted bitstream without decryption. Format compliance is very important because it allows preserving some features of the compression algorithm.

IV. SECURITY ISSUE FOR VIDEO ENCRYPTION

Several attacks which can get the access of encrypted video data which gives significant limitations of various encryption techniques. Discussion of different attacks gives some serious security issue.

A. Basic attack.

Most simple encryption technique is using spread spectrum and some simple image encryption software are subject to some kind of jitter attack. Certainly, spread spectrum signals are very robust to amplitude distortion and to noise addition, synchronization of the chip signal is very important and simple systems fail to recover this synchronization properly. There are more subtle distortions that can be applied[14].

B. Plaintext Attack

\Known plaintext attack means that some of the unencrypted data must be available. atleast one unencrypted frame must be known. This could realistically happen if we know the beginning is completely black for a few frames or if we know that all videos from this creator begin the same optimal There are two types of attacks on Zig-Zag permutation are introduced, a ciphertext simply attack, and a known plaintext attack. The Zig-Zag permutation algorithm is vulnerable to the ciphertext only attack, the attack relies on the fact of statistical properties of the DCT coefficient, where none zero AC coefficients are gathered in the upper left corner of the I block[15]. Count the number of non-zero ACs and DC coefficients from all blocks in an I-frame showed DC coefficients always have the highest frequency of nonzero occurrences. The another problem is that, the Zig Zag permutation algorithm cannot withstand the known plaintext attack.

C. Perceptual attack

Selective encryption of MPEG-2 video used in most current digital television applications. They use the detail that the typical high performance MPEG-2 encoded bitstreams only uses a small portion of bits in important headers. It can be simple to unclear such headers because of a usual practice in encoding of aligning these headers and the multiplex level at which encryption is performed [15]. However, fields in such headers can be quite unprotected to attack, even if obscured by

Selective encryption, for a variety of reasons the fields are frequently stationary, they can be guessed from external information that is probably available to an attacker, and they can be guessed from other information in the bitstream (e.g., picture type can be guessed from picture size). They evaluated each of these fields, and proposed and tested attacks. For example, they showed that a perceptual attack on the Quantized scale code syntactic element is feasible though with picture degradation in typical sequences there is a strongly peaked distribution for this code, and a perceptual attack would be to always use an expected value for this code [15].

V. SURVEY ON VIDEO ENCRYPTION

With the increasing capturing,recording and transmission of the digital content it is attraction of researchers community to provide protection of such large multimedia content.There is lots of research going on to provide protection in different domain as well as in between different stages of compression.

Reference [1],Z.Shahid.W. Puech presents a idea it allows the protection of HEVC (High Efficiency Video Coding). encryption is achieved using selective encryption (SE) of HEVC-CABAC binstrings in a format compliant manner. The SE approach for HEVC is different from that of H.264/AVC in several aspects. Truncated rice code is introduced for binarization of quantized transform coefficients (QTCs) instead of truncated unary code. it guarantees format-compliant and has exactly the same bit-rate. This technique requires very little processing power and is ideal for playback on portablr device devices.

Reference [6],Shiyi Xing propose a intraprediction mode by chaotic pseudo random sequence.intraprediction mode further modified by improvement in view of perception performance, plaintext scrambling space and key security and then presents an improved IPM encryption algorithm (IPMEA).It encrypts all the IPMs by chaotic pseudo-random sequence, scrambles them for the second time by circulating sequence controlled by key and gives a scheme of key distribution and synchronization [6]. Performance analysis and experimental results show that IPMEA can exhibit higher security than the existing ones and has little impact on code length.IPMEA gives a simple scheme of key distribution and synchronization. The relation between encryption and compression.one disadvantage of this method is to change in bit rate which may be affect format compliance of video[6].

Reference [7],S.Lain proposed a selective encryption scheme is based on Advanced Video Coding. while AVC encoding, such sensitive data as intra-prediction mode, residue data, inter-prediction mode and motion vector (MV) are partially encrypted.This encryption scheme gives protection against brute-force attack, replacement attack or known-plaintext attack, in this method encryption process combines with compression process with low cost, and maintain same format with some direct operations (such as displaying, time seeking, copying, cutting, etc.) supported.the Drawback of this technique is format compliance not always guarantees it might be change during encryption process. These properties make it not suitable for real time secure video transmission[7].

Reference [8], Z.Zhu propose a new design of Unitary Transforms for perceptual video encryption.encryption algorithms that are embedded into the video encoder, whereas this encoder typically consists of four functional blocks,predication block,,quantization block, transformation block and entropy coding.in this method entropy coding based on the multiple-Huffman-table encryption.which, however, usually leads to better encryption.drawback of this method is it use permutation encryption algorithm which leads to not robust in transcoding[8].

Reference [9],F. Dufaux and T. Ebrahimi propose a transform-domain scrambling technique for privacy protection.in this technique frames are coded as intra-frame, predictive-frame, or bidirectional-frame.in this method Pseudo random sign inversion is used in which each frame is divided into 16x16 macroblocks (MBs).In turn, each MB is composed of four 8x8 luminance blocks and two 8x8 chrominance blocks.The scrambling can effectively be applied on the quantized DCT coefficients This approach also guarantees that the scrambled video stream has a fully standard compliant syntax. At the decoder side, authorized users perform unscrambling of the coefficients.unauthorized users are still able to correctly decode the video stream, except for the scrambled coefficients. However,in this case introducing a drift.

Reference [10],Y.Zong proposed a stream cipher encryption algorithm which perform on H.264.in this methods combinations of encryption method with H.264/AVC codec, which encrypts and marks suitable H.264/AVC parameters independently,parameter like compression component, encryption component and watermarking component.Here, the compression component includes intra prediction, inter-prediction, variable length coding (VLC), etc., the encryption component includes IPM encryption, MVD encryption and residue encryption, and the watermarking component refers to residue watermarking. The encryption process and watermarking process are controlled by independent keys.

Reference [11],S.Lian proposed a commutative video encryption and watermarking during video compression process.this method provides constant bitrate using stream cipher encryption technique. In the intra-prediction mode, motion vector difference and discrete cosine transform (DCT) coefficients' signs are encrypted, while DCT coefficients amplitudes are watermarked adaptively. To avoid that the watermarking operation affects the decryption operation, a traditional watermarking algorithm is modified. The encryption and watermarking operations are commutative. Thus, the watermark can be extracted from the encrypted videos, and the encrypted videos can be re-watermarked it sustain confidentiality of video content, and provides a solution for signal processing in encrypted domain.it also provides better operation efficiency.this method also reduces the computational cost and selected parameters are encrypted partially.To sustain robustness , the coefficients are

selected adaptively according to macroblock type.

Reference [12],Z.Shahid.W. Puech proposed a method in which presents approach to protection of bitstreams of video.SE is used along with the compression in the entropy coding modules. H.264/AVC supports two types of entropy coding modules. Context-adaptive variable length coding (CAVLC)and context-adaptive binary arithmetic coding (CABAC). SE is performed in both types of entropy coding modules of H.264 video codec.SE is performed by using the advanced encryption standard (AES) algorithm with the cipher feedback mode on a subset of binstrings[12].

VI. COMPARATIVE ANALYSIS

In comparative analysis different approaches of video encryption compare. table shows brief description of all methods.

SE scheme	Encryption Domain	Encryption Algorithm	Format Compliance
[1]	Binstring	AES-CFB	Yes
[6]	IPM	Chaotic based	No
[8]	Transform	Permutation	No
[9]	Transform	Pseudo random	Yes
[10]	NAL	Stream Cipher	No
[11]	Transform	Stream Cipher	No
[12]	Binstring	AES-CFB	No

VII. CONCLUSION

In this paper, we presented, evaluated, and discussed video encryption schemes for H.264 and H.265. The choice of a video encryption scheme depends on the application-context, the security threats are in this scenario and which functionality of the bitstream and video data has to be preserved in the encrypted domain. A focus of this paper has been the interoperability of video encryption with existing processes for the video data such as intraprediction modes (IPMs),using different Huffman tables for different input symbols,perceptual video encryption at the transform stage, frame extraction,The diverse contributions cover a wide range of application scenarios for H.265.

VIII. ACKNOWLEDGMENT

I am indeed thankful to my guide **Dr. S. K. Jagtap** for her able guidance and assistance to complete this paper otherwise it would not have been accomplished. I extend my special thanks to Head of Department of Electronics & Tele-communication**, Dr. S. K. Shah** who extended the preparatory steps of this paper-work.I am also thankful to the head & Principle of STESS, SMT. Kashibai Navale College of Engineering, **Dr. A.V. Deshpande** for his valued support and faith on me.

REFFERENCES

[1] Zafar Shahid and William Puech,"Visual Protection of HEVC Video by Selective Encryption of CABAC Binstrings" in IEEE Trans. Multi-media,vol. 16, no. 1, Jan 2014.

[2] M. Grangetto, E. Magli, and G. Olmo,"Multimedia selective encryp-tion by means of randomized arithmetic coding,"IEEE Trans. Multi-media, vol. 8, no. 5, pp. 905 - 917, Oct. 2006.

[3] M. Grangetto, E. Magli, and G. Olmo, "A survey of H.264 AVC/SVC Encryption," IEEE transactions on circuits and systems for video technology, vol. 22, no. 3, pp. 905 - 917, Mar. 2012.

[4] M. Asghar, M. Ghanbari, and M. Reed, "Sufficient encryption with codewords and bin-strings of H.264/SVC," in IEEE Int. Conf.Trust, Security and Privacy in Computers and Communications ,Liverpool,pp. 443 - 450, U.K., Jun. 2012.

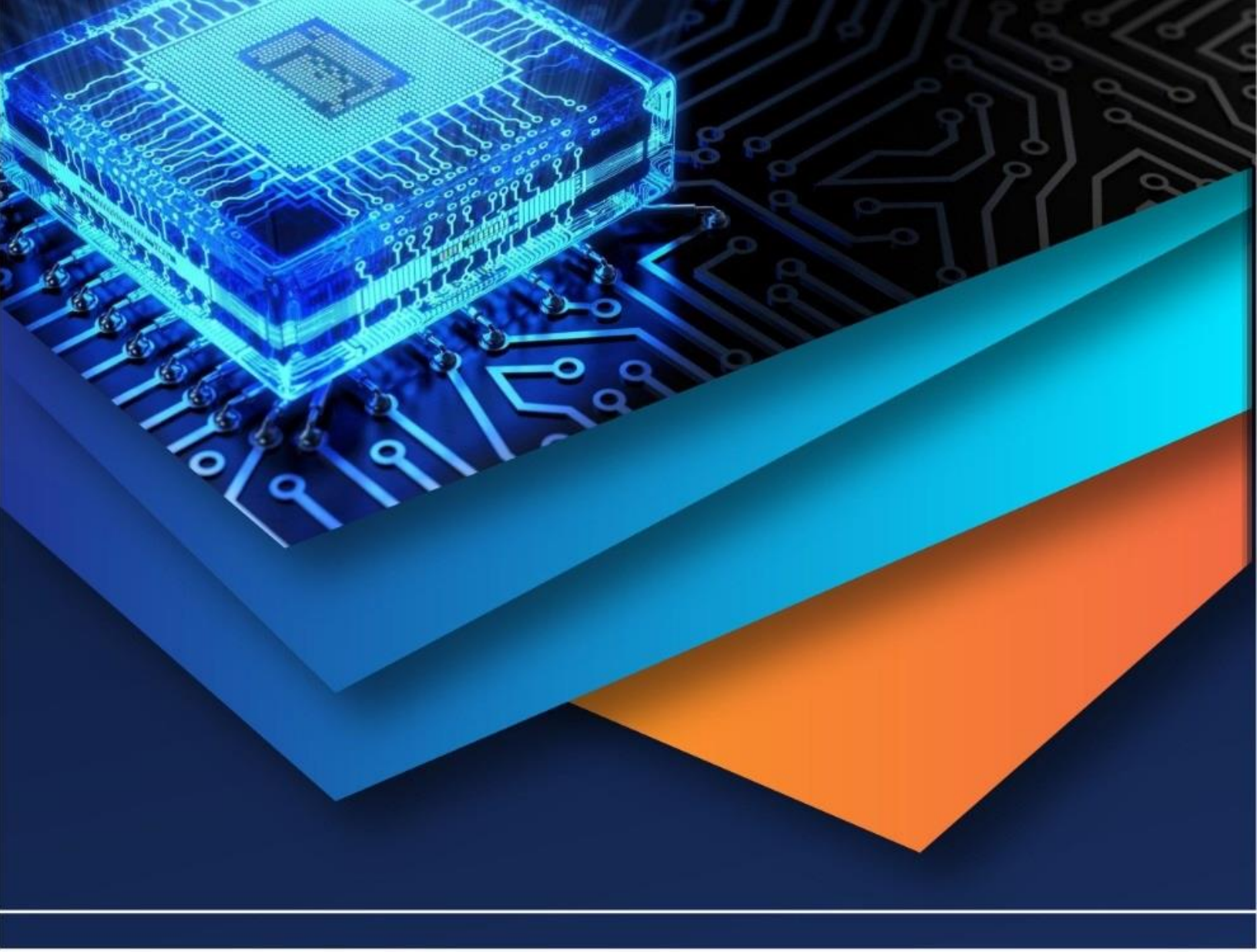
[5] Gary J. Sullivan, Jens-Rainer Ohm,Woo-Jin Han,and Thomas Wiegand,"Overview of the High Efficiency Video Coding (HEVC) Standard,"*IEEE transactions on circuits and systems for video technology*,vol. 22, no. 12, Dec. 2012

[6] M. Q. J. Jiang and S. Xing, "An intraprediction mode-based videoencryption algorithm in H.264," in Proc. Int. Conf. Multimedia Information Networking and Security,vol. 1, pp. 478 - 482 , Nov. 2009.

[7] S.Lian,Z.Liu,Z.Ren,andZ.Wa ng, "Selective video encryption basedon advanced video coding," Lecture Notes Comput. Sci., Springer-Verlag , no. 3768, pp. 281 - 290, 2005.

[8] S. K. A. Yeung, S. Zhu, and B. Zeng, "Design of new unitary trans-forms for perceptual video encryption," IEEE Trans. Circuits Syst.Video Technol, vol. 21, no. 9, pp. 1341 - 1345, Sep. 2011.

[9] F.DufauxandT.Ebrahimi,"Scramblingforprivacyprotectionin video surveillance systems," IEEE Trans. Circuits Syst. VideoTechnol, vol. 18, no. 8, pp. 1168 -1174, Aug. 2008.
[10] C. Li, X. Zhou, and Y. Zong, "NAL level encryption for scalable videocoding," Lecture Notes Comput. Sci., Springer , no. 5353, pp. 496 - 505,2008.
[11] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. VideoTechnol, vol. 17, no. 6, pp. 774 - 778, Jun. 2007.
[12] Z. Shahid, M. Chaumont, and W. Puech, "Fast protection ofH.264/AVC by selective encryption of CAVLC and CABAC for I & P frame," IEEE Trans. Circuits Syst. Video Technol, vol. 21, no.5, pp. 565 - 576, May 2011.
[13] HEVC, "High Efficiency Video Coding (HEVC) Text Specification Draft 6," Tech. Rep., ITU-T/ISO/IEC Joint CollaborativeTeamonVideoCoding(JCTVC),SanJose,CA,USA,2012.
[14]]F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, Attacks on copyright marking systems." In *Aucsmith* , pp. 218
[15] T. Lookabaugh et al., Selective encryption of MPEG-2 video," in Proceedings of the SPIE Multimedia Systems and Applications VI, (Orlando, FL), September 2003.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY