Global Journal of Computer Science and Technology
Graphics & Vision
Volume 13 Issue 9 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Analysis of H.264/AVC Encryption Techniques

By Dinesh Goyal, Srawan Nath & Dr. Naveen Hemrajani
Suresh Gyan Vihar University, India

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.

Keywords: h.264/avc; video encryption techniques; selective; layered; naïve.

GJCST-F Classification: E.3

An Analysis of H.264/AVC Encryption Techniques

Dinesh Goyal [α], Srawan Nath [σ] & Dr. Naveen Hemrajani [ρ]

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.

Keywords: h.264/avc; video encryption techniques; selective; layered; naive.

I. Introduction

Multimedia 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.

II. Encoding & Decoding

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.

Authors α σ : Suresh Gyan Vihar University, Jaipur.
e-mail: dgoyal@gyanvihar.org
Author ρ : JECRC University, Jaipur.

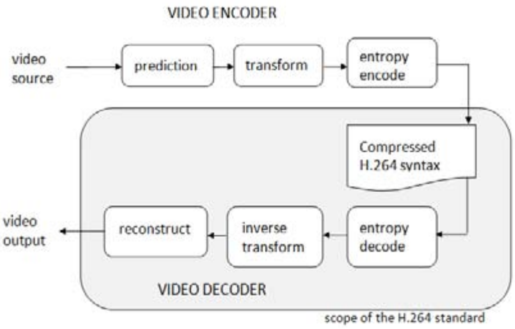


Figure 1 : H.264 video encoding and decoding process

III. 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.
- MPEG 4: MPEG-4 compression methods are used for texture mapping of 2-D and 3-D meshes, compression of time-varying streams, and algorithms for spatial, temporal and quality scalability, images and video. Scalability is required for video transmission over heterogeneous networks so that the receiver obtains a full resolution display. MPEG-4 provides high coding efficiency for storage and transmission of audio visual data at very low bit rates.
- MPEG 7: The MPEG-7 standard was approved in July 2001 (Chang, et al., 2001) to standardize a language to specify description schemes. MPEG-7 is a different kind of standard as it is a multimedia content description standard, and does not deal with the actual encoding of moving pictures and audio.
- H.261: The International Telecommunication Union (ITU) developed the H.261 standard for data rates that are multiples of 64Kbps. The H.261 standard uses motion compensated temporal prediction. It supports two resolutions, namely, Common Interface Format (CIF) with a frame size of 352 × 288, and Quarter CIF (QCIF) with a frame size of 172 × 144.
- H.263: The H.263 standard uses an encoding algorithm called test model (TMN), which is similar to that used by H.261 but with improved performance and error recovery leading to higher efficiency.
- H.263+: H.263+ is an extension of H.263 but has higher efficiency, improved error resilience, and reduced delay. It allows negotiable additional modes, spatial, and temporal scalability.

IV. 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).
- Video encryption algorithm: Bhargava, Shi, and Wang in 1996 and 1998 introduced four different video encryption algorithms : Algorithm I, Algorithm II (VEA); Algorithm III (MVEA); and Algorithm IV (RVEA).

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 ITU-T in March 2003. Researchers started work to make the H.264/AVC bit stream secure. Most of them tried to optimize the encryption process with respect to the encryption speed, and the display process.

V. 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:

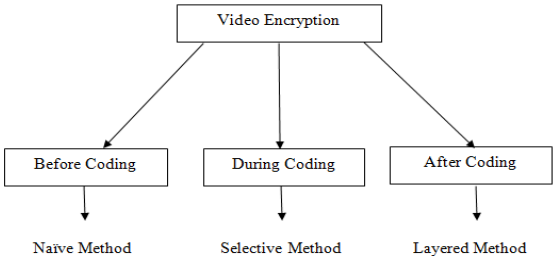


Figure 2 : Video Encryption Techniques

- *Fully Layered Encryption*: In this case the complete content of video is first compressed and then encryption is done with the use of standard algorithms like DES, RSA, AES, etc. This encryption technique is not appropriate in real time video applications because of heavy computation and slow speed.

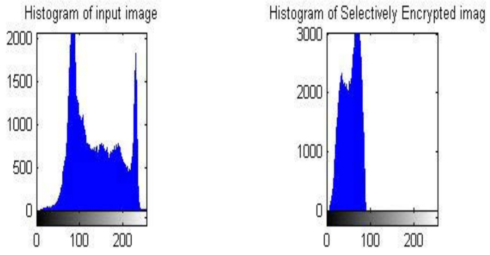


Figure 3 : Layered Encryption Histogram

Table 1 : Results of Fully Layered Method

Fields/Variables	I Frame	P Frame
No. of Frames	1	10
Time Taken Encryption	21.9	285.4
Time Taken for Encoding	71.1	216.73
Size of Frames Before Encryption & Encoding	4.52 KB	45 KB
Size of frame After Encryption & Encoding	604 Bytes	5.41 KB

- Selective Encryption: A communication encryption of many video and audio multimedia is not simply the application of established conventional encryption algorithms to their binary sequence. 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.

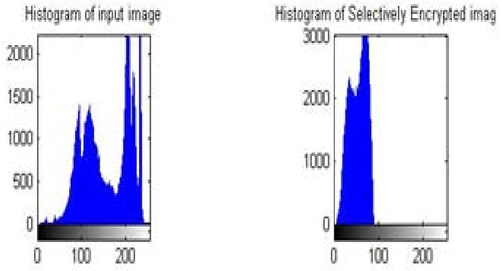


Figure 4 : Selective Encryption Histogram

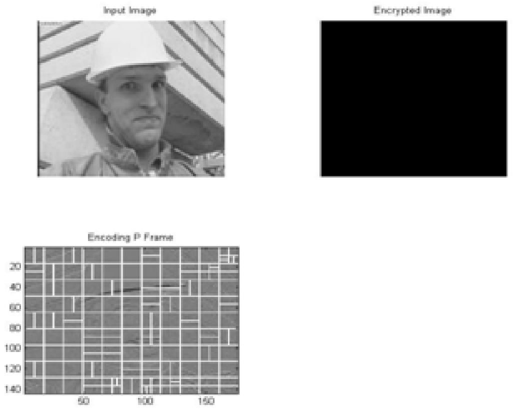


Figure 5 : Statistics of Selective Encryption

Table 2 : Results of Selective Method

Fields/Variables	I Frame	P Frame
No. of Frames	1	10
Time Taken Encryption	21.9	-
Time Taken for Encoding	71.1	248
Size of Frames Before Encryption & Encoding	4.52 KB	45 KB
Size of frame After Encryption & Encoding	8 KB	40 KB (notEncr.)

- 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.

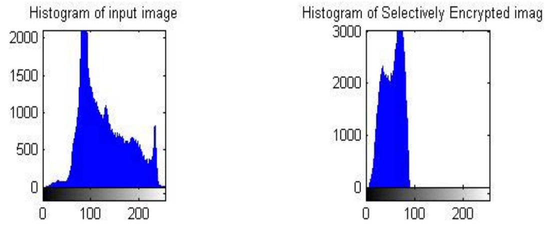


Figure 5 : P Frame Encryption Histogram

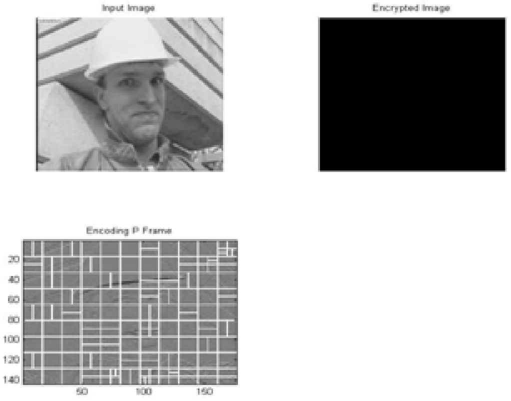


Figure 6 : Selective Naïve P Frame

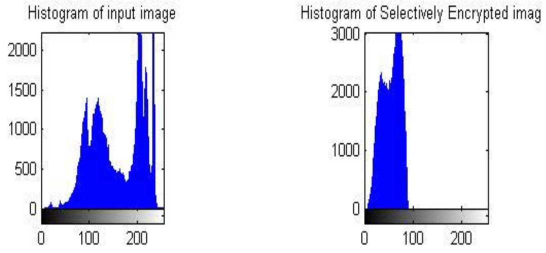


Figure 7 : Selective Naïve i Frame

Fields/Variables	I Frame	P Frame
No. of Frames	1	10
Time Taken Encryption	21.9	30
Time Taken for Encoding	43	43.9
Size of Frames Before Encryption & Encoding	4.52 KB	45 KB
Size of frame After Encryption & Encoding	4.1KB	5.49 KB

Table 3 : Results of Naïve Method

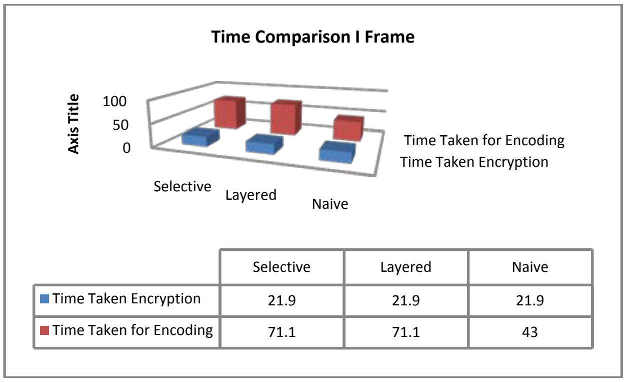
VI. Result Analysis of Video Encryption Methods

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).
2. In case of Selective encryption i.e. during encoding we have encrypted only the I frame and not the p frames as they are the following frames and have tried to optimize the results by implementing chaotic map based encryption.
3. For Fully layered encryption the encryption is performed on each layer of the encoded video i.e. I-Frame & P-Frames.

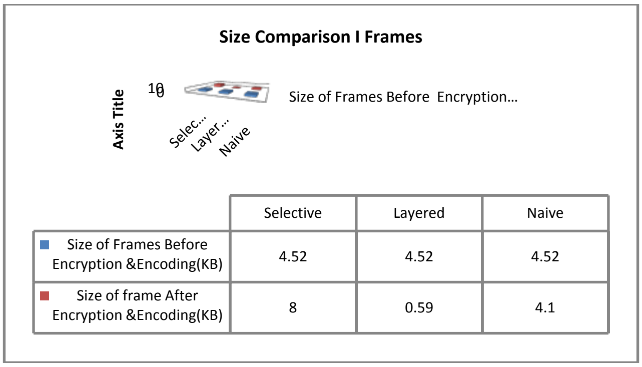
In figure 1, we have compared the time taken for encryption and encoding of I Frames in the Selective, Layered and Naïve Method.



	Selective	Layered	Naive
🟦 Time Taken Encryption	21.9	21.9	21.9
🟥 Time Taken for Encoding	71.1	71.1	43

Figure 1 : Time Comparison of I Frames in Selective, Layered and Naïve

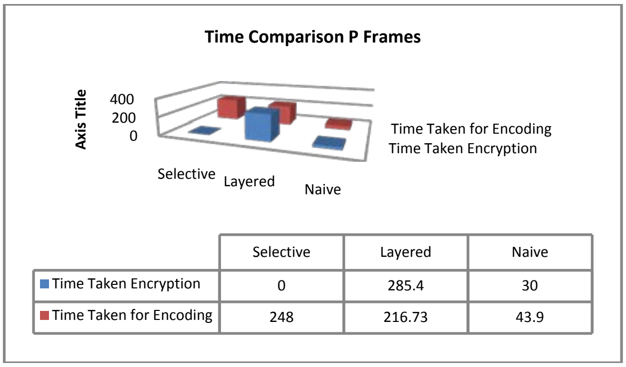
In figure 2, we have compared the size of I Frames before and after encrypted and encoded in the Selective, Layered and Naïve Method.



	Selective	Layered	Naive
🟦 Size of Frames Before Encryption &Encoding(KB)	4.52	4.52	4.52
🟥 Size of frame After Encryption &Encoding(KB)	8	0.59	4.1

Figure 2 : Size Comparison of I Frames in Selective, Layered and Naïve

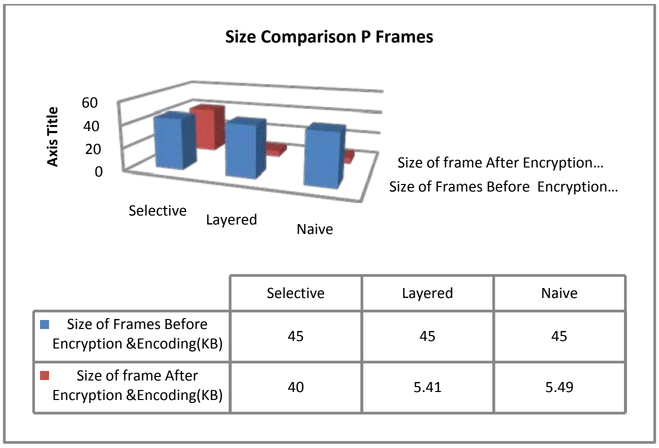
In figure 3, we have compared the time taken for encryption and encoding of P Frames in the Selective, Layered and Naïve Method.



	Selective	Layered	Naive
🟦 Time Taken Encryption	0	285.4	30
🟥 Time Taken for Encoding	248	216.73	43.9

Figure 3 : Time Comparison of P Frames in Selective, Layered and Naïve

In figure 4, we have compared the size of P Frames before and after encrypted and encoded in the Selective, Layered and Naïve Method.



	Selective	Layered	Naive
🟦 Size of Frames Before Encryption &Encoding(KB)	45	45	45
🟥 Size of frame After Encryption &Encoding(KB)	40	5.41	5.49

Figure 4 : Size Comparison of P Frames in Selective, Layered and Naïve

VII. 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, "trick-mode" 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 multi-view/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.

References Références Referencias

1. Su- Wan park, Sang-Uk shin. "Efficient Selective Encryption Scheme for the H.264/Scalable Video Coding (SVC)", Fourth International Conference on Networked Computing and Advanced Information Management, Volume 01, pp 371-376, 2008.
2. Iain Richardson, "An Overview of H.264 Advanced video coding". 2007 white paper. http://www.vcodex.com/files/H.264_overview.pdf (retrieved March 02, 2009).

3. Yuanzhi Zou, Tiejun Huang, Wen Gao, Longshe Huo. Nov, "H.264 video encryption scheme adaptive to DRM". IEEE Transactions on Consumer Electronics, pp. 1289 – 1297, 2006.
4. Lian, S., Liu, Z., Ren, Z., and Wang, Z., "Selective Video Encryption Based on Advanced Video Coding," Lecture Notes in Computer Science, Springer-Verlag 3768, 281–290 (2005).
5. Z. Shahid, M. Chaumont, W. Puech,"Fast Protection of H.264/AVC by Selective Encryption of CAVLC and CABAC for I & P frames", Journal of IEEE transactions on circuits and systems for video technology.
6. A A Muhit, M R Pickering, M R Frater and J F Arnold, "Video Coding using Elastic Motion Model and Larger Blocks," IEEE Trans. Circ. And Syst. for Video Technology, vol. 20, no. 5, pp. 661-672, 2010.
7. A A Muhit, M R Pickering, M R Frater and J F Arnold, "Video Coding using Geometry Partitioning and an Elastic Motion Model," accepted for publication in Journal of Visual Communication and Image Representation.
8. S. Lian, J. Sun, G. Liu and Z. Wang, "Efficient video encryption scheme based on advanced video coding," Multimedia Tools Appl, Vo138, No.1, pp.7S-89, May. 2008.
9. T.Wieg. Draft ITU-T Recommendation H.264 and Draft ISO/IEC 14496-10 AVC. Joint Video Team of ISO/IEC JTC 1/SC29IWG 11 & ITU-T SG16/Q6 Doc.JVT -GO5O, 2003.
10. J Ahn, H. 1. Shim, B. Jeon and I. Choi, "Digital Video Scrambling Method Using Intra Prediction Mode," in Pacific Rim Conf. Multimedia, Tokyo, Japan, pp.386-393, 2004.
11. Lingling Tong, Gang Cao, Jintao Li, "Layered Video Encryption Utilizing Error Propagation in H.264/AVC," in IEEE Symposium on Electrical & Electronics Engineering (EEESYM), 2012.
12. M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard," in International Journal of Computer Theory and Engineering, Vol. 2, No. 2 April, 2010.
13. Jay M. Joshi, Upena D. Dalal, "Selective Encryption using ISMACryp in Real Time Video Streaming of H.264/AVC for DVB-H Application," World Academy of Science, Engineering and Technology 55 2011.
14. Rajinder Kaur, Er. Kanwalpreet Singh, "Comparative Analysis and Implementation of Image Encryption Algorithms," International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 2, Issue 4, April 2013, Pg.170-176.
15. Ibrahim S. I. Abuhaiba, Hanan M. Abuthraya, Huda B. Hubboub, Ruba A. Salamah, "Image Encryption Using Chaotic Map and Block Chaining," International Journal of Computer Network and Information Security, July, 2012, Pg. 19-26.
16. Nidhi S Kulkarni, Balasubramanian Raman, and Indra Gupta, "Selective Encryption of Multimedia Images," XXXII National Systems Conference, NSC 2008, December 17-19, 2008.