audio data. Video fragment into number of frames instead of images because images have no capacity to store the audio data. When transfer video frames across the network then attackers will be attack on Sequential video frames that are require the pass the frames across the network randomly arrange the frames using shuffling block method. Shuffling block method useful for shuffling these frames with random position then forms new video.

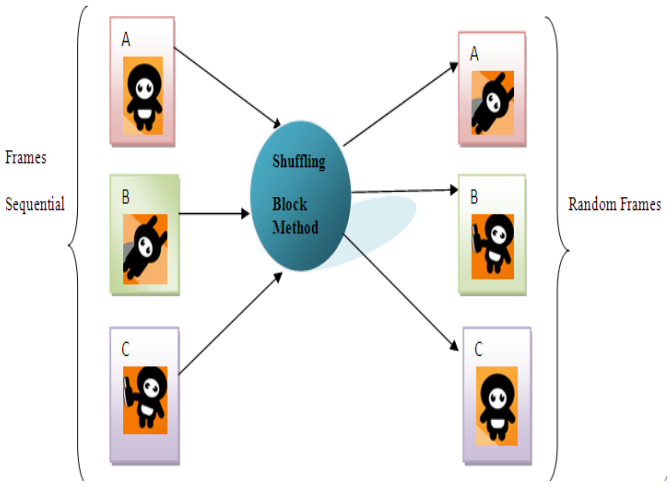

Figure 5: Shuffling Block Method [7] [3]

Shuffling block method used to shuffle audio streams of frames. Audio Streams easily shuffling but those streams Decryption/Decoding is very difficult and not understandable. Then random Shuffling Key at encryption the video frames with AES algorithm. This shuffling key also provide at decryption side. But one problem is there Brute-Force attacks have become more sophisticated, groups of expert video analysts may sit together and analyze the entire video frames by frame and bring together the original video [3].there is need increase the more and more security using AES Algorithm to prevent Brute-force attack. AES is used to encrypt the codeword's those are a stream of digital bits of image. AES is used to encrypt the Codeword's extraction from MVDs, DCs and ACs [3]. Extract only important as well as perceptive codeword's after that encrypts those important codeword's using AES. After encryption video will scramble with Codeword's. Finally, receiver get the Scramble video then use AES Algorithm again for Decoding/Decryption process and again start the process Same like that use in encryption. After decryption receiver get original video without alternatively contents.

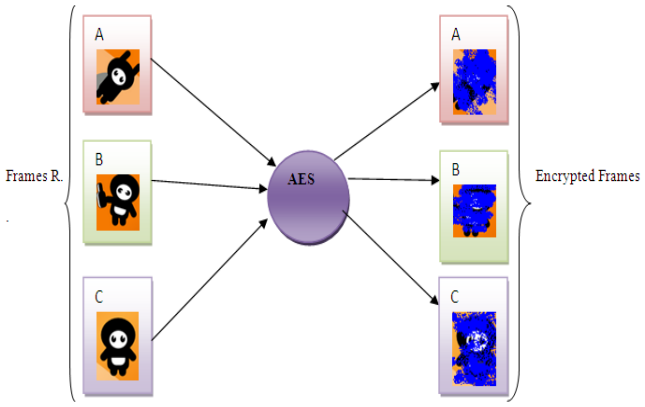

Figure 6: AES Encryption Algorithm [3] [7]

2.3 Video H.264/AVC Encryption

2.3.1 H.264/AVC

H.264 Advanced Video Coding (AVC) is a video compression format that is currently one of the most commonly used formats for recording, compression and distributed of video content [8]. H.264 standard first version was concluded in 2003.It is a block oriented motion compensation based standard jointly developed by Video Coding Experts Group (VCEG) of ITU-T and Moving Picture Expert Group (MPEG) of ISO/IEC.H.264 uses entropy Coding tools such as Context-adaptively switched sets of variable length codes called as CAVLC and Context-based adaptive binary arithmetic coding (CABAC) [8] and provides coding efficiency for various applications including video telephony, Video conferencing, storage(high definition DVD), Streaming video and so on [10]. Three basic profiles are Baseline profile designed to minimized complexity and provide high bandwidth, Main profile for compression coding efficiency capacity and Extended Profiles for combine the robustness of Baseline profile with higher degree of coding efficiency [11].

Format of H.264 video has a extensive relevance range that covers all forms of digital compressed video from low bit-rate internet streaming function to Digital cinema with nearly lossless coding[8].H.264 encoder and Decoder useful in video encryption and decryption.

After fragmentation prediction modes are Intra-Inter processing on sequential frames. Frame is divides into number of macroblock sequentially then it's called as slices. Prediction modes perform on each sub-macroblock of macroblock.

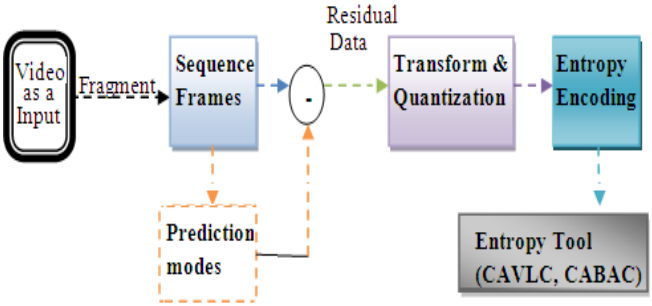

Figure 7: H.264 Encoder

DCT Transform is used to convert the particular domain signals into its similar frequency domain for removes temporal redundancies in the residual signal [9]. Quantization categories into two parts: Scalar quantiser maps one particular input signal from number of signals into one quantization output value and vector quantiser maps group of all input samples to group of quantized values. Entropy encoding converts the quantization scalar and vector signal data to compression bit-streams for transmission or storage and H.264/AVC use CABAC and CALVLC for variable length coding. H.264 decoder process is opposite from encoder process then give the original content of video without changeable.

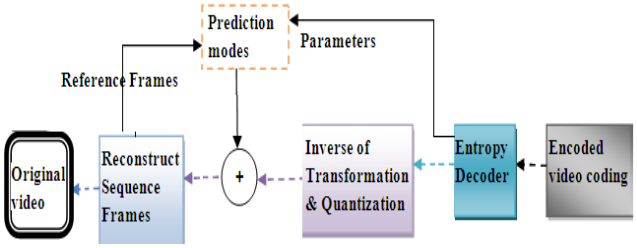

Figure 8: H.264 Decoder

2.3.2. Selective Encryption method to H.264/AVC:

When absentia of the reliable security to protect to multimedia application then it is risky to multimedia clients when transmission videos such as T.V. broadcast, medical data over network that time require Selective encryption scheme. This scheme used to select the part of compressed video data for encryption. They are encrypts only sensitive or important data not select the pixel wise whole data of compressed video. Result is reducing the computational cost.

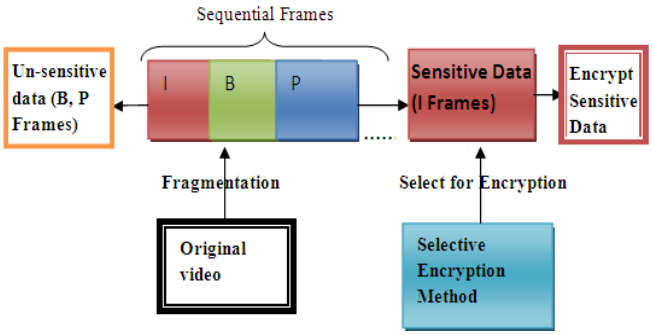

Figure 9: Structure of selective Encryption method

In figure, Technique is based on H.264/AVC I (Intra)-Frame, P (predicted)-Frame, B (Bidirectional Predicated)-Frame sequentially got from fragment the original video. Each frame contains a picture and collection of frames make video. I Frame independent from others frames, P-Frame predicated from previous frames and B- Frame both of previous Frames contains. To protect the video streaming information from against theft, alteration or misuse before transmission system encrypts the output of the H.264/AVC bit stream by the applied encryption algorithm (AES). Selective Encryption method selects only part of those frames they are unique and not continuously same. I-Frame was taken for encryption because this frame is unique not redundant data. Using this technique feasible solution problem and Minimum performance is occurring. Remove this problem via selective Encryption algorithm (SEA) with Advanced Encryption Standard (AES).

Advanced Encryption Standard (AES) is also known as Selection of the Rijndael Cryptosystem operates on 128-bit blocks arranged as 4x4 or 3 x 3 matrices with 8-bit entries [10]. Variable block length and key length are usable to AES for encryption of multimedia data. Performing encryption via AES is with different ways, different situation with suitable different methods. Applying AES at various situations as a Strong Key, Transformation with Rounding and Rounding with each four words [10].

Overview of requirements for H.264/AVC Encryption or Decryption:

- Requirements for the video encryption [10]: Security, error robustness, time efficiency for H.264/AVC bit streams should be more securely protected.
- Video Decryption: Sufficient quality of video content must be same original video after decryption of video.

3. Conclusion

The review on encryption scheme is on multimedia data such as images, audio and video. Cryptography is data encryption and decryption for confidentially data transfer from sender to receiver across the network. Video encryption is using Selective encryption scheme for Security. Video H.264/AVC encryption is performed with selective encryption with Advanced Encryption standard provides more security and high bandwidth or efficiency to transmit the video bit streams.

References

[1] FAN, Yibo “Algorithm and Hardware Design of Encryption Scheme for H.264/AVC” February 2009
[2] M. Abomhara, Omar Zakaria, Othman O. Khalifa” An Overview of Video Encryption Techniques” International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010
[3] Ajay Kulkarni ,Saurabh Kulkarni ,Ketki Haridas, Aniket More “Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study “ International Journal of Computer Applications (0975 – 8887) Volume 65– No.1, March 2013
[4] http://www.businessdictionary.com/definition/video.html
[5] Yibo Fan, jidong Wang ,Takeshi Ikenaga ,Yukiyasu tsunoo and satoshi Goto”A new Video Encryption Scheme For H.264/AVC
[6] Narsimha Raju C, UmaDevi Ganugula, Kannan Srinathan, C. V. Jawahar” A NOVEL VIDEO ENCRYPTION TECHNIQUE BASED ON SECRET SHARING”
[7] https://www.google.co.in/search?q=Cartoons+small
[8] http://en.wikipedia.org/wiki/H.264/MPEG-4_AVC

[9] Charles S. Lubobya1, Mqele M. Dlodlo1, Gerhard De. Jager1 and Keith L.Ferguson2," Optimization of 4x4 Integer DCT in H.264/AVC Encoder"

[10] 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 April, 2010.

[11] Gary J. Sullivan, Pankaj Topiwala, and Ajay Luthra" The H.264/AVC Advanced Video Coding Standard:Overview and Introduction to the Fidelity Range Extensions" H.264/AVC, August, 2004