An Analysis of H.264/AVC Encryption Techniques

Dinesh Goyal[1]

[1] Suresh Gyan Vihar University

Abstract

The video coding standards are developed to satisfy the requirements of different applications for various purposes, higher coding efficiency, better picture quality, and more error robustness. The new international video coding standard H.264/AVC aims at having significant improvements in coding efficiency, and error robustness in comparison with the previous standards. Most of the video compression algorithms are designed based on the H.264/AVC. In this paper, the video encryption techniques of H.264/AVC are analyzed. Performance analysis of the three algorithms namely Selective, Layered and Naïve is reported and its strength is discussed.

Index terms— h.264/avc; video encryption techniques; selective; layered; naïve.

1 Introduction

ultimedia is the combination of two or more media. The media in multimedia is in various forms such as graphics, photography, text, audio, video and animation. Each one serves as a powerful communication vehicle for both expressive and practical purposes.

H.264/MPEG-4 AVC is the latest international video coding standard. It was jointly developed by the Video Coding Experts Group (VCEG) of the ITU-T and the Moving Picture Experts Group (MPEG) of ISO/IEC. It uses state-of-the-art coding tools and provides enhanced coding efficiency for a wide range of applications including video telephony, video conferencing, TV, storage (DVD and/or hard disk based, especially high-definition DVD), streaming video, digital video authoring, digital cinema, and many others. ITU H.263, H.263L, H.26L, H.263E, ISO/IEC 14496. These video codecs are the Basis for MPEG4 Simple Profile. MPEG-4 adds advanced error detection and correction services on top of H.263. 3GPP and ISMA are versions of H.263 and MPEG-4 for streaming and mobile applications. These are really a variation of Transport stream.

H.264 is being widely accepted as the future platform of video compression for applications such as new HDTV services, portable game console, mobile broadcast video services, and video on solid-state camcorders, instant video messaging on cell phone. H.264 is the most advanced video coding standard available today. It uses many new coding techniques not available in MPEG2, MPEG4 and H.263.

2 II.

Encoding & Decoding ? : JECRC University, Jaipur.

The H.264/MPEG-4 Advanced Video Coding standard (H.264/AVC) has achieved a significant improvement in compression performance compared to prior standards.

The main objectives of the H.264/AVC standard are focused on coding efficiency, architecture, and functionalities. More specifically, an important objective was the achievement of a substantial increase of coding efficiency over MPEG-2 Video for high-delay applications and over H.263 version 2 for low-delay applications, while keeping implementation costs within an acceptable range. Doubling coding efficiency corresponds to halving the bit rate necessary to represent video content with a given level of perceptual picture quality. It also corresponds to doubling the number of channels of video content of a given quality within a given limited bit-rate delivery system such as a broad-cast network.

The architecture-related objective was to give the design a "network-friendly" structure, including enhanced error/loss robustness capabilities, in particular, which could address applications requiring transmission over various networks under various delay and loss conditions. The functionalities-related objectives included-as with prior video coding standards-providing support for random access (i.e., the ability to start decoding at points other than the beginning of the entire stream of encoded data) and "trick mode" operation (i.e., fast-forward, fast and slow reverse play, scene and chapter skipping, switching between coded bit streams, etc.), and other features.

H.264 Advanced Video Coding defines a format for compressed video data and it provides a set of tools that can be used in a variety of ways to compress and communicate visual information. Also, it is a stage in an evolving series of standardized methods for video compression. It is an industry standard for video coding, but it is also a popular format for coded video, a set of tools for video compression and a stage in a continuously evolving digital video communication landscape.

3   Video Compression Techniques

Role of video compression technology is to reduce the redundancies in the spatial and temporal directions. Spatial reduction physically reduces the size of the video data by selectively discarding up to a fourth or more of unneeded parts of the original data in a frame.

Temporal reduction, Inter-frame delta compression or motion compression, significantly reduces the amount of data pixels needed to store a video frame by encoding only the pixels that change between consecutive frames in a sequence.

Several important standards like the Moving Picture Experts Group (MPEG) standard, H.261, H.263 and H.264 standards are the most commonly used techniques for video compression.

? MPEG 1: MPEG-1 is mainly for storage media applications. Due to the use of B-picture, it may result in long end-to-end delay. The MPEG-1 encoder is much more expensive than the decoder due to the large search range, the half-pixel accuracy in motion estimation, and the use of the bi-directional motion estimation. ? MPEG 2: The MPEG-2 standard consists of several parts, of which the most important to us is the video part. The standard defines a compressed video bitstream and describes how it can be decoded. It is important to recognize that it does not describe how to take an input picture and compress it to make an MPEG-2 bitstream -it is not a coder specification. IV.

4   Video Encryption Techniques

In today's scenario there is an increasing demand for remote video communication.

The development of encryption systems main objective is to provide a secure and reliable way of information exchanges. However, the security aspects of video exchanges have yet to be fully addressed. Existing video coding standards do not incorporate requirements to have encryption capabilities.

Recently, researchers are focusing a lot of attention on secure digital media over the network. The field of multimedia security is growing extremely fast. In order to deal with the problem of processing overhead and to meet the security requirements of real -time video applications with high quality video compression, several encryption algorithms to secure video streaming have been proposed which are as follows:

? Pure permutation algorithm which simply scrambles the bytes within a frame of an MPEG stream by permutation. It is extremely useful in situations where the hardware decodes the video, but decryption must be done by the software. ? Zig-Zag permutation approach maps the individual 8x8 block to a 1x64 vector using a random permutation instead of mapping 8x8 blocks to a 1x64 vector in a Zig-Zag order using a random permutation list (secret key). V.

5   Comparative Analysis of Video Encryption

Security and privacy issues in multimedia technology have become an important concern.

Many multimedia applications require secure transmission, the level of security required depends on the sensitivity of the information in these applications. Due to which various video encryption techniques are developed. From these techniques three of them are discussed as follows: Current research is focused towards exploiting the format specific properties of many standard multimedia formats in order to achieve the desired performance. This is referred to as the selective encryption. This type of encryption is obviously preferred when compression and decompression algorithms can hardly keep up with the required bit rate, even when these algorithms are accelerated by a dedicated hardware. In few cases, encryption and decryption algorithms could also be accelerated by hardware. However, software implementations are often preferred due to their flexibility and low cost.

Selective encryption is a technique to save computational power, overhead, speed and time.

Selective encryption using chaotic map technique is used for encryption and compressing the data. The encryption process is divided into two first is to generate chaos based key and secondly, selective encryption. Also, in selective encryption the concentration is not on the image but on a single frame only which is to be encrypted and encoded after selection. The Joint Video Team (JVT) finalized the draft of the new coding standard for formal approval submission as H.264/AVC and was approved by ? Naïve Encryption: Encrypting

the entire multimedia stream using standard encryption methods is often referred to as the naïve approach. The naïve approach is usually suitable for text, and sometimes for small bit rate audio, image and video files that are being sent over a fast dedicated channel.

6 VI. Result Analysis of Video Encryption Methods

In this the results of three of the video encryption techniques are executed namely Selective, Naïve and Fully Layered Method and compared with their respective results.

The results shown above are taken after performing chaotic map based selective encryption on monochrome video. 1. In this work in Naïve encryption the normal input video is encrypted using pre-defined chaotic map based selective encryption (symmetric key).

7 Conclusion & Future Work

The H.264/AVC technology is designed to support the coding of video for a wide variety of applications. In addition to this H.264/AVC enabling efficient compression of digital video, it supports error/loss resilience, random-access operation, "trickmode" operation, region-of-interest preferential coding, stereo-view indicators, film-grain analysis/synthesis processing, and a variety of additional capabilities.

Further work is underway to add enhanced application capabilities for scalable and multiview/three-dimensional video coding.

In this paper the comparative analysis of mainly three video encryption schemes is being performed using H.264/AVC. And the video encryption schemes will be analyzed to observe the percentage of encryption in H.264/AVC and to determine the delay in transmission of video after encryption, using MATLAB and Image Processing Tool.

Analysis of results prove that naïve encryption is the best as it takes less time and encodes the video up to the minimum size. Though the selective encryption takes lesser time but its encoding space is more and encryption time is less, while layered requires more time for encryption and more time for encoding. Selective requires bit more time for encryption then naïve at the same time selective encodes video less.

Selective gives a benefit that its decoding process will be shorter as p frames are not be decrypted after decoding, while in case of naïve decoding time will be higher as the decoding time will involve both decryption and decoding process, also selective helps in ensuring the content of the video more readable for the end user, while in case of naïve decoding process can also lead to loss in data.

This work has been performed on monochrome H.264 video and this can be extended to the RGB and YUV H.264 video as a future research work. In which the above three video encryption schemes (Selective, Naïve and Layered) will be performed using H.264/AVC. And the video encryption schemes will be analyzed to observe the percentage of encryption in H.264/AVC and to determine the delay in transmission of video after encryption, using MATLAB Image and Video Processing Tool. The above encryption schemes are performed using chaotic map based and the same can also be performed using block based method as a future work.

New encryption tools can also be designed with the help of MATLAB, to reduce the encryption time. [1]
[2] [3]

---

[1]FAn Analysis of H.264/AVC Encryption Techniques

[2]An Analysis of H.264/AVC Encryption Techniques

[3]FAn Analysis of H.264/AVC Encryption Techniques
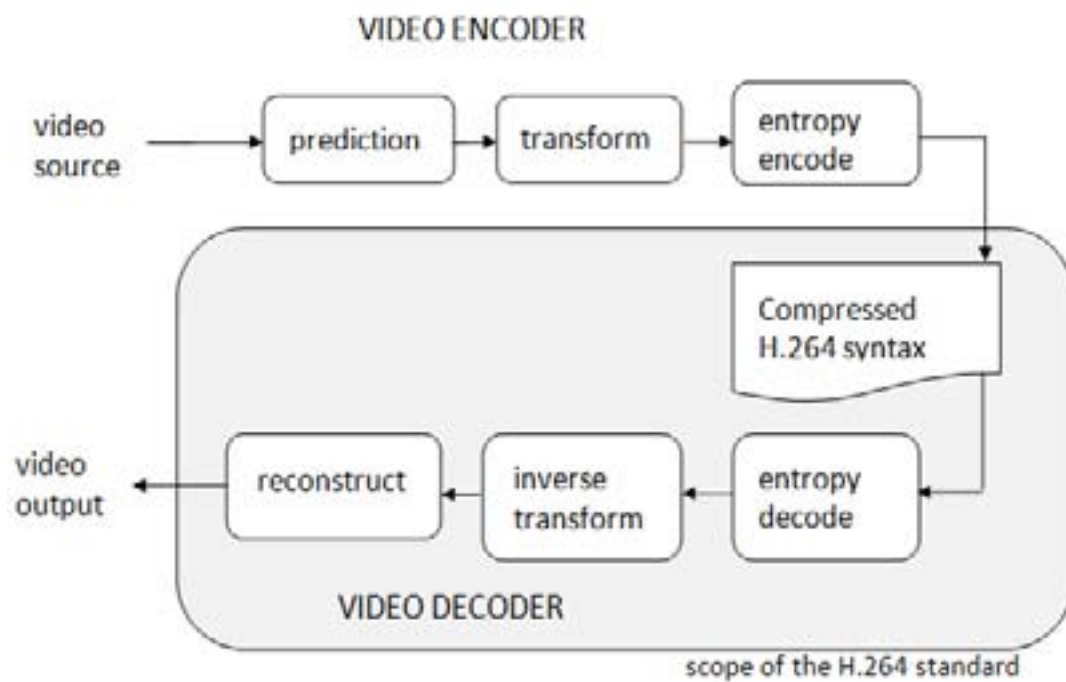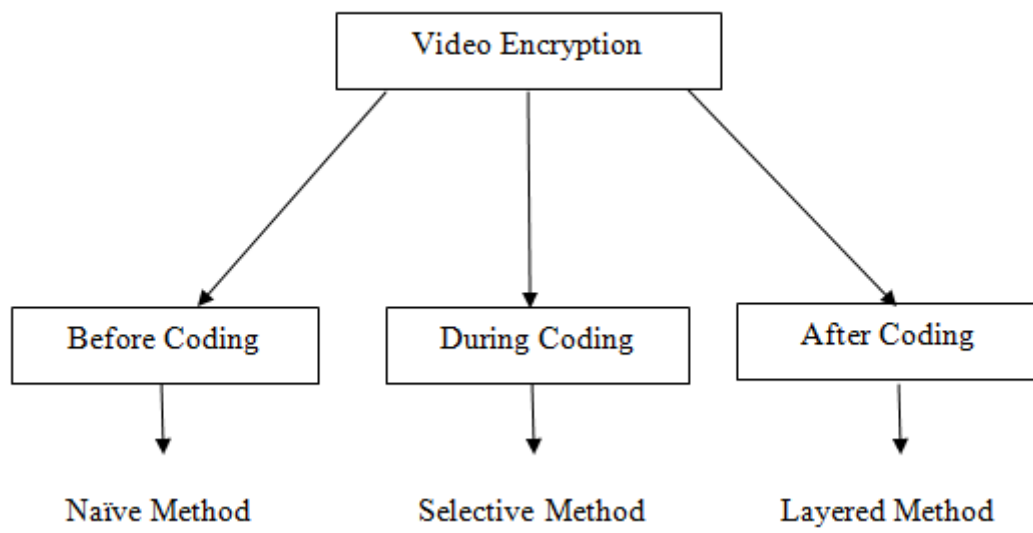
Figure 1: Figure 1 :
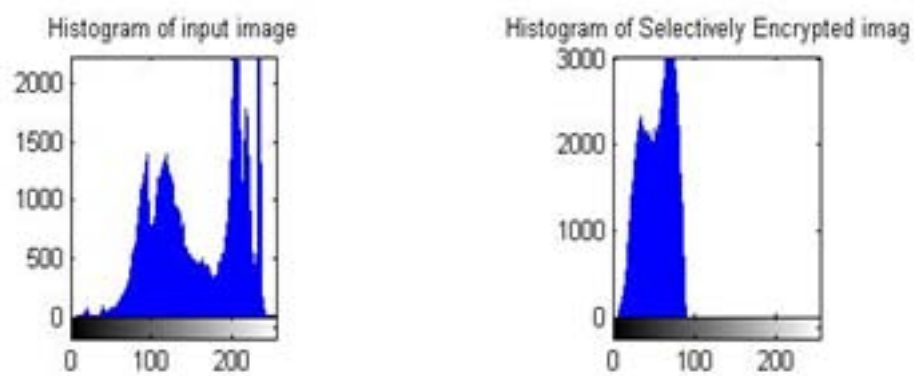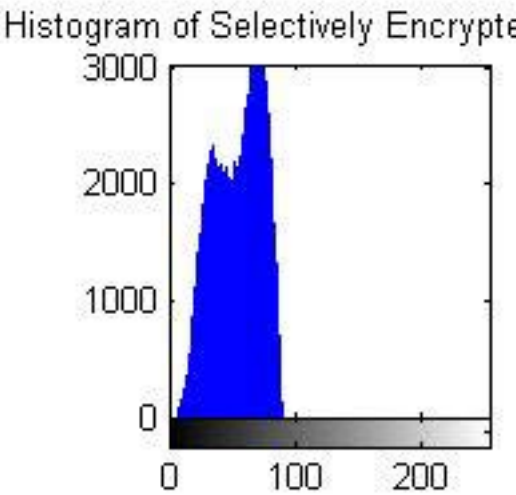

Figure 2:

2

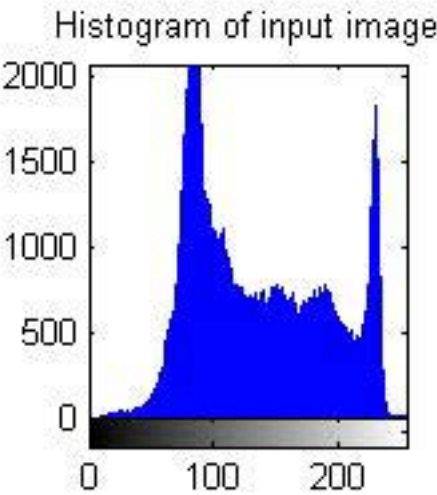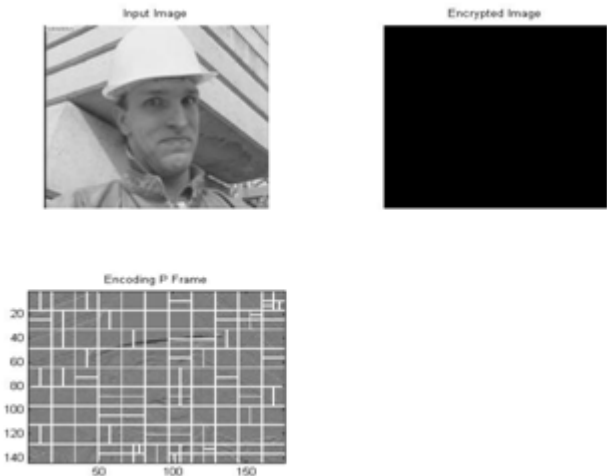Figure 3: Figure 2 :

3

Figure 4: Figure 3 :

4

Figure 5: Figure 4

567

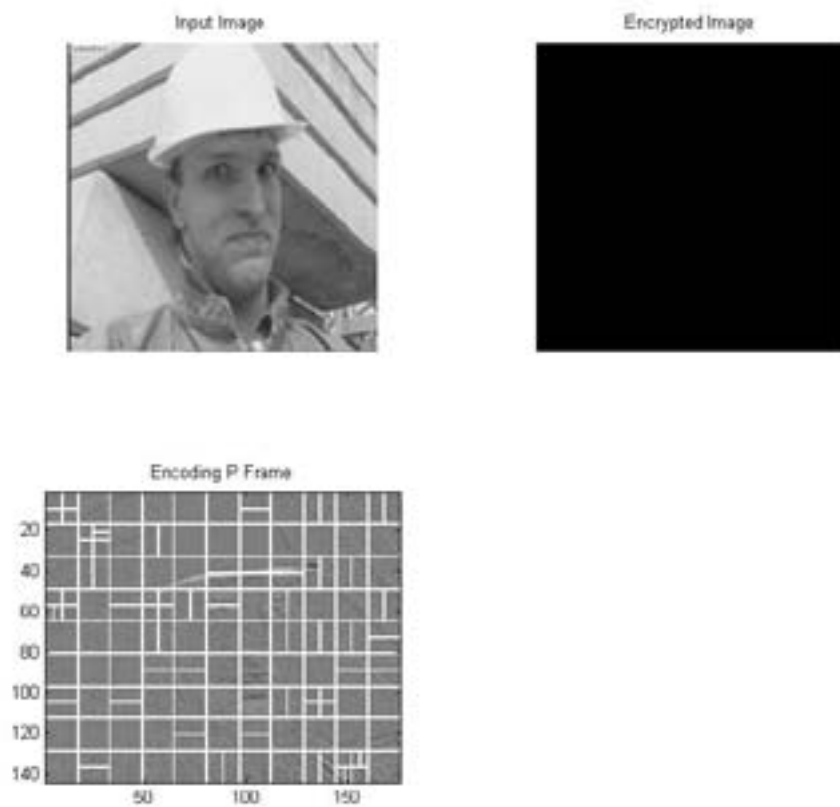Figure 6: Figure 5 :Figure 6 :Figure 7 :

Input Image

Encrypted Image

Encoding P Frame
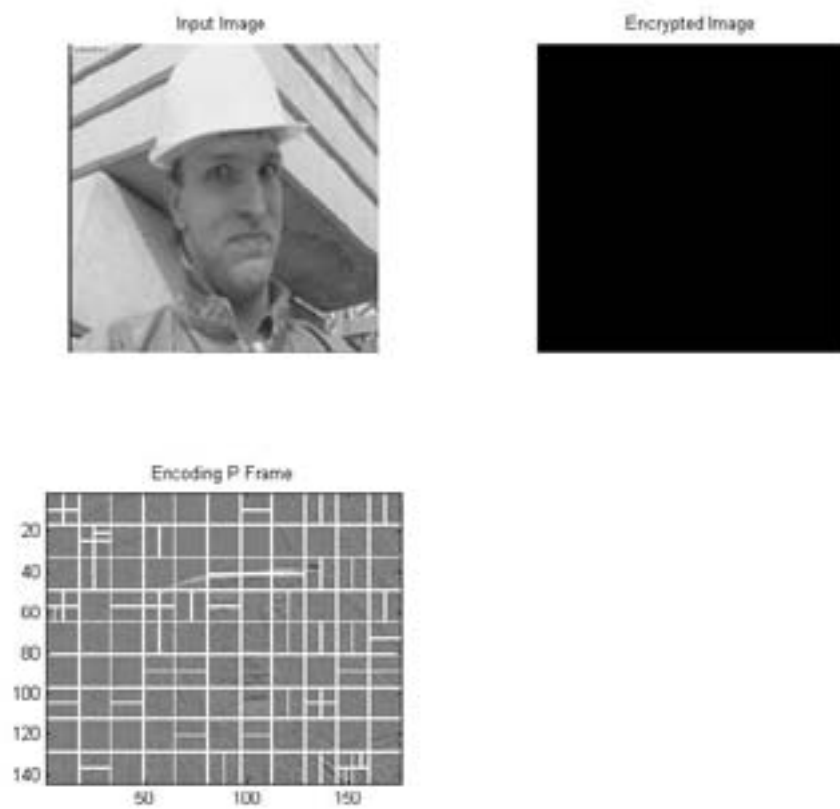
21

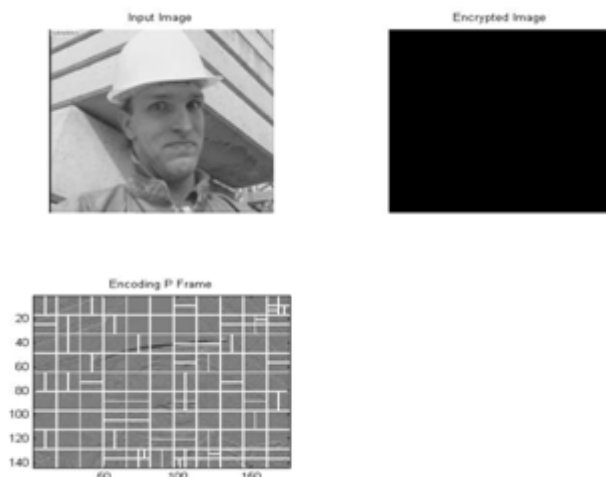Figure 7: 2 .FFigure 1 :
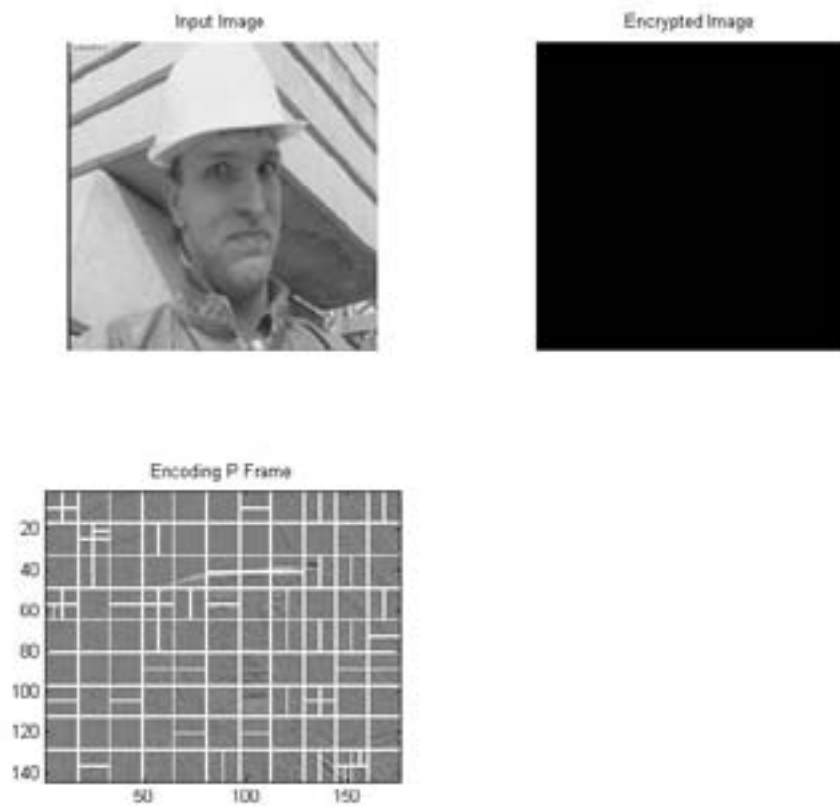
2

Figure 8: Figure 2 :

3

Figure 9: Figure 3 :

4

Figure 10: Figure 4 :

1

Figure 5 : Statistics of Selective Encryption

Figure 11: Table 1 :

2

Figure 12: Table 2 :

3

Figure 13: Table 3 :

139 [Doc and Jvt -Go5o ()] , Doc , Jvt -Go5o . 2003.

140 [Richardson] *An Overview of H.264 Advanced video coding*, Iain Richardson . (2007 white paper)

141 [Rajinder Kaur and Singh (2013)] 'Comparative Analysis and Implementation of Image Encryption Algorithms'.
142   Er Kanwalpreet Rajinder Kaur , Singh . *International Journal of Computer Science and Mobile Computing*
143   *(IJCSMC)* April 2013. 2 p. .

144 [J Ahn et al. ()] 'Digital Video Scrambling Method Using Intra Prediction Mode'. H 1 J Ahn , B Shim , I Jeon
145   , Choi . *Pacific Rim Conf. Multimedia*, (Tokyo, Japan) 2004. p. .

146 [Wieg] *Draft ITU-T Recommendation H.264 and Draft ISO/IEC 14496-10 AVC*, T Wieg . ISO/IEC JTC
147   1/SC29IWG 11 & ITU-T SG16/Q6.

148 [Su-Wan Park and Shin ()] 'Efficient Selective Encryption Scheme for the H.264/Scalable Video Coding (SVC)'.
149   Sang-Uk Su-Wan Park , Shin . *Fourth International Conference on Networked Computing and Advanced*
150   *Information Management*, 2008. 01 p. .

151 [Lian et al. (2008)] 'Efficient video encryption scheme based on advanced video coding'. S Lian , J Sun , G Liu ,
152   Z Wang . *Multimedia Tools Appl* May. 2008. 138 (1) p. .

153 [Abomhara et al.] 'Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard'. M
154   Abomhara , Omar Zakaria , O Othman , A Khalifa , B Zaidan , Zaidan . *International Journal of Computer*
155   *Theory and Engineering* 2 (2) .

156 [Shahid et al.] 'Fast Protection of H.264/AVC by Selective Encryption of CAVLC and CABAC for I & P frames'.
157   Z Shahid , M Chaumont , W Puech . *Journal of IEEE transactions on circuits and systems for video technology*,

158 [Zou et al. (2006)] 'H.264 video encryption scheme adaptive to DRM'. Yuanzhi Zou , Tiejun Huang , Wen Gao
159   , Longshe Huo . *IEEE Transactions on Consumer Electronics*, Nov. 2006. p. .

160 [Ibrahim et al. (2012)] 'Image Encryption Using Chaotic Map and Block Chaining'. S I Ibrahim , Hanan M
161   Abuhaiba , Abuthraya , B Huda , Ruba A Hubboub , Salamah . *International Journal of Computer Network*
162   *and Information Security* July, 2012. p. .

163 [Tong et al. ()] 'Layered Video Encryption Utilizing Error Propagation in H.264/AVC'. Lingling Tong , Gang
164   Cao , Jintao Li . *IEEE Symposium on Electrical & Electronics Engineering (EEESYM)*, 2012.

165 [Nidhi et al. (2008)] 'Selective Encryption of Multimedia Images'. S Nidhi , Balasubramanian Kulkarni , Indra
166   Raman , Gupta . *XXXII National Systems Conference*, 2008. December 17-19, 2008.

167 [Joshi and Dalal] 'Selective Encryption using ISMACryp in Real Time Video Streaming of H.264/AVC for DVB-
168   H Application'. Jay M Joshi , Upena D Dalal . *World Academy of Science, Engineering and Technology* 55 p.
169   2011.

170 [Lian et al. ()] 'Selective Video Encryption Based on Advanced Video Coding'. S Lian , Z Liu , Z Ren , Wang ,
171   Z . Lecture Notes in Computer Science 2005. Springer-Verlag. 3768 p. .

172 [A A Muhit et al. ()] 'Video Coding using Elastic Motion Model and Larger Blocks'. M R A A Muhit , M
173   Pickering , J F Frater , Arnold . *IEEE Trans. Circ. And Syst. for Video Technology* 2010. 20 (5) p. .

174 [A A Muhit et al.] 'Video Coding using Geometry Partitioning and an Elastic Motion Model'. M R A A Muhit
175   , M Pickering , J F Frater , Arnold . *Journal of Visual Communication and Image Representation*,