ENCRYPTION AND DATA HIDING IN H.264 VIDEO STREAM

Ravi kumar Nartu[1], Bipul Thakur[2], K.Satya Rahul[3]

[1]Ravi kumar Nartu , U.G. student
[2]Bipul Thakur, U.G. student
[3]K. Satya Rahul, Assistant Professor
[1, 2, 3]Dept. of Electronics and communication Engineering
[1, 2, 3]Godavari institute of engineering and technology, Andhra pradesh, India

---

Abstract - *Transmission of video over internet is prone to attacks from untrustworthy system and administrators. Hence it is necessary to perform encryption of video content for maintaining security of those contents. Data hiding in encrypted domain without decryption preserves the confidentiality of the content. For authentication and damage detection and covert communication, it is useful to embed secret information in these encrypted videos. A method is proposed where the secret information is embedded directly into encrypted video stream, thereby maintaining confidentiality of video content. The input video is compressed using H.264/AVC (Advance Video Compression) or HEVC (High Efficiency Video Coding encoder). This compressed video is converted into frames for the purpose of data hiding using codeword substitution and those encoded data hidden video is encrypted using DES (Data encryption standard) and random generated password. The codewords of residual coefficients, motion vector differences and intraprediction modes are encrypted using a stream cipher. Encrypted video along with encrypted file which contain password and frame number is send for storage or to receiver for decryption.*

Key Words: **HEVC/AVC Video, Data hiding, H.264/AVC (Advance Video Compression), random generated password.**

1.INTRODUCTION:

In modern communication systems, there exists a diversity of applications with the coded video being an important part. Flexibility with regard to the application, efficiency of coding and robustness to channel changes are the most important features that are demanded from the video codec. H.264/AVC (Advanced Video Coding) codec meet these demands representing a solution for different multimedia systems. The PSNR has demonstrated to be a way to compute the perceptual quality of images. It is widely used because its simplicity and immediacy to be computed. This paper presents the measuring of the image quality of a video raw file (*.yuv) and encoded-decoded generated file compression system based in the H.264/AVC standard. These results have been compared and graphs have been shown with the quality measured by means of the traditionally used Peak Signal to Noise Ratio (PSNR). This paper measure quality of video which will encode & decode by H.264/AVC codec. However, an increasing number of services and growing popularity of high definition TV are creating greater needs for higher coding efficiency. Moreover, other transmission media such as Cable Modem, xDSL, or UMTS offer much lower data rates than broadcast channels, and enhanced coding efficiency can enable the transmission of more video channels or higher quality video representations within existing digital transmission capacities.

1.1 LITERARY SURVEY

Video encryption has been heavily researched in the recent years. This survey summarizes the latest research results on video encryption with a special focus on applicability and on the most widely-deployed video format H.264 including its scalable extension SVC. The survey intends to give researchers and practitioners an analytic and critical overview of the state-of-the-art of video encryption narrowed down to its joint application with the H.264 standard suite and associated protocols (packaging/streaming)& processes(transcoding/watermarking).H.264/AVC is a document published by the international standards bodies ITU-T (International Telecommunication Union) and ISO/IEC (International Organization for Standardization/International, Electrotechnical Commission).

As video file consist of several image sequence, so considering the data hiding technique of image will also apply for video data hiding. The most widely used technique to hide data is the usage of the LSB (Least significant bit modifications). Although there are several disadvantages to this approach, the relative easiness to implement it, makes it a popular method. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm.

2. PROPOSED FRAMEWORK AND DESIGN

(A) Problem Definition:

Information hiding in encrypted media is a new topic of privacy-preserving requirements of cloud data management. The encrypted H.264/AVC bitstream, which consists of encryption of videos, data embedding, and data extraction phases. In the information hiding it follows the without decrypting the data, the data hiding and re-encryption takes place. The bit stream preserves exactly after encryption and data embedding. For the data embedding, we use the code word substitution technique, even though it does not know the original video content.H.264 is an industry standard for video compression, the process of converting digital video into a format that takes up less capacity when it is stored or transmitted. It defines a format (syntax) for compressed video and a method for decoding this syntax to produce a displayable video sequence. The standard document does not actually specify how to encode (compress) digital video - this is left to the manufacturer of a video encoder - but in practice the encoder is likely to mirror the steps of the decoding process.

(B) BLOCK BASED HYBRID CODING:

A digitized video signal consists of a periodical sequence of images called frame. Each frame consists of a two dimensional array of pixels. Each pixel consists of three color components, R, G and B. Usually, pixel data is converted from RGB to another color space called YUV in which U and V components can be sub-sampled. A block-based coding approach divides a frame into macroblocks each consisting of say 16x16 pixels. In a 4:2:0 format, each MB consists of 16x16 = 256 Y components and 8x8 = 64 U and 64 V components. Each of three components of an MB is processed separately. To compress an MB, we use a hybrid of three techniques: prediction, transformation & quantization, and entropy coding. The procedure works on a frame of video. For video sequence level, we need a top level handler, which is not covered in this paper. In the pseudo code, ft denotes the current frame to be compressed and mode could be I, P, or B. Prediction tries to find a reference MB that is similar to the current MB under processing so that, instead of the whole current MB, only their (hopefully small) difference needs to be coded. Depending on where the reference MB comes from, prediction is classified into inter-frame prediction and intra-frame prediction. In an inter-predict (P or B) mode, the reference MB is somewhere in a frame before or after the current frame, where the current MB resides. It could also be some weighted function of MBs from multiple frames. In an intra-predict (I) mode, the reference MB is usually calculated with mathematical functions of neighboring pixels of the current MB. The difference between the current MB and its prediction is called residual error data (residual). It is transformed from spatial domain to frequency domain by means of discrete cosine transform. Because human visual system is more sensitive to low frequency image and less sensitive to high frequency ones, quantization is applied such that more low frequency information is retained while more high frequency information discarded. The third and final type of compression is entropy coding. A variable-length coding gives shorter codes to more probable symbols and longer codes to less probable ones such that the total bit count is minimized. After this phase, the output bit stream is ready for transmission or storage

(C) SYSTEM ARCHITECTURE:

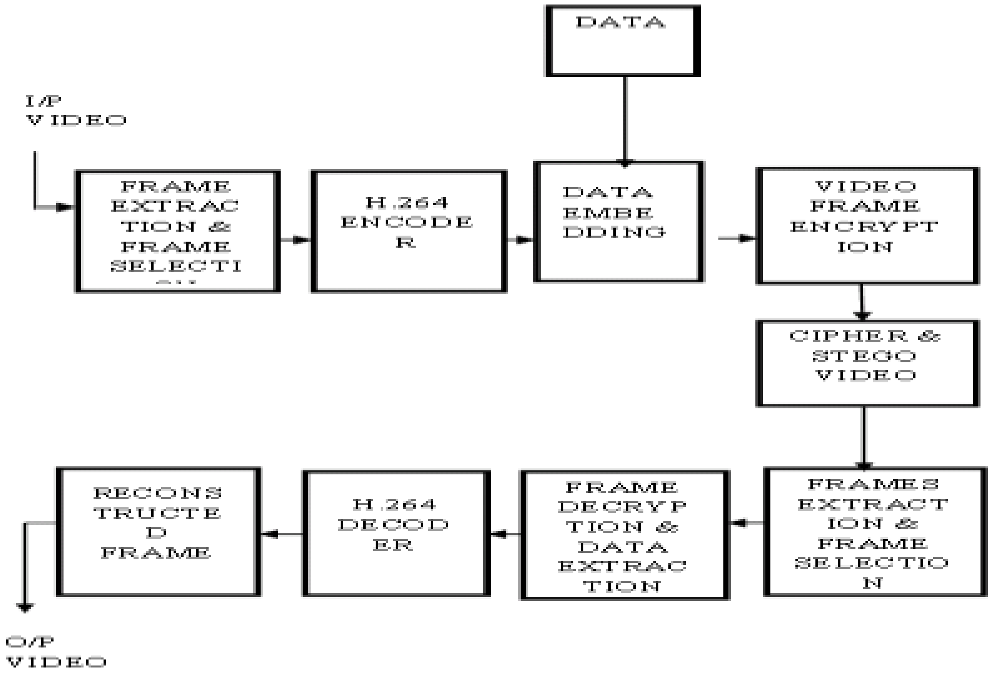

Figure 1: System Architecture of H264

(D) H.264/AVC VIDEO CODING:

Video compression systems are used in many consumer electronic devices such as digital camcorders or cellular phones. These applications make video compression hardware devices an inevitable part of many commercial products. H.264/AVC, as the most recent coding standard for video compression, significantly outperforms previous standards in bit-rate reduction, improving the performance of the existing applications and enabling the applicability of video compression to new real-time applications [4]. We knew that H.264/AVC offers up to 50% better compression than MPEG-2 and up to 30% better than H.263+ and MPEG-4 Advanced Simple Profile (ASP). In Figure 2, the top-level block diagram of an H.264/AVC encoder is shown. The video compression efficiency achieved in H.264/AVC standard is not a result of any single feature but rather a combination of a number of heterogeneous video coding tools. As a system, the H.264/AVC encoder processes video frames divided in basic units defined as Macro-Blocks (MBs). Each MB is a square tile of 16 × 16 luminance and 8x8 chrominance data for a 4:2:0 sampling. The entire encoding operation is distinguished into the forward (encoding) path and the inverse (reconstruction or decoding) path. The forward-encoding path predicts each MB using Inter or Intra prediction and it also Transforms and quantizes the residual.

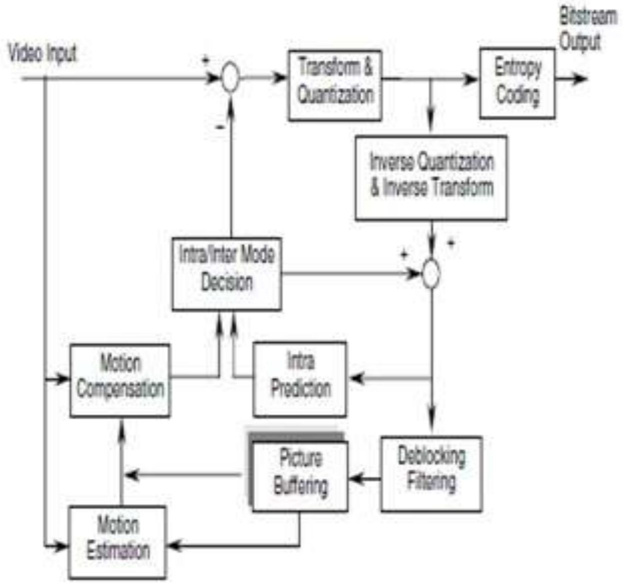

Figure 2: Block Diagram of H264 Encoder

Then it forwards the result to the Entropy Encoder module and forms the output packets in the form of a binary bit- stream. The inverse path involves the reconstruction of the MB from the previously transformed data by utilizing the Inverse Transform, the Inverse Quantization and the de-blocking filter.

The Motion Estimation and Motion Compensation (ME/MC) modules generate 1/2 and 1/4 pixel resolutions motion vectors and allow several MB partitioning. The Intra prediction module computes for each MB all four modes of the 16 × 16 luma processing requirement, also all the nine 4 × 4 luma modes and all the four 4 × 4 Chroma prediction modes. The "selection module" chooses the best mode for encoding between Intra mode and Inter (ME/MC) mode by using the low complexity rate distortion optimization technique . Figure 3 shows the inverse to block diagram of H.264/ AVC encoder as the H.264/AVC decoder.

(E) PREDICTION:

Prediction exploits the spatial or the temporal redundancy of a video sequence so that only the difference between actual and predict instead of the whole image data need to be encoded. There are two types of prediction: intra prediction for I-type frame and inter prediction for P-type (Predictive) and B-type (Bidirectional Predictive) frame. Intra Prediction: There exists high similarity among neighbouring blocks in a video frame. Consequently, a block can be predicted from its neighbouring pixels of already coded and reconstructed blocks. The prediction is carried out by means of a set of mathematical functions. In H.264/AVC, an I-type 16x16 4:2:0 MB has its luminance component (one 16x16) and chrominance components (two 8x8 blocks) separately predicted. There are many ways to predict a macro-block as illustrated in Fig. 2. The luminance component may be intra-predicted as one single INTRA16x16 block or 16 INTRA4x4 blocks. When using the INTRA44 case, each 44 block utilizes one of nine prediction modes (one DC prediction mode and eight directional prediction modes). When using the INTRA1616 case, which is well suited for smooth image area, a uniform prediction is performed for the whole luminance component of a macro-block. Four prediction modes are defined. Each chrominance component is predicted as a single 8x8 block using one of four modes. Motion vector difference: In this type, it protected the texture information as well as motion information. It is similar to intra prediction mode. It predicts the frames in a video.

Inter Prediction (Motion Estimation) : High quality video sequences usually have high frame rate at 30 or 60 frames per second (fps). Therefore, two successive frames in a video sequence are very likely to be similar. The goal of inter prediction is to utilize this temporal redundancy to reduce data need to be encoded. In Fig. 3, for example, when encoding frame t, we only need to encode the difference between frame t-1 and frame t (i.e., the airplane) instead of the whole frame t. This is called motion estimated inter-frame prediction. Multiple reference frames: In previous video coding standards, there is only one reference frame for motion estimation. In

H.264, the number of reference frames increases to 5, for P frame and to 10 (5 previous frames and 5 next frames) for B frame. More reference frames result in smaller residual data and, therefore, lower bit rate. Nevertheless, it requires more computation and more memory traffic. Quarter-pixel accuracy. In previous video coding standards, motion vector accuracy is half-pixel at most. In H.264, motion vector accuracy is down to quarter-pixel and results in smaller residual data.

(F) VIDEO ACQUISITION :

In this stage, test video acquire from public database. Image acquisition is the creation of a digitally encoded representation of the visual characteristics of an object, such as a physical scene or the interior structure of an object. The term is often assumed to implyor include the processing, compression, storage, printing, and display of such images. A key advantage of a digital image, versus an analog image such as a film photograph, is the ability make copies and copies of copies digitally indefinitely without any loss of image quality. Digital imaging can be classified by the type of electromagnetic radiation or other waves whose variable attenuation, as they pass through or reflect off objects, conveys the information that constitutes the image

(G) DATA HIDING :

- In this stage, we perform the data hiding.
- In that, secret data will be hided into the compressed frame based on edge based least significant bit method.
- Here, hybrid edge detection model is proposed. The hybrid models are such as Canny and LOG edge detection. Based on the canny and log, edge image was obtained from image.
- Then classify the pixels of the compressed frame into two categories which are non-edge pixels and edge pixels, respectively.
- After that, secret data is embedded in non-edge pixel of compressed frame.

LSB substitution technique is proposed for data embedding and extraction. Edge detection includes a variety of mathematical methods that aim at identifying points in a digital image at which the image brightness changes sharply or, more formally, has discontinuities. The points at which image brightness changes sharply are typically organized into a set of curved line segments termed edges. The same problem of finding discontinuities in one-dimensional signals is known as step detection and the problem of finding signal discontinuities over time is known as change detection.

(H) DATA FLOW DIAGRAM :

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modelling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

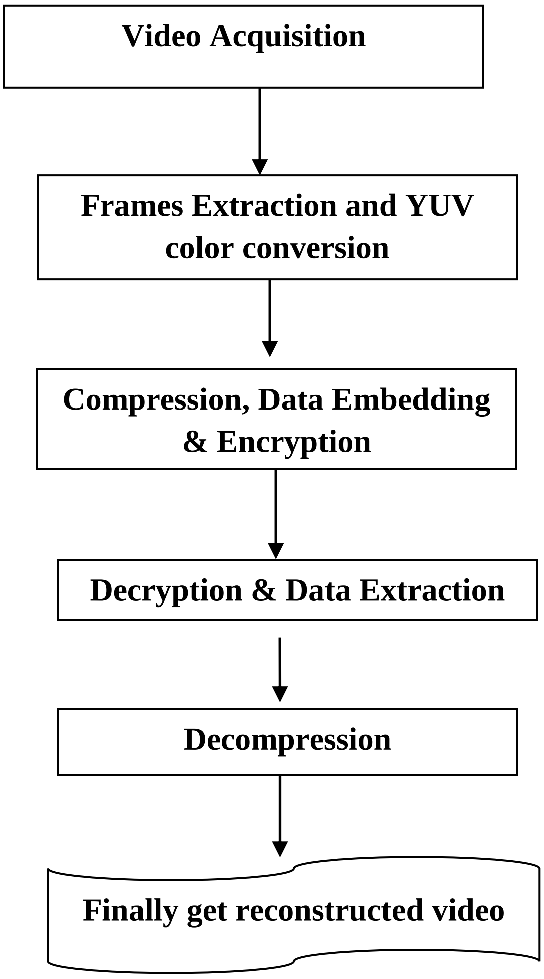
Video Acquisition
Frames Extraction and YUV color conversion
Compression, Data Embedding & Encryption
Decryption & Data Extraction
Decompression
Finally get reconstructed video

Figure 3 : Data flow diagram

(I) CLASS DIAGRAM :

In software engineering, a class diagram in the Unified Modelling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

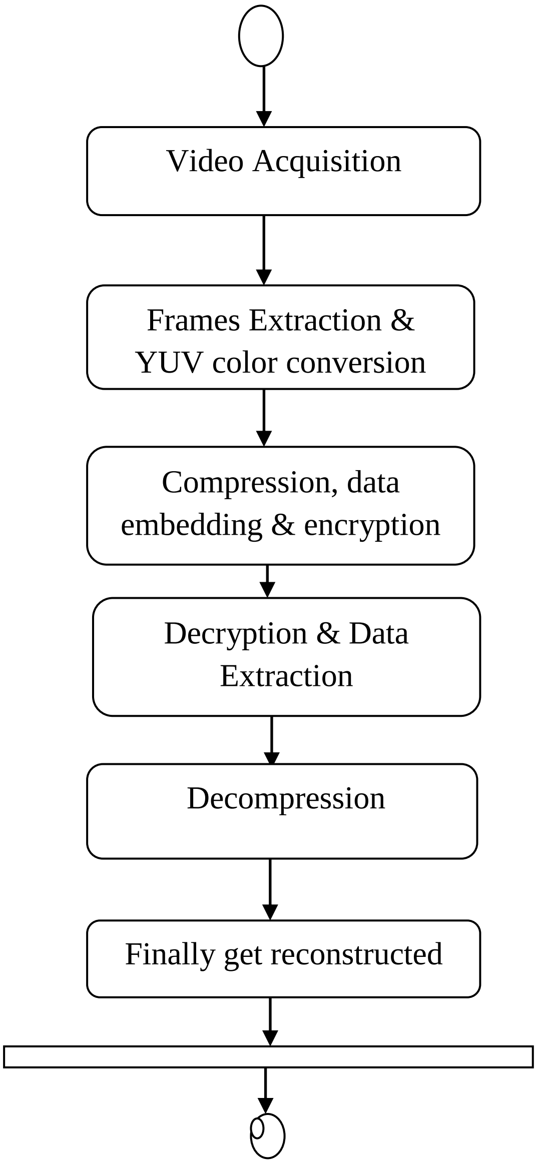
Video Acquisition
Frames Extraction & YUV color conversion
Compression, data embedding & encryption
Decryption & Data Extraction
Decompression
Finally get reconstructed

Figure 4 : Class diagram

(J) QUALITY MEASUREMENT :

PSNR the PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error. The range of PSNR value should be 1db to 100db.In Normal codec currently PSNR value will be nearly 50 db. If it is 100db means both file entered for processing are same, but it not possible

(K) SYSTEM REQUIREMENTS :

HARDWARE REQUIREMENTS :

❖ System	: Pentium Dual Core.
❖ Hard Disk	: 120 GB.
❖ Monito	: 15'' LED
❖ Input Device	: Keyboard, Mouse
❖ Ram	: 1GB.

(L) SOFTWARE REQUIREMENTS :

❖ Operating system	: Windows 10.
❖ Coding Language	: MATLAB
❖ Tool	:MATLAB R2013A

3. CONCLUSIONS

In this paper, an efficient commutative encryption and data hiding scheme based on H.264 codec is presented, which provides reliability control functionalities. Data embedding and video encryption are accomplished during H.264 compression process. The security analysis results demonstrated and proved the proposed scheme can achieve perception security and cryptographic security. Furthermore, experimental results also show that the video distortion caused by data hiding is very low and that the achieved capacity is enough to embed a reliability proof as well as some other data.

FUTURE SCOPE

- In this, the algorithms along with the architectural design and FPGA implementation for H.264 Advanced Encoder for all nine modes of intra predictions have been presented. The present work throws open a number of work that may be undertaken by researchers in future.
- The design of proposed encoder is modular and flexible, the functional modules such as intra prediction, TQIQIT residing in FPGAs presently can be replaced by ASIC resulting in compact, Low power, high speed and cost-effective system suitable for volume production.
- A video decoder can be designed and fabricated by modifying the algorithms and architectures presented for encoder.
- A low power design suitable for portable systems may be implemented for both encoder and decoder by designing multipliers and adder circuits which consume major power in the design presented

- Key management is a critical issue in all encryption based security systems, as it cannot be separated from the design of secure multimedia distribution. In most distribution architectures, multimedia content is encrypted with a symmetric key which also needs to be protected in transmission to the receiver. Hence, the storage and security requirements of key management need to be discussed in greater detail in future proposals.

ACKNOWLEDGEMENT

The authors can acknowledge any person/authorities in this section. This is not mandatory.

REFERENCES

[1] T. Stütz and A. Uhl, ``A survey of H.264 AVC/SVC encryption,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 3, pp. 325_339, Mar. 2012.

[2] Y. Tew and K. Wong, ``An overview of information hiding in H.264/AVC compressed video,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 2, pp. 305_319, Feb. 2014.

[3] Y.-Q. Shi, X. Li, X. Zhang, H.-T.Wu, and B. Ma, ``Reversible data hiding: Advances in the past two decades,'' *IEEE Access*, vol. 4, pp. 3210_3237, May 2016.

[4] Z. Shahid, M. Chaumont, and W. Puech, ``Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 5, pp. 565_576, May 2011.

[5] Y. Wang, M. O'Neill, and F. Kurugollu, ``A tunable encryption scheme and analysis of fast selective encryption for CAVLC and CABAC in H.264/AVC,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 9, pp. 1476_1490, Sep. 2013.

[6] B. Boyadjis, C. Bergeron, B. Pesquet-Popescu, and F. Dufaux, ``Extended selective encryption of H. 264/AVC (CABAC)-and HEVC-encoded video streams,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 4, pp. 892_906, Apr. 2017.