Module 6

CHAPTER 6

Multimedia Security

Introduction

In the modern world, various media types such as text, audio, image and video have managed to enter the network arena. Reasons for this is quicker sharing and acquiring the data in a quicker period of time and this is amply supported by the considerable cheap availability of resources like high bandwidth. This step has raised many challenges opposing the former's success. One of the most challenging issues is the lack of security of the data.

Multimedia is content based. Computer and network security do not sufficiently address the needs of content security because they often process information at the bit-level which does not allow appropriate consideration of the semantics of the information.

Multimedia communication plays an important role in multiple areas in today's society including politics, economics, industries, militaries, entertainment, etc. It is of utmost importance to secure multimedia data by providing confidentiality, integrity, and identity or ownership. Multimedia security addresses the problems of digital watermarking, data encryption, multimedia authentication, digital rights management

Syllabus Topic : Requirements and Properties

6.1 Requirements and Properties

In the field of Multimedia, there is an increased requirement for security, due to various threats which includes replication of digital data without any information loss, and manipulations of the same without any detection. As the utility and usage of the Internet has grown considerably, multimedia documents are easily copied through unauthorized and illegal channels. It is following this reason that the authors of the work hesitate to publish their work electronically, fearing the threat that it can be pirated easily.

Once the information or the content is acquired by miscreants, it can be easily modified by employing some specific software tools and further, can be claimed by them as their own work. This is definitely a horrendous act

that has subsequently wasted the efforts and hard-work put in by the original author, depriving them from getting due rewards and honour for the same.

In order to put things in its place, there should be some mechanism which would uniquely sort out the problem by identifying the document and its owner. The mechanism ought to be convincing enough in providing evidences of a document's ownership and substantiate it by providing credible proof. The mechanism should be able to trace the spots where leaks have occurred and to map out all the modifications that have been done to the document. It should also take into consideration the problem of modification of the data by any of the third party or un-authenticated clients, as it forms the root cause for fake ownership.

Threats are the conditions of possible specific actions that are enforced over the document that makes it counterfeit and illegal, as against the wishes of its owner or creator. The most important threats which ought to be handled to ensure the security of the multimedia system are :

- **Threat of confidentiality :** This threat represents the possibilities of accessing the data or document via unauthorized channels. With the growing usage of Internet, the chance of its occurrence is highly likely and is hard to get it dispelled out, unless effectively addressed.
- **Threat of integrity :** This is a threat to the content of the document by unauthorized entities, where the resource can be altered without any detection.
- **Threat of availability :** This threat highlights the condition where a person, who is not supposed to possess a document, actually has it, by obtaining the same through illicit channels.

Fig. 6.1.1 : Security triad

Some of the important security requirements that have to be implemented in ensuring an approximate fool-proof security are :

- **Confidentiality :** This requirement emphasizes the permit of only authorized access to the document or content and prevents the unauthorized access of resources. Cryptographic mechanisms are used to prevent the unauthorized access of resources. Private-key and public key crypto systems are use to achieve confidentiality. However, after decryption, unauthorized access cannot be prevented.
- **Data Integrity :** It is required by this security requirement that the data be identically maintained from its source to destiny, and has not been accidentally or maliciously modified, altered, or destroyed, and remain unchanged right throughout the operations such as transfer, storage, and retrieval.

- The modification of the information can be detected by using one-way hashing function and digital watermarking. In one-way hashing function encrypted information can be easily calculated from the given input by applying a hash-function. But in reality, it is virtually not possible to compute the actual information from the encrypted one.
- Also, the hash function is non-inverseable and hence this combined with other techniques can be used for maintaining data integrity. In digital watermarking technique, the embedded message is robust to alterations, i.e. even if the original document is altered; the watermark embedded in the document remains as such. If it is altered, then it will affect the actual information also.
- **Data Origin Authenticity :** When a document is found, the origin of that resource should be traceable. The origin of the resource can be traceable by using message authentication code, digital signature and watermarking, from which the exact identity of the person, to whom the document belongs, can be identified.
- **Entity Authenticity :** Entities participating in the communication should prove that they are the one they claim to be. This proves that the communication is carried out between the correct entities. response protocol is used to ensure that the communication is carried out between the correct entities.
- In this protocol, the time-variant challenge is provided to the participating entity, which proves its identity by giving proper response using the secrete key associated that entity.
- **Non-Repudiation** It should be possible to detect and prove the rightful ownership of that document. Many authors are worried about distributing their works in fear that it may be copied illegally or represented as another's work. Non-repudiation facilitates the identification of the end users who have copied the document.
- The rightful ownership of that document should be detected and proven. Non-repudiation facilitates the identification of the end users who have copied the document. The rightful ownership of that document can be detected and proven.

Syllabus Topic : Mechanisms - Digital Signatures, Steganographic Methods

6.2 Security Mechanisms

Security mechanisms are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service.

Examples of common security mechanisms are as follows :

- Cryptography
- Digital Signatures
- Steganography
- Watermarking

6.2.1 Digital Signatures

- A digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.
- A Digital Signature is a type of signature, but the only difference is that it involves the use of mathematical pin or algorithm to sign and validate the authenticity of a document, file or software instead of pen and paper. Digital signatures rely on certain types of encryption to ensure authentication.
- A digital signature is used to make sure that the file(s) sent digitally belongs to a designated source and reaches the intended receiver in its original format without any tampering. In simple terms, a digital signature works in the same way as an envelope seal does.
- Imagine wanting to send a physically signed document from one country to another. You would need to send the documents by means of a courier. This process involves loads of paperwork and thereby wasting invaluable time. Instead, if you had just used a digital signature, the documents could have been sent electronically in a matter of minutes. This way you can save time as well as money. Numerous studies conducted around the world show that using digital signatures can save a whole working week for any working professional. The time saved combined with the undeniable savings in money is surely going to fuel the rapid acceptance of digital signatures around the world.

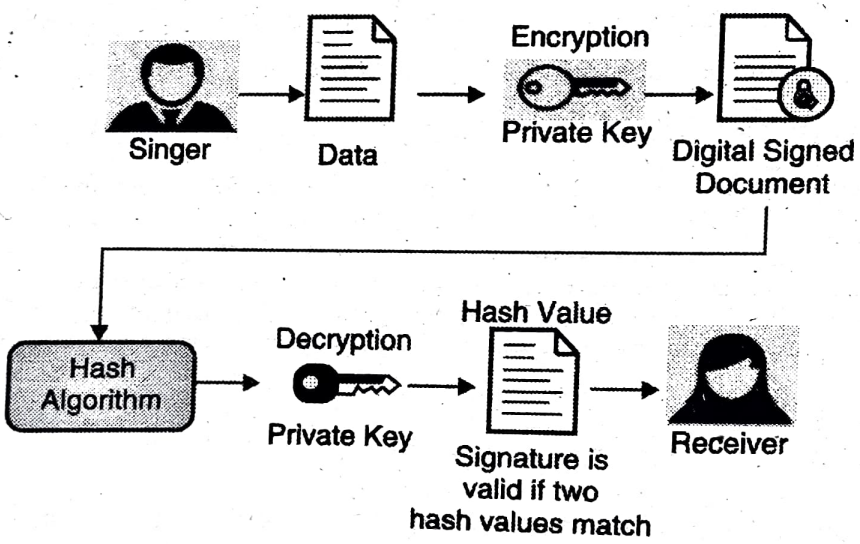

Fig. 6.2.1

How does a Digital Signature Work?

- Digital signatures are based on Public Key infrastructure. By this mechanism, two keys are generated, a Public Key and Private Key. The private key is kept by the signer and it should be kept securely. On the other hand, the receiver must have the public key to decrypt the message.

- For example, a person named Tulshiram wants to send an encrypted message to Poonam. As stated above, Tulshiram must have a private key to sign the message digitally.
- Before encrypting the message using the private key, an algorithm named 'MD algorithm' encrypts the message to be sent by Tulshiram into a 128/256-bit format known as a hash value. Then Tulshiram's private key encrypts this hash value. On completion of both the processes, Tulshiram's message is said to be digitally signed.
- On the side of Poonam, the digitally signed message is decrypted with the help of the signer's public key. The public key decrypts the message and converts it into another hash value. Then the program which is used to open the message (e.g., MS Word, Adobe Reader etc.) compares this hash value to the original hash value which was generated on Tulshiram's side. If the hash value on Poonam's side matches with the hash value generated on Tulshiram's side, then the program will allow the message to open up and displays the message "The document has not been modified since this signature was applied." The program will not allow the document to open if both the hash values don't match.

6.3 Steganography

- Steganography is a useful technique for hiding data behind the carrier file such as image, audio, video etc. and that data securely transfer from sender to receiver. The cryptography is also another technique which is used for the protecting information.
- The Combining encryption methods of cryptography and steganography enables the user to transmit information which is masked inside of a file in plain view. This will provide more security to transferring data.
- The Steganography is an ancient art of hiding information. It refers to the science of "invisible" communication. Steganography is defined as the art and science of communicating in a way which hides the existence of the communication.
- The art of hiding information in ways that prevent the detection of hidden messages. Transmitting secret messages through innocuous cover carriers in such a manner that the existence of the embedded message is undetectable. E.g Invisible inks, character arrangement, covert channels etc.
- Hiding information within electronic media requires alternations of the media properties that may introduce some form of degradation or unusual characteristic.

6.3.1 Steganographic Categories

Steganography is classified into three categories, Pure Steganography, Secret Key Steganography and Public Key Steganography.

- **Pure steganography** does not require the exchange of a cipher such as a stego-key. It assumes that no other party is aware of the communication.
- **Secret key steganography** where the secret (stego) key is exchanged prior to communication. This is most susceptible to interception. Secret Key Steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message.
- **Public key steganography** where a public key and a private key is used for secure Communication. The sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public Key Steganography provides a more robust way of implementing a steganographic system because it can utilize a much more robust and researched technology in Public Key Cryptography.

6.3.2 Types of Steganography

- The process of steganography technique can be defined into 4 categories such as Text, Image, Audio and Video. In text steganography text files are used to hide data. Here in this system the confidential data can be of any format like text, audio, video or image.
- The cover is a file in which the data is hidden is a text file. Technique used to achieve confidentiality is LSB (Least Significant Bit) i.e. modifying least significant bit of the cover file.
- In image steganography image files like Bit Map Picture (BMP), PNG (Portable Network Graphics), JPEG (Joint Picture Expert Group), TIFF (Tagged Image File Format) etc. are used to hide data. Technique used to achieve confidentiality are LSB (Least Significant Bit), spread spectrum etc.
- In audio steganography sound files like AVI (Audio Video Interleaved), MPEG (Moving Picture Expert Group), FLV (Flash Video) etc. are used to hide data. Techniques used to achieve confidentiality are LSB, spread spectrum etc.
- The best format is wave format since the reading of the bits of data is easier in wave file, also the compression is good in wave files and the distortion of data is very less in wave files.
- In video steganography video files like AVI, MVI, DAT etc. are used to hide data. Techniques used to achieve confidentiality are LSB, spread spectrum, ecliptic curve method etc.

1. Image Steganography

- The image steganography is used to hide a secret message inside an image. The most widely used technique to hide secret bit inside the LSB of the cover image. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24 bit color image, a bit of each of the red,

green and blue color components can be used, so a total of 3 bits can be stored in each pixel in this way we can use more secret bit to hide data in it.

- In image steganography image files like BMP, PNG, JPEG, TIFF, GIF etc. are used to hide data. Technique used to achieve confidentiality is LSB, spread spectrum etc. In Spatial Domain Embedding steganography algorithm is based on modifying the least significant bit layer of images. This technique makes use of the fact that the least significant bits in an image could be thought of random noise and changes to them would not have any effect on the image.
- The message bits are permuted before embedding, this has the effect of distributing the bits evenly, thus on average only half of the LSB will be modified. Popular steganographic tools based on LSB embedding vary in their approach for hiding information. Some algorithms change LSB of pixels visited in a random walk, others modify pixels in certain areas of images, or instead of just changing the last bit they increment or decrement the pixel value.

2. Audio Steganography

- The sender embeds secret data of any type using a key in a digital cover file to produce a stego file, in such a way that an observer cannot detect the existence of the hidden message. In many schemes a method of audio steganography based on modification of least significant bits (LSB) the audio samples in the temporal domain or transform domain have been proposed.
- Some of these methods employ LSB technique and combine it with other techniques such as error diffusion, minimum error replacement (MER) and temporal masking effect. Another method embeds covert messages in the LSB of wavelet transform and recently in the integer transform. The main objectives of the LSB based schemes are to raise payload or the maximum amount of the information to be embedded and to prevent audio quality degradation. The best format is wave format since the reading of the bits of data is easier in wave file, also the compression is good in wave files and the distortion of data is very less in wave files.
- In Phase coding technique the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. The basic Spread Spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. The SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal.

3. Video Steganography

- Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too.

- The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. The video steganography is nothing but a combination of image and audio steganography.

6.3.3 Steganographic Methods

Steganography methods can be classified mainly into Substitution, Transform domain, Statistical and Distortion.

- Substitution methods substitute redundant parts of a cover with a secret message.
- Transform domain techniques embed secret information in a transform space of the signal.
- Statistical methods encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.
- Distortion techniques store information by signal distortion and measure the deviation from the original cover in the decoding step.

6.3.3(A) Substitution Methods

1. Two component based LSB

- Two component based LSB is a secured robust approach of information security. It presents two component based LSB (Least Significant Bit)methods for embedding secret data in the LSB's of blue components and partial green components of random pixel locations in the edges of images.
- An adaptive LSB based steganography is proposed for embedding data based on data available in MSB's of red, green, and blue components of randomly selected pixels across smooth areas. It is more robust as it is integrated with an Advanced Encryption Standard(AES).

2. Pixel Intensity based steganography

- Pixel Intensity based technique makes use of RGB values of colour images to enhance imperceptibility. In the three channels RED, BLUE, GREEN the LSB of any one of the 3 channels is used as a pointer to decide embedding capacity in the other two channels. In the randomization technique, the LSB of any one of the channels (RGB) are used to indicate how data has to be hidden in the remaining 2 channels.
- If the last two bits of the channel are 00 there is no hidden data, if it is 01 data is embedded only in channel 2, if it is 10 data is embedded in channel 1 and if it is 11 data is embedded in both the channels. Three methodologies are used. They are,
  1. RED is used as default pointer.
  2. User selects any channel as pointer.

3. Pointers are chosen based on a cyclic sequence and data is embedded. Images were taken and same size data is embedded using all methodologies.

- Based on the histogram study and the values of MSE and PSNR (Mean Square Error and Peak Signal to Noise Ratio) the 3rd method i.e. the randomized method has better secrecy and performance with enhanced embedding capacities.

6.3.3(B) Transform Domain Methods

1. Multiple secret images are hidden in a cover image using IWT

This method uses two gray scale images of size 128 × 128 that are used as secret images and embedding is done in RGB and YCbCr domains. The quality of stego images is good in RGB domain by comparing the PSNR values. Integer Wavelet Transform (IWT) is used to hide secret images in the color cover image. The cover image is represented in the YCbCr color space. Two keys are obtained, encrypted and hidden in the cover image using IWT.

2. Using Image Steganography to Establish Covert Communication Channels

This method shows use of image steganography to breach an organization's physical and cyber defences. This method utilizes computer vision and machine learning techniques to produce messages that are undetectable and if intercepted cannot be decrypted without key compromise. To avoid detection DWT (Discrete Wavelet Transform) is used. The goal of a computer vision system is to allow machines to analyze an image and make a decision as to the content of that image. The computer vision can be categorized as Model-Based and Appearance Based which uses example images and machine learning techniques to identify significant areas or aspects of images that are important for discrimination of objects contained within the image. Machine learning is different from human knowledge/ learning. A computer has to make decision of the presence of a face based on the numbers contained in a 2D matrix. The feature is identified by using Haar feature selection. The goal is to identify the set of features that best distinguishes between images in the different classes. In this method the cover image does not contain a secret message, rather the classification of the image yields the hidden message. Since the proposed algorithm utilizes ordinary unmodified images, there are no inherent indicators of covert communication taking place.

6.3.3(C) Statistical Methods

A lossless data hiding

- A lossless data hiding which is robust against JPEG / JPEG 2000 compression. The image is split into 8 × 8 blocks and each block is split into two subsets (A, B).

- For each block the difference value α is calculated where α is the arithmetic average of differences of pixel pairs within the block. This α is selected as a robust quantity for embedding the information bit. Each bit of the secret message is associated with a group of pixels e.g. A block in an image.
- The bit embedding strategy used is as follows, if α is located within a threshold and to embed bit 1, shift α to right/left beyond a threshold by adding/subtracting a fixed number from each pixel value within one subset. To embed 0, the block is intact. If α is located outside the threshold, always embed 1 thus shifting the value α away beyond a threshold. Then error correction code is applied.

6.3.3(D) Distortion Methods

Image blurring with sequential LSB embedding

- In this method image restoration technique is used. The image is blurred before hiding the message image using special point spread function and randomly generated key. Sequential LSB embedding in the R plane is done in this project.
- The number of rows and columns of the message image is encrypted in the first row of the cover image. Before inserting, the original message image is blurred using the specific PSF (Point Spread Function). The parameters used for blurring with PSF are used as keys during deblurring.
- The secret key values are sent through a secure channel (Tunnelling). The secret image is recovered using the two keys and a third key, which is randomly generated and depends on the content of the hiding message.

6.4 Multimedia Application

Multimedia can be used for entertainment, corporate presentations, education, training, simulations, digital publications, museum exhibits and so much more. With the advent multimedia authoring applications like Flash, Shockwave and Director amongst a host of other equally enchanting applications, your multimedia end product is only limited by your imagination. Multimedia is imperative, not only to bring life to your presentation with its captivating images and special effects, but also to create a unique multimedia solution that matches your impeccable tastes as well as your corporate requirements.

6.4.1 Distributed Multimedia Systems

A distributed multimedia system comprises several types of components, such as media servers, meta-databases, proxies, routers and clients. In addition, a large number of adaptation possibilities exist, from simple frame dropping up to virtual server systems that dynamically allocate new resources on demand. The main problem is determining which kind of component can best be used for each kind of adaptation.

The following non-exhaustive list gives an overview of the tools and their major features :

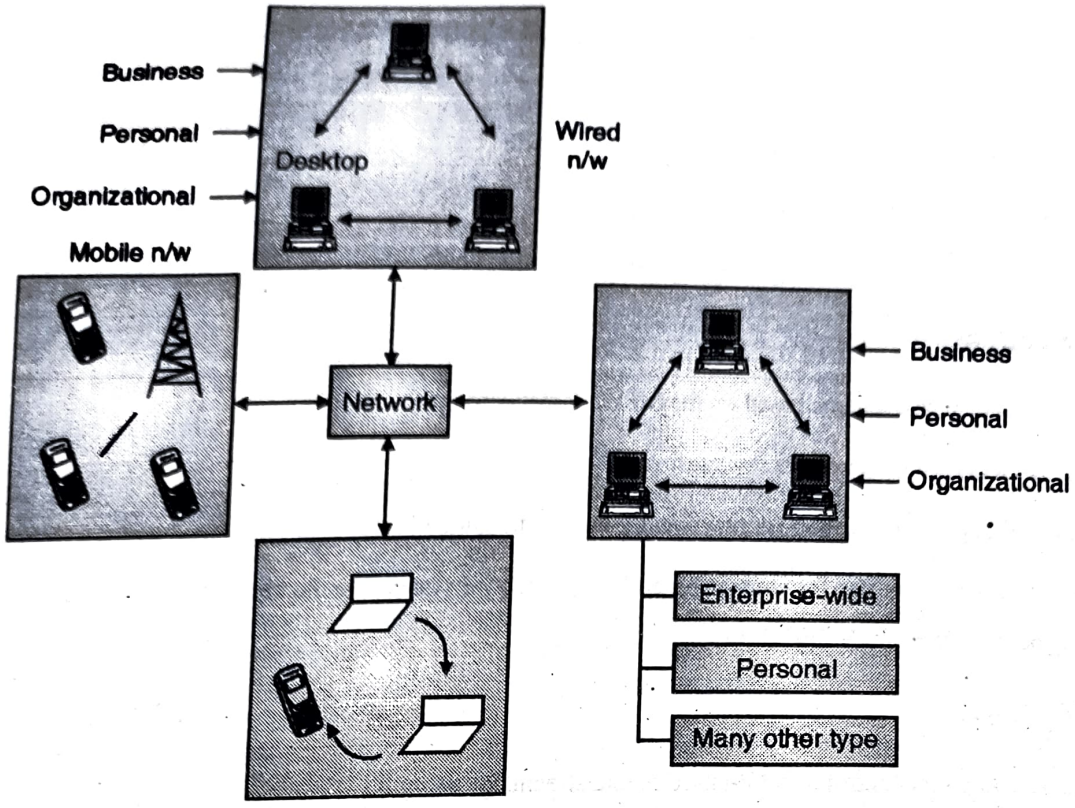

Fig. 6.4.1 : Distributed multimedia system

1. Media Server

- Standard compliant media streaming by using RTSP and RTP/UDP.
- Communicates terminal capabilities of the client device and user preferences using standardized MPEG-21 descriptors.
- Supports real-time adaptation of media content according to the clients' terminal capabilities, the user preferences, and the available network resources; for example, mobile devices get a lower stream quality than high-performance workstations with good network access.
- Implements standardized RTP extensions to allow intelligent retransmission of lost video frames where necessary.
- Can be run in a distributed environment that supports proactive service and content replication and migration operations; this is especially helpful when content adaptation steps are not allowed due to legal constraints or the user insists on the original stream in its full quality.
- Supports proactive adaptations by actively measuring and forecasting available server and network resources on and between server nodes.

2. Proxy Server

- Incorporates both a server and a client implementation (since a proxy must act as a server to the client and a client to the server).
- Caches elementary streams in different quality versions.
- Implements quality-aware replacement strategies.
- Can be dynamically relocated in the vicinity of requesting clients.

3. Meta-database

- Multimedia database schema based on the MPEG-7 standard.
- Multimedia indexing framework.
- Cost-based query optimization for range and k-nearest neighbour searches.
- Application-level libraries for content-based image retrieval systems, audio recognition tools, video browsing tools, and quality aware MPEG-4 proxies.

4. Media Player

- Standard compliant control of RTP-based media streams by using RTSP.
- Supports parallel presentation of many videos in different viewers, in different qualities.

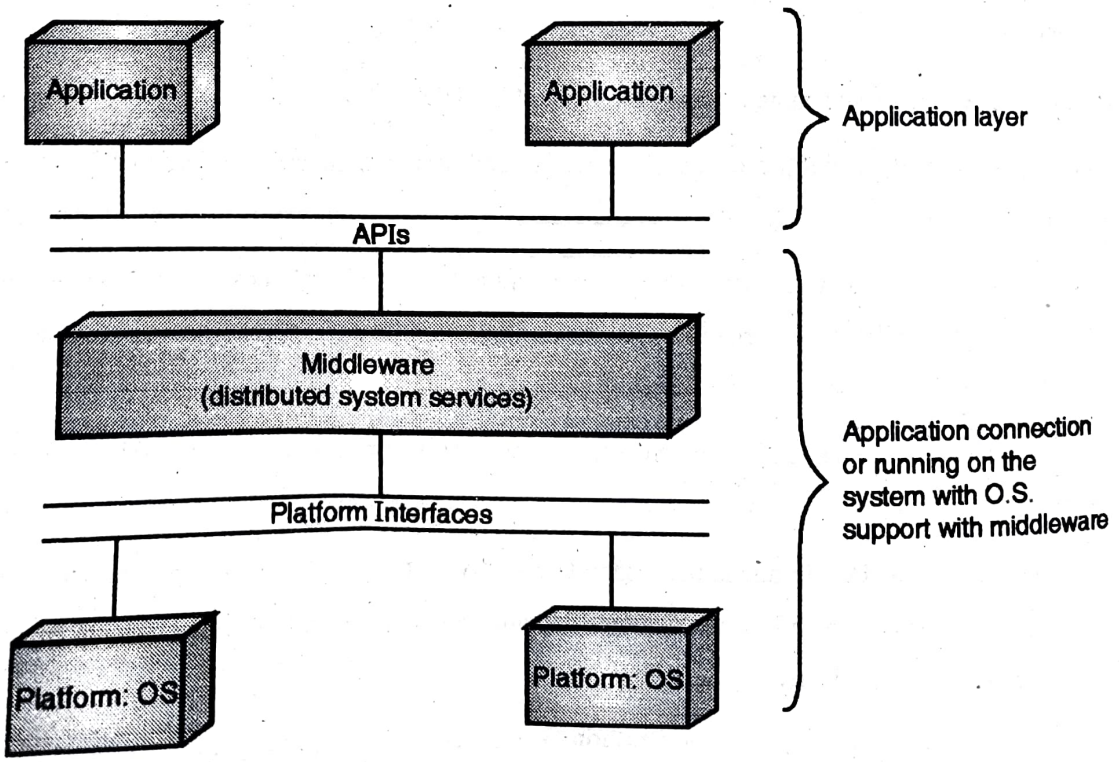

Fig. 6.4.2 : Various layer of DMS

Components of a Distributed Multimedia System

- Distributed multimedia system consists of three different basic components: an Information server, a wide area network and a multimedia client on the user site. The user interface or the multimedia client deals with the issues related to presentation and manipulation of multimedia objects and the interaction with the user.
- Multimedia client consists of a computer with a special hardware such as a microphone, high-resolution graphics display, stereo speakers, and a network interface. The user interacts with the system via a computer keyboard, mouse or a hand held remote control. The network provides the communication mechanism between the user and the server. The multimedia traffic requires transfer of large volumes of data at very high speeds, even when the data is compressed. Continuous media as video and audio require guarantees of minimum bandwidth and maximum end-to-end delay (jitter).
- The server is responsible for managing multimedia databases and also composing general multimedia objects for the user. The composition of the object is a complex process of integrating and synchronizing multimedia data for transport, display and manipulation.
- The system usually consists of multiple users, servers and networks as shown below :

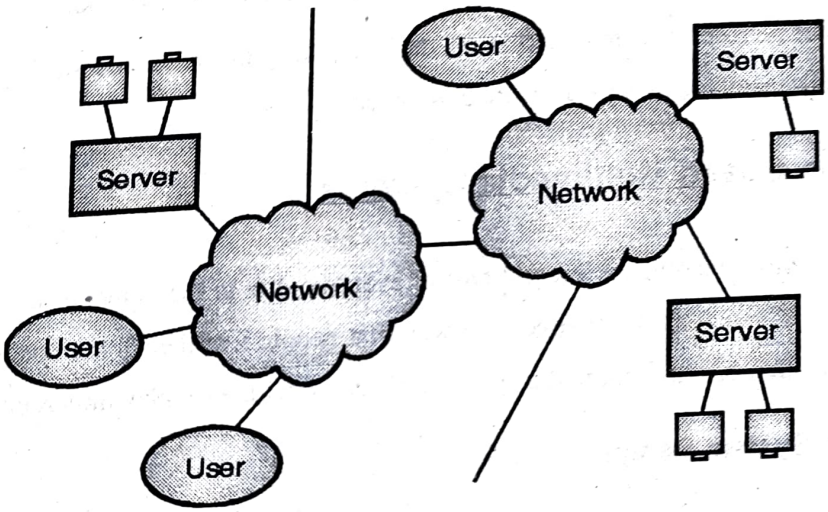

Fig. 6.4.3 : Component of distributed multimedia system

Now let us discuss each of these components in some detail.

I. User Terminal

- A Multimedia terminal consists of a computer with a special hardware such as a microphone, high-resolution graphics display, stereo speakers, and a network interface. The user interacts with the system via a computer keyboard, mouse or a hand held remote control. Many of the user terminals still resemble traditional computers. Because of this, additional development work is required before the terminals can meet the requirements of the multimedia data and the user.

- Because of the large size of the multimedia objects and real - time requirements the multimedia terminal or the network should include large data buffers. To restore the temporal relationship of a data stream, stream handlers should be connected to the data buffers. To synchronize the possible multiple data streams and to control the stream handlers, a synchronization and streaming manager is required. Since multimedia data objects are large, the terminal should also include compression and decompression hardware.

ii. Network and Communication

- Multimedia communication differs from the traditional communication. The multimedia traffic requires transfer of large volumes of data at very high speeds, even when the data is compressed.
- Especially for interactive multimedia communication the network must provide low latency. Continuous media as video and audio require guarantees of minimum bandwidth and maximum end-to-end delay. The variation in delay referred to as jitter, and loss of data must also be bound.

iii. Multimedia Server

- Current personal computers, workstations and servers are designed to handle traditional forms of data. Their performance is optimized for a scientific or transaction – oriented type of workload.
- These systems do not perform well for multimedia data, requiring fast data retrieval and guaranteed real time capabilities. The I/O capacity is usually a severe bottleneck.

6.4.2 Information Based Multimedia Systems

Information Systems have become an integral part of everyday life in the home, businesses, government, and organizations. Information Systems have changed the way that people live their lives, conduct business, even run the government. In Information based multimedia system artificial intelligence play important role.

Intelligent Multimedia System Design

Intelligent multimedia system consist of following :

- Language parsing and generation that processes and support synchronized multimedia input and output streams.
- Knowledge representation and inferencing to provide reasoning ability.
- Knowledge bases and models to provide a basis for its decision making ability.
- Automated knowledge based medium selection and formulation of responses.

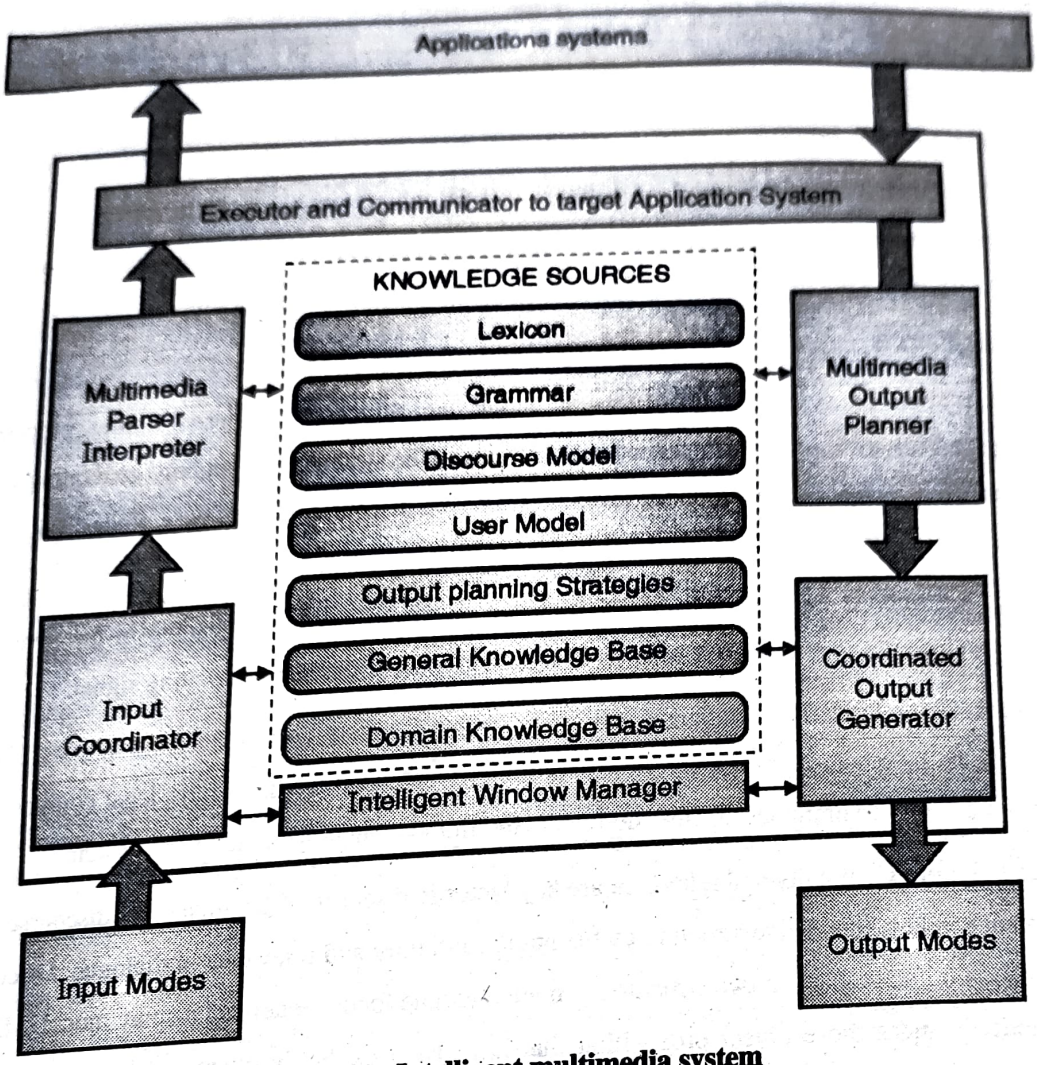

Fig. 6.4.4 : Intelligent multimedia system

Each block in intelligent multimedia system is described below :

- **Input Modes :** Intelligent multimedia system accepts inputs from three input devices namely, speech input device, keyboard and mouse device pointing to objects on the graphics display.
- **Output Modes :** Intelligent multimedia system produces output for three output devices namely, high resolution graphics display, monochrome display and speech output device.
- **Input Coordinator :** this module accepts inputs from input devices and fuses the input streams into a single compound streams maintaining temporal order of tokens in the original streams.
- **Multimedia Parser Interpreter :** It is a augmented transition network that has been extended to accept the compound stream produced by Input Coordinator and produce an interpretation of this compound stream.

- **Executor and Communicator to target Application System :** It is used to take appropriate action. Action may be a command to the mission planning system, database query, or an action that entails participation of the system interface only.
- **Multimedia Output Planner :** It is a generalized ATN that produces a multimedia output stream representation with component targeted for different devices.
- **Coordinated Output Generator :** It translate output representation into visual /auditory output. It is also responsible for producing the multimedia output in a coordinated manner in real time.
- **Knowledge Sources**
- Intelligent multimedia system includes several knowledge sources to be used during processing. The knowledge sources are used for both understanding inputs to the system and planning/ generating output from the system. Knowledge sources includes lexicon, grammar, discourse model, user model, output planning strategies, general knowledge base, domain knowledge base
- **Lexicon :** a lexicon is the collection of all the token or signal that carry meaning in the given language. Intelligent multimedia system lexicon consists of words, graphics figures, and pointing signal.
- **Grammar :** Grammar defines the language used by system for multimedia inputs and outputs. The grammar defines how the morphemes, tokens and signals of the lexicon can combine to form legal composite language structures. Lexicon and grammar together define the multimodal language used by the system.
- **Discourse Model :** Continuity and relevance are key factor in discourse. The attentional discourse focus space representation is key knowledge structure that support continuity and relevance in dialogue. Discourse model representation of focus space in two structures : main dialogue focus model and display model. Main dialogue focus model includes those object proposition that have been explicitly expressed by user. Display model represent all the objects that are in focus because they are visible on one of the monitors.
- **User Model :** relevant aspects of user in human-computer interaction is his level of expertise in current task. Aspect of user modeled in intelligent multimedia systems user model are (1) the degree of importance that user attaches to the different object types as function of task, which is called as entity rating system. (2) the stage of current task on which the user is currently engaged.
- **General Knowledge Base :** general information includes words knowledge applicable across different task domains. These include information concerning the visual presentation or verbal expression of the objects. General knowledge base includes words and symbols used to express an object, which symbol are appropriate under which condition and when particular colors is used
- **Domain Knowledge Base :** Domain knowledge is representation of different types of mission plans that the user would be engaged in constructing. The domain knowledge base includes a model or structure to represent each type of mission plan and the component of each type of plan.

- **Intelligent Window Manager :** It does function of window placement, window removal, window layout and window sizing.

6.4.3 Conference Systems

- Each day, enterprises, governments, educational institutions, healthcare organizations, financial institutions and others are striving to be more productive and effective in their businesses. Video conferencing has become integral to their successfully achieving those goals. Yet video conferences must be secure and video participants must feel protected when sharing sensitive information during a video call.
- A video conference is a live, visual connection between two or more people residing in separate locations for the purpose of communication. At its simplest, video conferencing provides transmission of static images and text between two locations. At its most sophisticated, it provides transmission of full-motion video images and high-quality audio between multiple locations.
- Video conferencing should support encryption, and so there is a greater risk of sensitive data falling into the wrong hands. Other, more modern systems, like Webx and Google Hangouts, transmit data through a router or other server where it is decrypted and stored before being delivered. Encryption capabilities have advanced greatly, meaning there is no reason for security conscious companies to use unencrypted or outdated systems. Encryption of stored video means that in the event of unauthorized access to video files, this won't result in exposure of sensitive data.
- Consumer services like Apple's FaceTime, Google's Hangouts and Microsoft's Skype have made video conferencing ubiquitous on desktops and mobile devices that have an embedded camera.
- In the business world, desktop video conferencing is a core component of unified communications applications and Web conferencing services, while cloud-based virtual meeting room services enable organizations to deploy video conferencing with minimal infrastructure investment.
- For businesses, the tangible benefits of video conferencing include lower travel costs especially for employee training and shortened project times as a result of improved communications among team members.
- The intangible benefits of video conferencing include more efficient meetings with the exchange of non-verbal communications and a stronger sense of community among business contacts, both within and between companies, as well as with customers.
- On a personal level, the face-to-face connection adds non-verbal communication to the exchange and allows participants to develop a stronger sense of familiarity with individuals they may never actually meet in person.

6.4.4 Virtual Reality

☞ Virtual reality (VR)

- Is a term that applies to computer-simulated environments that can simulate physical presence in places in the real world, as well as in imaginary worlds. Most current virtual reality environments are primarily visual experiences, displayed either on a computer screen or through special stereoscopic displays, but some simulations include additional sensory information, such as sound through speakers or headphones.
- Some advanced, haptic systems now include tactile information, generally known as force feedback, in medical and gaming applications. Furthermore, virtual reality covers remote communication environments which provide virtual presence of users with the concepts of telepresence and telexistence.
- Users can interact with a virtual environment or a Virtual Artifact (VA) either through the use of standard input devices such as a keyboard and mouse, or through multimodal devices such as a wired glove, the Polhemus, and omnidirectional treadmills.
- The simulated environment can be similar to the real world for example, in simulations for pilot or combat training or it can differ significantly from reality, such as in VR games. In practice, it is currently very difficult to create a high-fidelity virtual reality experience, due largely to technical limitations on processing power, image resolution, and communication bandwidth; however, the technology's proponents hope that such limitations will be overcome as processor, imaging, and data communication technologies become more powerful and cost-effective over time.
- Virtual reality is often used to describe a wide variety of applications commonly associated with immersive, highly visual, 3D environments. The development of CAD software, graphics hardware acceleration, head mounted displays, database gloves, and miniaturization have helped popularize the notion.

☞ Multimedia and Virtual Reality

- **Multimedia (MM) :** Computer systems allowing for integrated access to a range of data through the means of stiimulating human senses using digital technologies
- **Virtual Reality (VR) :** Computer systems able to combine a mixture of real world experiences and computer generated material to allow for simulated real world representation
- From a Geographical Information System (GIS) perspective MM and VR are the means to an end - handling (integrating, storing, accessing and viewing) a multitude of spatial data using a variety of tools. Can be considered under the general heading of visualisation : methods therefore vary depending on whether usage is for private investigation or for public demonstration; whether data is accessed interactively or in a pre-

determined manner; and whether there is data investigation and interrogation or whether mere presentation suffices.

- **Virtual Reality data**

VR addresses the construction of artificial worlds, with clear spatial dimensions databases for VR can structure and store data using methods beyond the conventional abstractions of GIS.

- **Virtual Reality tools**

- Under computer control allowing access to the artificial worlds with internet viewers, VR navigators and dedicated stand-alone hardware stations.
- The hardware components of a multimedia and/or a Virtual Reality PC or workstation
- Multimedia requires perception and interaction with use of visual and auditory participation, i.e. the production of vision and sound, Virtual Reality additionally requires tactile and vestibular participation.
- A Virtual Reality system may be considered to be an expansion of a multimedia system into a multi-sensory system.

The additional components of a Virtual Reality PC or workstation may include any of the following :

- Tactile interaction
  - Head Mounted Display (HMD) - wide field of view, an amoriphically projected stereo.
  - Tactile feedback devices, vibrotactile displays - teletactile feedback glove, virtual joystick.
- Force feedback
  - Teleoperation systems - force feedback joystick, remote manipulator arm, joystring.
- Vestibular
  - Motion platforms - flight simulators, motion simulators.
- Other interactive devices
  - 2 degrees of freedom (DOF) - mouse, joystick, 2-d tablet with gesture recognition, touch screen.
  - 6 degrees of freedom - wand, 6 DOF mouse, data glove, force ball.
  - Wired clothing - datasuit.
  - Biological input (biosensor) - voice recogniser, skin temperature probe, myoelectric (muscle) sensor, cerebroelectric (brain) sensor.

Applications

VR can be used in a GIS in two ways :

- A tool for purely viewing three dimensional models of data.
- This can be purely in an office situation or in the field overlaying three dimensional data on top of real world data.
- Applications of the latter in underground pipe work, user can 'see' network under their feet.
- The whole user interface to the GIS dataset, allowing for the display of VR, MM and standard data in three dimensions.
- This would envolve the creation of a virtual interface.
- Possibility of viewing any data easily from any angle.

Education

- Self-led interaction with the real world, especially for children.
- Introducing geographical concepts, displaying distant 'realities' possibilities, using MM and VR, of the 'virtual fieldtrip'.
- Use of MM for local studies and global geography knowledge building, whilst integrating with other National Curriculum subjects such as history, economics, biology, geology and information technology.

Scientific research

- Creating three and four dimensional views of spatial data.
- Preliminary views of integrated data sets prior to verification of data linkages and casualties MM integration and overlay of datasets, for example; vector data with attribute information on raster satellite imagery.
- Physical geography data, e.g. meteorological, geological, oceanographic data ideally suited to its four dimensional nature, VR applications include environmental monitoring, hazard and risk assessment, atmospheric modelling, planning and forecasting, pollution analysis, terrain visualisation, multi-variate analysis.
- Military for training purposes and scenario building, particularly VR representations of terrain.
- Entertainment improving realism of interaction with spatial data.
- Built environment VR applications in architectural simulation, urban planning, resource modelling.
- Archival of geographic information MM storage of the disparate range of data which can convey geographical information.

Review Questions

Q. 1 Explain requirement and security of multimedia system.

Q. 2 Explain the working of digital signature.

Q. 3 Explain the Steganography types.

Q. 4 Explain the various Steganography methods.

Q. 5 Explain the distributed multimedia system.

Q. 6 Explain Component of distributed multimedia system.

Q. 7 Explain Information Based Multimedia Systems.

Chapter Ends...

❑❑❑