Data Hiding by Code word Substitution (Encrypted H.264/AVC Video Stream)

Yogita A Pawar, Prof. Shrilekha Mankhair

***Abstract*— Digital videos are the very popular because of their frequency on their internet. There are various techniques are present for hiding private data in videos. Digital video needs to be stored in encrypted format. For the purpose of content notation and or tampering these it is necessary to perform data hiding in these encrypted video.**

This dissertation proposes following three parts that is H264 /AVC, video encryption, data embedding, data extraction. The working of the system incorporates three stages, first the analyzing property of H.264/AVC codec the codewords of intraprediction modes, the codewords of motion vector differences, and the codewords of residual coefficients are encrypted with stream ciphers. second data hider may embed additional data in the encrypted domain by using codeword substitution technique, without knowing the original video content This technology will help future innovations and researchers in military application, video in medical field and other applications . In this technology data hiding in encrypted domain without decryption preserves the confidentiality of the content. It is based on the use of new technology to improve efficiency.

***Index Terms*— Data hiding, H.264/AVC, Codeword Substituting, Encrypted domain.**

I. INTRODUCTION

H.264/AVC video streams would avoid leakage of video content which can help address the security and privacy concerns with cloud computing. Similarly when medical videos or surveillance videos have been encrypted for protecting the privacy of the people a database manager may embed the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain.With the increasing demands of providing video data security and privacy protection data hading in encrypted H.264/AVC videos will become popular in the near future.

A. Background

There are various works have been focused on image only few joint data hiding and encryption approaches that focus on video have been proposed.

The widespread of the internet and world wide web has changed the way digital data is handled. Data hiding deals with the ability of embedding data into a digital cover with a minimum amount of perceivable degradation that is the embedded data is invisible or inaudible to a human observer. Data hiding consists of two sets of data namely the cover medium and the embedding data which is called the message. The digital medium or the message can be text,audio,picture, or video depending on the size of the message of the capacity of the cover .Watermarking is known to be a very difficult task robustness distortion payload ,security, complexity are many constraints to deal with. When applied to a video stream the difficulty seems to be growing into image watermarking.

B. Motivation

The H.264 video coding standard has been developed and standardized collaboratively by both the ITU-T VCEG and ISO/IEC MPEG organizations.H.264/AVC represents a number of advances in standard video coding technology, in terms of both coding efficiency enhancement and flexibility for effective use over a broad variety of network types and application domains H.264/AVC is a video compression format i.e. standard for high definition digital video.

C. Objective

The main objective is to enhance compression performance and provides a provision of a network friendly video representation addressing conversational applications. H.264/AVC has achieved a significant improvements in rate distortion efficiency relative to existing standards H.264 /AVC covers all common video conferencing and high definition video storage. To address the need for flexibility and customizability ,the H.264/AVC design covers a video coding layer (VCL) ,which is designed to efficiently represent the video content, and a network subtraction layer(NAL) which formats the VCL representation in a manner appropriate for conveyance by a variety of transport layer or storage media. Relative to prior video coding methods, as exemplified by MPEG-2 video, some highlighted features of the design that enable enhanced coding efficiency include the following enhancement of the ability to predict the values of the content of a pictures to be encoded.

1. Variable block size motion compensation with small block sizes.
2. Quarter sample accurate motion compensation.
3. Motion vectors over picture boundaries.
4. Multiple reference picture motion compensation.
5. Decoupling of reference order from display order.
6. Decoupling of picture representation methods from picture referencing capability.
7. Weighted prediction
8. Improved skipped and direct motion inference .
9. Directional spatial prediction for intra coding .
10. In the loop deblocking filtering.

Manuscript received March 04, 2015.

Yogita A Pawar: Department of Electronics & Telecommunication, GSMCOE Savitribai Phule University, Pune, India
Prof. Shrilekha Mankhair: Department of Electronics & Telecommunication, GSMCOE Savitribai Phule University, Pune, India

II. LITERATURE SURVEY

There are several methods and devices used to data encryption and data embedding in video stream. Several research works are being performed by many institutions throughout the world to offer the best scheme in terms of cost effectiveness. This section gives a brief review on various methods of video encryption and embedding.

A. Literature Survey

Today in the market different encryption algorithm used. The studies of various published international papers have been done. Before more technologically advanced solutions to security are discussed it is useful to outline basic properties of the traditionally used scheme and explain their main properties and limitations.

0.61) Encryption and modified watermarking: This scheme provides the watermarking to provide confidentiality and ownership. This scheme performs the texture information by considering MVD encryption (motion vector direction) and IPM encryption (Intra prediction mode).

Advantages: Preserves the confidentiality of the content.
Disadvantages: The original content is first watermark and then watermarked content is encrypted. Another is the approaches do not operate on the compressed bit.

2) Encryption and reversible watermarking: This scheme proposed which performs reversible watermarking simultaneously during compression process. The reversible watermarking scheme embeds the watermark into the encrypted domain.

Advantages: Provides the access right and authentication of the video contents simultaneously.
Disadvantages: Little bit overhead, the watermarked bit stream is not fully format compliant.

3) SELECTIVE ENCRYPTION ALGORITHM**:** Video encryption often requires that the scheme be time efficient to meet the requirement of real time and format compliance. This algorithm works on partial encryption algorithm. It provides approach for selecting sensitive data to encrypt to make it time efficient, secure and format compliance.

4) Enhanced Selective Encryption: It operates in compressed domain based on context adaptive binary arithmetic coding.
Advantages: Suitable for streaming over heterogeneous network because of number change in bit rates.

Disadvantages: Performed on the entropy coding stage of H.264/AVC using AES encryption algorithm in CEB mode. Hence it does not affect the bitstream and H.264/AVC bit stream compliance.

5) Encryption scheme and codeword substitution technique: The previous methods performs encryption and data embedding almost simultaneously during H.264/AVC compression process and not on compressed domain. Hence the compression and decompression cycle is the time consuming and hampers real time implementation.

Advantages: Data hiding performed entirely in the encrypted domain and thus preserves confidentiality of the content. The schemes operates operate directly on the compressed bit stream. The scheme can ensure both the format compliance and strict file size preservation. In order to adapt to different application scenario, data extraction is possible either from encrypted domain or from decrypted domain.

III. BLOCK DIAGRAM

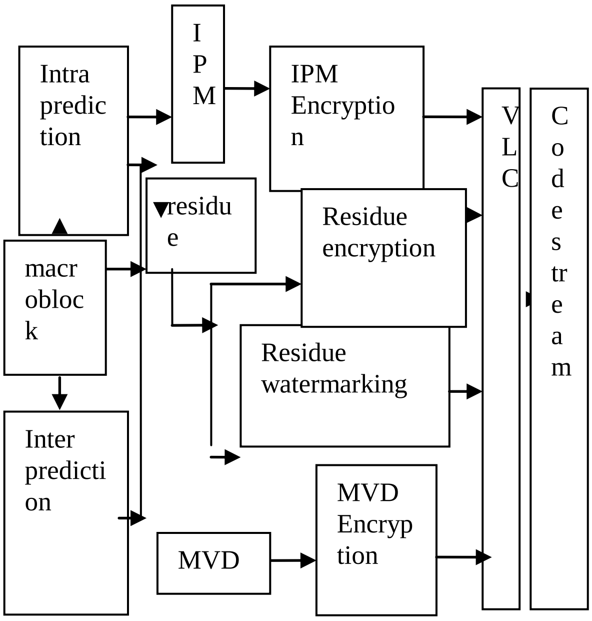


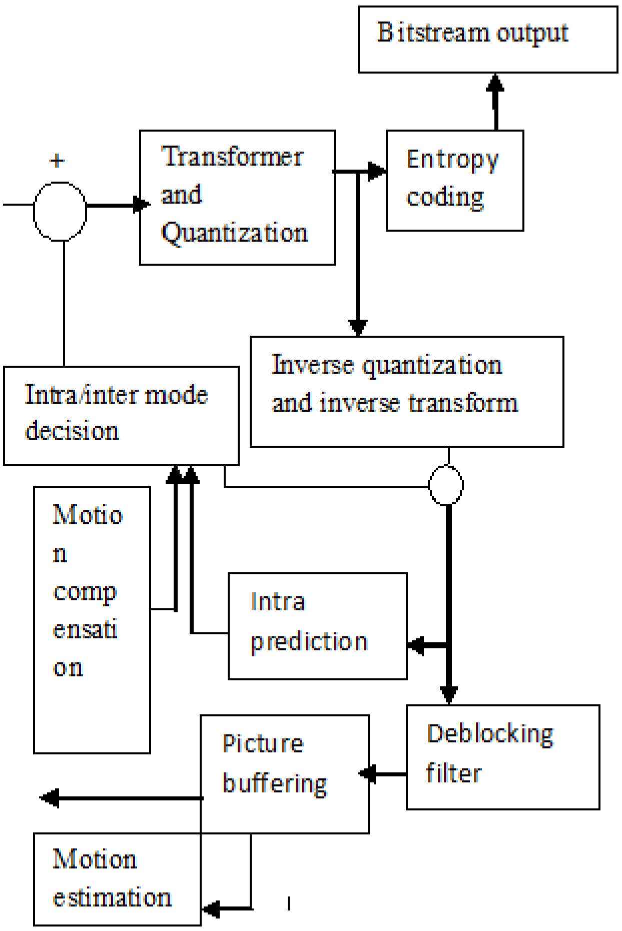
Fig.1 Watermarking and encryption scheme based on H.264/AVC

In this paper the main objective is H.264/AVC video encryption, data embedding and data extraction. The content owner encrypts the original H.264/AVC video stream using standard stream ciphers with encryption keys to produce an encrypted video stream. Then the data hider can embed the additional data into the encrypted video stream by using code word substituting method without knowing the original video content.

At the receiver end the hidden data extraction can be accomplished either in encrypted or in decrypted version. In the encrypted bit stream of H.264/AVC the proposed data embedding is accomplished by substituting eligible codeword of levels. Since the sign of levels are encrypted, data hiding should not affect the sign of levels. Besides the codewords substitution should satisfy the following three same limitations. First the bit stream after codeword substituting must remain syntax compliance. So that it can be decoded by standard decoder. Second to keep the bitrate unchanged the substituted codeword should have the size as the original codeword. Third is data hiding does cause visual degradation but the impact should be kept to minimum.

IV. SYSTEM ANALYSIS

1. H.264 ENCODER



The design of H.264 follows classic hybrid video coding approach. The frames are processed in 16* 16 macroblocks. Each macroblock can be predicted using previously processed macroblock of the same frame or other frames (inter prediction).The macroblocks can be further subdivided (sub macroblock partitions),the smallest block size is 4*4.A coded video sequence always starts with the coded data of an intra predicted from (I frame).The distortions of I frames spread on all subsequently decoded frames due to inter prediction. Following an I frame interpredicted frames that may use one reference frame (P frame) or two reference frames (B frame) follow.Inter prediction is conducted by motion estimation and motion compensation, which are conducted with quarter pixel accuracy. The motion vectors (MVS) of a block are predicted by neighbouring blocks and the motion vector difference (MVD) is actually, coded in the bitstream. There are two distinct coding modes in H.264, namely CAVLC & CABAC.

2. SYSTEM PENTIUM IV 2.4 GHZ

Pentium IV is a line of single core,desktop,laptop and entry level server central processing units introduced by intel on Nov.20.2000 and shipped through Aug 8.2008. They had a seventh generation x86 micro architecture of the Pentium pro.in 1995.netburst different from P6 by featuring a very deep instruction pipeline to achieve very high clock speeds. Intel claimed that Netburst would allow clock speeds of up to 10 GHz.however,problems with heat dissipation limited CPU clock speed to a much lower 3.8 GHz.

3. HARDDISK 40 GB

It is designed to expedite exchanging huge amounts of data between this device and any desktop or notebook computers.

4. RAM 256 MB

The 256 MB SDRAM is a high CMOS dynamic random access memory containing 268,435,456 bits. It is internally configured as a quad bank DRAM with a synchronous interface (all signals are registered on the positive edge of the clock signal,clk).Each of the x4's 67,108,864 bit banks is organized as 8192 rows by 2048 columns by 8 bits. Each of the x16's 67,108,869 bit banks is organized as 8192 rows by 512 columns by 16 bits.

5. EDITORS AND DESIGNERS

Visual studio has different editors and design tools first is graphical user interface designer and second is code editor.

6. PROPERTIER WINDOW

Each control we have user interface has lots of properties we can set. This is done in properties windows.

7. BUILD AND DEBUG TOOLS

In visual studio various build and debugging tools are present. Below we see the build menu. The most used tool is build solution (F6).

8. DEBUG MENU

Debug menu is most used tool start debugging.

9. CODING LANGUAGE C#.NET

C# is pronounced "see sharp" C # is an object oriented programming language and part of the .NET family from Microsoft C # is very similar to C++ and Java .C # is developed by Microsoft and works on windows platform.

10. NET.FRAMEWORK

The .NET framework (pronounced "dot net") is a software that runs primarily on Microsoft windows. It includes a large library and supports several programming languages which allow language interoperability (each languages which allow language).

11. IDE –MICROSOFT VISUAL STUDIO .NET 2010

There exist different versions of visual studio such as visual studio premium and visual studio ultimate. The visual studio product family shares a single integrated development environment (IDE) that is composed of several elements the menu bar, standard toolbar, various tool windows docked or auto hidden on the editor space. The tool windows menus, and toolbars available depend on the type of project of file you are working in. The most common application are as follows.

Application-
1. Windows from application
2. Console application
3. WPF application
4. ASP.NET web application
5. Silverlight application

12. TOOLBOX

Announcement system is nothing but a speaker system which is connected at the output of the system for announcement purpose. As per the system application, according to the visual based guide the respective saved audio file is played using a speaker system. The toolbox contains all the necessary controls. The NET library is available to all the programming languages that .NET supports. Programs written for the .NET framework execute in a software environment known as the common language runtime (CLR), an application virtual machine that provides important services such security, memory management and exception handling. The class library and the CLR together constitute the .NET framework.

V. CONCLUSION

An attempt has been made to make a high robust and more secured device which is exclusively designed for security and privacy. Privacy preserving for encrypted media is new topic for growing research field. In the codeword substitution based hiding an algorithm is used to embed additional data in encrypted H.264/AVC bit stream which consists of video encryption, data embedding and data extraction phases. The advantages of the system are fully compliance with the H.264/AVC syntax.

This technique facilities better way for data hiding directly in the encrypted domain without decryption of the context thus preserves confidentiality of the content.

REFERENCES

[1].Dawn Xu Rangding Wang andYun Q. shi Fellow “data hiding in encryption H.264/AVC video streams by codeword substitution” IEEE Trans.Inf.Forensics security vol 9.no.4 Apr 2014.

[2]. Shrutika S. Giradkar Antara Bhattacharya.”A Survey paper on various encryption and data hiding methods for video streams”.The international journal of science and research (IJSR), Vol 3 Issue 1,November 2014.

[3]. K.S.Aiswarya ramji D.R.Dr. Srrrja mole S.S. “A Survey paper on data hiding technique based on codeword substitution algorithm” International Journal of Engineering Research, Vol 3 issue 1 2015.

[4Ming Li,Michel K. Kullhandjian Dimitris A pados, stella N. Batalama , Senior Member , Michael , “Extracting Spread Spectrum Hidden data from digital media ,” IEEE Tran on Information Foensis and Security Vol 8 No.& 2013.

[5]. K.D. Ma W. M. Zhang , X.F. Zhao, N. Yu and F.Li , “Reversible data hiding in Encrypted images by reserving room before encryption .” IEEE pp 553- 562- 2013.

[6]. S.W. Park and S.U.Shin combined scheme of encryption and watermarking in H.264/Scalable video coding (SVC) “New directions Intell Interact . Multimedia Vol 142 , No.1 , pp. 351- 361- 2008.