# Secured Video Transmission at Low Bit Rate

Dr. S. Vaidya
Department of
Instrumentation Engineering
SGGSIET
Nanded, India

Poorva Waingankar
A.P. / H.O.D (ETRX)
Department of Electronics
Thakur College of
Engineering and Technology

Sujata S. Dubal
A.P. (ETRX)
Department of Electronics
Thakur College of
Engineering and Technology

## ABSTRACT
In this paper a video signal processing algorithm is proposed which is Modified H.264/AVC as a solution for Bandwidth saving through LBR (Low Bit Rate) applications to ensure acceptable video quality. Based on this concept, where the intraframe pictures are hybrid wavelet-based coded and the interframe pictures are coded with a Modified H.264/AVC encoder and decoder is proposed. Use of Modified H.264/AVC algorithm shows that this proposed hybrid encoder and decoder not only retains the same quality of the video but also lowers down the bit rate of the video considerably. AES based encryption and decryption system is proposed for added security for transmission and reception. The proposed algorithms are characterized by their efficient compression ratio, good PSNR, MSE results and lower bit rate as well as its efficient implementation in MATLAB.

## General Terms
Performance, Design, Experimentation, Security, Standardization.

## Keywords
Modified H.264/AVC, AES, Encoder and Decoder, Matlab, low bit rate.

## 1. INTRODUCTION
## 1.1 Related Background
Video (file types like AVI and MPEG) is a collection of several images being shown. Each image is called frames and the amount of images shown per second is called frames per second or simply FPS. The more frames per second your video has, the better, since more realistic the image will be. Videos are usually saved using at least TV quality settings, i.e. 30 frames per second. One way to reduce the video file size is reducing the number of frames per second. The file size is reduced, so its quality. In order to reduce the video file size, a video compression technique is used, which works by removing from the video parts of the image that were already shown [1].

This means that compressed video doesn't have the same quality as the original video. Unlike conventional Analog video, Digital Video is stored / transmitted very differently.

Analog video essentially turns the picture into a waveform and transmits it in terms of an electrical/radio wave.

Digital Video on the other hand, stores the video in 0's and 1's, storing a color value for each pixel of each frame. There are several ways to store color data, the two main ones being RGB and YUV [2].

## 1.2 Broader Aspect
Coding for low bit rate video applications has gained a special interest among the video coding community especially with the emergence of many applications such as video conferencing, video telephony, surveillance, and monitoring. In each case, video and audio information are transmitted over telecommunication links, including networks, telephone lines, ISDN and radio. The bandwidth required for the transmission of digital video is very much insufficient. So the compression of digital video is required to reduce the rate of information that is to be transmitted using the telecommunication links [3].

## 1.3 Converge to Focus
### 1.3.1 The H.264/AVC Algorithm
A hybrid video encoding algorithm typically compresses videos. Each picture is split into blocks. The first picture of a video sequence (or for a "clean" random access point into a video sequence) is typically coded in Intra mode (which typically uses some prediction from region to region within the picture but has no dependence on other pictures). For all remaining pictures of a sequence or between random access points, typically inter-picture coding modes are used for most blocks. The encoding process for Inter prediction (ME) consists of choosing motion data comprising the selected reference picture and MV to be applied for all samples of each block [4].

### 1.3.2 Results to Highlight the Focus Area
The present work deals with compressing and decompressing a video for lower bit rate. Modified H.264/AVC algorithm has been used for Interframe compression whereas Hybrid Wavelet has been used for Intraframe compression. The results are shown for various videos where the bit rate of the video has been reduced to a larger extent [5].

## 2. IMPLEMENTATION
## 2.1 Encoder / Decoder Design
The design is done using Hybrid H.264/AVC algorithm. The encoder block first slices video into frames. These frames are then applied to the Interframe which uses Hybrid H.264/AVC.

Further these frames are given to the Intraframe block where Hybrid Wavelet is applied to these frames. The decoder block works exactly opposite to the encoder block. The bits are converted into frames which are further given to the Intraframe block. Frames are further passed on to the Interframe block. Final video having lower bit rate is thus achieved.

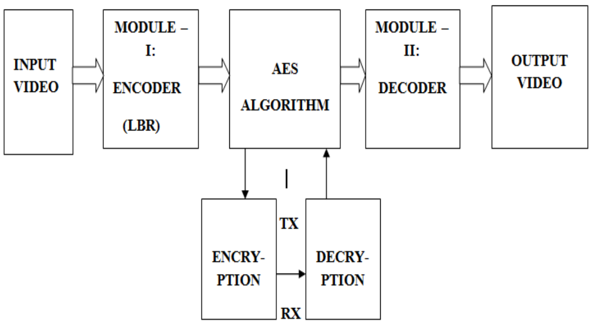


**Figure 1: Block diagram of Encoder and Decoder**

In the above block diagram Input video is first given to the Encoder section then for increasing the security while transmission AES is introduced as it is a highly secure algorithm. The data is further passed on to the Decoder section and finally we get output video with acceptable picture quality. AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware, is relatively easy to implement, and requires little memory. Unlike its predecessor DES, AES does not use a Feistel network.

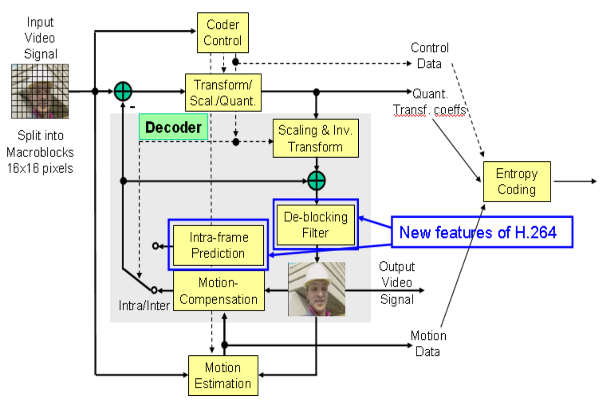


**Figure 2: Basic Structure of H.264/AVC Block**

An intra (I) macroblock is coded without referring to any data outside the current slice. I macroblocks may occur in any slice type. Every macroblock in an I slice is an I macroblock. I macroblocks are coded using intra prediction, i.e. prediction from previously-coded data in the same slice [6]. For a typical block of luma or chroma samples, there is a relatively high correlation between samples in the block and samples that are immediately adjacent to the block. Intra prediction therefore uses samples from adjacent, previously coded blocks to predict the values in the current block [7].
Inter prediction is the process of predicting a block of luma and chroma samples from a picture that has previously been coded and transmitted, a reference picture. This involves selecting a prediction region, generating a prediction block and subtracting this from the original block of samples to form a residual that is then coded and transmitted. The block of samples to be predicted, a macroblock partition or sub-macroblock partition, can range in size from a complete macroblock, i.e. 16 × 16 luma samples and corresponding chroma samples, down to a 4 × 4 block of luma samples and corresponding chroma samples [8].
The reference picture is chosen from a list of previously coded pictures, stored in a Decoded Picture Buffer, which may include pictures before and after the current picture in display order.
The offset between the position of the current partition and the prediction region in the reference picture is a motion vector. The motion vector may point to integer, half- or quarter-sample positions in the luma component of the reference picture. Half- or quarter-sample positions are generated by interpolating the samples of the reference picture [9].
Each motion vector is differentially coded from the motion vectors of neighbouring blocks. The prediction block may be generated from a single prediction region in a reference picture, for a P or B macroblock, or from two prediction regions in reference pictures, for a B macroblock. Optionally, the prediction block may be weighted according to the temporal distance between the current and reference picture(s), known as weighted prediction [10]. In a B macroblock, a block may be predicted in direct mode, in which case no residual samples or motion vectors are sent and the decoder infers the motion vector from previously received vectors [12].

## 2.2 AES Design

At the start of the Cipher, the input is copied to the State array using the conventions. After an initial Round Key addition, the State array is transformed by implementing a round function 10, 12, or 14 times (depending on the key length), with the final round differing slightly from the first Nr 1 - rounds. The final State is then copied to the output [11].

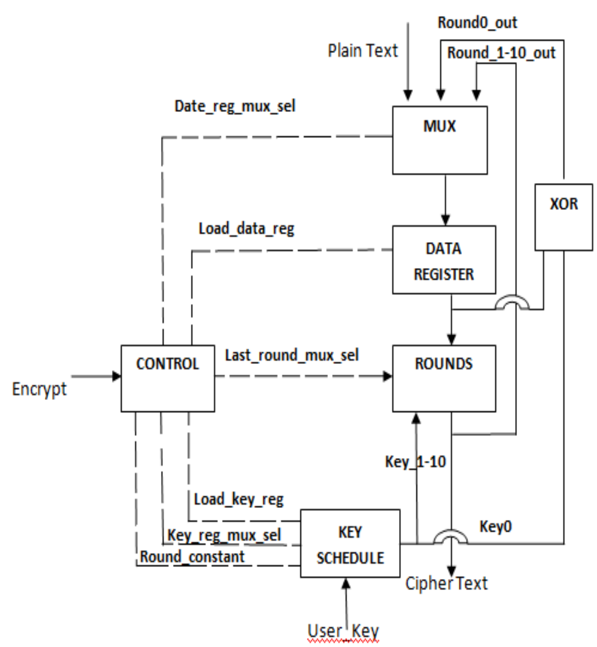


**Figure 3: AES Encryptor Block**

The Cipher transformations can be inverted and then implemented in reverse order to produce a straight forward Inverse Cipher for the AES algorithm. The individual transformations used in the Inverse Cipher - InvShiftRows (), InvSubBytes (), InvMixColumns () and AddRoundKey() – process the State and can be implemented in the inverse way as that of Encryption Cipher [11].

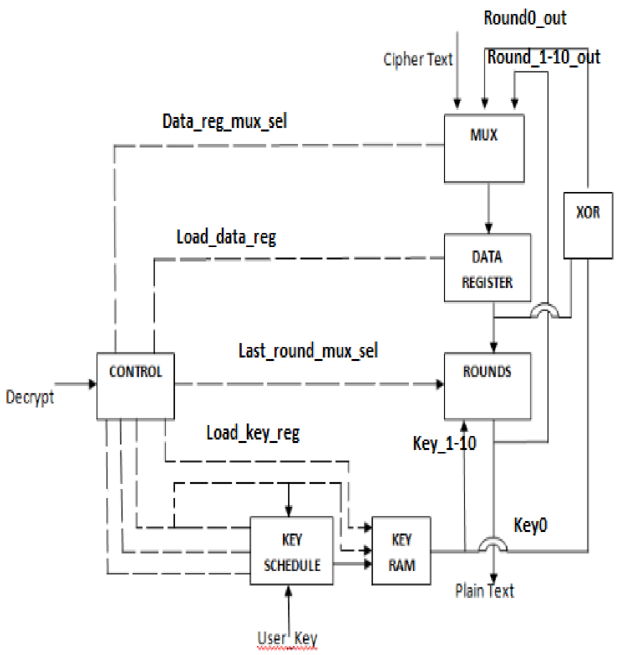


**Figure 4: AES Decryptor Block**

## 3. RESULTS

The processing of the video is divided into seven parts. First part deals with decompressing the originally compressed video which gives us the actual parameters of that video. The second part deals with the Interframe compression, which reduces the number of frames in the video. The third part deals with the Intraframe compression, which reduces the redundancy in each frame. The fourth part deals with the AES encryption, which encrypts the data for secure transmission. The fifth part deals with the AES decryption, which decrypts the data to recover the original data. The sixth part deals with the Inverse Intraframe Decompression, which recovers the redundant data in each frame. The seventh part deals with the Inverse Interframe Decompression, which adds number of frames to reconstruct the original video. Parameters such as Size and Bit Rate of the video are considerably reduced by using Modified H.264/AVC algorithm compared to the Actual and AVI video. The Actual video is obtained by first decompressing the compressed file format which will yield actual size and Bit Rate of the video. The AVI video format is obtained directly from file extensions such as .avi which is compressed form of original video using general H.264/AVC standard [13].

Thus, the results shows that, Modified H.264/AVC algorithm gives better results as compared to the general H.264/AVC as well as other standards with respect to size and bit rate of the video.

### 3.1 High – End Video

Modified H.264/AVC algorithm is applied to the video clip. The clip is of 7 seconds which is divided into 107 frames. Interframe compression is then applied to these 107 frames which reduces the frames by using the Modified H.264/AVC algorithm. Wavelet transform coding is used for Interframe compression which uses SPIHT technique. SPIHT builds a tree structure of the frames and takes only the most important frames. Further Intraframe compression is applied to the frames. Hybrid wavelet transform algorithm is used for Intraframe compression. It reduces the data in each frame thus further compressing the video. The video is decompressed using Inverse Interframe and Inverse Intraframe decompression technique.

**Figure 5: Original Video**

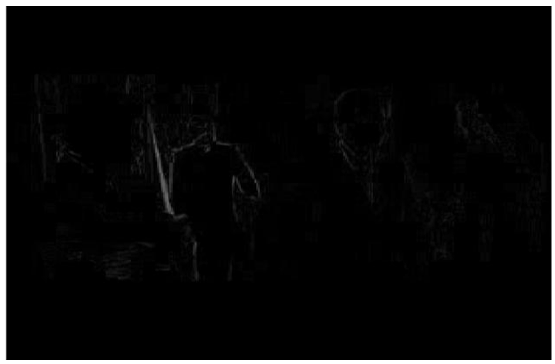

**Figure 6: After Interframe Compression**

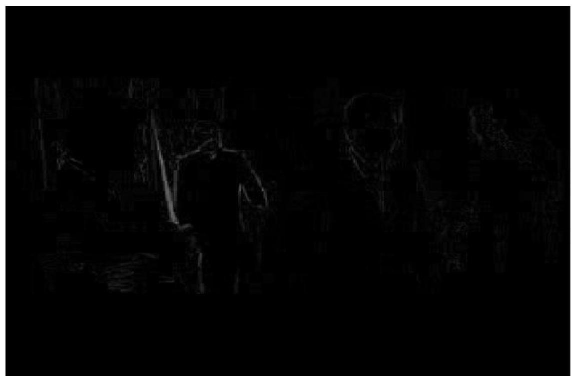

**Figure 7: After Intraframe Compression**

**Table 1: Comparison of Size and Bitrate of the video**

| HIGH END VIDEO | SIZE (Kb) | COMPRESSION RATIO (%) | BITRATE (Kbps) |
|---|---|---|---|
| ORIGINAL VIDEO | 3.2238*104 | 0 | 7.6032*103 |
| INTERFRAME COMPRESSION | 8.6757*103 | 26.9117 | 2.0461*103 |
| INTRAFRAME COMPRESSION | 6.2715*103 | 43.3732 | 1.4791*103 |
| AES ENCRYPTION | 6.2715*103 | 0 | 1.4791*103 |
| AES DECRYPTION | 6.2715*103 | 0 | 1.4791*103 |
| INVERSE INTRAFRAME DECOMPRESSION | 1.3617*104 | 217.1233 | 3.2115*103 |
| INVERSE INTERFRAME DECOMPR5ESSION | 2.7167*104 | 199.5096 | 6.4073*103 |

**Video Parameters**

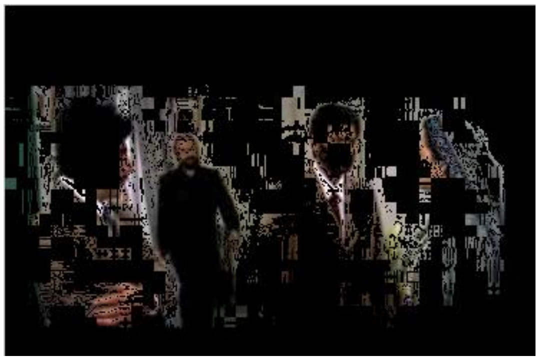

**Figure 8: After Intraframe Decompression**

**Figure 9: After Interframe Decompression**

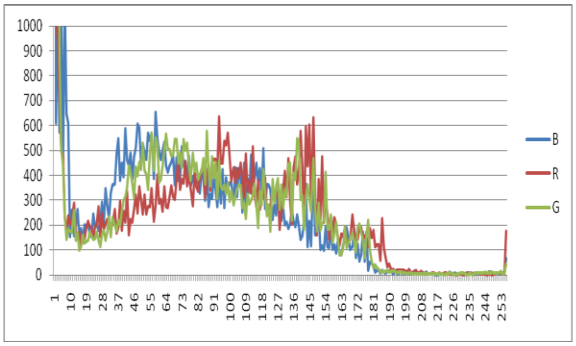


**Figure 10: R, G and B contents of the video**

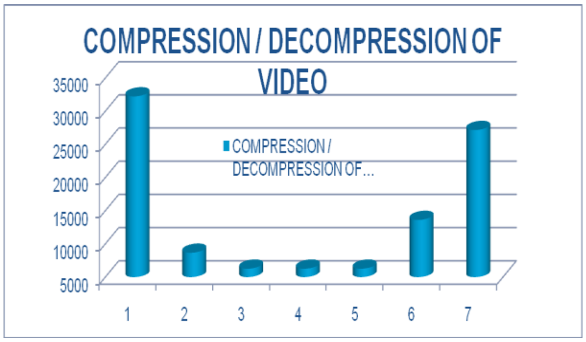


**Figure 11: Stepwise compression of the video**

## 3.2 AES Algorithm

AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain-text into the final output of cipher-text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher-text back into the original plain-text using the same encryption key [11].

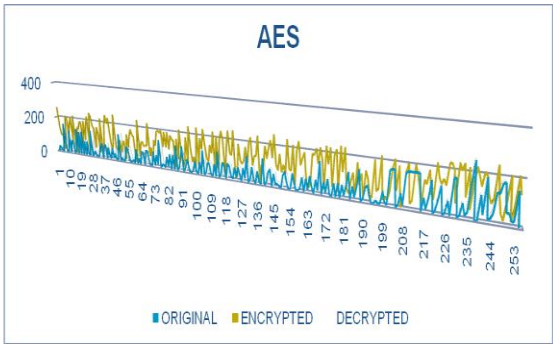


**Figure 12: Encryption and Decryption using AES**

### 3.3 PSNR and MSE Graphs

The peak signal to noise ratio is high as compared to the original video whereas the mean square estimation is low as compared to the original video. The frame wise compression of the whole video is shown in the graph where compression takes place in each frame. The compression in each frame is due to the Modified H.264/AVC technique which modifies the existing algorithm by using Wavelet transform coding (WTC) instead of CABAC coding (Content based adaptive binary arithmetic coding) [14].

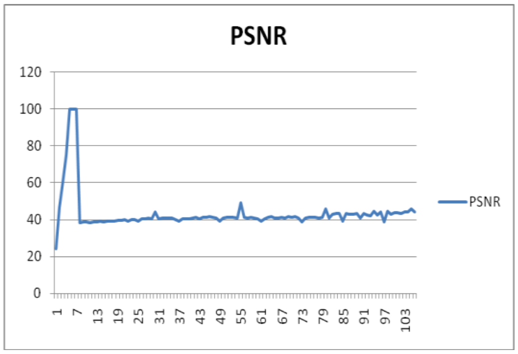


**Figure 13: PSNR of the video**

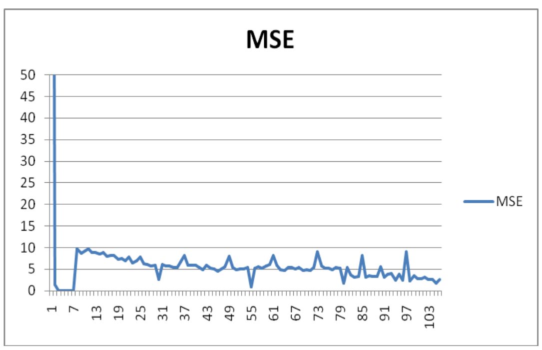


**Figure 14: MSE of the video**

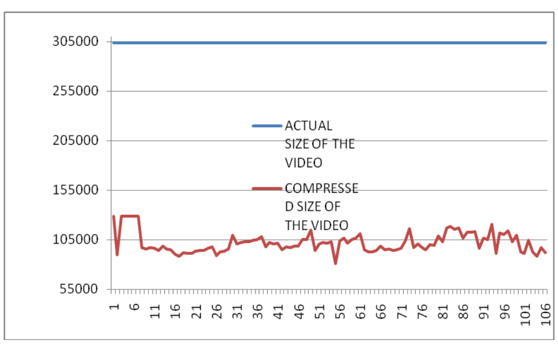


**Figure 15: Frame wise Compression of the video**

### 3.4 Comparison with Existing Standards

From the graphs we can conclude that, the size of the video is reduced in comparison with existing H.264/AVC algorithm. The above video of a nun was having a size of 32 Mb which is reduced to 23 Mb by using standard H.264/AVC whereas it is reduced to 6 Mb by using the above Modified H.264/AVC algorithm. The above video of a nun was having a bit rate of 7.6 Kb/sec which is reduced to 5.7 Kb/sec by using standard H.264/AVC whereas it is reduced to 1.4 Kb/sec by using the above modified H.264/AVC algorithm. Thus we can conclude that, the main factors of a video such as size and bit rate are reduced considerably as compared to the existing standards by using the modified H.264/AVC algorithm.

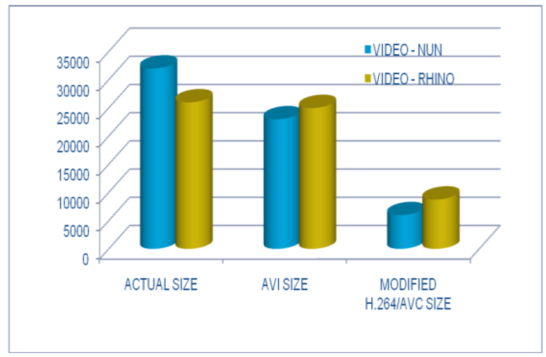


**Figure 16: Graph of Size of the video**

**Table 2: Comparison of Size**

| VIDEO SIZE | ACTUAL SIZE | AVI SIZE | MODIFIED H.264/ AVC SIZE | % AVI with respect to ACTUAL | % MOD. H.264/AVC with respect to ACTUAL |
|---|---|---|---|---|---|
| VIDEO -NUN | 32*103 Kb | 23*103Kb | 6*103 Kb | 71.88 | 18.75 |
| VIDEO RHINO | 26*103 Kb | 25*103 Kb | 8.76*103Kb | 96.15 | 3.69 |

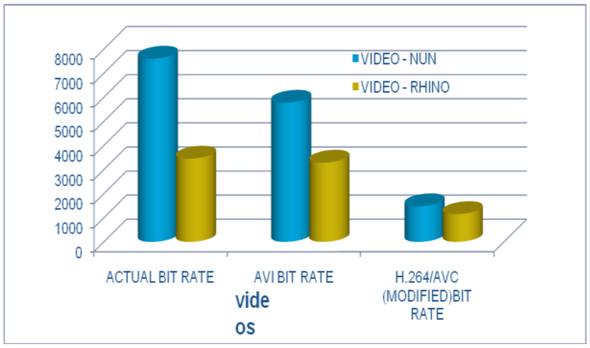


**Figure 17: Graph of Bit rate of the video**

**Table 3: Comparison of Bit rate**

| VIDEO SIZE | ACTUAL SIZE | AVI SIZE | MODIFIED H.264/ AVC SIZE | % AVI with respect to ACTUAL | % MOD. H.264/AVC with respect to ACTUAL |
|---|---|---|---|---|---|
| VIDEO -NUN | 32*103 Kb | 23*103Kb | 6*103 Kb | 71.88 | 18.75 |
| VIDEO RHINO | 26*103 Kb | 25*103 Kb | 8.76*103Kb | 96.15 | 3.70 |

## 4. CONCLUSION

The low bit rate Modified H.264/AVC algorithm is implemented using MATLAB. Video processing is done for low bit rate video and bit rate is scaled down considerably using Modified H.264/AVC algorithm. Quality of the video is achieved to some extent (acceptable level) after applying best combination of compression algorithms. Large amount of data was send faster and less number of bits to represent the same were used. The algorithm works on all types and formats of video.

AES algorithm was implemented for better security. Encryption and Decryption of the video has increased its security. Verification of the results is done using various videos. Modified H.264/AVC is tested on High-end videos (clips from movies). The algorithm is modified for efficient implementation for transmission of videos at low bit rate. System efficiency is overall increased.

## 5. APPLICATIONS

H.264/AVC is currently been used in the Digital Video Broadcast project (DVB), the Advanced Television Systems Committee (ATSC), AVCHD is a high-definition recording format designed by Sony and Panasonic. AVC is an intraframe compression only format, the CCTV (Close Circuit TV) or Video Surveillance are the various applications of the Hybrid H.264/AVC codec.

## 6. FUTURE SCOPE

The project further can be extended for audio.
Design of CODEC can be done which can be interfaced with VLSI based chip design.

## 7. ACKNOWLEDGEMENTS

I would like to thank my guide Ms. Poorva Waingankar (H.O.D), as despite her busy schedule she was always kind and patient to listen my difficulties and indicate me the right path.

I would also like to thank Dr. B.K. Mishra (Principal), for his invaluable help, constant encouragement and constructive suggestions at every stage of development. Finally, I would like to thank all my friends and colleagues who have directly and indirectly contributed in implementation of this algorithm.

## 8. REFERENCES

[1] Gary J. Sullivan, Senior Member, IEEE and Thomas Wiegand, "Video Compression-From Concepts to the H.264/AVC Standard", Proceedings of the IEEE Trans. vol.93.No.1.January 2005.

[2] M. T. Orchard and G. J. Sullivan, "Overlapped block motion compensation: An estimation-theoretic approach," IEEE Trans. Image Process., vol. 3, no. 5, pp. 693–699, Sep. 1994.

[3] Markus Flierl, T. Wiegand and B. Girod, "Rate-Constrained Multi-Hypothesis Motion-Compensated prediction for video coding", IEEE – 2000.

[4] B. Girod, A. Aaron, S. Rane, and D. Rebollo-Monedero, "Distributed video coding", Proc. IEEE, vol. 93, no. 1, pp. 71–83, Jan-2005.

[5] H. Schwarz, D. Marpe and T. Wiegand, "Overview of the scalable video coding extension of the H.264/AVC standard", IEEE Transactions on Circuits and Systems for Video Technology, September 2007.

[6] Ian E.G. Richardson, "H.264/AVC and MPEG – 4 video Standards", Wiley Publications.

[7] Ian E.G. Richardson, "The H.264 Advanced Video Compression Standard", Wiley Publications

[8] Thomas Wiegand and Gary J. Sullivan, "The H.264/AVC Video coding standard", [Standards in a nutshell] IEEE Signal Processing Magazine [148], March 2007.

[9] G. J. Sullivan and R. L. Baker, "Motion compensation for video compression using control grid interpolation," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP), 1991, pp. 2713–2716.

[10] G. J. Sullivan, "Multi-hypothesis motion compensation for low bit rate video coding," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, 1993, pp. 437-440.

[11] National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL), Advanced Encryption Standard (AES), Federal Information Processing (FIPS) Publication 197, November 2001.

[12] Karel Rijkse, KPN Research, "H.263 Video Coding for Low bit Rate Communication", IEEE Communications Magazine December 1996.

[13] G. J. Sullivan and T. Wiegand, "Rate-distortion optimization for video compression", IEEE Signal Process. Mag., vol. 15, pp. 74–90, Nov. 1998.

[14] I.E. Richardson, C.S. Kannangara, M. Bystrom, J. Philp and Y. Zhao, "Implementing fully Configurable Video coding", ICIP 2009, IEEE 2009.