3.1 Authoring Tools

**Intro to authoring tools**

- Multimedia authoring integrates text, audio, images, animations, and video using various software tools.
- Authoring tools provide an environment for organizing and editing multimedia projects.
- They enable the creation of interactive presentations by combining different media elements.
- Two primary target users are professionals and average business users.
- Ad hoc users prefer simple tools, while professionals prioritize efficiency and flexibility.
- Professional authoring often occurs in centralized studios with high-quality equipment.
- Ad hoc authoring happens on desktops with non-professional equipment.
- Quality standards are crucial for user engagement.
- Authoring systems encompass various aspects like data access, storage, and compression.
- Objects may be temporarily stored in a cache before being compressed and moved to storage.
- Control applications manage authoring systems, determining storage and compression formats based on equipment and standards.
- Control systems handle cache storage and manage compressed objects for dispatch to multimedia servers.

**features of authoring tools:**

Editing Features:
Authoring tools enable creation, editing, and transformation of various media types.
Example: Macromedia Flash includes a sound editor, eliminating the need for separate software.

Organizing Features:
Tools facilitate organization through navigation diagrams, storyboarding, and flowcharting.
Some offer visual flowcharting or overview features to showcase project structure.
Navigation diagrams aid project organization, while web-authoring programs include helpful diagram tools.

Visual Programming and Scripting:
Visual programming with icons simplifies tasks like playing sounds.
Scripting allows customization and creation of features not directly supported by the software.

Document Development Tools:
Tools offer features like importing pre-formatted text, indexing, complex search, and hypertext linking.

Interactivity Features:
Enable end-users to control content and information flow.
Levels of interactivity include simple branching and conditional branching.

Playback Features:
Authoring systems should include playback facilities for testing assembled elements.

Support for External Sources:
Support for CD-ROM, Laser Disc, and Video for Windows sources.
Allows integration of audio, video, and computer files directly into projects.

Hypertext Capabilities:
Enables linking of graphics, animations, and text, useful for representing large textual information.

Cross-Platform Capability:
Some tools are available on multiple platforms and offer file conversion features.

Run-time Player for Distribution:
Includes run-time software for packaging and distributing final products, often with CD-ROMs.

Internet Playability:
Authoring systems provide means to convert output for delivery within HTML contexts, catering to multimedia delivery via the web.

**Design issues multimedia authoring:**

Display Resolution:
Standardization of display resolutions to ensure compatibility across various systems.
Consideration of factors like display protocol standardization and corporate norms for service and network traffic degradations.

File Format and Data Compression:
Use of reliable conversion tools for managing various data formats.
Standardization on one or two compression formats for each type of data object.

Network Interfaces:
Standardization of protocols in WANs and interconnections between LANs and WANs to ensure seamless transfer of multimedia objects.

Storage Formats:
Availability of attribute information about objects outside the object itself to aid in decision-making without decompressing the object.
Attribute information includes compression type, object size, creation date, source file name, etc.

Service Degradation Policies:
Establishment of corporate norms for service degradations, especially for objects created at high resolution viewed at lower resolutions.
Policies can include declining further requests, providing playback at lower resolution, dropping intermediate frames, or providing service in blocks.

**types of authoring systems:**

Dedicated Authoring Systems:
Designed for single users and single streams of objects.
Simple design for single-object handling but complexity increases with multiple object streams.
Users need not be multimedia experts, but interfaces should be intuitive.
Structured design approach aids in separating visual and procedural components.

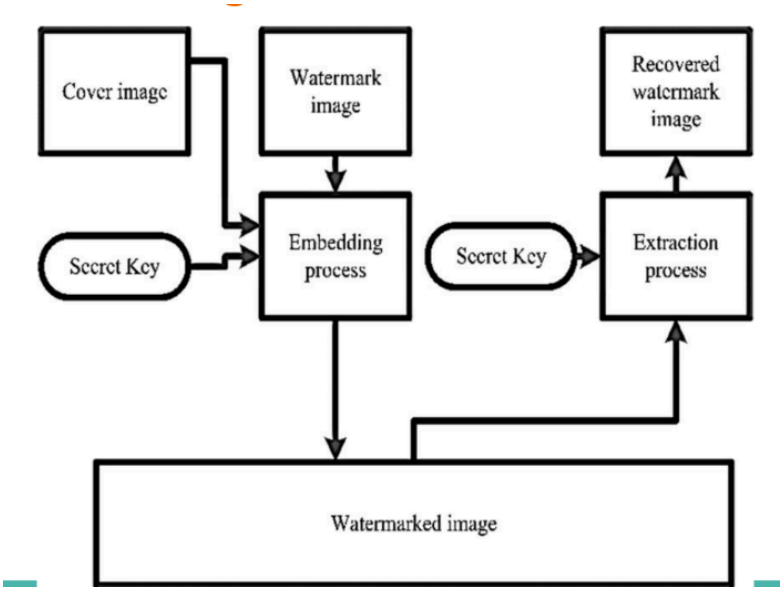
Timeline-Based Authoring:
Objects are placed along a timeline, either graphically or through scripting.
Objects play at specified points on the timeline.
Limited flexibility for object manipulation once placed on the timeline.
Editing components can cause reassignment of objects on the timeline.

Structured Multimedia Authoring:
Based on structured object-level construction of complex presentations.
Involves constructing the presentation structure and assigning detailed timing constraints.
Capabilities include viewing the complete structure, maintaining object hierarchy, zooming into specific components, etc.
Provides a clear representation of timing relations between components and supports various multimedia types.

Programmable Authoring Systems:
Offers automation of routine tasks through program interpreters.
Enhances capabilities with powerful functions based on image processing and analysis.
Allows tasks like returning timestamps, deleting or copying movie segments, and more.
Example: Locating video "silences" before new segments by automating the process rather than manual searching.

**Digital Watermarking**

Digital Watermarking
● It is a kind of marker covertly embedded in a digital media such as audio, video or image which enables us to know the source or owner of the copyright.
● This technique is used for tracing copyright infringement in social media and knowing the genuineness of the notes in the banking System.




Visible Watermarks:
Visible watermarks are semi-transparent text or images overlaid on the original image.
They allow the original image to be viewed while providing copyright protection by marking it as the owner's property.
More robust against image transformations, making them preferable for strong copyright protection of digital intellectual property.

Invisible Watermarks:
Invisible watermarks are embedded images that cannot be perceived by the human eye.
Only electronic devices or specialized software can extract the hidden information to identify the copyright owner.
Used to mark specialized digital content, such as text, images, or audio, to prove authenticity.

**Classification of watermarking**

1. Spatial Domain:

Least Significant Bit (LSB):
This technique embeds the watermark by replacing the least significant bits of selected pixels with the bits of the watermark data.
It is a simple and widely used method due to its ease of implementation.
While it offers high perceptual transparency, it is vulnerable to common signal processing operations and attacks.

Additive Watermarking:
Additive watermarking directly modifies pixel values by adding a watermark signal to the original image data.
The watermark signal alters the pixel values slightly to encode the watermark information.
This method is relatively straightforward and can provide good imperceptibility, but its robustness against attacks may vary depending on the implementation.

2. Transform/Frequency Domain:

Discrete Cosine Transform (DCT):
DCT transforms the image from the spatial domain to the frequency domain, where the watermark is embedded in the transformed coefficients.
It allows embedding in perceptually significant parts of the image, improving robustness against certain attacks.
However, DCT-based techniques may be computationally more expensive and less robust against geometric attacks.

Discrete Wavelet Transform (DWT):
DWT divides the image into spatial directions (horizontal, vertical, diagonal), enabling embedding in stable regions with distinct texture characteristics.
It offers robustness against common attacks such as compression, filtering, and geometric transformations.
DWT-based watermarking techniques are commonly used in applications where preserving visual quality and robustness are essential requirements.

Discrete Fourier Transform (DFT):
DFT transforms the image into its frequency components, making it robust against geometric attacks and translation invariance.
While DFT-based techniques offer robustness, they may be computationally more expensive compared to other methods.
They are suitable for applications where maintaining robustness against geometric distortions is crucial.

3. Other Techniques:

Spread Spectrum Modulation Based Technique:
This approach modulates the watermark signal with a pseudo-random sequence, spreading it across a wide frequency range.
It offers robustness against common attacks such as noise addition, compression, and filtering.
Spread spectrum watermarking is widely used in applications such as digital rights management and copyright protection, where robustness and security are paramount.

**Applications of watermarking**

Digital watermarking finds numerous applications across various industries. Let's delve into some of these applications in more detail:

1. Broadcast Monitoring:
Content Protection: Watermarking can safeguard copyrighted content by embedding unique identifiers within the audio or video signal. This allows broadcasters to trace leaked or pirated content back to its source, discouraging illegal distribution.
Ownership Identification: Broadcasters can mark their content with logos, trademarks, or metadata using watermarks, establishing ownership and preventing unauthorized usage or rebranding.

Audience Measurement: Watermarking enables broadcasters to track viewership data such as audience demographics and viewing habits. This information aids in understanding audience preferences and tailoring programming or advertising strategies accordingly.

Quality Control: Watermarks with specific codes or information can be embedded to monitor broadcast signal quality, ensuring accurate and reliable delivery of content to viewers.

2. Ownership Assertion:
Watermarking allows rightful owners to validate ownership of digital content, overcoming limitations of textual copyright notices that are easily removable or portable.

3. Transaction Tracking:
Also known as fingerprinting, this application involves uniquely identifying each copy of a work, similar to individual fingerprints. Watermarks record recipient information for each legitimate distribution of the work, aiding in tracking and tracing unauthorized copies.

4. Content Authentication:
Watermarking verifies the integrity of watermarked information, ensuring it hasn't been tampered with. Applications include trusted cameras, video surveillance, digital insurance claim evidence, and digital rights management systems.

5. Copy Control and Fingerprinting:
Watermarking prevents the creation of illegal copies by embedding identifiers (e.g., serial numbers) into digital content. Owners can trace the source of unauthorized copies, aiding in copyright enforcement and protection.

**Steganography**

Steganography is the technique of hiding data within an ordinary, nonsecret file or message to avoid detection;
● The hidden data is then extracted at its destination.
● Steganography use can be combined with encryption as an extra step for hiding or protecting data.
● The word steganography is derived from the Greek word steganos, meaning "hidden or covered," and the Greek root graph, meaning "to write."
● Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content.
● The secret data can be hidden inside almost any other type of digital content.
● The content to be concealed through steganography -- called hidden text -- is often encrypted before being incorporated into the innocuous/ harmless-seeming cover text file or data stream.
● If not encrypted, the hidden text is commonly processed in some method to increase the difficulty of detecting the secret content.

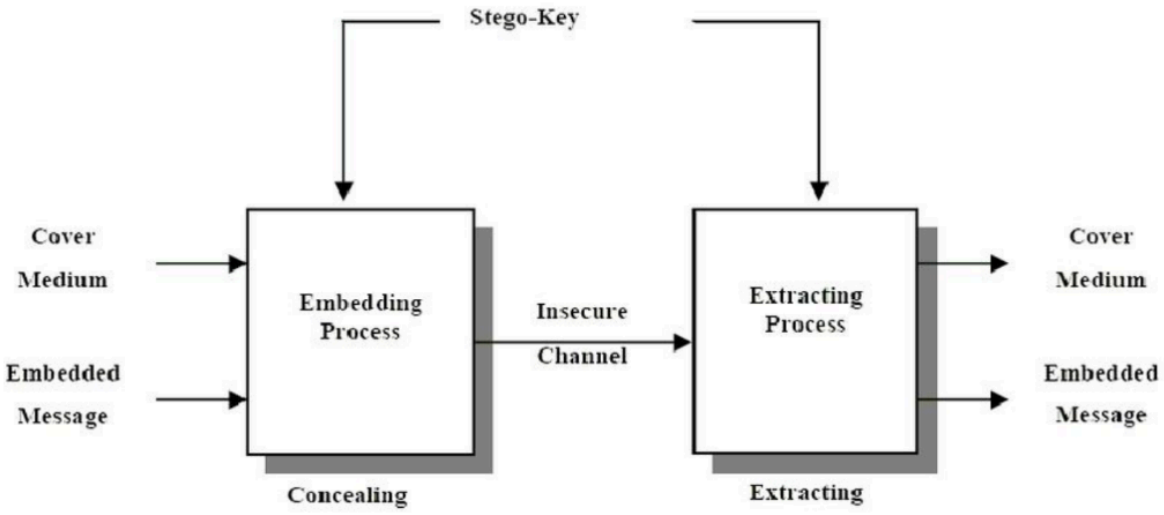
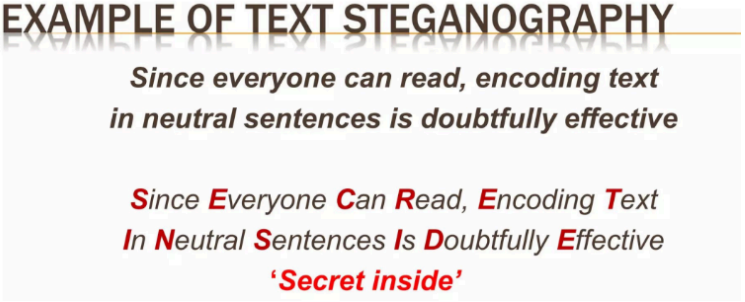



Fig. 1: The General Steganography System

**types of steganography**

1. Text Steganography:
Involves hiding data within text files by embedding secret information behind specific elements of the text, such as every nth letter of each word.
Various approaches exist for concealing information within text files.




2. Image Steganography:
Conceals information within images, utilizing pixel intensities to hide data.
Common method: Least Significant Bit (LSB) substitution, where the least significant bit of each pixel in the image is replaced with bits of the secret message.

3. Audio Steganography:
Embeds information within audio channels, often used for digital copyright security.
Watermarking is a common approach, hiding one piece of information (message) within another element of information (carrier).

4. Video Steganography:
Hides information within computer video formats, utilizing videos as carriers for concealing data.
Techniques like discrete cosine transform (DCT) can insert values imperceptible to the human eye into video frames.

5. Network or Protocol Steganography:
Conceals information within network protocols such as TCP, UDP, ICMP, or IP.
Utilizes covert channels within the OSI layer network model for hiding data.
Involves selecting a network protocol as the carrier, modifying certain fields or parameters to encode the secret data, and transmitting the manipulated network traffic over communication channels.
Reception on the recipient side involves analyzing the modified aspects of network packets or protocol messages to extract the hidden information.

**Image Authentication**

● Authentication plays an important role in protecting image against unauthorized access. Digital images are transmitted over insecure channels such as the internet.
● Authentication methods provide a means of ensuring the integrity of an image. Therefore there is need to protect these images against various attempts to manipulate them and it is important to make an effective method to solve image authentication problem that is ensuring the integrity of an image.
● Due to increase in the multimedia applications, image authentication techniques have gained attention. The existing image authentication methods are watermarking, cryptography.
● Digital watermarking is the science and art of embedding copyright information called watermarks in the files.
● Cryptography includes encryption and decryption to transfer documents or images.

**Issues in image authentication**

1. Digital Manipulation:
With the widespread availability of sophisticated image editing software, digital manipulation of images has become increasingly common.
Common manipulations include retouching, cropping, adding or removing objects, and adjusting colors or lighting.
Detecting such manipulations requires advanced forensic analysis techniques, making it challenging to verify the authenticity of images.

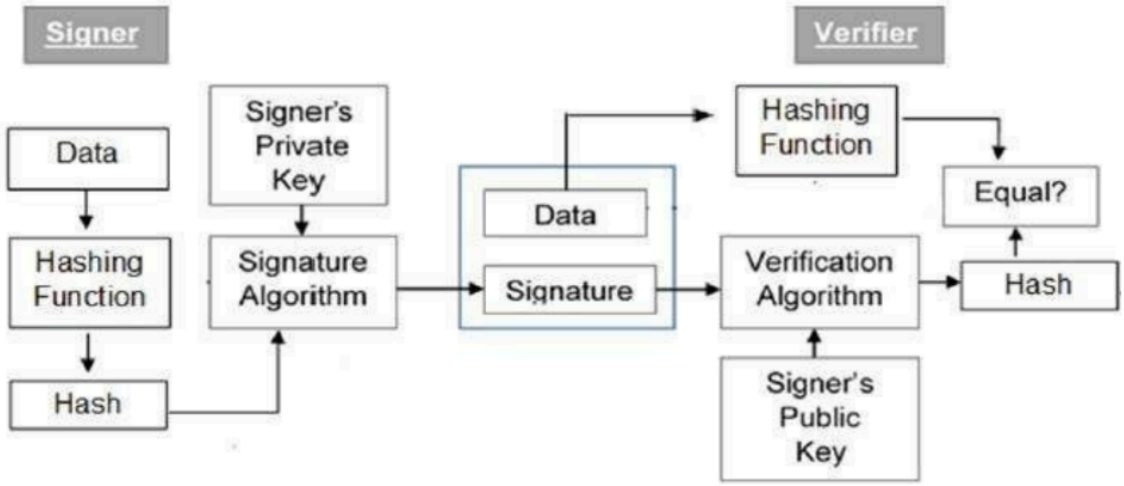
2. Forgery and Tampering:
Images may be forged or tampered with for various malicious purposes, including spreading misinformation, fabricating evidence, or perpetrating fraud.
Detecting forged or tampered images requires extensive forensic analysis, involving digital image processing, statistical analysis, and comparison with known authentic images.

3. Metadata Alteration:
Image metadata, such as EXIF data, contains valuable information about the image's capture settings, date, time, and location.
However, metadata can be easily altered or stripped from an image, undermining its reliability for authentication purposes.

4. Deepfake Technology:
Advancements in artificial intelligence and machine learning have given rise to deepfake technology, enabling the creation of highly realistic synthetic images and videos.
Deepfakes pose significant challenges for image authentication, as they can deceive traditional authentication methods and algorithms.

5. Legal and Ethical Considerations:
Image authentication raises legal and ethical concerns, particularly in legal proceedings, journalism, and forensics.
The admissibility of digitally authenticated images as evidence in court cases, privacy concerns, and the ethical implications of image manipulation are crucial factors to consider.

**Digital Signature Based Image Authentication**
Digital Signature Based Image Authentication is a method that leverages digital signatures to verify the authenticity and integrity of digital images. Here's how it works:




Digital Signatures Overview:
Digital signatures are mathematical schemes used to verify the authenticity of digital messages or documents.
They provide confidence to the recipient that the message came from a known sender and has not been tampered with.

Application to Images:
Similar to handwritten signatures in the physical world, digital signatures bind a person or entity to digital data.
Digital signatures are generated using cryptographic techniques, with a private key known only to the signer.

Key Pairs:
Each person or entity using digital signatures has a public-private key pair.
The private key is used for signing, while the public key is used for verification.

Signing Process:
The signer feeds the image data into a hash function to generate a unique hash value.
This hash value, along with the signer's private key, is then fed into a signature algorithm to create the digital signature.

The digital signature is appended to the image data.

Verification Process:
The verifier receives the image data along with the digital signature.
The verifier feeds the digital signature and the signer's public key into a verification algorithm.
Simultaneously, the verifier runs the same hash function on the received image data to generate a hash value.
The verification algorithm outputs a value based on the comparison of the computed hash value and the digital signature.
If the comparison matches, the verifier can be confident that the digital signature is valid, indicating the authenticity and integrity of the image.

Benefits:

Message Authentication: Verifying the digital signature assures the verifier that the sender, possessing the private key, created the signature.
Data Integrity: Any modification to the image data will result in a mismatch between the computed hash value and the digital signature, ensuring data integrity.
Non-Repudiation: The signer cannot deny signing the data in the future, providing evidence in case of disputes.