CHAPTER 1
INTRODUCTION

1.1. Overview

Multimedia consists of many things in one. The simplest definition of multimedia is “the combination of two or more media.” The media in multimedia comes in various forms: graphics, photography, text, audio (sound effect, music, voice-over and so on), video and animation. Each one serves as a powerful communication vehicle for both expressive and practical purposes. When melded together media will allow for a more dynamic and engaging experience. Whereas resultant is improved on even further when there is cooperation and coordination between the disparate media components.

Marshall McLuhan was a leading and influential media communication theorist who coined the familiar phrase “The medium is the message”. He believed that it’s “medium that shapes and controls the scale and form of human association and action.” According to McLuhan the focus should not be on the content or what is being said, but the medium by which it is delivered. The subject matter is by no means irrelevant, but the delivery format is a crucial factor in how the message comes across. This is where the immense power and influence of multimedia lie.

Media, by definition, is the plural of medium. It has evolved to mean “facilitating or linking communication”—be it via a phone, the Web, TV, or some other instrument. Speaking directly with a person one on one is immediate and does not require mediation. This is communication in its purest form.

The purpose of a medium is to assist in the conveying of a message. When using more than one type of medium, we refer to it as multimedia, whether or not it is computer-based. At one time, media mainly applied to newspapers as a way to disseminate news and information to the masses. Now, media encompasses many forms of communication.

Multimedia is a synergistic process whereby various media elements work together to make a stronger, more cohesive whole. A combination of media adds richness and provides a complete sensory experience.

Multimedia once meant a slide projector and a tape recorder being played simultaneously. For instance, 50 years ago, photographic images in slide form were projected on a screen or wall while audio attempted to synchronize with the sequence or played as “background” music.

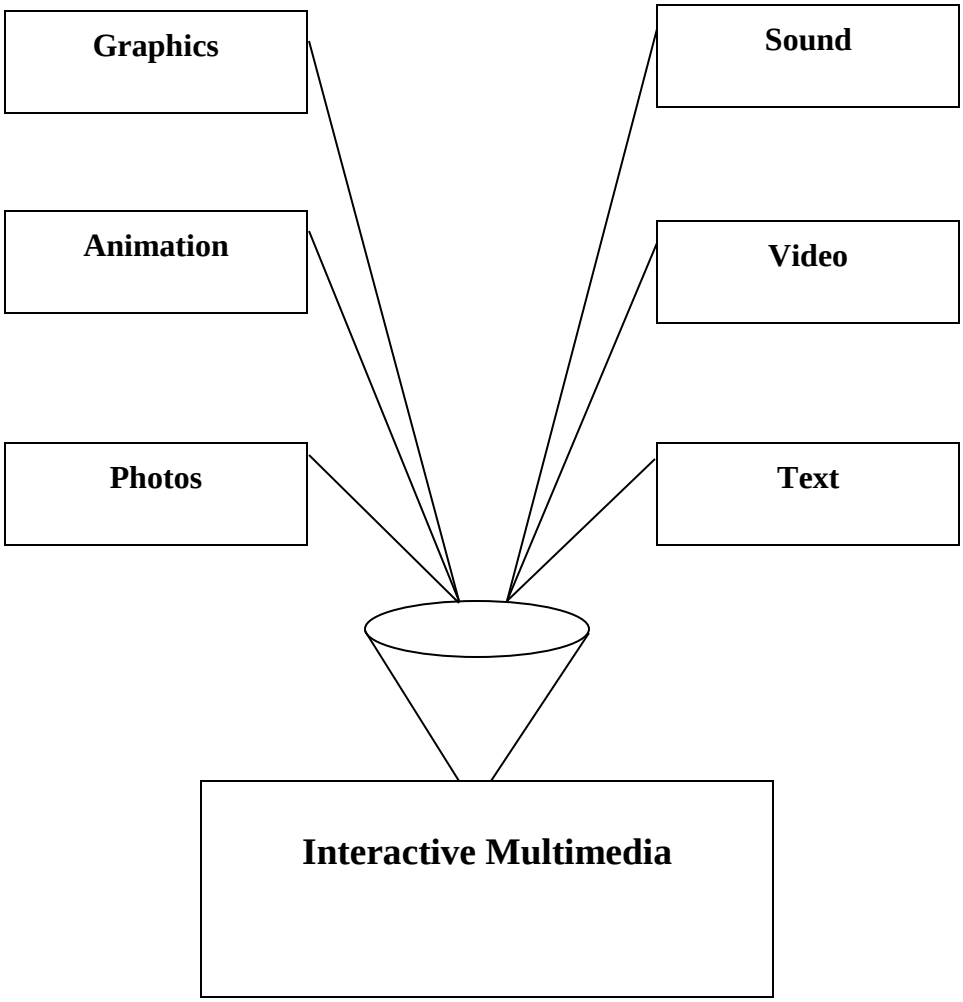


Fig 1.1. Disparate multimedia elements funneling into one unit

In 1967, pop artist Andy Warhol organized “multimedia” events called the Exploding Plastic Inevitable, where he showed films combined with live performances that were illuminated with flashing, colored lights to create a multisensory atmosphere. The technology necessary for joining individual media did not exist at that time. Computers were not accessible to the general public and those that did exist were large, complex, costly, and primarily geared toward scientists and researchers.

Today, the term multimedia is associated almost exclusively with the computer, and the components that make up a multimedia program are digital. Various media are brought together to perform in unison on the computer as a single entity, and they are programmed or scripted using authoring software or programming languages. Diverse forms of communication are combined with multimedia to allow for a myriad of outcomes.

In the early 1900s, Vannevar Bush, an American computer scientist who developed patented devices, came up with inventive ideas about ways to link information. He saw the potential of storing information with built-in connections to other data. Bush called his notion associative indexing, which would link information in a way that is more meaningful to the user, rather than the more traditional numerical and alphabetical classifications. He developed the Memex System in 1945, and although it was never implemented, it would have allowed the operator to input notes and drawings using an early method of photocopying. Data was interconnected and could be stored for later recall. His theory led to the development of interlinked hypertext methods, similar to those that are used today.

Douglas Engelbart was another computing pioneer who was way ahead of his time. He is credited with inventing office automation devices such as the mouse, multiple window screens, electronic mail, and videoconferencing during the 1960s. Engelbart was trying to find ways to create a synergy between the user and the computer with an emphasis on human–computer interaction. He worked on collaborative hypermedia systems, which paved the way for current interactive multimedia approaches.

We can notice multimedia everywhere or one can say “Multimedia here and multimedia there”.

In the same period, an online website with Flash animation may also increase the acceptance, if the use of a smart way. Considering that flash animation is an important key for the achievement of the Flash website. Do not overload flash animation, or make your website navigation too complicated. In order to get a visitor's attention and stay awake and not let them loose patience and leave your overloaded Flash website! In many ways, multimedia will help you improve your acceptance of information, but it will go far beyond that. People can also develop multimedia applications, such as interactive multimedia tutorials to save time coach or to your customers. Provide this kind of multimedia support, your customers could seriously improve their training process and save them time.

Over years, multimedia and interactive promoting services got more cost-effective.

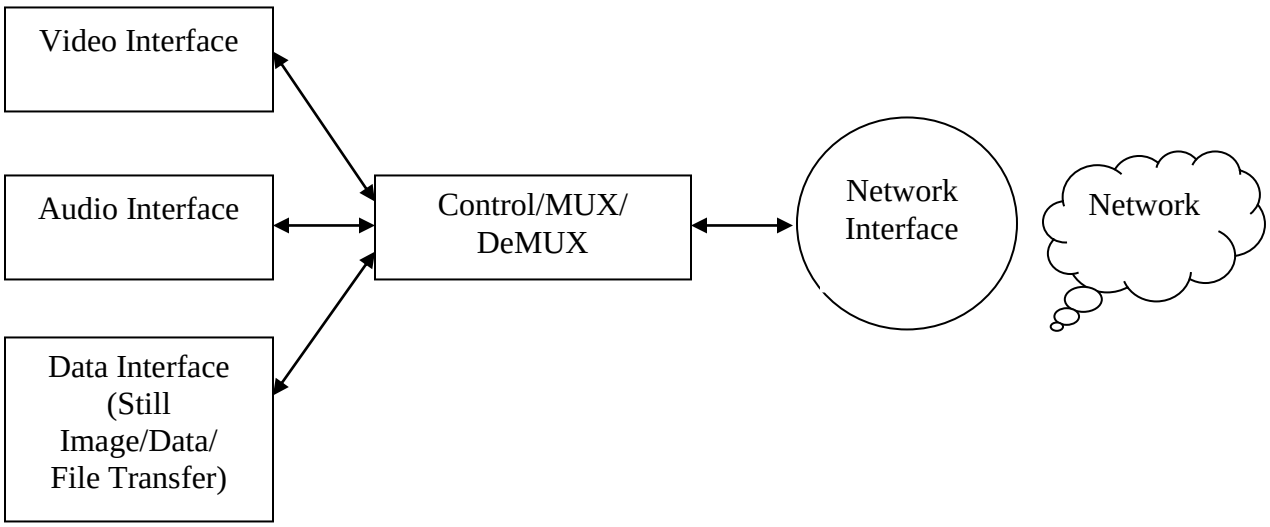


Fig 1.2. Multimedia Communication System

Multimedia is the use of information content and information processing of multiple forms of media (such as text, sound, graphics, animation, video, interactivity) to inform or entertain the user. Multimedia also refers to the use of electronic media to store and experience multimedia content. Multimedia is similar to traditional mixed media art, but a wider range. The term "rich media" is synonymous with interactive multimedia.

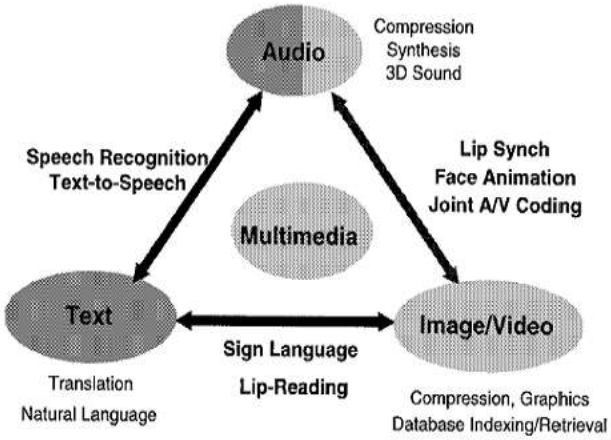


Fig 1.3. Interaction of Media in Communication

Multimedia can be broadly divided into linear and nonlinear category. Progress linear activities without any navigation control audience, such as film screenings. Nonlinear content providers for the use of user interaction with a computer game or self-paced computer-based training to control the progress. Nonlinear content is also known as hypermedia content.

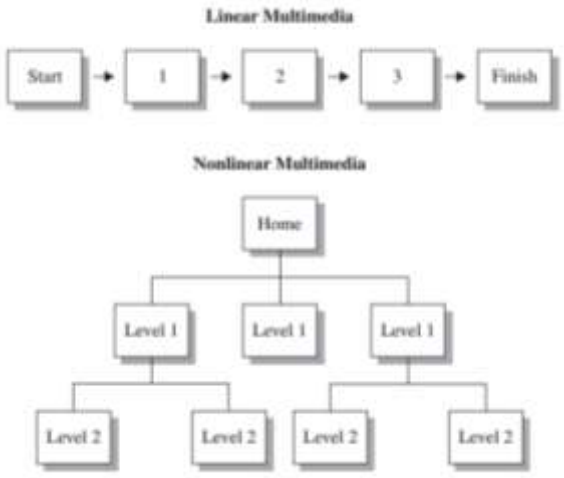


Fig 1.4. Linear vs. Non-linear Multimedia

Multimedia presentations can be live or recorded. A recorded presentation may allow interactivity via a navigation system. A live multimedia presentation may allow interactivity via interaction with the presenter or performer.

Multimedia applications include many types of media. The primary characteristic of a multimedia system is the use of more than one kind of media to deliver content and functionality. Web and desktop computing programs can both involve multimedia components. As well as different media items, a multimedia application will normally involve programming code and enhanced user interaction. Multimedia items generally fall into one of five main categories and use varied techniques for digital formatting.

Text: It may be an easy content type to forget when considering multimedia systems, but text content is by far the most common media type in computing applications. Most multimedia systems use a combination of text and other media to deliver functionality. Text in multimedia systems can express specific information, or it can act as reinforcement for information contained in other media items. This is a common practice in applications with accessibility requirements. For example, when Web pages include image elements, they can also include a short amount of text for the user's browser to include as an alternative, in case the digital image item is not available.

Images: Digital image files appear in many multimedia applications. Digital photographs can display application content or can alternatively form part of a user interface. Interactive elements, such as buttons, often use custom images created by the designers and developers involved in an application. Digital image files use a variety of formats and file extensions. Among the most common are JPEGs and PNGs. Both of these often appear on websites, as the formats allow developers to minimize on file size while maximizing on picture quality. Graphic design software programs such as Photoshop and Paint.NET allow developers to create complex visual effects with digital images.

Audio: Audio files and streams play a major role in some multimedia systems. Audio files appear as part of application content and also to aid interaction. When they appear

within Web applications and sites, audio files sometimes need to be deployed using plug-in media players. Audio formats include MP3, WMA, Wave, MIDI and RealAudio. When developers include audio within a website, they will generally use a compressed format to minimize on download times. Web services can also stream audio, so that users can begin playback before the entire file is downloaded.

Video: Digital video appears in many multimedia applications, particularly on the Web. As with audio, websites can stream digital video to increase the speed and availability of playback. Common digital video formats include Flash, MPEG, AVI, WMV and QuickTime. Most digital video requires use of browser plug-ins to play within Web pages, but in many cases the user's browser will already have the required resources installed.

Animation: Animated components are common within both Web and desktop multimedia applications. Animations can also include interactive effects, allowing users to engage with the animation action using their mouse and keyboard. The most common tool for creating animations on the Web is Adobe Flash, which also facilitates desktop applications. Using Flash, developers can author FLV files, exporting them as SWF movies for deployment to users. Flash also uses Action Script code to achieve animated and interactive effects.

H.264/MPEG-4 AVC is the latest international video coding standard. It was jointly developed by the Video Coding Experts Group (VCEG) of the ITU-T and the Moving Picture Experts Group (MPEG) of ISO/IEC. It uses state-of-the-art coding tools and provides enhanced coding efficiency for a wide range of applications including video telephony, video conferencing, TV, storage (DVD and/or hard disk based, especially high-definition DVD), streaming video, digital video authoring, digital cinema, and many others.

ITU H.263, H.263L, H.26L, H.263E, ISO / IEC 14496. The video codec support MPEG4 simple base class. Top H.263 MPEG-4 increases the advanced error detection and correction services.

3GPP and ISMA is a version of H.263 and MPEG-4 streaming and mobile applications. These are the real change of the transport stream.

Also known as JVT of the ITU H.264 ITU-T recommendations. H.264 MPEG-4 Part 10 ISO14496-10 AVC Advanced Video Coding AVC. H.264 has been widely regarded as the video compression applications, such as the new high-definition television service, portable game consoles, mobile broadcast video services, as well as solid-state video camera on the phone the next platform instant video communications. H.264 is currently the most advanced video coding standard provides today. It is used in MPEG2, MPEG4, and H.263 do not have many new coding techniques.

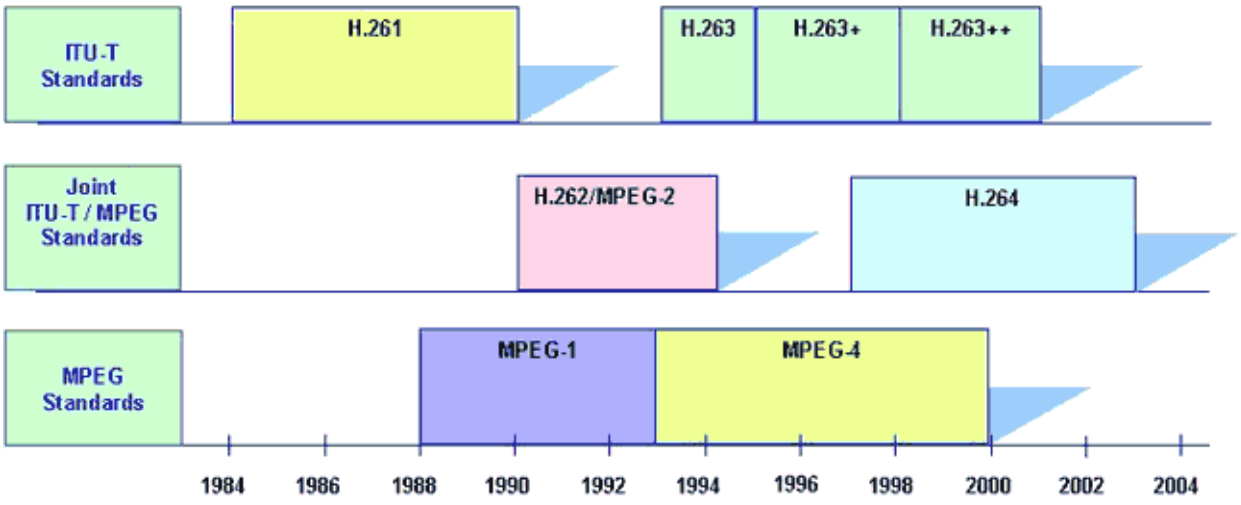


Fig 1.5. Chart shows the evolution of video coding standards.

This revolutionary new technology is expected to drive the entire application, and play a significant cost savings in a wide range of video applications.

Examples include:

• transmission of high-definition television programs, twice as efficient than using MPEG2

• In an ordinary red laser DVD store two hours of HD movies

• promote the emergence of high-definition content PVR for consumer use

• By the time the recorded content transcoding to double H264 personal video recorder to store programs

• Affordable high image quality solid / hard drive based camcorder

Mobile devices • CIF quality video programs

		Standards		
		MPEG-2	MPEG-4 ASP	MPEG-4 H.264
Features	I, P, B-frames	✓	✓	✓
	Interlace	✓	✓	✓
	Coding	Huffman	Huffman	Huffman or Arithmetic
	Block size	fixed 16x16	fixed 16x16	variable down to 4x4
	¼ pixel		✓	✓
	GMC		✓	
	Loop Filter (aka deblocking filter)			✓
	Slice-based motion prediction			✓
	Multiple reference frames			✓
	MB AFF (improved interlaced management)			✓
	RDO (Rate Distortion Optimisation)			✓
	WP (Weighted Prediction)			✓
	Switching pictures (for fast change channel)			✓

Fig 1.6. Difference between various standards

With the rapid growth of the Internet and multimedia applications in the distributed environments, it has become easier for digital data owners to transfer multimedia documents all over the world via the Internet. As a result, multimedia security has become one of the most important aspects of communications with the increasing volume of digital data transmission. Security has been a great issue for research, intelligence bureau and copyrights. Data hiding for purpose of security can be done in three ways. Secret data can be hidden into an unimportant medium so no

illegitimate person will expect its existence into this medium this is called steganography. Another way is to deform the secret data into an unusable or non-interpretable form is called cryptography. At last if some secret data having the owner identification is hidden in the medium to claim the originality of the medium, this process is called watermarking. The recent emergence of embedded multimedia applications such as mobile-TV, video messaging, and telemedicine have increased the impact of multimedia and its security on our personal lives. For example, a significant increase in the application of distributed video surveillance technology to monitor traffic and public places has raised concerns regarding the privacy and security of the targeted subjects.

Multimedia content encryption has attracted more and more researchers and engineers owing to the challenging nature of the problem and its interdisciplinary nature in light of challenges faced with the requirements of multimedia communications, multimedia retrieval, multimedia compression and hardware resource usage. Now the basic details of all these techniques are discussed below.

1.1.1. Video Container and Video CODEC

Video format consists of different technology concept: one is containers and another is codec. Containers are sometimes called as wrappers. Container basically describes the structure of file: where the various pieces are stored, how they are interleaved and which codec are used by which pieces. It may specify an audio codec as well as video. It is used to package the video & its components and is identified by a file extension such as .AVI, .MP4 etc. A codec is a way of encoding audio or video into a stream of bytes such as MPEG1, H.264 etc. It is the method used to encode the video and is the chief determiner of quality. A multimedia video file comes in various formats, each of them possess a level of popularity based on several specifications. Based on availability and usage, the most popular types of multimedia video formats are Joint Photographic Expert Group (JPEG), Audio Video Interleave (AVI) and Moving Pictures Expert Group (MPEG). Mobile devices and online streaming services often use Flash video (FLV), Windows Media Video (WMV), and the 3rd Generation Partnership Project (3GP). Other common

multimedia video formats include QuickTime Movie (MOV), Matroska (MKV), and RealMedia® (RM). DivX® and Ogg are also popular among users.

1.1.2. Real Time and Non-real Time Streaming

Multimedia Streaming is defined as delivering a multimedia file from server to the client via network connection.

It is of two types: One is Real Time Streaming; in which live streaming is done i.e. a live event while occurring is delivered to the client whereas other is Non-Real Time Streaming; in this on demand streaming is done i.e. an archived lecture or movie is delivered to the client.

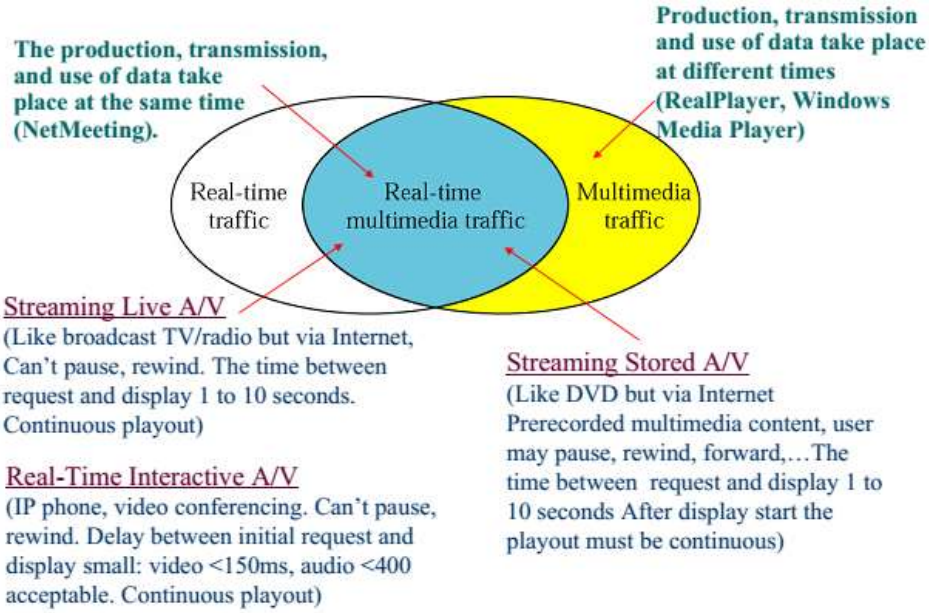


Fig 1.10. Multimedia Traffic

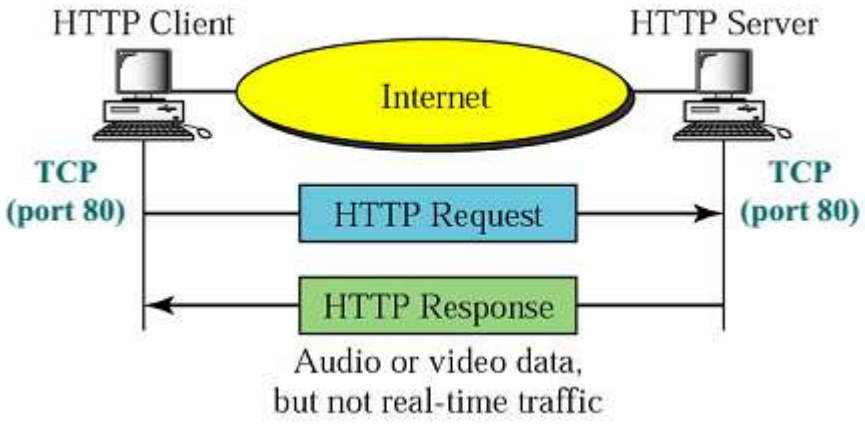


Fig 1.11. Non-Real Time Multimedia

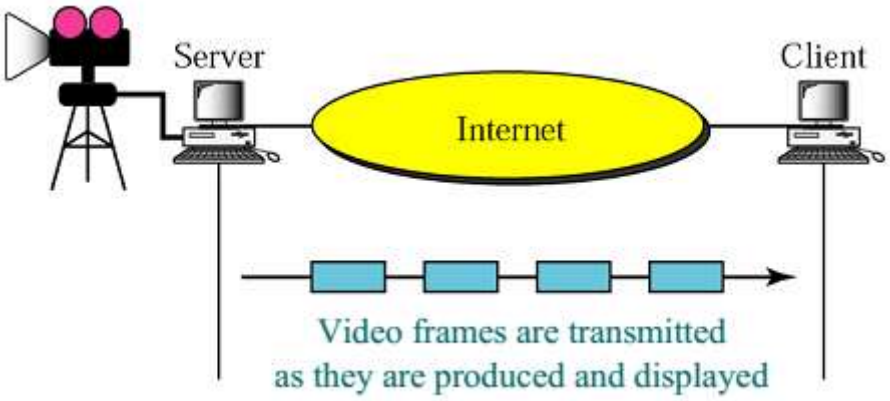


Fig 1.12. Real Time Multimedia

1.1.3. Video Encoding and Decoding:

In Multimedia, video signals differ from image signals in several ways. The most important difference is that video signals have a camera frame rate of anywhere from 15 to 60 frames/s, which provides the illusion of smooth motion in the displayed signal.

1.1.4. Video Encryption and Decryption Techniques

In today's scenario the communication of multimedia have grown dramatically in recent years. Today, we are even witnessing an increasing demand for remote video communication. The development of encryption systems aims to provide a secure and reliable way for information exchanges. However, the security aspects of video exchanges have yet to be fully addressed. Existing video coding standards do not incorporate requirements to have encryption capabilities.

In many cases, the compressed video data is treated like any other types of data and encryption is carried out only after the video encoding process is fully completed, while decryption takes place at the receives side before the start of the video decoding process (Bergeron and Catherine, 2005). Naïve algorithem is a method to

encrypt every byte in the (MPEG) Moving Picture Experts Group files (Agi and Gong, 1996).

This method adds more latency and involves more computations. However, encryption of the whole compressed bit stream is very expensive in terms of both delay and processing time. Researchers have proposed selective encryption where partial encryption is done on selected bits of the video bit stream. This algorithm allows insertion of the encryption mechanism inside the video encoder (e.g. MEPG-2, MPEG-4, and H.264/AVC). The selected bits for encryption are chosen based on the considered video standard and according to each of their encrypted configuration to give a non-desynchronized and fully standard-compliant bit stream (Bergeron and Catherine, 2005). Moreover, video bit streams are typically huge even after compression, and current data encryption and decryption algorithms are relatively slow. Thus, using these encryption techniques to encrypt the whole video bit stream, increases the overall processing time drastically, going beyond 1/30 of a second per frame, leading to higher computational overhead.

Currently, researchers are focusing a lot of attention on secure digital media over the network. The field of multimedia security is growing extremely fast. In order to deal with the problem of processing overhead and to meet the security requirements of real - time video applications with high quality video compression, A variety of encryption algorithms to ensure that the video stream has been proposed (Salah , 2003 ; Habib and Pong , 2006 ; Halawa and Elkamchouchi, 2008), as follows:

• Pure replacement algorithm. It is simply the number of the scrambled MPEG stream of bytes in a frame by arranging the . It is very useful in the case of hardware decoding videos , but software should done all the decryption.

• randomly arranged in a zigzag arrangement used instead of 8 × random arrangement corresponding list (secret key) used in the Z -shape 8 to each of the vector sequence 1x64 8 × 8 block is mapped to 1x64 vector.

• Video Encryption Algorithm : Bhargava , Shi , Wang launched four different video encryption algorithm in 1996 and 1998 : Algorithms I, II algorithm (VEA); algorithm III (MVEA); and algorithms four (RVEA).

Joint Video Team (JVT) to finalize the H.264/AVC coding standard formally approved the new draft submitted and March 2003 (Richardson , 2007) approved the ITU-T 's . Researchers began to work to make safe H.264/AVC bitstream. Most of the m trying to encrypt the encryption process with respect to speed and display process optimization . Polygala , and so on. (2006) proposed an encryption scheme is based on the analysis of H.264/AVC entropy coding system and adaptive digital rights management (DRM). Nithin, and so on. (2007) proposed a new H.264 sign bit selective encryption algorithm , encryptes transform coefficients and motion vectors , and to decrypt the secure transcoding. Yajun , et al. (2007) designed a new selective encryption scheme based on H.264 .

1.2.H.264 Advanced Video Compression Standard

The H.264/MPEG-4 Advanced Video Coding Standard (H.264/AVC) is the latest video coding standard jointly developed by ITU-T Video Coding Experts Group (VCEG) and ISO / IEC Moving Picture Experts Group (MPEG). H.264/AVC compression has achieved a significant improvement in performance compared to the previous standard, and provides a solution to these dialog (video telephony) and the non-session (storage, broadcast, or streaming) applications, video network friendly representation.

H.264 Advanced Video Coding defines a format for compressed video data and it provides a set of tools that can be used in a variety of ways to compress and communicate visual information. Also, it is a stage in an evolving series of standardized methods for video compression. It is an industry standard for video coding, but it is also a popular format for coded video, a set of tools for video compression and a stage in a continuously evolving digital video communication landscape.

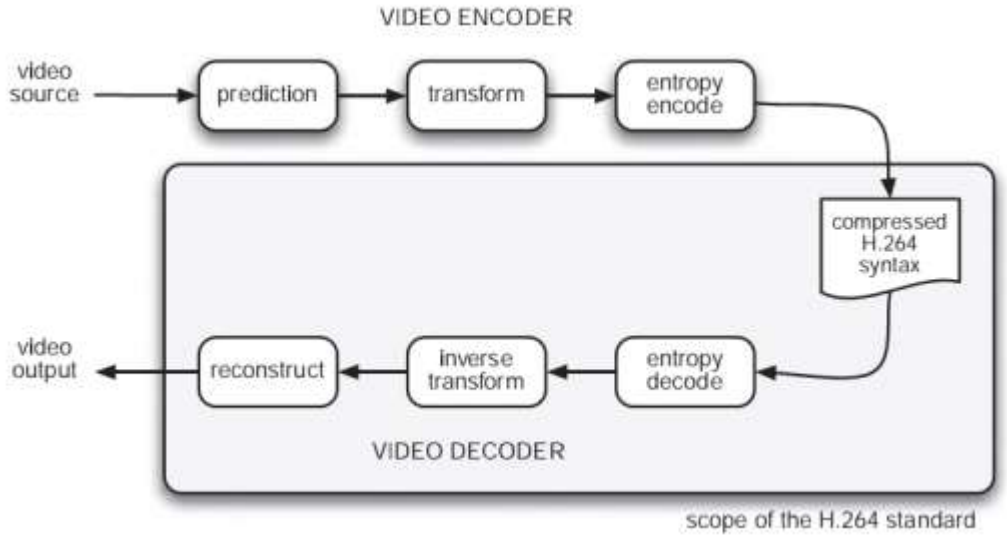


Fig 1.13. H.264 video coding and decoding process

1.2.1. Concept of Video Coding

Act or compressed into compressed data of a smaller number of bits in the process . Video compression (coding) is adapted to convert a digital video transmission or storage format, and generally reduces the number of bits processed . Compression includes a pair of complementary systems, compressor (encoder) and a decompressor (decoder) . The source data encoder is converted into a compressed form occupies bits before transmission or storage to reduce the number , and the decoder of said compression format is converted back to the original video data . The encoder / decoder pair is often described as a codec (encoder / decoder) .

Data compression by removing redundancy, that is a faithful reproduction of the data component is not necessary to achieve. Many types of data including statistical redundancy , and can be effectively compressed using lossless compression , so that the output of the reconstruction data in the decoder is a perfect copy of the original data. Unfortunately, lossless compressed image and video information so that only the amount of compression .

Lossless image compression standard and can be , you can achieve optimum is about 3-4 times the compression ratio. Lossy compression is necessary to achieve higher Compression. After lossy data compression system , decompression is not identical Source data and a higher compression ratio can be achieved at the expense of lossVisual quality. Lossy video compression system is based on subjective redundancy is removed , which can be removed in principle perceived image or video sequence without significant effect element in the visual quality of the observer.

Most video coding method while using time and space redundancy to achieve compression . In the time domain , there is usually a high correlation between the video capture or about the same time similarities between the frames . Temporally adjacent frames , i.e. a continuous sequence of time frames , are usually highly correlated , particularly if the time sampling rate or frame rate is high. In the spatial domain , which is usually close to each other , i.e. adjacent to the sample value is typically very similar to a high correlation between pixels

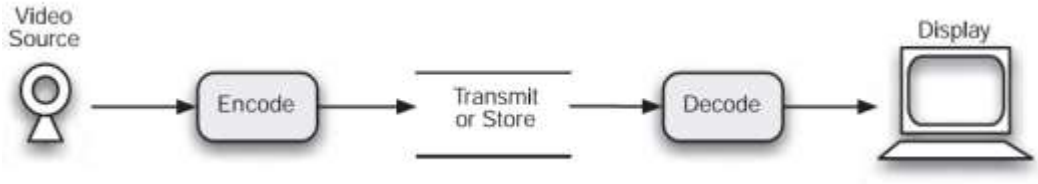


Fig 1.14. Encoder / Decoder

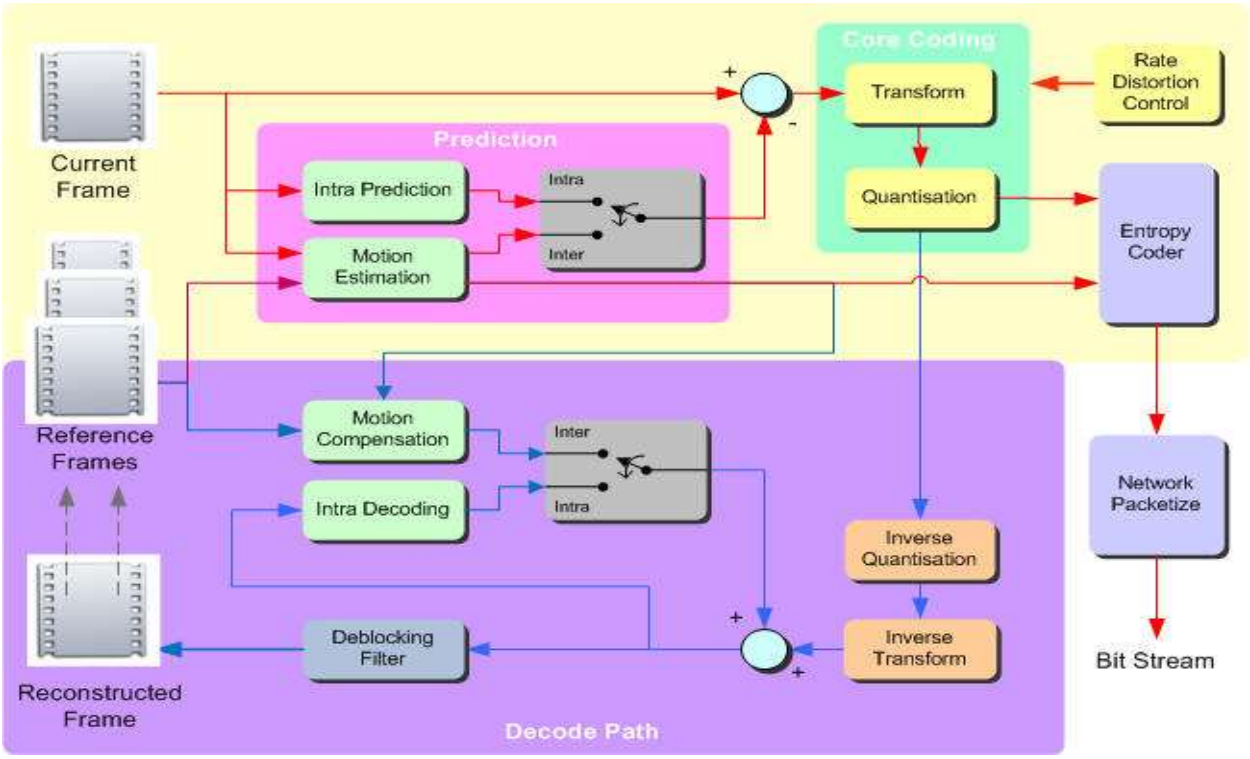


Fig 1.15. H.264 Encoder and decoder block diagrams (in detail)

1.3.Dissertation Objective

The Objective of the dissertation is to analyze the Video Encryption Schemes for Uncompressed or Container Video. The performance of all types of encryption techniques will be analyzed on parameters like, cost overhead, delay and quality of encryption. This will provide us detailed comparative analysis of video encryption schemes; to prove which of them is much more efficient for Container Video.

1.4.Research Contribution

1. Made a study of various video container formats
2. Performed comparative analysis of video encryption techniques on different container video formats.

MAT LAB

MATLAB is a high level of numerical computation, visualization and programming language and interactive environment. Using MATLAB, you can analyze the data, the development of new algorithms, and create models and applications. Languages, tools, and built-in math functions, allowing you to explore a variety of ways, and to reach a solution faster than spreadsheets or traditional programming languages such as C / C + + or Java.

You can use MATLAB range of applications, including signal processing and communications, image and video processing, control systems, test and measurement, computational finance, computational biology. Industry and academia in more than one million engineers and scientists using MATLAB, technical computing language. We will develop a highly efficient video compression algorithm, MAT LAB**.**

1.5 Dissertation Outline

Chapter 1 as described above gives the overview and objective of research. (types of video/real time & non real time streaming/video encoding/video encryption/problem statement/methodology of research)

Chapter 2 describes literature survey related to video containers & encryption schemes. Also discusses various relevant references. (Video Containers/Video Encryption/Matlab/References/ Motivation)

Chapter 3 describes the encryption methodologies of container video.

Chapter 4 describes the experimental results of implemented work. Also, describes comparative analysis of video encryption schemes in container video using simulation model.

Chapter 5 describes the result analysis.

Chapter 6 includes the conclusion and future scope related to the research work.

Chapter 7 reference section contains the references which are used for research work and dissertation report.

CHAPTER 2
LITERATURE SURVEY

2.1. Introduction

Multimedia is the integration of various types of media forms . It contains graphics, text , video, audio, etc. For example , audio and video clips related to a presentation would be considered " multimedia presentation ." Involving animation, sound and text educational software is called " multi-media software ." CD and DVD is usually considered a " media format " because we can store large amounts of data and various parts of multimedia require a lot of disk space.

The word multimedia comes from latin word "MULTUS", meaning " many " and the media means " middle " and " center ." Multimedia Therefore , the general sense refers to information storage, transmission , display and perception " more intermediaries " between information sources and sinks or more devices. The use of different media is a combination of any of the medium , which may or may not involve the communication of the computer. Multimedia consists a variety of formats from a PowerPoint slide show to a interactive simulation (learning circuit) , and in most cases it is considered to increase the user experience and the information provided leads to much easier and faster understanding . The concept of presenting information in various formats is a old phenomenon, but when we examine the concept of multimedia, it usually means that various "digital" format (Wikipedia, 2006) presented information .

The various elements of multimedia , including video , text, graphics, sound and animation . Elements are used in multimedia existed before . Multimedia is a combination of such elements into a powerful new tool .Better Quality of the text is the largest multimedia advantage . In general , the text gives important information . Text serves as the much importatnt of all another media elements tying together ; Sound is used to provide emphasis or highlight from one page to another transition. Sound synchronization screen display, so that teachers in presenting a lot of information .

Creative use of sound , to stimulate the imagination , became hindered by improper use or annoyance ; video describes information by using the visualization capabilities , although there is no doubt , this is the strenth to choose how we see , as well as interact. And digital video , digital video content is provided in the education of new and exciting possibilities. Video can stimulate interest in the information if it is resting on the relevant pages , is not " overdone ." One of the most important justification , the video may be its ability to respond to the dramatic mood caused by the individual ; animation has capability to display status changes over time , or slow information presented to students , so that they have time to take it in smaller blocks. Animation, when added with the user input , various options allow students to watch the change over time depending on the variables. Animation is useful to prove an idea or a concept to explain . Video is usually taken from life, and the animation is based on the pictures ; cards offer the most creative ability, a learning phase. They can be drawings, photos , charts , spreadsheet from the CD-ROM, or take some views with the help of Internet . Scanner may also be included painted work . Standing Committee commented, " picture recognition memory capacity is virtually unlimited ." Reasons for doing so is to use the image of a huge range of cortical skills : shape, colour , size, line , visual rhythm , texture, and especially imagination.

Television (TV) is for transmitting and receiving moving images , which can be a communication medium monochrome (black and white) or colored , with or without sound . " Television " may also refer to a specific TV , television programs or television transmission. Computer is an electronic device designed to work with the information . The term computer is from the Latin word "computare ' is derived , which means calculations. Computer without a program can not do anything it decimal number by a string of binary digits expressed in the Word, " computer " usually refers to a central processing unit , plus built-in memory . literacy and computer-related child care experience should include a balance of open events and more closed learning activities. (Segers and Verhoeven , 2002) . computers do provide a lot of children language students and teachers both children showed greater interest in the use of computer programs and the environment happy when they also found that using a computer than see the conclusion that there is more motivation for kids to use the computer, use the computer

more fun more focused , and the emergence of the " more " of that experience . computer seems to have been highly excited children , who generally have a very positive experience on the computer , and often stay in the time of the task (Lee McCarrick , 2007 annual) long slide projector is a tool to view photo slide which has four main components : a light bulb , reflector and " condensing " lens light directly onto the slide , slide the focusing lens holder . a heat-absorbing glass is generally flat sheet is placed between the converging lens and the slide glass to avoid damage to the sliding such infrared-absorbing glass . slides and the light passes through the transparent lens , the resulting image is enlarged and projected onto a screen . so the audience can see its reflection .

Video is recording a visual image of the electronic media activities , copying and playback. Still image frame sequence comprises a video codec , and the compressed format , the change between images. Quality will depend on the second color space , resolution video applications such as early childhood education , and promote strong brain development , preparing children to school, build a stronger workforce and economic frames differ. Animation is an attractive young audience and most of the students , and even display a high level of media literacy and knowledge about animation in the early years . The word " animation " means " to animate ", which used to bring the life such as the Earth's rotation is better able to capture video motion or animation better solution . Through traditional animation story offers a huge knowledge and practical context.

With the help of multimedia we can create high -quality learning environment . we can create a more realistic learning environment through its various media and allow learners the ability to take control of interactive multimedia can provide an effective learning environment, different types of learners. Multimedia learning materials can be better, and it can create more opportunities for the development of different other types of media , and available for learners with existing knowledge linking new knowledge more cognitive connections. Multimedia teaching should be more effective than classroom teaching . Because it improves students' attitudes multimedia learning materials may be

effective . Information is presented using multimedia instruction seems to be a potential learning advantages compared to traditional classroom teaching . Multimedia can also cause learners to participate in the error message , thereby reducing the learning . Multimedia can be the most effective medium by allowing instructional designers use specific information to improve the presentation of learning . For instructions of educational multimedia important, and positive impact , we need to make multimedia instructional design decisions (Lawrence , 1995) . Initial stage is a crucial stage in a new born's education in life . If any guardian want to develop a good foundation for success , so that the whole concept clearly a child, and then in the future students will be able to master the difficult things easy (Surman , 2008) . It wholly depend on effective learning and teaching method. Learning process in teaching makes a educational system more effective and successful.Eduacation plays an important and critical role in student's life .

Educational technology refers to those materials , procedures , organization, ideas , equipment, apparatus or machine to make teaching learning process more effective , successful and memorable. The main role of media is to learn from practice. Students first saw the object , and then learn. Multimedia can have the specail ability to promote , as with the help of multimedia and natural way , children learn the similarities of learning , that is, with the help of seeing information and pictures. Visual message and graphics represented , students may be more enthusiastic for success and vocabulary learning methdologies . Vocabulary study guide and curriculum should reconsider their use of multimedia in their presentations (Kim and Gilman , 2008) . The use of interactive multimedia in the teaching process is a growing phenomenon. Multimedia assist students in the learning process in a very important role.

2.2. Types of Video CODEC

A multimedia video file comes in various formats such as .flv, .mov, .3gp etc. Some of the popular video formats are explained as follows:

3GP: The .3gp file format or the 3GPP is a multimedia container format that was created by the Third Generation Partnership Project, to be specifically used, accessed, played and transferred over high-speed wireless 3G networks. It is most notably known to be used and accessed on mobile phones, and is the predominant file format on almost all mobile phones that has video capture features.

The standard data structure of .3gp files is quite similar to the MPEG-4 Part 14 container format, although it also contains many encoding formats specification in the ISO base media file format (MPEG-4 Part 12). The final resulting media data in the .3gp file however is usually significantly altered to lower the file size and bandwidth requirements to a level where it would be easily accessible to mobile phones.

The .3gp video stream can be encoded in MPEG-4 Part 2 or H.263 or MPEG-4 Part 10 (AVC/H.264), while the audio stream can be encoded in several AMR and AAC formats. In terms of pure quantitative ratio, the .3gp file format actually borrows more definitions and specifications in the MPEG-4 Part 12 container format than in the MPEG-4 Part 14, although most of these are simply “alterations” of what could be generally found in any MP4 container format.

All of the specifications of the .3gp file format are defined by the recommendations given by the ETSI 3GPP technical specification.

WMV: WMV (Windows Media Video acronym) is to create a compressed video file format developed by Microsoft. The most common container WMV files are ASF (Advanced Streaming Format) format * wmv or *. ASF end. In this case, the protection of intellectual property management support WMV DRM. Sometimes it is stored in an AVI or Matroska container format of. When a WMV file is packaged in an ASF container format, it can become intellectual property protection, due to the digital rights management facilities. The standard was officially approved in 2006 for the VC-1. The original video format is WMV RealVideo competitors as designed by Microsoft for Internet streaming applications. Such as WMV Screen and WMV video formats are

designed for specialized content. Elliptic curve cryptography key exchange, DES block cipher, a custom block cipher, RC4 stream cipher and SHA-1 hash function allows digital rights management support interlaced video, non-square pixels, frame interpolation supports variable bit rate, average constant bit rate and composition bitrate.

AVI: It was first developed in late 1992 as a means to allow both video and audio playback at the same time. Its file compression capabilities made it a popular choice among users who had limited space in their hard drives. Advances in both compression techniques and information-sharing technology allowed AVI to maintain its popularity for years, as the file format continues to be one of the most downloaded multimedia video formats. AVI videos bear the .avi file extension.

MPEG: It was developed in 1993 and was used primarily to contain video and audio information for video compact discs (VCDs). The format's first version, MPEG-1, needed to downsize images in order to adhere to bit rate limitations, resulting in videos of relatively poorer quality than what was then available. Upgrades to the format allowed for high-definition, scalable resolutions and improved file compression. Audio data contained in MPEG files are usually compressed within the MPEG Audio Layer III (MP3) format, one of the most popular multimedia audio formats available. Commonly-used file extensions for MPEG multimedia video formats include .mpeg, .mpg, and .mp4. Video sharing websites such as YouTube often use FLV and WMV as their multimedia video formats of choice. The formats allow for faster and smoother streaming of data over the Internet as compared to other formats, albeit with a loss of video quality. Upgrades to the technology allow users to opt for high-definition video, but streaming speeds become significantly slower as a result. File extensions include .flv and the more advanced .f4v for FLV, and .wmv for WMV.

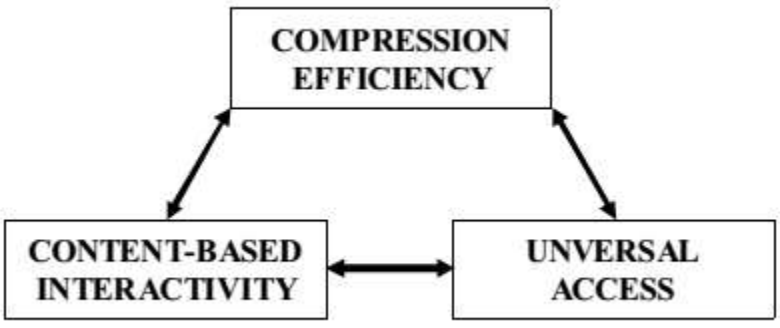


Fig 1.8. Functionalities in MPEG-4 Visual Standard

MOV: QuickTime is a file format used to store and play movies with sound. While the developed countries and supported primarily by Apple Computer, this flexible format is not limited to Macintosh operating systems. It is also commonly used in Windows systems, and other types of computing platforms. In Windows, QuickTime files usually appear with the "MOV" file extension. Since 2002, Apple has begun using MPEG4 video encoding among its QT streams, producing better, if not excellent, video quality.

MOV QuickTime-wrapped files using file extensions. QuickTime content (MOV,. QT), developed by Apple Computer, is used to store and play movies with sound file format. This flexible format is not limited to Macintosh operating systems. It's also commonly used in Windows systems, and other types of computing platforms.

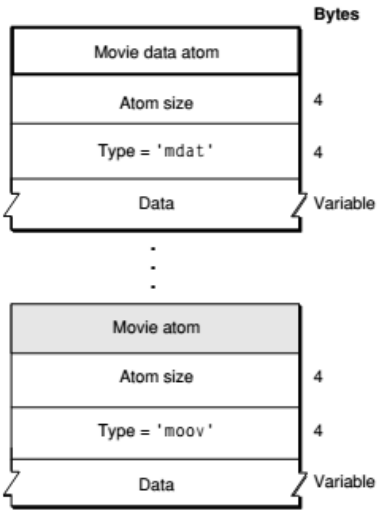


Fig 1.9. Quick Time File Format (.mov)

3GP is most commonly seen in videos taken by 3rd-generation mobile telecommunication (3G) phones. The format, though poor in quality compared to other file types, boasts much smaller file sizes, making it an ideal format for the smaller disk space found in mobile phones. 3GP is usually shared through Multimedia Messaging Services (MMS) and storage device transfers, but is uploaded and downloaded over the Internet as well.

During the selection of codec the following criteria should be followed:

- Compression level
- Quality of compressed video
- Compression/Decompression speed

Using the above criteria a codec produces high quality video at high levels of compression, but a powerful computer with hardware acceleration is needed to playback the video in real-time. For reducing file size there are many other considerations such as: By reducing the frequency of Key Frames and by reducing the number of colour palettes to 8 bit.

2.3. Video Container Formats under Consideration

Containers : We take a look at some of the container, and then in some codec. Video file extension usually refers to the container. Several containers , they are almost always tend to use a number of different codecs codecs and other containers .

1. Audio Video Interleave (AVI): developed by Microsoft and released with Windows 3.1. AVI digital video files , has been working. Despite its popularity has faded, you can find all over the web leaves a lot of AVI video. Recently , AVI has abandoned Microsoft's WMV (Windows Media Video) .
2. Advanced Systems Format (ASF): ASF is a proprietary Microsoft container typically include Microsoft's WMV file compression codec - make things confusing , often specified file , WMV, ASF. ASF container has a variety of formats , which may include DRM (Digital Rights Management) copy protection of a form of advantage .
3. The QuickTime (MOV or QT): QuickTime , which is developed by Apple , and supports a variety of formats. Although this is a proprietary format and Apple decided to support it .
4. Advanced video encoding , HD (AVCHD): AVCHD is a very popular container , H.264 data compression - digital camera formats , including cooperation between Sony and Panasonic . This is a file-based format , which means the disk or other storage device

to store and playback. It supports standard definition and high definition , unlike 720-1080 .

5. Flash Video (FLV, SWF): Flash was originally by a company called Adobe , Macromedia , which was acquired by the development in 2005. Flash memory has been for some time, there are several versions, some are better than others. Older versions of Flash video , often using the Sorenson codec. This is a container format video streaming across the network is very widely used. Its main drawback is that it be played on iOS devices such as iPad or iPhone

2.2.1. AVI

Audio Video Interleaved (also **Audio Video Interleave**), known by its initials **AVI**, is a multimedia container format introduced byMicrosoft in November 1992 as part of its Video for Windows technology. AVI files can contain both audio and video data in a file container that allows synchronous audio-with-video playback. Like the DVD video format, AVI files support multiple streaming audio and video, although these features are seldom used. Most AVI files also use the file format extensions developed by the Matrox OpenDML group in February 1996. These files are supported by Microsoft, and are unofficially called "AVI 2.0".

AVI is a derivative of the Resource Interchange File Format (RIFF), which divides a file's data into blocks, or "chunks." Each "chunk" is identified by a FourCC tag. An AVI file takes the form of a single chunk in a RIFF formatted file, which is then subdivided into two mandatory "chunks" and one optional "chunk".

2.2.2. DAT

The DAT project was approved in November 1994 and focused on the expansion of MPEG - 1 compression technology in the cost of higher bandwidth utilization to cover the bigger picture and higher quality. DAT is designed for digital television broadcasting applications, usually four to 15 Mbps (up to 100 Mbps), such as digital high-definition

television (HDTV), interactive storage medium (ISM), and cable TV (CATV) between the bit rate (Sikora, 1997; Ali, 1999).

The standard DAT consists of several parts, of which the most important is that our video section. The standard defines a compressed video bit stream, and explains how it is decoded. To realize that it does not describe how the input image and compress it to make a DAT bit stream is very important - it's not an encoder specifications. An encoder designers complete freedom to choose which standards to use, and how to use them. Therefore, the best is to DAT standard toolkit for video compression, from which you can choose the appropriate tools for different applications.

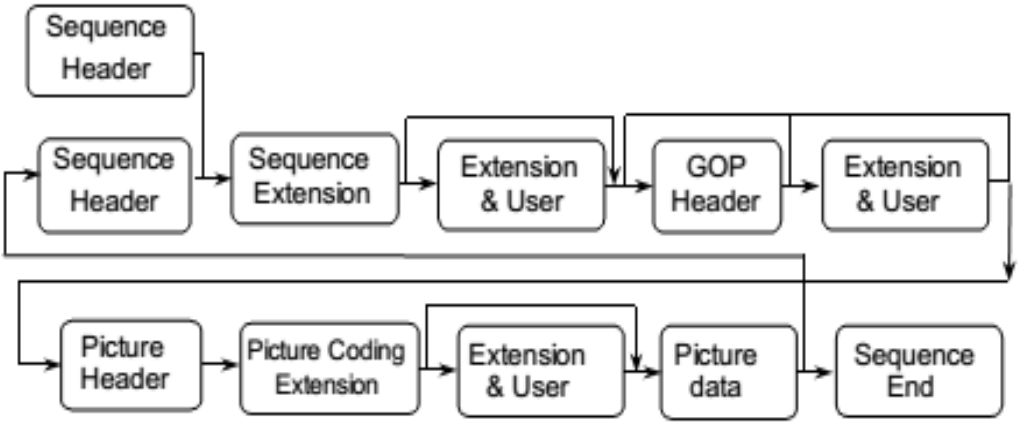


Fig 2. DAT Data Structure and Syntax

2.2.3. AVCHD (Advanced Video Coding High Definition)

It is a format for the recording and playback of high-definition (HD) video (usually with the multilateral trading system extension). Debuted in the middle of 2006 , AVCHD is jointly developed by Sony and Panasonic, mainly for high -definition video camera consumers. So far, all popular HD camcorder manufacturer provides support AVCHD video products , such as the Canon HF S200, Hitachi DZ - BD10HA, JVC GZ-HM1, AVCHD Sony and Panasonic , let alone who use entirely .

Advantages AVCHD MTS/M2TS video format

1 . Record high-definition video on a random-access media , including 8 cm DVD discs, hard drives and removable flash media such as SD / SDHC memory card and "Memory Stick" cards. This is why the AVCHD format can be eliminated based on high-definition video recording format , such as a key factor in other types of HDV .

2 . AVCHD format uses MPEG - 4 AVC/H.264 (AVC) video compression codec and either Dolby AC - 3 (Dolby Digital) or linear PCM (for lossless audio data encoded) audio compression codec . It allows AVCHD MTS video featuring efficiently reduce the size of data files , providing sufficient recording time , while maintaining high -quality HD shooting .

3 . Compatibility with Blu-ray Disc . Due to the structure of AVCHD video from Blu-ray Disc specification is derived , it is designed to be compatible with Blu-ray Disc format , can be used for high-definition video DVD media production , although not all Blu-ray players are compatible with AVCHD discs.

4 . What makes AVCHD (and other films , like AVC, MPEG - 4, AVI, MKV, MOV and other relatively) unique and advanced video compression format is that it contains the function to enhance multimedia presentations, such as: menu navigation , slide shows and subtitles .

Four ways you will benefit from AVCHD MTS video

1 . With the right AVCHD video player , you can easily enjoy the full 1920x1080 resolution must be your desire to play AVCHD video from .

2 . Convert and burn AVCHD to play on the DVD player, Blu-ray is also a better way to enjoy high-definition recording and storing video .

3 . Since advertising information , said : Broadcast yourself , winx make YouTube also accept AVCHD video willingly. So there is no boundary to upload AVCHD to YouTube and share your funny online HD video.

4 . As the professional AVCHD or AVCHD video converter video editing software , you can convert and edit AVCHD videos and more to expand the use , like AVCHD transfer to iPhone, AVCHD to iPad, iPod 's , iMovie medium , iTunes , etc.

2.3. Video Encryption Techniques

Security and privacy issues in multimedia technology have become an important concern. Many multimedia applications require secure transmission, the level of security required depends on the sensitivity of the information in these applications. Moreover, some applications such as TV broadcast require a suitable secure transmission system. In these applications, the digital video clip undergoes compression and encryption at the sender's end and decryption and decompression at the receiver's end. Real-time transmission must be achieved at the rate of approximately less the 1/30 of a second per frame. Video bit streams are typically huge in size even after compression, and current data encryption and decryption algorithms are relatively slow, and using these encryption techniques to encrypt the whole video bit stream can cause the overall processing time to increase tremendously, going beyond 1/30 of a second per frame, leading to computational overhead. The field of multimedia security has been growing extremely fast, and achieving secure multimedia transmission over the network is currently receiving a lot of attention from the research community.

Naïve Method is used before coding and due to which the thrust is much more than the other encryption algorithms. Due to which its security is greater than selective method.

Selective Method is time consuming as it is applied during the coding of the Video Encryption. Due to which its security is much more than the any other methods.

Layered Method is used after the coding of video, performed on the selected bits. So, it's an easy process but very true that it reduces security.

Security Factor plays a major role in the above three methods, which is discussed in further chapters with details.

In order to overcome the problem of processing overhead and to complete the requirements of real -time video formats with high quality video compression, several encryption algorithms video streaming has been proposed to meet the requirements .

Most of these algorithms attempt to check the feasibility of the encryption process with respect to the encryption speed, and the display process. Some of the proposed video encryption schemes are reviewed in the section below.

2.3.1. Naïve Algorithm

Naive algorithm is the most direct method to the entire motion picture experts group (MPEG) (MPEG, 1988) using a standard video stream encryption scheme such as DES or AES of each byte is encrypted. The concept behind the naive algorithm for MPEG stream is treated as text data, do not use any special structure (AGI and Palace, 1996; Salah, 2003; Habib et al, 2006).

Naive algorithm by using standard encryption scheme, because, to date, there is no efficient algorithm that can crack the encryption schemes such as AES or Triple DES to ensure the security of the entire MPEG data stream. However, the algorithm can not be applied to a large video, because it is very slow, especially using Triple DES while. Because the encryption operation, the delay increases, the cost would be unacceptable real-time video encryption.

2.3.2. Selective Encryption Algorithm

To reduce the processing overhead (Nithin, et al, 2007) the amount and meet the safety requirements of real-time video applications , selective encryption techniques have been proposed (and Lintienshan Nahrstedt, 1998). The purpose of this program is to be encrypted by using MPEG hierarchical structure (for example , encryption of all the headers and I-frames , encryption features all the I- frame MPEG ING different levels of selective partial data stream and all I blocks P and BF rames). Based substantially on the selective encryption of MPEG I- frames , P- frames and B- frame structure. It Encrypted I - frame only because , in theory , P and B frames are useless I do not know the appropriate frame .

Selective encryption is used to encrypt the only part of the compressed video stream , in order to reduce the computational complexity of the technique (Bharagava and Shi , 1998 ; Deniz , et al, 2007, ...) . It is not a new one I DEA, because it has made several applications , especially in multimedia systems (Lookabaugh et al, 2003) . Selective encryption

Can be used to reduce power consumption by the encryption function of the digital content. As the only specific portions of the bit stream is encrypted , the selective encryption system can also enable new features, such as allowing the preview content . For selective encryption work , it needs to rely on a small part of the compression algorithm the relative importance of the feature set of the original data signal in a compressed bit stream. Selective encryption algorithm has excellent characteristics such as real-time transmission and to prevent error propagation . Therefore, it is likely to be based H.264/AVC video data security technology main research directions. In the past decade , several different selective encryption algorithms have been proposed.

Selective Encryption having many subtypes. Some of them are as follows:

2.3.2.1. Pure Permutation Algorithm

Pure by simple replacement algorithm arranged in the frame by an MPEG stream scrambling byte. It is, in the case of a video decoding hardware is very useful, but the decryption must be done in software.

2004, Slagell show that pure replacement algorithm vulnerable to known-plaintext attack, and therefore, its use should be carefully considered. This is because, compared with the known cipher text frame, the opponent or hacker can easily find out the secret permutation list. Once the replacement list figured out, or be aware of all the frames can be easily decrypted. It must be pointed out that in an MPEG stream of I-frames is sufficient to decrypt the replacement list, according to the Shannon theorem.

2.3.2.2. Zig-Zag Permutation Algorithm

In the Zig-Zag permutation approach (Tang, 1996), instead of mapping the 8x8 block to 1x64 vector in “Zig-Zag” order, it maps the individual 8x8 block to a 1x64 vector by using a random permutation list (secret key). Zig-Zag permutation algorithm consists of three main steps:

A. Generated order list of 64.
B. Complete the division process. Assuming DC coefficients are represented as 8 - bit binary number D7, D6, D5, D4, D3, D2, D1, D0 which is then split into two digital D7, D6, D5, D4 and D3, D2, D1, D0. Then , D7 number , D6, D5, D4 is placed a number of DC coefficients and d3 , D2, D1, D0 is placed into the AC coefficients. Splitting process is based on the following observations :

1. DC coefficient value of an AC coefficient is greater than the value .
2. After the split , the extra space is required to store the division number 1 ,

This will increase the size of the MPEG data stream . However, it must be noted that in the last AC coefficient which can be set to zero, no significant visual degradation of the block value of the least significant .

C. random permutation applied to the split blocks.
As the list based on a random permutation mapping and mapping zigzag sequence has the same computational complexity , the encryption and decryption process is very little overhead added to video compression and decompression process . However, this method reduces the video compression rate, since the discrete cosine distortion probability distribution arrangement transform (DCT) coefficient , using the Huffman table that is not ideal . Lintienshan and Nahrstedt (1997 , 1998, introduced two types of zigzag arrangement ciphertext only attack and known-plaintext attack attack.

Zigzag arrangement algorithm is vulnerable to a ciphertext only attack, attack relies on DCT coefficients , which are non-zero AC coefficients are gathered in the upper left corner of the fact that the statistical properties of the I block. By the Lintienshan and

Nahrstedt (1997; 1998) the number of AC and DC coefficients from statistical analysis of an I frame zero and all the blocks following comments :

• DC coefficient always has the highest frequency of zero appears .

• AC1 and AC2 frequency is among the top six Frequency

• AC3 to AC5 is among the top 10

The second problem is that the algorithm can not afford a zigzag arrangement known plaintext attack. Suppose we know in advance (known plaintext) some frames of the video, the key can be easily done by simply comparing with the corresponding known plaintext encryption frame figured out . To solve this problem, a method called binary sequence of coin flipping method and arrangement of the two different lists can also be used . For each 8x8 block , a coin flip. If it is a tail of one of the permutation list (key 1) is applied to the block. If it is a head , the replacement list 2 (KEY2) is applied to the block. This approach is vulnerable to a known plaintext attack as well, because the tendency of non-zero AC coefficients in the upper left corner of the block , collect. Therefore, it would be easy to determine which key rival to be used (Lookabaugh et al, 2003) .

2.4. What is MATALB?

MATLAB is a numerical computing environment and programming language. Creator of The Math Works , MATLAB allows easy matrix operations , functions, and data mapping , algorithm , creating the user interface , and the interface with the program in other languages . Although it specializes in numerical computing , an optional toolbox interfaces with the Maple symbolic engine , making it a complete computer algebra system . It is composed of industry and academia over one hundred million people , in most modern operating systems, including Windows, Mac OS, Linux and Unix running .

The image is represented as a three-dimensional matrix : for each point stores its coordinates. In MATLAB Image Processing Toolbox provides a comprehensive reference standard algorithms , functions, and for image processing, analysis , visualization, and algorithm development applications. You can perform image

enhancement, image deblurring , feature detection , noise reduction , image segmentation, geometric transformations and image registration . Many toolbox functions are multithreaded to take advantage of multicore and multiprocessor computers advantages.

Image Processing Toolbox supports a different image types, including high dynamic range , Gigabit pixel resolution , embedded ICC profiles, and faults . Visualization capabilities , allowing you to explore the images, check the pixel area , adjust the contrast and create a profile or histogram manipulation of interest (ROI) in the area. And toolbox algorithms can restore degraded image , detection and measurement capabilities , analyze shapes and textures , and adjust the color balance .

In MATLAB graphics provide some direct tools to create an interesting view of the surface. MATLAB shown in the same sign . Several plots stored as a movie frame allows us to do animation. Animation in MATLAB like a real movie , the camera's position and purpose , can be adjusted.

2.5. Related Papers

In this chapter, a background related to the research was reviewed. A general background video compression techniques and a comparison between H.264/AVC and existing standards were presented. The following section presents a brief discussion of the new features in H.264/AVC standard.

There are hundreds of research journal papers and conference papers on video compression schemes of H.264 Advanced Video Compression Standards and some of them are used for brief reviewing for literature survey. Cryptography is a method to convert the information into a form different from its original form that depicts to be of no use. The area of visual cryptography is much relevant to the visual media like images. The steganography can be encrypted before embedding into the original content. One can use his eyes to decode the information once all the shares are stacked up together. This method is adopted due to simple encryption and decryption process. Inclusion of the

concept of threshold in visual cryptography makes multi-model method robust against collusion and forgery attacks.

Thomas Wiegand and Gary J. Sullivan presented H.264/AVC (Advanced Video Coding) Standard in nutshell. In this, they focused evolution and objective of H.264/AVC with the functioning and structure of H.264 with block diagram of encoding process. And made a comparison between other standards with respect to their performance and speed/complexity.

Borko Furht, Daniel Socek and Ahmet M. Eskicioglu presented the fundamentals of multimedia encryption techniques. In this article a focused study is performed for multimedia encryption techniques such as AES or DES. It involves careful analysis to determine and identify the optimal encryption method when dealing with audio and video data. And briefly describe the selective encryption, layered and naïve approach.

Tong Ling , CAO Gang and Li Hu Jintao is known for its clever use of H.264/AVC error propagation characteristics of strong encryption framework layered video video encryption scheme. In the present study layered encryption , the degree of protection is achieved by changing the zoning for the three levels of data encryption . Encrypted data base layer distorting the video at least , while the middle layer is the main object of special protection . In this manner, the entire frame of the enhancement layer is encrypted. This encryption method is applicable to various hierarchical framework and a typical encryption method is based on the existing implanted .

Jay · M. · Josh and Upena D. Dalal presents an enhanced selectivity ISMACryp real-time video encryption scheme used in handheld devices. In this regard , ISMACryp encoded , H.264/AVC (Advanced Video Coding) , while all of the data structure as it is. Available in two models ISMACryp ; 's CTR mode (counter
Type) and CBC mode (Cipher Block Chaining) mode. ISMACryp these two models are 128-bit AES algorithm. AES-CTR mode is discussed here. AES algorithm is more complex and requires a large execution time is not suitable for real-time applications like live TV , video chat or video conference handheld devices . Objectives of the proposed

system is to obtain data on the safety video deep understanding of multimedia technology and selective encryption of H.264/AVC using real-time video applications to provide security. Based H.264/AVC baseline constraint NAL unit content profiles five levels of security proposed . Intra -prediction mode of the selective encryption to provide different levels of residual data, the inter prediction mode or only the motion vector encryption.

Jay · M. · Josh and Upena D. Dalal proposed selective encryption using ISMACryp H.264/AVC video streams in real-time application of DVB-H . ISMA Encryption and Authentication (ISMACryp) is a DVB-H (Digital Video Broadcasting - Handheld) service of technical protection devices for portable handheld TV system selected . The ISMACryp encoded H.264/AVC (Advanced Video Coding) , while all of the data structures ASIT yes. Available in two models ISMACryp ; 's CTR mode (Countertype) and CBC mode (Cipher Block Chaining) mode. ISMACryp these two models are 128-bit AES algorithm. AES algorithm is more complex, requiring the implementation of which is not suitable for real-time applications like live TV larger time . In this paper proposed five security updates based H.264/AVC NAL unit in the baseline constraints content.

SAURABH Kulkarni , Ketki HARIDAS and Aniket, A comparative study between other algorithms, more presented in the proposed video encryption algorithm V / S 's . In this proposed an innovative encryption algorithm, using H.264 video compression to securely exchange highly confidential video. To maintain a balance between security and computing time , the proposed algorithm of the video frames and audio shuffling , and AES encryption for selectively sensitive to the video code words. Unauthorized use of this method to watch video files can be prevented , so the algorithm provides a higher level of security.

Deepali P. Chaudhry and Vaibhav Exe Nat Narawade proposed multimedia selective encryption and compression schemes . In this case, selective encryption is done by using the Advanced Encryption Standard (AES) algorithm to compress and use H.264/AVC standard. The system comprises two main functions ; first video stream encoding /

encryption by performing the two processes (the first video input sequence coding by the H.264/AVC encoder , and the encoded bit stream (I- frame) is encrypted using AES block encryption section) . And the second function is performed by two processes encryption and decryption of video / decoder (designated I- frame is encrypted stream , I-frames of the decrypted and decoded with H.264/AVC decoder) .

M. Abomhara, Omar Zakaria , the Ottoman Caliphate Australia , AA and BB Zidan Zidan is recommended to use AES encryption to enhance selective encryption H.264/AVC. Security In this , the purpose of the proposed system is to get video multimedia technology has a profound understanding of data to explore how to encrypt and decrypt the real-time video applications can be implemented , and to strengthen the selective encryption of H.264/AVC .

Abdullah · Muhit, Mark R. Pickering , Michael Frater , and John · F · Arnold proposed a new strategy to predict the expansion , combined with the non- translational motion prediction . 2-D cosine basis functions elastic motion model used this method to estimate the non- translational motion between blocks . In order to achieve superior performance , the program utilizes the multi-level partition larger block advantage**.**

Li Chunhua , spring source and Yuzhuo proposed layered scalable video coding selective encryption scheme. Here , the main features of the program is the use of SVC characteristics. This approach is fully in line with the needs of SVC encryption and encryption at the network level summary execution of the layer (NAL) of . Depending on the importance of the structure and the base layer and enhancement layer , the type of encryption domains . For the base layer , the intra prediction mode (IPM) , and the remaining signs are selected. For the enhancement layer , temporal scalability , and spatial / SNR scalability is different . In addition, key generation and distribution scheme is proposed. Stream cipher , leak extraction (LEX) algorithm to reduce the computational cost.

Z. Shahid , M. Chaumont and W PUECH proposed a new method for protecting the art video codec H.264/AVC bitstream state . Here , the selective encryption (SE) , with the compression block in the entropy encoding process . H.264/AVC supports two entropy coding module . Context-based adaptive variable-length coding (CAVLC) is supported in H.264/AVC main configuration file support H.264/AVC baseline updates and context-adaptive binary arithmetic coding (CABAC). SE run in both types of this video codec entropy coding module . The encryption step performed by the same or CAVLC entropy coding CABAC.

CHAPTER 3
VIDEO ENCRYPTION TECHNIQUES

Multimedia security is a method for preventing or unauthorized access or distribute multimedia content to prevent unauthorized way to achieve. These methods are based largely on cryptography, they either provide communications security , or the fight against piracy (DRM and watermarking) security. Multimedia data communications security can be achieved by means of conventional encryption techniques. The multimedia data may be encrypted using a password system completely , e.g. DES, IDEA , or AES, the network and should , in a secure way even high-speed transmission . Encryption and transmission through different video network can be used to protect video content. In general , large -scale digital video , so movie compression formats, such as MPEG, or H.264/AVC usually transmitted. Multiple encryption algorithms have been proposed for secure video stream. In many cases, when a static text or multimedia data rather than real-time streaming media , it can be treated as a normal binary data, and using conventional encryption techniques.

A cryptographic system is also called a password or cryptography. Called plaintext message is encrypted , and the encrypted message is called a ciphertext. Said plaintext and ciphertext by the P and C, respectively . A password encryption process can be described as C = EKE (P), where Ke is the encryption key and E (•) is the encryption function . Similarly, the decryption process is : P = DKD (C), wherein the decryption key Kd and D (•) is the decryption function . According to Kerckhoffs' principle, password security should rely only on the decryption key Kd values , because the enemy could recover from the observed ciphertext plaintext , once they get the Kd.

There are two encryption relationship between Ke and Kd following . When Ke = Kd value , the password is known as the private key password or symmetric cryptography . For private key cryptography , encryption, decryption keys must be transmitted via a separate secret passage ted from the sender to the receiver. When Ke ≠ Kd value , the password is known as public key encryption or asymmetric encryption. For public key

cryptography , encryption key Ke released, and secret decryption key Kd , but no additional secret channel is needed to shift the focus .

According to the structure of the encryption , passwords can be divided into two categories: block ciphers and stream ciphers . A block cipher to encrypt a plaintext block from the block , and each block is mapped to another block having the same size . Stream ciphers encrypt plaintext with the encryption key from the pseudo random sequence control (called a key stream) .

Password security password should be strong enough for all types of attacks . For most of the password , the following four attacks should be tested : 1) ciphertext only attack - the attacker can only get ciphertext ; 2) known plaintext attack - the attacker can get some plaintext and corresponding ciphertext ; 3) Choose - plaintext attack , the attacker can choose some plaintext corresponding ciphertext ; 4) select - ciphertext attack - the attacker can choose some ciphertext and the corresponding plaintext

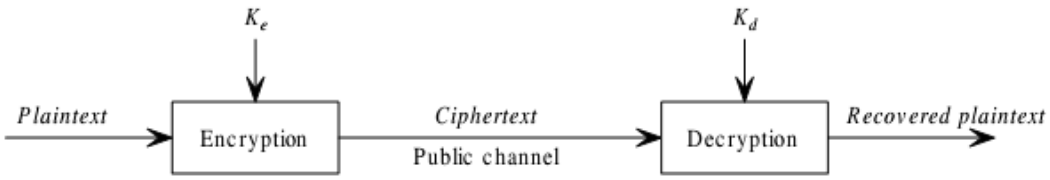


Fig 3.1. Encryption and decryption of a cipher

The two main components in the encryption process are the algorithms and the keys. The algorithms are complex mathematical formulas that dictate the rules of how the plaintext will be encrypted to cipher text. Keys are strings of random bits that are used by the algorithms. In certain encryption technology, when two endpoints need to communicate with each other using encrypted data, you must use the same algorithm, and most of the time, the same key. In other encryption technology, you must use a different but related keys for encryption and decryption purposes. Either a symmetric encryption algorithm algorithm that uses a symmetric key (also called secret key), or an asymmetric algorithm, which uses an asymmetric key (also called a public key and a private key).

3.1. Symmetric Key Algorithms

In symmetric key encryption, the sender and receiver use the same key for encryption and decryption. As shown in figure 3.1, symmetric key encryption is also called a secret key, because both sender and receiver have to keep the key secret and properly protected. If two users want to exchange data using secret key encryption, both of them must obtain a copy of the same key.

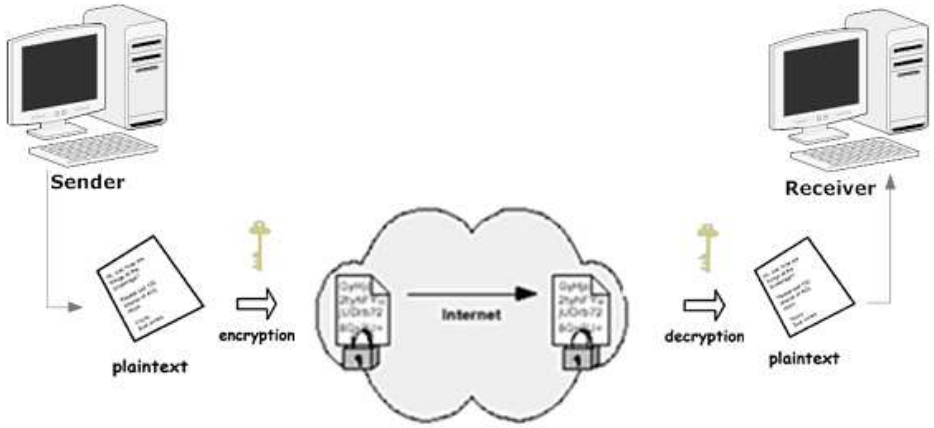


Fig 3.2. Symmetric Key Algorithm

If one wants to communicate with another person, then he needs to have three separate keys, one for each person. It seems simple enough, but if one wants to communicate with hundreds of people, keeping track of and using the correct key that corresponds to each specific receiver can be a daunting task. The more people a person wants to communicate with, the more keys he needs to keep. The equation used to calculate the number of symmetric keys needed is n*(n-1)/2 = number of keys, where n represents the number of users (Harris, 2007). Basically, a symmetric key encryption method is entirely dependent on the level of security is to maintain a good user secret key. If the key is known by an intruder, then use that key to encrypt all data can be decrypted. This is what makes it even more complicated is how symmetric key is actually shared and updated, if necessary. If a person wants to communicate with one another for the first time, he has to figure out how to send the correct key to the second person in a safe manner. It is not a safety-critical delivery by mail or courier delivery, get it to the

user, because the key will not be protected, can easily be intercepted and used by potential attackers.

Symmetric key can provide confidentiality, but they can not perform authentication because there is no way to prove through the encrypted who, if two people are using the same keys are actually sent the message.

The following is a symmetric key system advantages and disadvantages:

Advantages

It is much faster than asymmetric key system .

• Its security depends on the length of the key . With the large-size keys , the algorithm will be difficult to break , because the symmetric algorithm is relatively simple mathematical functions bit encryption and decryption process.

• It does not require much computing power.

Shortcoming

• It requires a security mechanism provides a key.

• Each user needs a unique key , if a user has a personal contact N , then the N key must be kept secret in order to increase as the number of individuals , so there is no number keys.

• symmetric key management can be problematic .

• provide confidentiality , but could not be verified because the key is shared .

Despite all the problems and shortcomings of using a symmetric key , they are still used in many applications because they are very fast , hard working, if a large key size is used to break . Symmetric key can handle large amounts of data , it will take an unacceptable amount of time and asymmetric key encryption and decryption (Kessler , 1998) .

The data depending on their role in the secret key encryption scheme can be further divided into several major types . If an encryption algorithm , and all bits of a block , the algorithm is called block encryption algorithm . However , if the algorithm is applied to each individual bit , which is called encryption stream. Treat the incoming data stream encrypted as a bit stream . The bit is then subjected to a mathematical function individually . The key generation is needed to provide a data bit with the bit key XOR , and generates the encrypted stream . In block encryption algorithm, however, the data is divided into blocks of a set of bits . Time for each block (Harris, 2007) is encrypted.

The most popular is the secret key encryption algorithm Data Encryption Standard (DES), Triple DES (Wilhelm , 1999 ; Federal Information , 1999) and the Advanced Encryption Standard (AES). In this study, the focus of the discussion focused on only a symmetric algorithm, the Advanced Encryption Standard (AES) is used for this study

3.1.1. Advanced Encryption Standard (AES)

In 1997 , the U.S. National Institute of Standards and Technology (NIST) initiated a process,

Choose a symmetric key encryption algorithm used to protect sensitive (unclassified)

Statutory duty to promote the NIST Federal Information and asked to submit a new standard to replace the aging DES. In 1998 , NIST announced the acceptance of the 15 candidate algorithms , and requires encryption research social assistance in the analysis of candidates . This analysis included a preliminary review of the safety and efficiency characteristics of each algorithm . Results and selected MARS NIST 's review of the preliminary study , RC6 ™, Rijndael algorithm , snakes and Twofish algorithms as finalists. Having reviewed further public analysis finalists , NIST has decided to propose Rijndael algorithm as the Advanced Encryption Standard (AES), in November 2001 , Rijndael algorithm encryption system was selected as the Advanced Encryption Standard (AES). Rijndael encryption algorithm running on the system data blocks 128 , arranged in a 4 × 4 matrix with 8 - bit key . The algorithm may use a variable block length and key

length ; latest specification allows key length 128 , 192 or 256 and length 128 , 192 or 256 or any combination of .

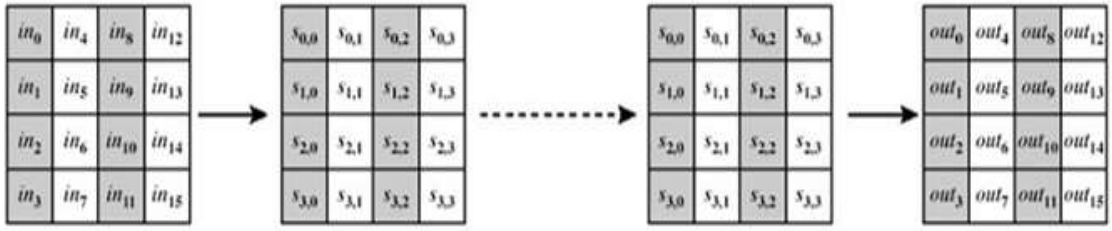
Rijndael is designed with the following features :

• Resistance against all known attacks

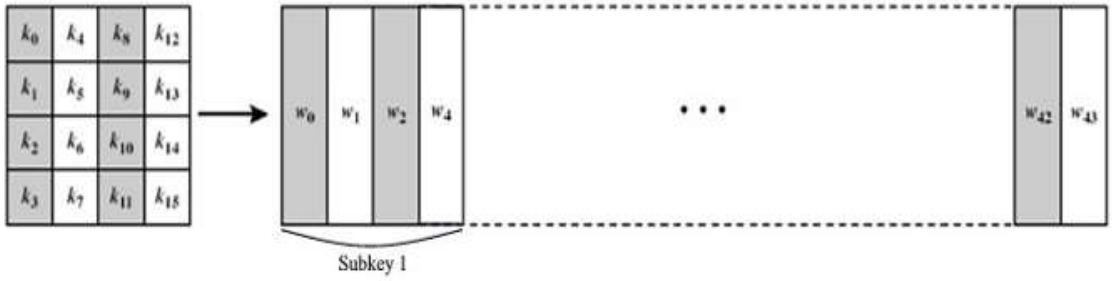
• In broad platform speed and code compactness

• Simple design

AES overall structure can be seen in the figures given above . The input is used both for encryption and decryption of a single block 128 and is called a matrix . This block is copied into being modified at each stage of the algorithm, and then copied to the output matrix of the state order. Both the plaintext and the key is depicted as a 128-bit byte of a square matrix . This key is then extended to key scheduling word (the W matrix) array. But it must be noted that the internal byte order is determined by the matrix column . The same applies to the W matrix.



(a) Input, state array, and output



(b) Key and expanded key

Fig 3.4. Data structures in the AES algorithm

3.2. Asymmetric Key Algorithms

Asymmetric key algorithm is also known as public key algorithm. Public key cryptography was first used by the U.S. Stanford University professor Martin Hellman and graduate students , Hui Philippines , in 1976 (Whitfield and Hellman, 1976) publicly . They describe both can be firmly and reliably by a non-secure communications channel , and having to share a secret key for communication , and by using two keys instead of a single key of the key distribution problem handling dual-key cryptosystem . Public key , which can be known by everyone , and a private key and should be kept confidential and only known by the owner , as shown in Figure 3.2 .

The message is encrypted using a key , and other keys needed to decrypt the message . Public and private keys are mathematically related . However, this does not mean that if someone gets the public key , he / she can calculate the private key , but if someone gets the private key , and then there will be a serious problem , because the private key can only be accessed by the owners did not others (Harris, 2007 ; Kessler , 1998) .

In asymmetric key algorithm used to encrypt each key and decryption. If the data is encrypted using the private key , it can not be decrypted by a private key , it must be decrypted by the corresponding public key.

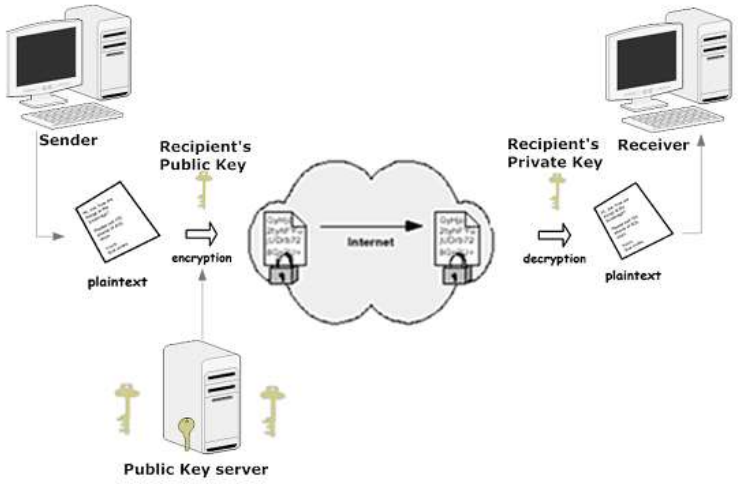


Fig 3.5. Asymmetric Key Algorithm

Public key encryption to provide confidentiality and authentication is performed . If confidentiality is required, the sender and the recipient's public key to encrypt , because who has the corresponding private key is the only one that can decrypt the data . This is called secure message format. When it is necessary to authenticate the user , the data will be encrypted with the sender's private key , then anyone with the corresponding public key will be able to decrypt the data . This allows the receiver to know the data has been encrypted person who owns the private key. The message format data encrypted with the private key is known as an open , such confidentiality is not required. As long as there is no copy of the corresponding public key can decrypt the data .

Asymmetric algorithms work much slower than symmetric algorithms , because they use more complicated math to perform its functions, and therefore requires more processing time. With the public key , you can send , rather than tracking a unique key for each of them out of your public key they need to communicate with people .

Below is a symmetric key system advantages and disadvantages:

Advantage

• Better than symmetric key distribution system .

• Better than symmetric system scalability .

• provide confidentiality and authentication is performed .

Shortcoming

• work slower than symmetric systems .

• involve math -intensive tasks .

One of the most commonly used public key algorithm today Rivest - Shamir Adelman (RSA) algorithm , which is 1977 by Ron Rivest, Adi Shamir , and Len Adelman development . RSA is based on integer factorization into prime idea

	Symmetric Encryption	**Asymmetric Encryption**

Functionality	Allows efficient communication between two parties in a closed environment.	Enables security in settings in which symmetric encryption simply does not work or is more difficult to implement.
Computational Efficiency	Computes incredibly fast, since the relatively simple operations used are executed very efficiently.	Computes slowly, using computationally heavy and complex operations, based on the difficulty of solving number-theoretic problems.
Key Size	Uses 128-bit symmetric keys, which are considered very secure.	Employs key sizes of at least 1000 bits to achieve sufficient, lasting security.
Hardware	Performs simple algorithms, requiring relatively inexpensive hardware.	Implements complex and time-consuming algorithms that need more powerful hardware.
Security	No difference. Security is based on the strength of the algorithm and size of the key. Good algorithms exist for both encryption methods and key size effectiveness.	

Table 3.1. Symmetric Encryption vs Asymmetric Encryption

Advanced Encryption Standard (AES) and DES (3DES or) is a common block cipher . AES or 3DES Whether you choose depends on your needs. This section focuses on the differences in safety, performance. 3DES is based on the DES algorithm , and thus , the discussion will focus on the first of DES . DES, developed in 1977 , is designed to work better hardware than software. DES alternative and replacement of all 16 boxes were a lot of bit operations. For example , the switch 30 of the bit 16 is very simple hardware than software . DES encrypted data in 64-bit block size, effectively using a 56 -bit key. 56 key space of about 72 trillion possibilities . While this seems great , but based on today's computing power, it is not enough, and are vulnerable to brute force attacks .

Thus , DES can not cope with the advancement of technology, it is no longer suitable for the realization of a security .

Rijndael algorithm has been selected as the Advanced Encryption Standard (AES), instead of 3DES. AES is a modified version of the Rijndael algorithm. It was submitted to the experts by Joan Daemen and Vincent Rijmen . When considered together, security, performance , efficiency, and flexibility combined with the implementation of the Rijndael algorithm , making it a suitable choice of AES. By design , AES is faster in software, hardware effectively. It works even faster than the AES small devices , such as smart phones, smart cards provide a higher level of security , due to the larger block sizes and longer key lengths . AES uses a 128- bit fixed block size , and with 128 , 192 and 256 -bit key. Rijndael algorithm , in general , have sufficient flexibility to 32 with a minimum of 128 and a maximum of 256 key and any multiple of the block size of the work . Although AES hardware implementation in the speed and efficiency of some abstract advantage over 3DES , 3DES may be faster in some places to support 3DES is relatively mature

3.3. Comparative Analysis of Video Encryption Algorithm

3.3.1. Fully layered Encryption

In this case, the complete contents of the video is first compressed and then encrypted using a standard algorithm, such as DES, RSA, AES encryption, etc. This technique is not suitable for real-time video applications, because a lot of calculations and slow speed to complete.

3.3.2. Selective Encryption

Multimedia is composed of various constraints , for streaming media communications security is a difficult task . Such constraints include real-time processing , non-dedicated channel with limited or different bandwidth and high bit-rate multimedia . Thus, many audio and video multimedia encryption communication is not established in a

conventional encryption algorithm is simple to apply to their binary sequence. It involves careful analysis , to identify and determine the best encryption method.

The current study focused orientation to achieve the desired performance attributes use many standard multimedia formats specific format. This is called selective encryption . This is clearly the preferred type of encryption , compression and decompression algorithms as difficult to keep the required bit rate , even if the algorithm is accelerated by a dedicated hardware . In a few cases , the encryption and decryption algorithms can also be accelerated by hardware . However, the software is often due to its flexibility and low cost preferred. In this video frame is encrypted with the use of selective encryption algorithm , wherein each byte of the video is not encrypted. Selective encryption techniques to save computing capacity , cost , speed, time . Faster compared to the selective encryption , the encrypted data is complete .

Selective encryption can be performed in three ways :

1 . Regional Selective Encryption

2 . Based on selective encryption block

3 . Selective encryption based on chaotic map

Here, the chaotic map data encryption and compression based on selective encryption . In this technique, the encryption process is divided into two first key is generated based on chaos Secondly, selective encryption . In addition, there is no concentration of the selective encryption in the image , however, only a single frame is to be encrypted , and the coding selection .

Chaotic map is designed for a color image , which is an array of 3D design data stream . Because a lot of explosions along the network and transfer the contents to ensure that video content is becoming increasingly important. The traditional approach to encode the data bits of the data stream is encrypted. The algorithm presents several interesting features , such as selective encryption, the main purpose of selective encryption is to reduce the amount of data encryption . General Method for the selective separation of the

two encryption , public part is unprotected and private part, that the protected part . Chaotic map is used to encrypt the input data, which provide security.

3.3.3. Naïve Encryption

Encryption Standard encryption methods use the multimedia stream is often referred to as the existing methods. Naive method is usually applied to text , sometimes for small bit-rate audio, image and video files being sent a quick dedicated channel . The most direct way to each byte in the whole H.264/AVC stream encryption may be performed , such as DES or AES using standard encryption scheme. Thought simple algorithm is taken as the MPEG bit stream and text data without any special care structure .

Naive algorithm provides security interests , the whole H.264/AVC stream every bite is encrypted and did not like to break the Triple DES algorithm or AES. For the large size of the video is not the right solution , because it is a very slow speed in particular , when we use the Triple DES. Delay increases the cryptographic operations and overload would be unacceptable real-time video encryption. Secure Real-time Transport Protocol , or short-term SRTP, is a naive way to apply. In SRTP, multimedia data packets , each packet is individually encrypted using AES . As a naive approach enables the use of traditional password security system at the same level . Unfortunately, the encrypted bit stream is not generally possible higher bit rate multimedia , especially when the transfer is completed with a non-dedicated channels.

Figure 3 shows a logical and immature stages of selective encryption method during execution

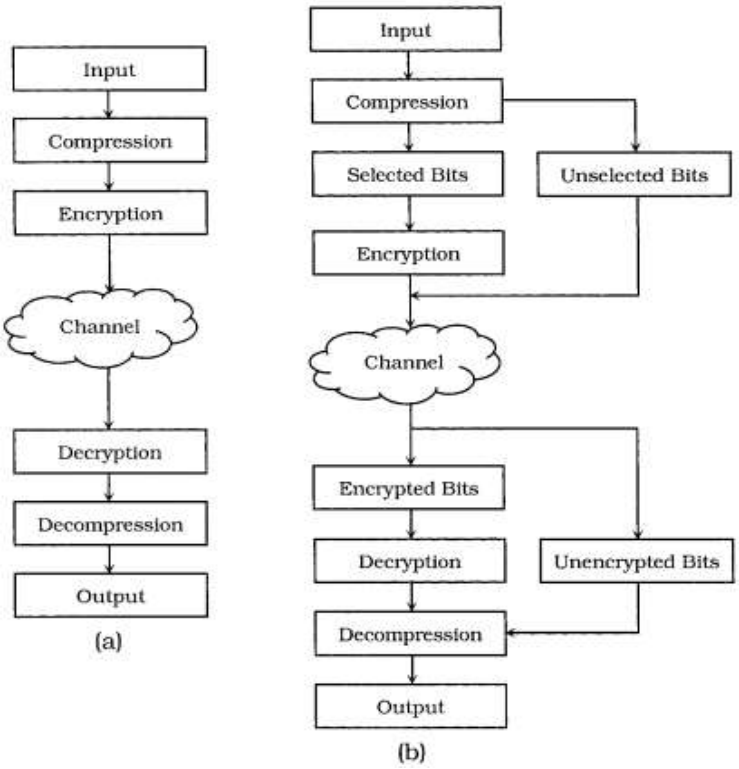


Fig 3.6. Logical Stages during Multimedia Encryption using
(a) Naïve Approach (b) Selective Approach

CHAPTER 4
EXPERIMENTS AND RESULTS

MATLAB is a numerical computing environment and programming language. Creator of The Math Works , MATLAB allows easy matrix operations , functions, and data mapping , algorithm , creating the user interface , and the interface with the program in other languages . Although it specializes in numerical computing , an optional toolbox interfaces with the Maple symbolic engine , making it a complete computer algebra system . It is composed of industry and academia over one hundred million people , in most modern operating systems, including Windows, Mac OS, Linux and Unix running .

Using MATLAB to calculate every aspect of mathematics. Below are some of the most commonly used for mathematical calculations :

- the matrix and array processing
- 2 - D and 3 - D graphics and graphics
- Linear Algebra
- algebraic equations
- nonlinear function
- Statistics
- Data Analysis
- Calculus and Differential Equations
- numerical calculation
- Credits
- Transform
- Curve Fitting
- a variety of other special features

Some basic features of MATLAB as follows :

- This is a high-level language for developing numerical computation , visualization , and applications .

• It also provides repeated exploration, design and interactive problem-solving environment .

• It provides mathematical functions for linear algebra , statistics, Fourier analysis, filtering , optimization, numerical integration and solution of ordinary differential equations vast library .

• It provides a built-in graphical visualization of data and tools for creating custom curve .

• MATLAB programming interface provides a development tool for improving code quality and maintainability and maximize performance .

• It provides for building applications custom graphical interface tools.

• It provides functionality integrated MATLAB based algorithms with external applications and languages , such as C, Java 's , NET and Microsoft Excel.

MATLAB is widely used in science and engineering covers physics, chemistry, mathematics and engineering streams all areas of computing tools. It is used in various applications , including:

• Signal Processing and Communications

• Image and Video Processing

• Control System

• Test and Measurement

• Computational Finance

• Computational Biology

Now, in the MATLAB Image Processing Toolbox provides a comprehensive reference standard algorithms , function, and image processing, analysis , visualization, and algorithm development applications. You can perform image enhancement, image deblurring , feature detection , noise reduction , image segmentation, geometric transformations and image registration . Many toolbox functions are multithreaded to take advantage of multicore and multiprocessor computers advantages.

Image Processing Toolbox supports a different image types, including high dynamic range , Gigabit pixel resolution , embedded ICC profiles, and faults . Visualization capabilities , allowing you to explore the images, check the pixel area , adjust the contrast and create a profile or histogram manipulation of interest (ROI) in the area. And toolbox algorithms can restore degraded image , detection and measurement capabilities , analyze shapes and textures , and adjust the color balance .

MATLAB also provides basic video processing functions using a limited number of short video clips and video formats. The only supported video container MATLAB functions are built-in AVI container , through features such as aviread, AVIFILE, movie2avi and aviinfo. Here , aviread for reading AVI movie to movie and frame storage structure MATLAB , and aviinfo return to the field in a structure as an AVI file that contains information about the argument . In addition, the mmreader used to construct a multimedia object reader can read video data from a variety of multimedia file formats .

Processing video files comprising the steps of :

1 . Frame using an image conversion frame2im .

2 . Any image processing technique used .

3 . The result is converted back to a framework with im2frame .

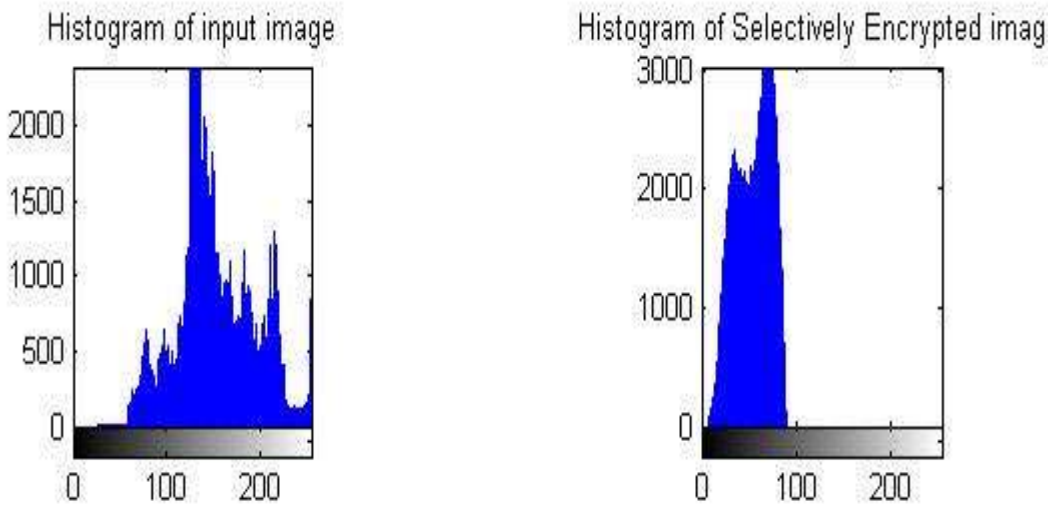
MATLAB function associated with the preparation of video files as follows:

• AVIFILE: then create a new AVI file can be filled in a variety of ways with the video frames.

• movie2avi: Creating a MATLAB movie from AVI files

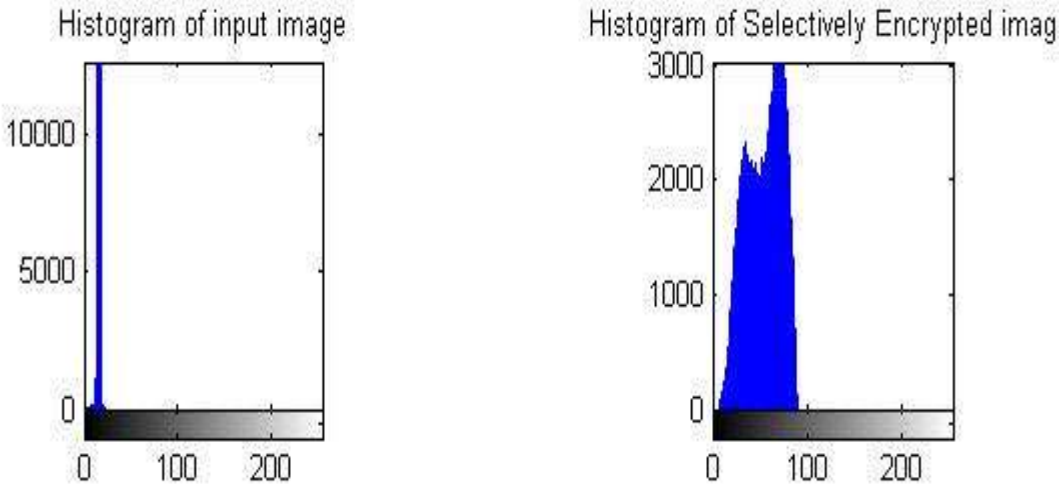
In this experiment comparative analysis of Selective encryption is performed on AVI, DAT & MTS video using MATLAB.

Scenario 1, Here Selective Encryption is performed on 10 frames of an AVI Video format of size 89 KB



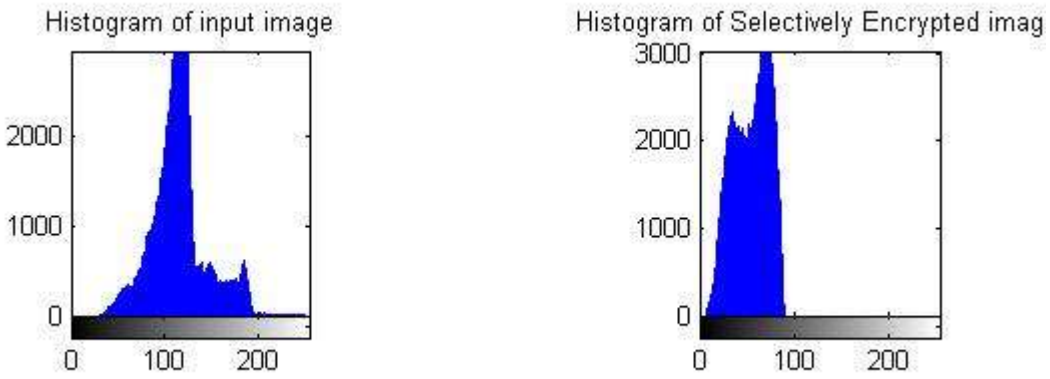
Picture 1. Histogram Results of Selective Encryption of AVI Video

Scenario 2, Here Selective Encryption is performed on 10 frames of an DAT Video format of size 51 KB



Picture 2. Histograms Results of Selective Encryption of DAT Video

Scenario 3, Here Selective Encryption is performed on 10 frames of an MTS Video format of size 3509 KB



Picture 3. Histograms Results of Selective Encryption of MTS Video

CHAPTER 5
RESULT ANALYSIS

In this the results of three types of the video formats are encrypted using selective encryption technique and compared with their respective results.

The results shown in previous chapter are taken after performing chaotic map based selective encryption on monochrome video.

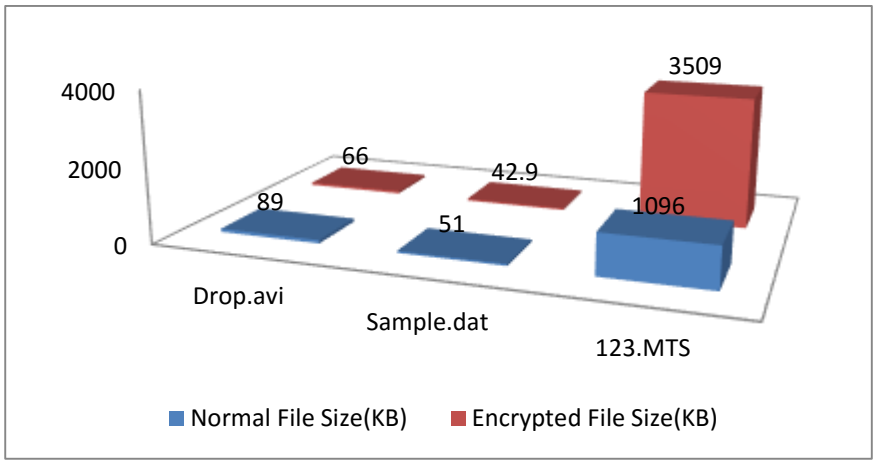
1. In this work in AVI format the normal input video is encrypted using pre-defined chaotic map based selective encryption (symmetric key).
2. In case of DAT format i.e. during encoding we have encrypted video by implementing chaotic map based encryption.
3. For AVCHD video the encryption is performed on using chaotic based video encryption.

The comparison between the results of three video encryptions is as follows:

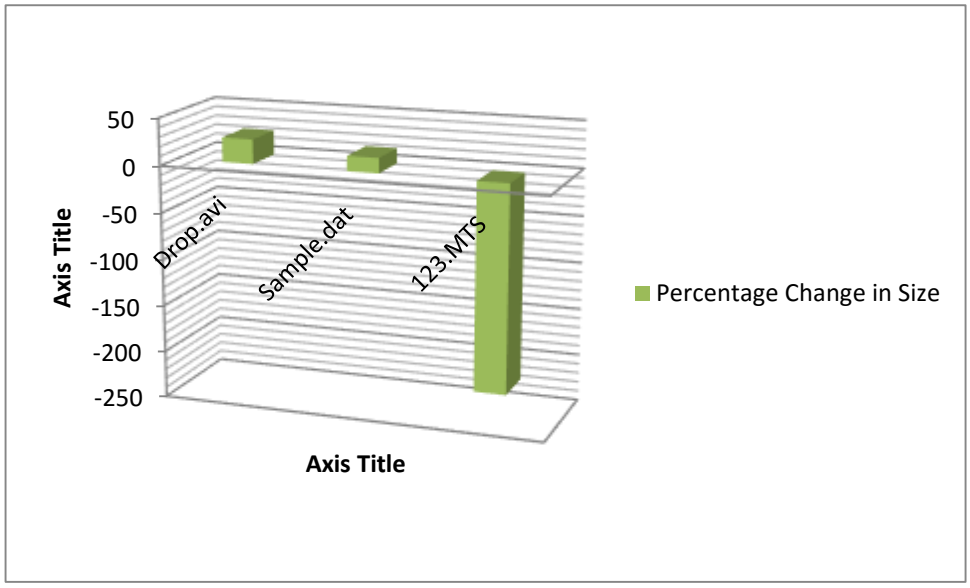
	AVI Format	DAT Format	AVCHD Format
Name of File	Drop.avi	Sample.dat	123.MTS
No. of Frames	10	10	10
Normal File Size(KB)	89	51	1096
Encrypted File Size(KB)	66	42.9	3509
Encryption time	26.009	26.225	30.27

Table 1. Comparison Table of Selective, Layered and Naïve

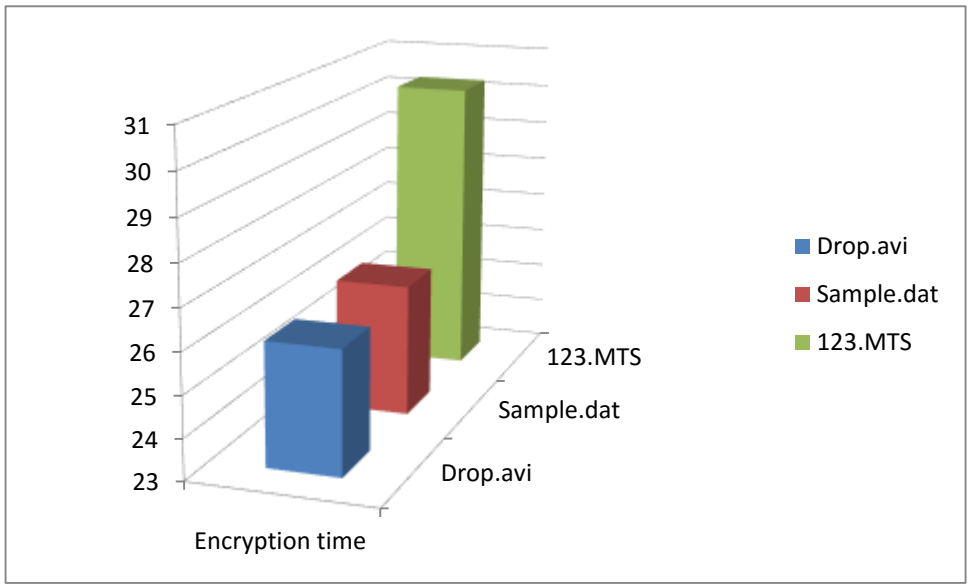
In figure 1, we have compared the size of encrypted video and normal video of all three formats



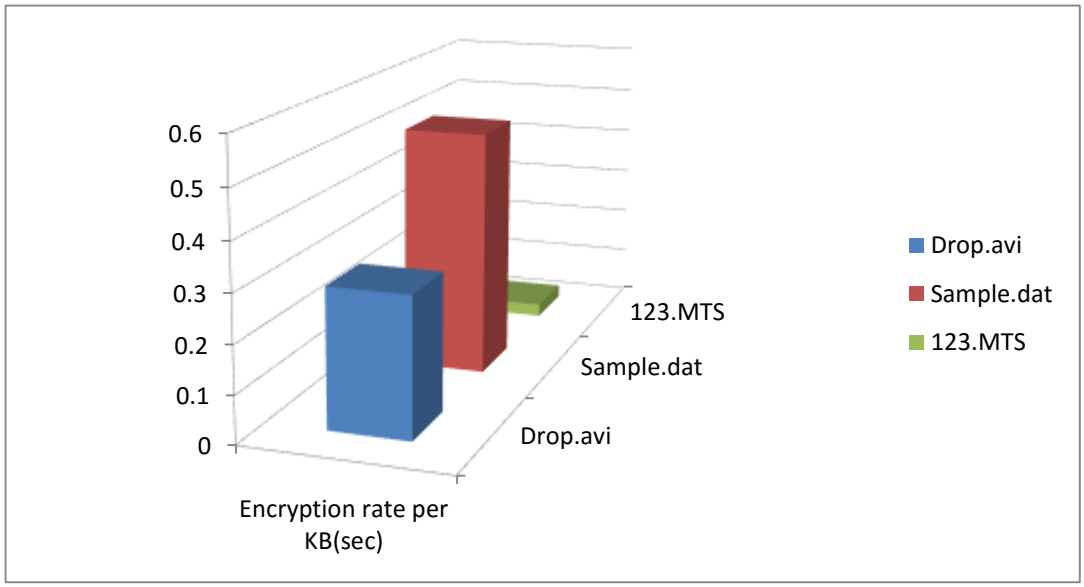
In figure 2, we have compared the percentage change in size of encrypted video with respect to normal video of all three formats



In figure 3, we have compared the time taken for encryption of video of all three formats



In figure 4, we have compared the encryption rate for encryption of video of all three formats



CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1. Conclusion

In this work We take a look at some of the container, and then in some codec. Video file extension usually refers to the container. Several containers , they are almost always tend to use a number of different codecs codecs and other container.
The AVI format, DAT format and AVCHD format are container video formats which are encrypted using chaotic map video encryption technique and results are taken depending upon these analyses, using MATLAB Image and Video Processing Tool.

Analysis of results prove the following points :

1. Encryption of AVCHD increases its size while encryption of other two decreases their size.
2. Encryption rate is least in AVCHD i.e. time taken to encrypt the AVCHD is least in terms of KB
3. Encryption time for AVCHD is most in terms of frames(10 each).
4. AVI video is reduced to 75% during encryption this can save lot of time for transmission

6.2. Future Work

In future this work can further be extended to codec and container codecs too.
These formats can also be analyzed for block based and other video encryption techniques.
New encryption techniques may be devised for reducing the size and encryption rate for the purpose of streaming applications.

CHAPTER 7
REFERENCES

1. Su- Wan park, Sang-Uk shin. " Efficient Selective Encryption Scheme for the H.264/Scalable Video Coding(SVC)" , Fourth International Conference on Networked Computing and Advanced Information Management, Volume 01, pp 371-376 , 2008.
2. Iain Richardson, "An Overview of H.264 Advanced video coding". 2007 white paper. http://www.vcodex.com/files/H.264_overview.pdf (retrieved March 02, 2009).
3. Yuanzhi Zou, Tiejun Huang, Wen Gao, Longshe Huo. Nov, "H.264 video encryption scheme adaptive to DRM". IEEE Transactions on Consumer Electronics, pp. 1289 – 1297, 2006.
4. Lian, S., Liu, Z., Ren, Z., and Wang, Z., "Selective Video Encryption Based on Advanced Video Coding," Lecture Notes in Computer Science, Springer-Verlag 3768, 281–290 (2005).
5. Z. Shahid, M. Chaumont, W. Puech,"Fast Protection of H.264/AVC by Selective Encryption of CAVLC and CABAC for I & P frames", Journal of IEEE transactions on circuits and systems for video technology.
6. A A Muhit, M R Pickering, M R Frater and J F Arnold, "Video Coding using Elastic Motion Model and Larger Blocks," IEEE Trans. Circ. And Syst. for Video Technology, vol. 20, no. 5, pp. 661-672, 2010.
7. A A Muhit, M R Pickering, M R Frater and J F Arnold, "Video Coding using Geometry Partitioning and an Elastic Motion Model," accepted for publication in Journal of Visual Communication and Image Representation.
8. S. Lian, J. Sun, G. Liu and Z. Wang, "Efficient video encryption scheme based on advanced video coding," Multimedia Tools Appl, Vo138, No.1, pp.7S-89, May. 2008.
9. T.Wieg. Draft ITU-T Recommendation H.264 and Draft ISO/IEC 14496-10 AVC. Joint Video Team of ISO/IEC JTC 1/SC29IWG 11 & ITU-T SG16/Q6 Doc.JVT -GO5O, 2003.

10. J Ahn, H. 1. Shim, B. Jeon and I. Choi, "Digital Video Scrambling Method Using Intra Prediction Mode," in Pacific Rim Conf. Multimedia, Tokyo, Japan, pp.386-393, 2004.
11. Lingling Tong, Gang Cao, Jintao Li, “Layered Video Encryption Utilizing Error Propagation in H.264/AVC,” in IEEE Symposium on Electrical & Electronics Engineering (EEESYM), 2012.
12. M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B Zaidan, “Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard,” in International Journal of Computer Theory and Engineering, Vol. 2, No. 2 April, 2010.
13. Jay M. Joshi, Upena D. Dalal, “Selective Encryption using ISMACryp in Real Time Video Streaming of H.264/AVC for DVB-H Application,” World Academy of Science, Engineering and Technology 55 2011.
14. Rajinder Kaur, Er. Kanwalpreet Singh, “Comparative Analysis and Implementation of Image Encryption Algorithms,” International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 2, Issue 4, April 2013, Pg.170-176.
15. Ibrahim S. I. Abuhaiba, Hanan M. Abuthraya, Huda B. Hubboub, Ruba A. Salamah, “Image Encryption Using Chaotic Map and Block Chaining,” International Journal of Computer Network and Information Security, July, 2012, Pg. 19-26.
16. Nidhi S Kulkarni, Balasubramanian Raman, and Indra Gupta, “Selective Encryption of Multimedia Images,” XXXII National Systems Conference, NSC 2008, December 17-19, 2008.