IJITKM Volume 6 • Number 2 • July-December 2013 pp. 170-175

Video Encryption for Secure Video Transmission in IPTV

Jaishree Tanwar[1] Deepak Dembla[2] Ashish Kumar[3]

[1]M.Tech Student [2]Professor & HOD [3]Assoc. Professor
Arya Institute of Engineering and Technology, Jaipur, India
jaishreetanwar86@gmail.com, deepak_dembla@yahoo.com, aishshub@gmail.com

Abstract- Internet Protocol television (IPTV) or IP Television is a method of preparing and distributing television signals over an IP based data network. With the continuous increase of digital communications on internet like video on demand (VOD), multimedia data security is becoming an important issue. But because of lack of security the adversary can have access to data, illegal copying and redistribution of content become simpler and easier. To meet security requirements, many encryption algorithms have been proposed. In this paper, we have proposed dual channel encryption algorithm for content protection in IPTV. This video encryption algorithm replaces traditional encryption schemes thus reducing the time cost of encoding and decoding. The dual channel conversion is done by scanning frames one by one for all the layers(R, G and B) which is guided by binary subscriber/customer id, which is unique for every subscriber thus making the video transmission secure. Proposed dual channel encryption algorithm is implemented on MATLAB 7.8.0 and results shown significant decrease in encryption time as compared to existing algorithms.
Keywords- VOD, IPTV, Content Protection, STB, Video encryption.

I.INTRODUCTION

IP video is placing a high demand on network infrastructures, especially as the number of high-definition subscribers and on-demand services grows. Now days, IP video has to come from an intelligent infrastructure that offers service providers flexibility, reliability and growth. Initially, broadcast or multicast services were used for traffic generation, but now TV viewing behavior is shifting away from linear viewing towards non-linear or time-shifted viewing. Traffic will be increasingly dominated by interactive services, such as Video on Demand (VOD) and Network-based Personal Video Recorders (nPVRs)[1]. Internet Protocol Television (IPTV) is one of the system that deliver television (cable TV type) services to the end user by the use of an IP broadband network. Internet service providers and traditional telecommunications service providers can utilize their IP networks to deliver broadcast TV, Video on Demand (VOD) and other Internet services to the customer [2].

IPTV is also defined as multimedia services such as television/video/audio/text/ graphics /data delivered over IP based networks managed to provide the required level of security, interactivity and reliability. The video channels and programs are delivered to the television sets through a broadband connection, instead of being delivered through conventional terrestrial, cable television and satellite signal formats. The streams of video are encoded as a series of IP packets and then carried out by the public internet means which can be received by customer by having a set-top box and service subscription [3]. The services provided by IPTV is a complete package that allows customers to watch TV, video on demand and browser the internet. In order to receive the IPTV signals a computer or a television set with a set-top box is required.In IPTV related services, such as terrestrial TV, cable TV and VOD, content security is an important issue. The Conditional Access (CA) technique [4], similar to CAS, traditionally used to control the TV program view. It uses Set- top box which decrypts the encrypted program from head-end. Generally, there are 2 main types of technological solutions to Content Protection in IPTV systems. The one is CAS (Conditional Access System), similar to the conventional Conditional Access (CA) system applied in digital television (DTV). Here the encryption engine typically uses a DES algorithm for encryption [5]. The other one is DRM (Digital Rights Management) systems, whose solutions are often intended to be cross-platform to work on PCs, PDAs and mobile phones as well[6]. DRM solutions are using video stream data encryption methods usually AES method[7].

Content or service delivered through IPTV needs to be protected as illegal copy and redistribution of IPTV content become simpler and easier. Now days, copyrighted audiovisual contents are gradually shared and distributed illegally. As in the digital TV, customers can also make a complete copy of broadcasted IPTV content without deteriorating audio or visual qualities at all. The copy of broadcasted content is easily made by using PVRs (personal video recorders) attached to the broadcasting receiving devices. This critical problem of copying the content can be removed by using the proposed dual channel encryption, which is presented in the paper. The paper is

divided as following sections, in section II, we discuss the literature review. The proposed solution, dual channel video encryption algorithm is explained in section III. Section IV presents the experimental set-up and section V discusses experimental results. Finally section VI concludes the paper.

II.RELATED WORK

Jolly Shah et al [8] have presented a survey on various video encryption algorithms and found that various important and rich variety of video encryption algorithms have been proposed. We conclude that discussed video encryption algorithms follow full encryption, selective encryption, zig-zag permutation, motion vector encryption, DCT cofficient encryption and partial encryption techniques.All these existing techniques are based on the encryption of the specific I,B or P type of frames and are not secure against cryptanalysis attack.

The methodology proposed by Mukut Roy et al. uses one bit selection algorithm that will select the higher intense bits in order to achieve higher visual degradation [9]. In this methodology, they used AES encryption algorithm for encryption as it supports more security level, more key length and low memory requirement. Thus it enhances the cryptographic security of the encryption algorithm which will be well suited for real-time data transmission application.

A Fast Random Bit Encryption method is proposed by K. John Singh in [10]. The proposed algorithm employs multi-level encryption along with key encryption thus making it more secure. This algorithm is a lightweight encryption algorithm and takes video data from a compressed domain. But the comparison of heavyweight and lightweight algorithms shows that heavyweight algorithms take more time for encryption because during the execution time their resource utilization very is high and the lightweight algorithms consume fewer resources, so they spend only less time for execution. But they are considered as less secured algorithms.

Lei Chen et al.[11] proposed four encryption methods. The set of these four selective data encryption methods are used for protecting MJPEG video streaming. The encryption methods and scenarios proposed in this paper, are based on the principle of selecting the most important data for encryption. The four scenarios represent a wide range entertainment applications and of daily work where secure MJPEG video streaming can be applied. Using selective data encryption, these methods target to protect video data, specifically MJPEG (Motion JPEG) video streams. This proposed method is derived from the fact that JPEG images are encoded using prioritized pixel information. The proposed algorithm performs well in terms of CPU load and frame rate at playback.

Analyzed encryption methods have several drawbacks. Some perform encryption at the encoding level, which provides good protection level but leads to incompatibilities at decoding end. The encryption is okay but for playing the video at customer side whole video is sent to the video buffer at a time. This way even the copy during communication cannot be done but it can be copied through the video buffer, the video which is in original form. Partial encryption methods are more lightweight and requires less computational steps but they are less secure as compare to heavyweight algorithms. All studied video encryption techniques are based on the encryption of I, B and P frames or MB(macro blocks) and uses heavyweight algorithms like AES, DES and RSA for encryption, which requires additional computational steps.

III.PROPOSED DUAL CHANNEL ENCRYPTION SCHEME

The proposed dual channel encryption algorithm for video data is mentioned below. Here the original video file is divided into dual channel data, but each channel does not have the complete information about the original video. The division of video data is done into two files which have the video frames in a scrambled sequence. The dual channel division is unique for everyvideo and for every subscriber as it uses the subscriber id for the key generation. So to access the video only a genuine subscriber is authenticated.

A. Architecture of Proposed Encryption Scheme

The dual channel technique comprises of several modules. The various modules are VOD server, Encoding server, transmission channel and set top box (STB). Each module has its significant role in the system. The flowchart of the proposed solution are shown in figure.1, explaining the functioning of various modules.

Video demand is played by the customer and he enters his customer ID for verification. This ID is verified by the VOD server which also confirms whether the requested video exists or not. VOD server is the permanent storage where all the videos are kept and are properly indexed for efficient searching. After confirmation of video existence and customer account verification the video file is forwarded to the encoding server which is installed with our proposed dual channel video encoding method.

A combined key consisting of the video id and the customer id is created here which is the secret key for the whole process. This secret key generation process is same for encoding and decoding process. The encoding server encodes the original video file into the dual channel files. The original video is not stored in the encoding buffer but

only the encoded dual channel files are stored here. These encoded files are deleted from the encoding buffer when the whole file is successfully transmitted to the set top box.

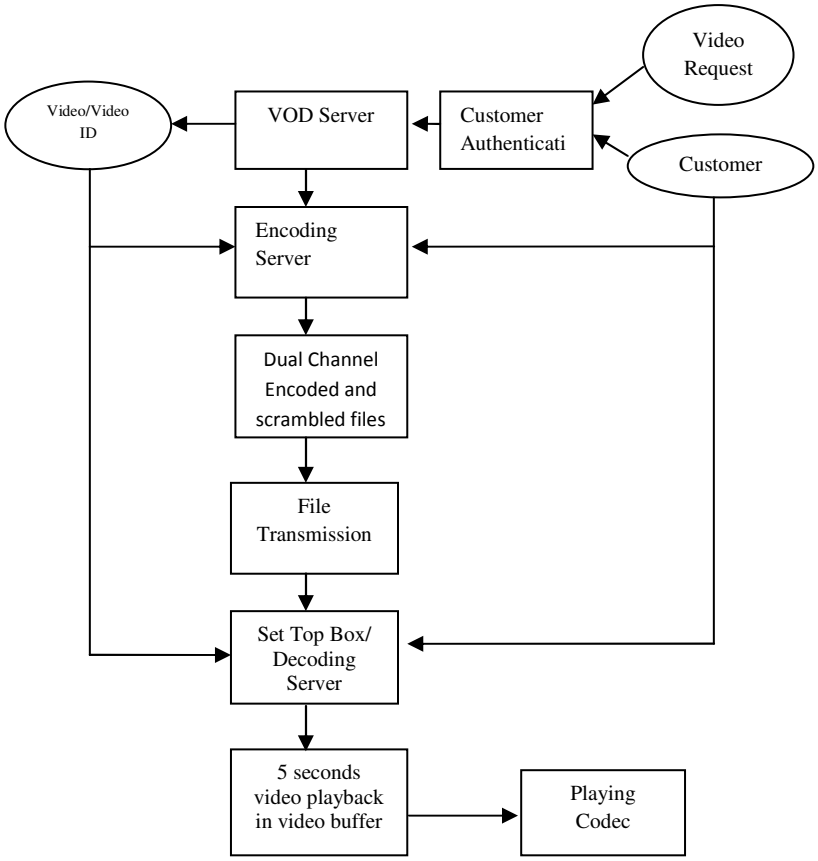

Figure.1: Flowchart of the proposed schema

When a video is received at the decoding set top box, CRC verification is done on the dual channel video stream. If the CRC check is successful it means that the video stream has not been tampered so it is forwarded to the decoding module where the decoding of the dual channel channel files to the video file is done. The video of only five seconds playback in both direction is decoded at a time and sent to the video buffer. As soon as that part of the video is played it is removed from the video buffer. It enhances the security of the video. While the video is in dual channel encoded form there is no use to copy this video since only the authenticated person can play this video and when the video is in video buffer, only five seconds of playback is kept there also it is deleted as soon as it is played. So there is no chance of copying the video from the buffer. The video is secure because of these two strategies implemented by us. Dual channel video encoding together with small duration video buffering makes the strategy robust and secure than any other available strategy.

B. Algorithm for Proposed Dual Channel Encryption

Step 1 Customer System Initialization
Step 2 VoD server Initialization
Step 3 Video list generation
Step 4 GUI for video name input
Step 5 GUI for customer id and secret key input
Step 6 Customer Authentication
Step7 Requested Video Availability Checking
Step 8 Transferring Video to Encoding Server

Video Encoding Process

i. Requesting keys from the key generation server
ii. Dividing the video into frames
iii. Dividing of the frames into RGB layers
iv. Scrambling of the layers in the video frames
v. Scrambling of the frame sequence
vi. Division of scrambled layers into two dual channel data files

Step 9 CRC generation for individual dual channel file

vii. Generator polynomial for CRC is decided using the customer access code
viii. CRC for the two dual channel files is calculated
ix. CRC is appended to the end of dual channel files

Step 10 Encoding time = Time taken from Step 9 and Step 10

Step 11 Dual channel files Transmission to the customer set top box

Step 12 Buffering of video into decoding server buffer

x. Once complete dual channel files have been buffered Encoding server deletes the files from its buffer

Step 13 Set Top Box Processing

xi. Requesting keys from the local key generation server

Step 14 CRC verification

xii. CRC calculation for dual channel data files
xiii. If CRC matches to the appended CRC then content is authentic, so here we are considering security point of view from the customer side also

Step 15 Decoding Process Begins

xiv. Descrambling of the frames to their original locations
xv. Descrambling of the pixels to their original locations inside the frames
xvi. Joining the first 10 seconds of the playback
xvii. Playing the movie
xviii. Controlling the movie playback using the scroll bar
xix. If the movie is scrolled then earlier contents in the video buffer are flushed out and fresh 10 seconds playback for current scroll location is pushed into the video buffer.
xx. At a time only 10 seconds of playback is in the video buffer in the original video format.
xxi. If there is no change in scroll then while the current 10 seconds playback is played, next 10 seconds are decoded and made ready to play, so there is no jitter in continuous playback.
xxii. Delete the dual channel files from the decoding buffer once the whole movie is played once or a maximum time of session is over.

Step 16 After whole video has been played current session is closed, now if the subscriber wants to play again then he has to login again. This prevents the re-access of the video content without payment.

C. Implementation Code for Proposed Dual Channel Encryption

The dual channel encryption is logically done using the following pseudocode. The frames are scanned one by one for all the layers (R, G & B). The dual channel division is guided by binary subscriber id. The frame division takes place if the binary bit is '1'.

```
%Module for encryption
for h=1:ai.NumFrames
for z=1:3 % For RGB layers
if mm>length(subsid)
        mm=1;
end
if subsid(mm)=='1'
        fseq1(ll,:,:)=mov(h).cdata(:,:,z); % Take the first frame of the video and its first layer
                                            pixel by pixel
        ll=ll+1;
else
        fseq2(kk,:,:)=mov(h).cdata(:,:,z); % Take the first frame of the video and its first
                                            layer pixel by pixel
        kk=kk+1;
```

```
end
    mm=mm+1;
end
end
```

As the proposed encryption method does not require encryption of specific I, P or B frames, thus reducing the computational complexity of solution.

IV. EXPERIMENTAL SET-UP

The performance is analyzed against parameters such as encryption time, decryption time and compression ratio of video files of different sizes. MATLAB 7.8.0 version has been used which incorporates proposed encryption algorithm and is able to encrypt and decrypt video files. MATLAB , the language of technical computing, is a high-level language and interactive environment for visualization, numerical computation, and programming. Using MATLAB, we can develop algorithms, analyze data, and create applications and models. The language, built-in math functions and tools enable us to explore multiple approaches and reach to a solution which is faster than with traditional programming languages, such as C/C++ or Java or spreadsheets.

V. RESULTS AND ANALYSIS

The evaluation of proposed encryption method is done via video files of different sizes. The existing algorithms and proposed algorithms are analysed for encryption time.

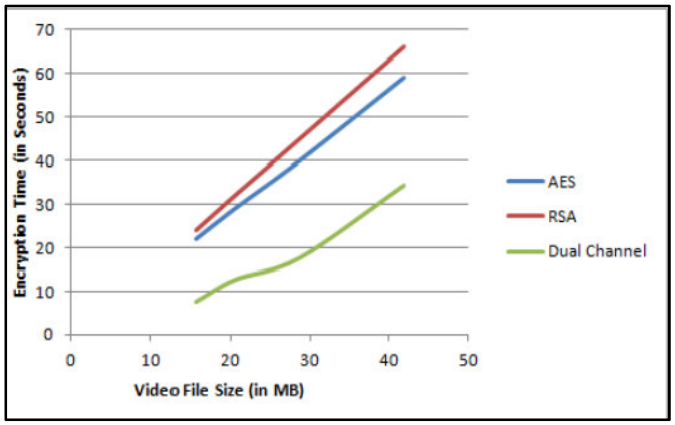

Figure.2:Comparison of Dual channel algorithm and existing algorithms with encryption time

Figure.2 exhibits encryption time vs video file size shows the encryption time taken by various heavyweight algorithms like AES and RSA against the dual channel encryption algorithm. The results of experiment proves that our proposed method takes less encryption time as compared with the heavyweight encryption algorithms, which includes high computational steps thus more time for encryption. This approach is unbreakable without knowing the actual secret key generation algorithm which is known to the encoding and decoding server only. Even the customer id and secret key is leaked still the decoding can be done on a standalone set top box which decodes the video in small chunks. Overall there is no storage whether temporary or permanent where this video is kept completely at a time. Compression ratio for a video simply suggests the reduction in the size of the encode video in comparison to the original video. The method incorporated to calculate the compression ratio is to take ratio of the dual channel based compressed video size and the original uncompressed video.

encryption_ratio=encoded_video_size/umcompressed_video_size

Since we wanted to keep the process very simple to implement in embedded devices we developed an algorithm which require minimum mathematical complexity and can give maximum security. Still the compression ratios of average 70% (as shown in figure.3) has been achieved which is quite effective for a secure approach.

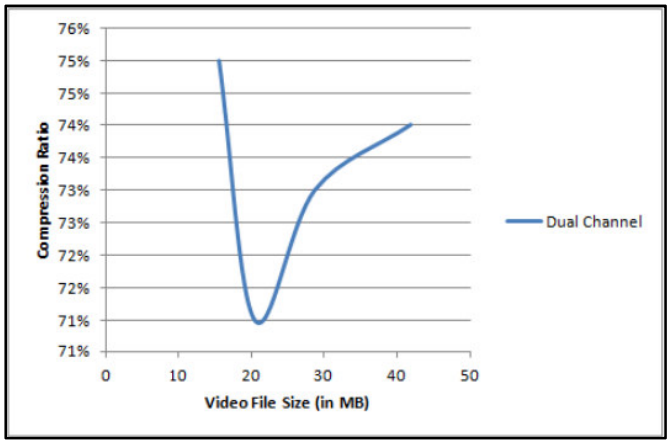

Figure.3: Compression ratio for various videos by the proposed algorithm

The analysis clearly shows that proposed encryption method ensures good video content protection level, substantially reducing encryption time and compareably decryption time also and without any high computational power. The proposed method has advantage of speed and security that is the algorithm is fast and secure, because of dual channel file division on the basis of R, G and B layers of individual frames.

VI. CONCLUSION AND FUTURE WORK

This paper presented an in-depth discussion of the dual channel encryption algorithm, which will deal with the security issues and requirements for protection of content and service for IPTV. The dual channel encryption features the content and service protection for IPTV by integrating various kinds of security mechanisms on the IPTV signal receiving side as well as on the head-end side. This paper will be a reference for establishing comprehensive and practical security dual channel encryption algorithm for content protection system for IPTV. The future work will be to implement this algorithm on various platforms.

REFERENCES

[1]White Paper on "Video Transport and Distribution for IPTV Networks" by Matt Hallam (Senior New Business Development Manager) and Tom Rarick (Senior Principal Engineer).

[2] Seong Oun Hwang, "Content and Service Protection for IPTV," in IEEE Transactions On Broadcasting, Vol. 55, No. 2, June 2009.

[3] Ashish Kumar, Jaishree Tanwar and Chandresh Bakliwal, "A Dual Channel Technique for Content Protection in IPTV" in International Journal of Electronics and Computer Science Engineering ISSN: 2277-1956/V2N1-370-374.

[4] T. Jiang, S. Zheng and Y. Hou, "Secure Communication between Set-top Box and Smart Card in DTV Broadcasting," in IEEE Transactions on Consumer Electronics, Vol. 50, No. 3, AUGUST 2004, pp.882-886.

[5] "Cisco Wireline Video/IPTV Solution Design and Implementation Guide, Release 1.1" , Cisco Systems, Inc,2006.

[6] ZHANG Hua, ZHAO Li, CHEN Chunxiao, YANG Shiqiang, ZHOU Lizhu," Content Protection for IPTV-current state of the art and challenges", in IMACS Multiconference on "Computational Engineering in Systems applications "(CESA), October 4-6, 2006, Beijing, China.

[7] V. Simanaitis, A. Liutkevicius, A. Vrubliauskas, E. Kazanavicius, "Efficient MPEG-2 Transport Stream Encryption Method for Low Processing Power Mobile Devices", in Electronics And Electrical Engineering Issn 1392 – 1215 2012. No. 2(118)

[8] Jolly shah and Dr. Vikas Saxena, "Video Encryption: A Survey", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011

[9] Mukut Roy and Chittaranjan Pradhan, "Secured Selective Encryption Algorithm for MPEG-2 Video", 978-1-4244-8679-3/11/$26.00 ©2011 IEEE.2011.

[10] K. John Singh and R. Manimegalai, "Fast Random Bit Encryption Technique for Video Data", European Journal of Scientific Research ISSN 1450-216X Vol.64 No.3 (2011), pp. 437-445.

[11] Lei Chen, Narasimha Shashidhar and Qingzhong Liu, "Scalable Secure MJPEG Video Streaming", 2012 26th International Conference on Advanced Information Networking and Applications Workshops, 978-0-7695-4652-0/12 $26.00 © 2012 IEEE.