Part ONE:

Week 1: Introduction to Multimedia Security

Let we start with this Video:

Fake	Original

Overview of Multimedia

Multimedia refers to digital content that integrates multiple forms of media, including text, images, audio, video, and animations. The increasing reliance on digital multimedia in various domains, such as education, healthcare, entertainment, and forensics, has necessitated the development of robust security mechanisms to ensure data protection, confidentiality, and authenticity. The widespread use of multimedia applications in social media, cloud storage, and online streaming further exacerbates concerns related to data security and unauthorized access.

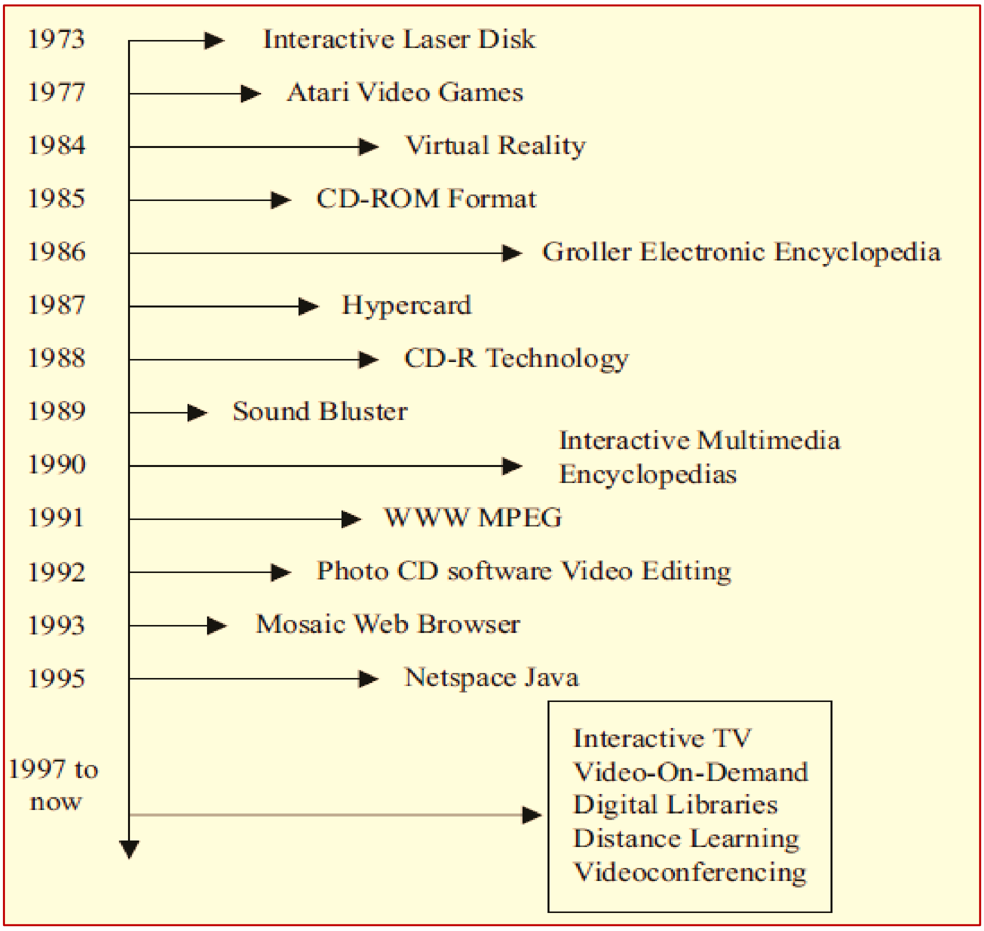


Figure: Timeline of multimedia applications

Importance of Multimedia Security

- **Data Integrity**: Ensures that multimedia content remains unaltered during transmission or storage.
- **Authenticity**: Verifies the origin and ownership of multimedia data.
- **Confidentiality**: Protects sensitive multimedia content from unauthorized access.
- **Non-Repudiation**: Prevents content creators or distributors from denying their involvement.

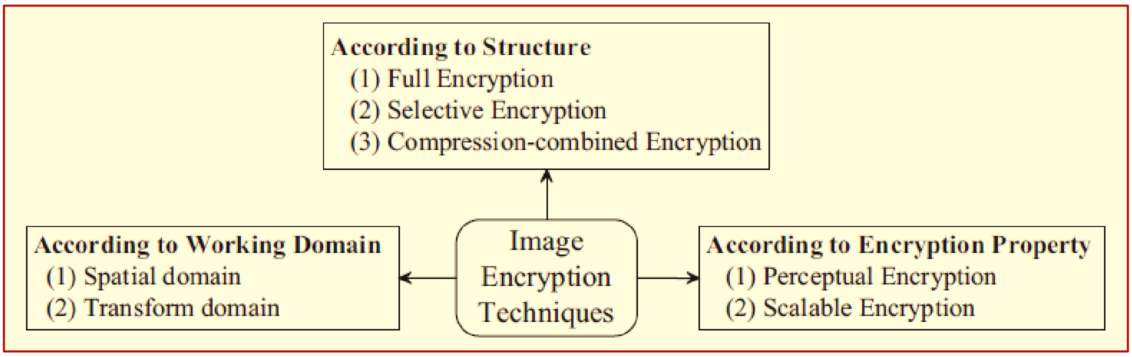
Key Challenges in Multimedia Security

- **Collision Resistance**: Ensuring hash functions are robust against attacks.
- **Quantum Threats**: The rise of quantum computing poses risks to traditional cryptographic systems.
- **Efficiency:** Optimizing security algorithms for large multimedia files.
- **Anti-Forensic Techniques:** Adversaries continuously develop methods to bypass forensic tools

Types of Multimedia Content

Multimedia content can be categorized into different types based on its format and usage:

1. **Images**: Digital images, stored in formats such as JPEG, PNG, GIF, and BMP, are widely used in photography, social media, and medical imaging. Due to their nature, images can be vulnerable to manipulation, unauthorized usage, and information embedding techniques such as steganography, which involves hiding secret messages within an image. A general classification of image encryption techniques can be illustrated in the following Figure:


According to Structure
(1) Full Encryption
(2) Selective Encryption
(3) Compression-combined Encryption
According to Working Domain
(1) Spatial domain
(2) Transform domain
Image Encryption Techniques
According to Encryption Property
(1) Perceptual Encryption
(2) Scalable Encryption

As a new trends, the Multimedia security must **force on the concept of Privacy-Preserving.** One of the best applications now is Cloud-based storage. As multimedia data continues to grow exponentially, ensuring privacy while leveraging cloud-based storage has become a critical challenge. Traditional security measures often focus on encryption and access control but fail to address the nuanced privacy concerns of users.

Privacy-preserving multimedia security is an emerging trend that emphasizes protecting sensitive information while enabling efficient storage, processing, and sharing of multimedia content in the cloud. This approach is particularly vital in applications like healthcare, finance, and personal media storage, where data sensitivity is paramount.

Cloud-based storage offers scalability, accessibility, and cost-efficiency, making it a popular choice for storing multimedia data. However, it also introduces privacy risks, such as unauthorized access, data breaches, and misuse of sensitive information. Privacy-preserving techniques ensure that even if data is stored or processed in the cloud, user privacy remains intact. The following scenario explain this concept as in figure:

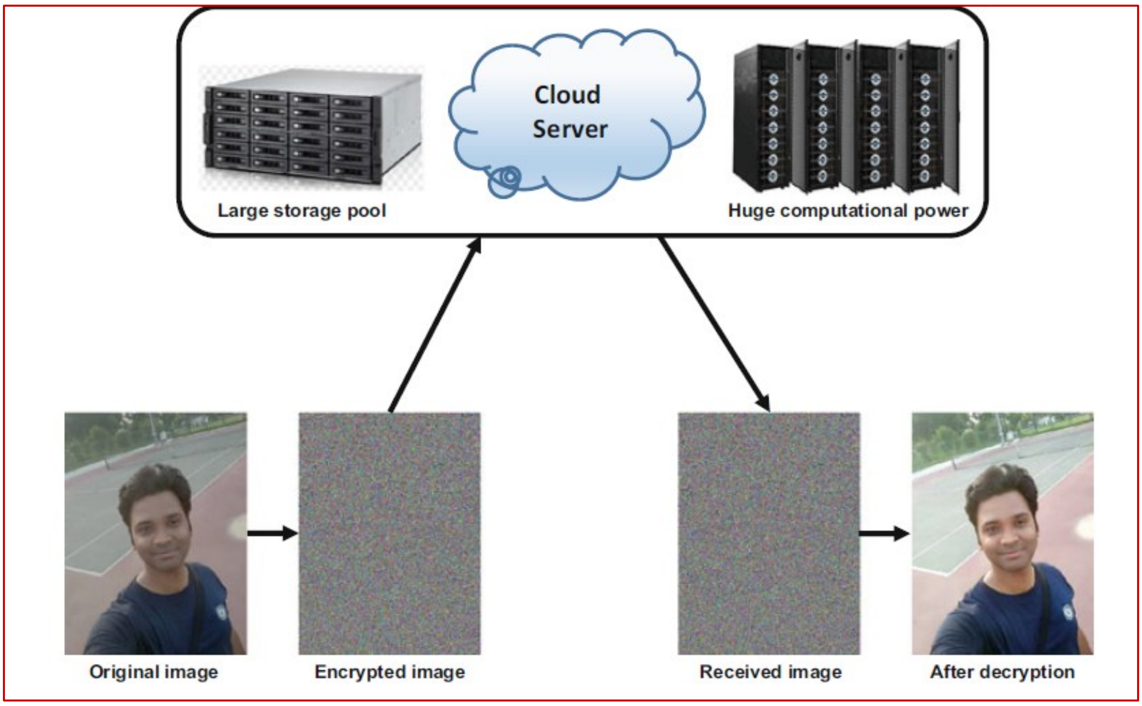


Figure: Privacy-preserving cloud-based image processing

2. **Audio**: Digital audio files, including formats such as MP3, WAV, and AAC, are utilized in communication, entertainment, and security applications. Audio content can be susceptible to unauthorized modification, eavesdropping, and watermarking attacks.
3. **Video**: Video files, commonly stored in formats such as MP4, AVI, and MKV, play a crucial role in areas such as surveillance, video conferencing, and online streaming. The large size and high bandwidth requirements of video files pose additional challenges for encryption and secure transmission.
4. **Text and Animation**: Text data, whether standalone or embedded within multimedia, forms a fundamental component of digital content. Animation, which combines multiple frames or multimedia elements, is widely used in entertainment, education, and simulations.

Types of Multimedia Content

Multimedia Type	Description	Common Formats
Images	Digital images used in photography, medical imaging, and social media. Vulnerable to manipulation and steganography.	JPEG, PNG, GIF, BMP
Audio	Digital sound files used in communication and entertainment. Susceptible to modification and eavesdropping.	MP3, WAV, AAC
Video	Multimedia files used in surveillance, streaming, and conferencing. Encryption challenges due to large file sizes.	MP4, AVI, MKV
Text & Animation	Embedded or standalone text and animations in multimedia content. Used in entertainment and education.	TXT, HTML, GIF, SWF

Security Threats and Challenges

As multimedia content is widely shared and distributed over the internet and various digital platforms, it faces numerous security threats and vulnerabilities that must be addressed.

1. Unauthorized Access and Piracy

The unauthorized distribution and replication of multimedia content, commonly known as digital piracy, pose significant challenges to copyright enforcement.

Hackers and cybercriminals often exploit vulnerabilities in digital rights management (DRM) systems to gain unauthorized access to protected multimedia content. Implementing advanced DRM mechanisms and access control strategies is critical to mitigating piracy.

Table 1: Common Digital Piracy Methods and Countermeasures

Piracy Method	Description	Countermeasure
Torrenting	Peer-to-peer file sharing of copyrighted content	Content fingerprinting, ISP tracking
Illegal Streaming	Unauthorized websites hosting premium content	DRM, watermarking
File Hosting	Uploaded copyrighted content on cloud platforms	DMCA takedown, encrypted metadata

2. Tampering and Forgery

The manipulation of multimedia content, including image and video forgery, poses significant risks in the digital age. With the advent of artificial intelligence, deepfake technology has emerged, allowing malicious actors to alter video and audio content in highly realistic ways. Digital forensic techniques, such as content authentication and robust watermarking, are essential to detecting and preventing tampered multimedia files.

3. Data Integrity and Authentication

Ensuring the integrity and authenticity of multimedia content is crucial for preventing unauthorized modifications and data corruption. Integrity verification techniques such as cryptographic hash functions and checksum algorithms play a vital role in detecting alterations in multimedia data. Additionally, digital signatures and blockchain-based verification systems enhance trust in multimedia transactions and communications.

Table 2: Cryptographic Hash Algorithms for Data Integrity

Algorithm	Hash Length	Security Level
MD5	128-bit	Weak (collision-prone)
SHA-256	256-bit	Strong (widely used)
SHA-3	224-512-bit	Advanced security

4. Privacy and Surveillance Concerns

The increasing use of multimedia data in surveillance systems, facial recognition, and biometric authentication raises privacy concerns. Multimedia content often contains personally identifiable information (PII), making it susceptible to misuse and unauthorized tracking. Privacy-preserving encryption techniques, anonymization methods, and regulatory frameworks, such as the General Data Protection Regulation (GDPR), are critical in safeguarding user data.

The Role of Cryptography in Multimedia Security

Cryptography plays a pivotal role in securing multimedia content by ensuring confidentiality, integrity, and authenticity. Various cryptographic techniques are employed to protect multimedia files from unauthorized access, tampering, and forgery.

1. Encryption Techniques

Encryption is the process of converting multimedia data into an unreadable format to prevent unauthorized access. The two primary encryption methodologies used in multimedia security include:

- **Symmetric Encryption (AES, DES)**: Symmetric encryption algorithms, such as the Advanced Encryption Standard (AES) and Data Encryption Standard (DES), are commonly used for encrypting large multimedia files due to their efficiency and fast processing speeds. These encryption schemes use a single key for both encryption and decryption, making key management a critical factor.
- **Asymmetric Encryption (RSA, ECC)**: Asymmetric encryption methods, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), utilize a pair of public and private keys for secure communication. These methods are frequently used in digital signatures and secure key exchange mechanisms in multimedia security.

2. Digital Watermarking

Digital watermarking is a technique used to embed hidden signals within multimedia content for purposes such as copyright protection, content authentication, and forensic tracking. Watermarking can be categorized into:

- **Robust Watermarking**: Designed to withstand common attacks such as compression, cropping, and format conversion.
- **Fragile Watermarking**: Used for tamper detection, where any modification to the multimedia content results in the degradation of the watermark.
- **Blind and Non-Blind Watermarking**: Differentiates between watermarking techniques that require or do not require the original multimedia file for verification.

Figure: Classification of watermarking algorithms based on domain used for the watermarking embedding process

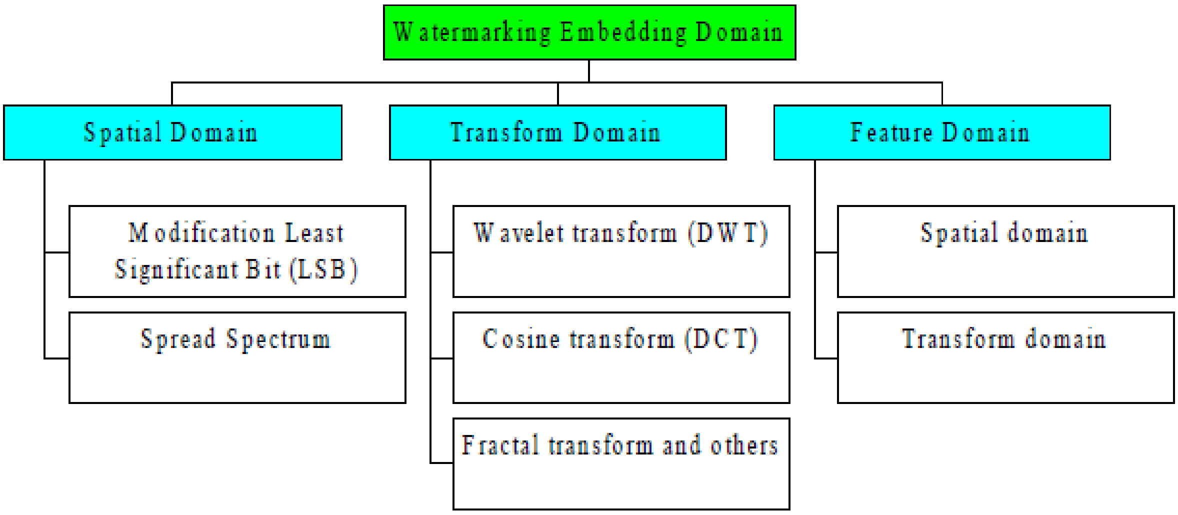


Figure: Classification of watermarking technology based on applications

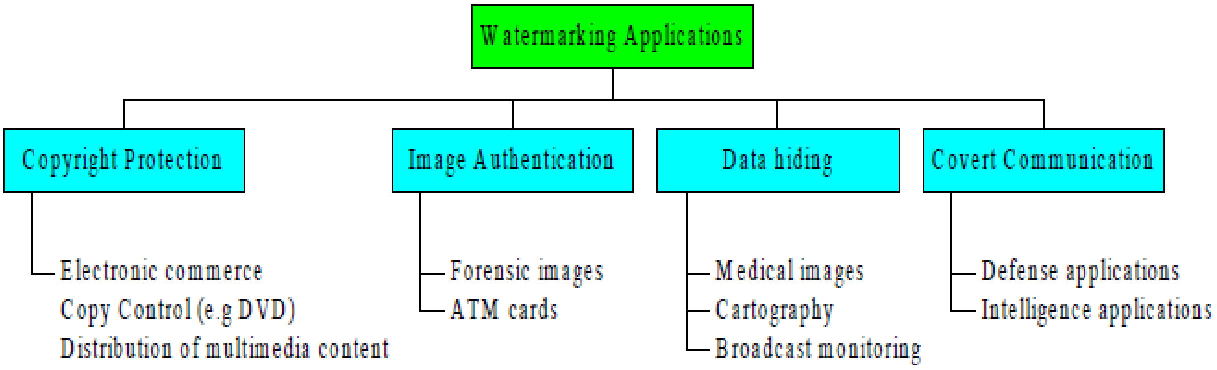
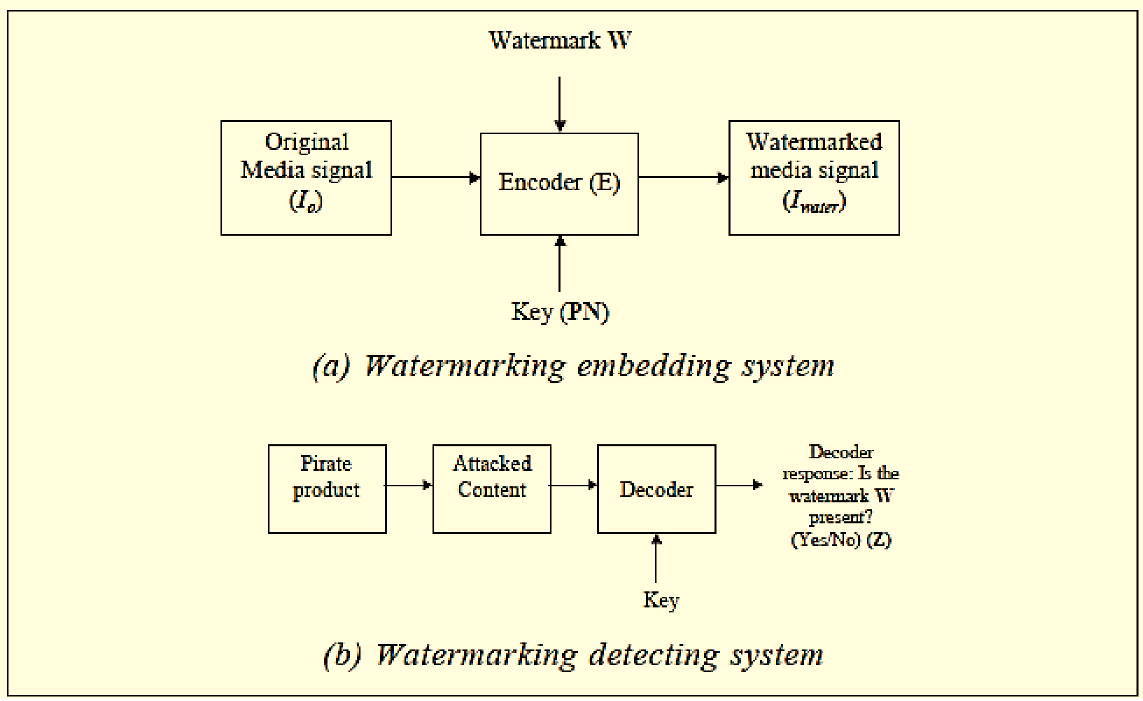
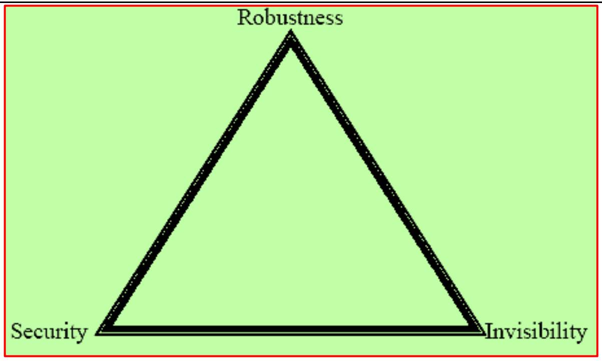


Figure: Embedding and Detecting systems of digital watermarking


Watermark W
Original Media signal (I_o)
Encoder (E)
Watermarked media signal (I_{water})
Key (PN)
Pirate product
Attacked Content
Decoder
Decoder response: Is the watermark W present? (Yes/No) (Z)
Key

(a) Watermarking embedding system

(b) Watermarking detecting system

 **Digital watermarking requirements triangle**	The important test of a watermarking method would be that it is accepted and used on a large, commercial scale, and that it stands up in a court of law. None of the digital techniques have yet to meet all of these requirements. **In fact, the first three requirements (security, robustness and invisibility) can form sort of a triangle, which means that if one is improved, the other two might be affected.**

3. Hashing and Digital Signatures

Hashing techniques and digital signatures play a crucial role in ensuring the integrity and authenticity of multimedia data.

- **Cryptographic Hash Functions (SHA-256, MD5)**: Hashing converts data into a fixed-length string, while digital signatures use cryptographic keys to verify the origin and integrity of the data. These techniques are widely applied in multimedia systems, such as image authentication, video watermarking, and secure communication protocols. Secure Hash Algorithms (SHA) and Message Digest (MD5) functions generate fixed-size hash values that serve as unique identifiers for multimedia files. Any modification to the file alters its hash value, signaling potential tampering. Hashing plays a critical role in multimedia security by providing a unique fingerprint for data. Key applications include:

Application	Description	Example
Image Authentication	Verifies the integrity of images by comparing hash values before and after transmission.	A quantization-based image authentication system uses hashing to detect tampering.
Video Watermarking	Embeds hash values as watermarks to ensure content authenticity and prevent piracy.	Hash-based watermarks are used in digital rights management (DRM) systems.
Password Storage	Securely stores user passwords as hashed values, often with added salt for enhanced security.	Salting prevents rainbow table attacks, ensuring robust password protection.

- **Digital Signatures**: Digital signatures provide authentication and non-repudiation for multimedia files by using cryptographic key pairs. Public key infrastructure (PKI) enables secure verification of digital signatures to ensure that multimedia content remains unaltered and originates from a trusted source. Digital signatures provide a mechanism to verify the authenticity and integrity of multimedia data. The process involves:

Step	Description	Example
Hashing the Data	Generate a hash value of the multimedia file.	SHA-256 is commonly used for hashing16.
Signing the Hash	Encrypt the hash using the sender's private key.	RSA or ECDSA algorithms are used for signing1.
Verification	Decrypt the signature using the sender's public key and compare hashes.	Email systems use digital signatures to verify message authenticity16.

In Fact, **Digital Signature Workflow as follow:**

1. Sender: Hash the data → Sign the hash with private key → Attach signature to data.
2. Receiver: Decrypt signature with public key → Compare hashes → Verify authenticity.

The Role of Cryptography in Multimedia Security can be summarized as follow:

Cryptographic Technique	Function	Examples
Symmetric Encryption	Encrypts multimedia data using a single key.	AES, DES

Asymmetric Encryption	Uses public/private key pairs for secure transmission.	RSA, ECC
Digital Watermarking	Embeds a hidden signal for copyright protection.	Robust, Fragile, Blind
Hashing & Digital Signatures	Ensures integrity and authenticity.	SHA-256, MD5

Case Study: Deepfake Technology and Its Security Implications

Deepfake technology, powered by artificial intelligence, has revolutionized the way multimedia content can be manipulated. While it has applications in entertainment and media, it also poses serious threats to security. Deepfake videos can be used to create false information, impersonate individuals, and spread misinformation. Governments and organizations are investing in forensic techniques to detect and mitigate deepfake-related threats. Implementing cryptographic watermarking and blockchain-based authentication mechanisms is being explored as a countermeasure to deepfake manipulation.

Discussion Questions

1. How does digital piracy impact the entertainment and media industry, and what measures can be taken to prevent it?
2. What are the ethical concerns associated with deepfake technology, and how can security mechanisms be employed to combat its misuse?
3. How does digital watermarking contribute to multimedia security, and what are its limitations?
4. In what ways can cryptographic techniques be integrated with multimedia security frameworks to enhance content protection?
5. What role does artificial intelligence play in both strengthening and compromising multimedia security?

Summary

This week's lecture introduces the fundamental concepts of multimedia security, highlighting the different types of multimedia content, the major security threats they face, and the role of cryptographic mechanisms in protecting them. Ensuring the security of multimedia data requires a combination of encryption, watermarking, hashing, and authentication techniques. The next lecture will delve deeper into cryptographic fundamentals and their applications in multimedia security.

Role and types of Biometrics in Multimedia security

Introduction:

Biometrics refers to the measurement and analysis of unique physical and behavioral characteristics, which are increasingly utilized to enhance security across various multimedia platforms. These technologies can be broadly classified into two categories: physiological biometrics, such as fingerprint and facial recognition, which rely on anatomical traits, and behavioral biometrics, which focus on patterns of behavior. The growing reliance on biometric systems underscores their significance in addressing contemporary security challenges, such as unauthorized access and identity theft, thereby making them a vital component of modern security frameworks in industries including finance, healthcare, and law enforcement.

The role of biometrics in multimedia security is particularly notable due to its effectiveness in authenticating users and safeguarding sensitive information. By employing unique identifiers, biometric authentication serves as a robust defense mechanism against fraud, enhancing data integrity and user trust in digital environments.

Applications of biometric technology in multimedia security range from access control systems that secure confidential files to mobile payment systems that ensure safe transactions, illustrating the versatile uses of these technologies in everyday life.

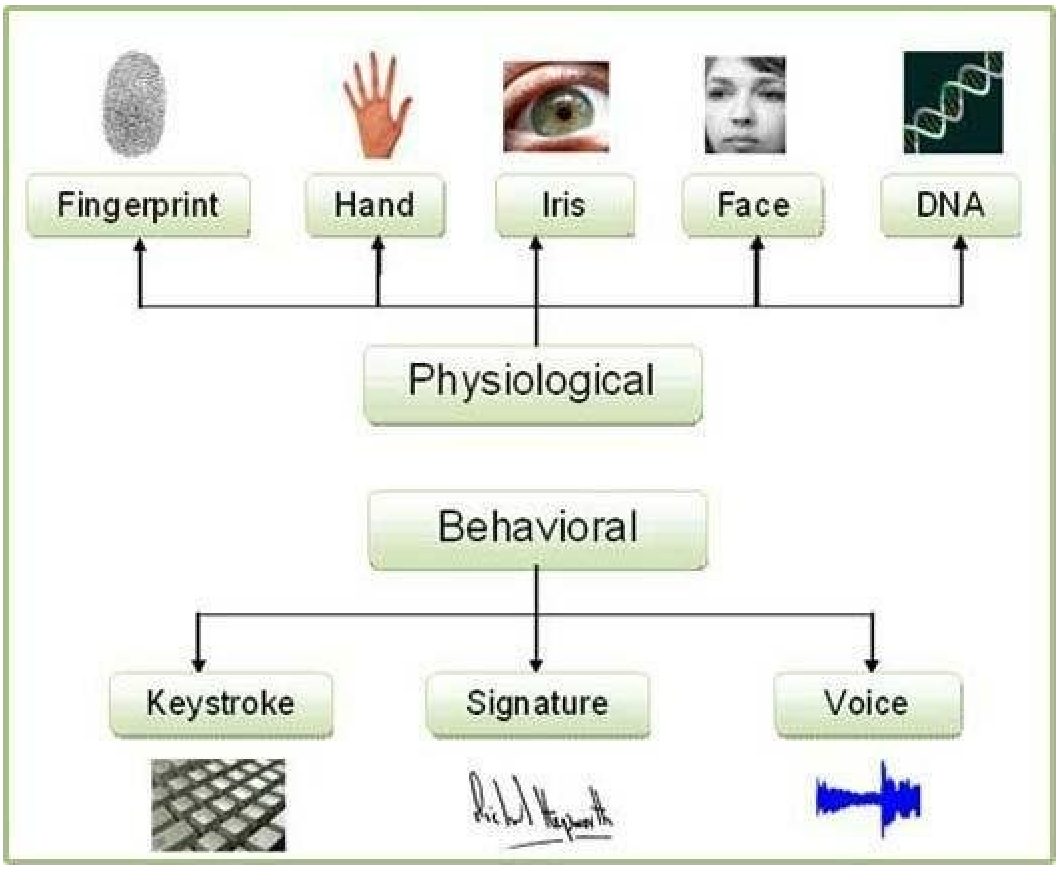
Despite the advantages, the implementation of biometric systems raises significant concerns regarding privacy and ethical considerations. The collection and storage of biometric data can lead to privacy infringements, particularly if individuals are not adequately informed about how their data will be used. Additionally, issues surrounding the security of biometric information pose risks, as compromised biometric data cannot be changed like passwords, leading to potential misuse.

This duality of enhancing security while also raising privacy concerns has led to ongoing debates about the ethical implications of biometric technology.

As biometric technology evolves, emerging trends such as the integration of artificial intelligence and the development of multi-modal biometric systems promise to enhance both security and user experience. These advancements not only aim to improve accuracy and reliability but also seek to address the pressing privacy concerns associated with biometric data handling. Consequently, the ongoing evolution of biometrics continues to shape the landscape of multimedia security, making it a crucial topic in discussions about technology and privacy in the digital age.

Types of Biometrics

Biometrics can be categorized into two main types: physiological biometrics and behavioral biometrics, each leveraging unique characteristics for identification and authentication purposes.



Physiological Biometrics

Physiological biometrics rely on anatomical or physiological traits that are relatively stable over time.

Fingerprint Recognition

This method analyzes the unique patterns and ridges on an individual's fingertips. Fingerprint recognition is widely employed in access control systems, smartphones, and law enforcement applications due to its reliability and ease of use.

Facial Recognition

Facial recognition technology captures and analyzes the distinct features of an individual's face, such as the distance between the eyes and the shape of the jawline. This technology has become increasingly prevalent in security systems and mobile devices, allowing for quick and accurate identification.

Iris Recognition

Iris recognition utilizes the unique patterns found in the colored part of an individual's eye. This biometric method is considered robust due to the stability of iris patterns over time, making it suitable for high-security environments like airports.

Retina Scanning

Retina scanning examines the unique blood vessel patterns located at the back of the eye. This form of biometric authentication is highly secure and is often used in sensitive locations, such as military installations, for stringent identity verification.

Behavioral Biometrics

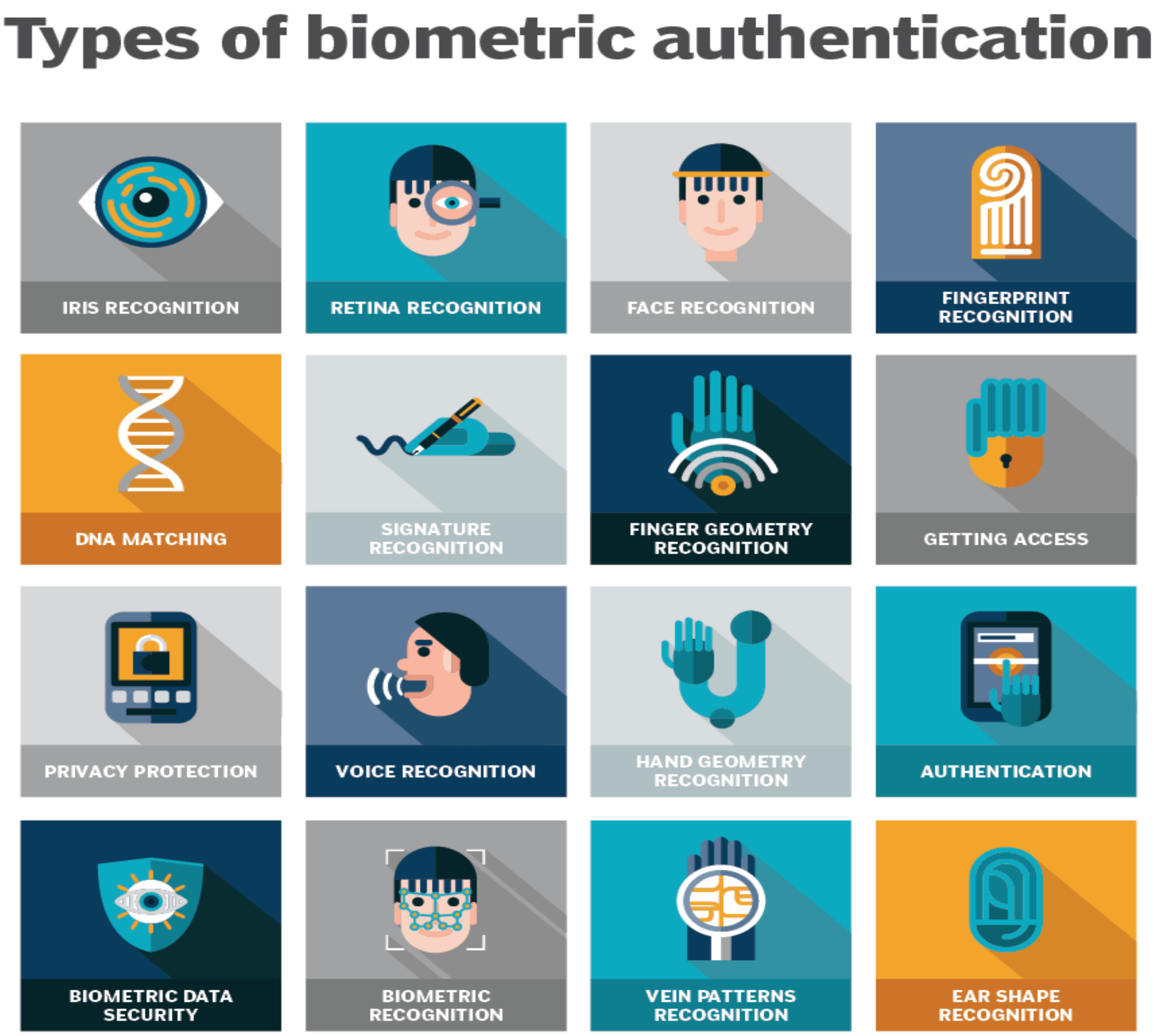
Behavioral biometrics focus on the distinctive patterns of behavior exhibited by individuals.

Role of Biometrics in Multimedia Security

Biometric technology plays a crucial role in enhancing security measures across various multimedia platforms. As the digital landscape evolves, the necessity for robust authentication methods becomes paramount to protect sensitive information and prevent unauthorized access.

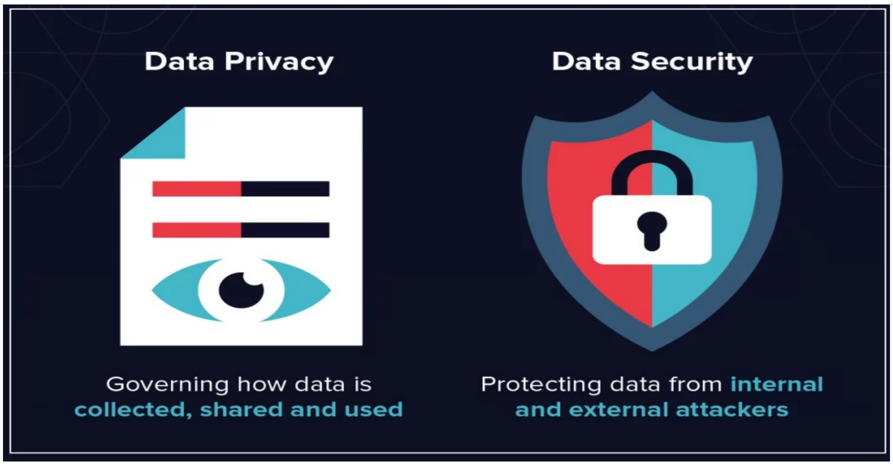
Authentication Mechanisms

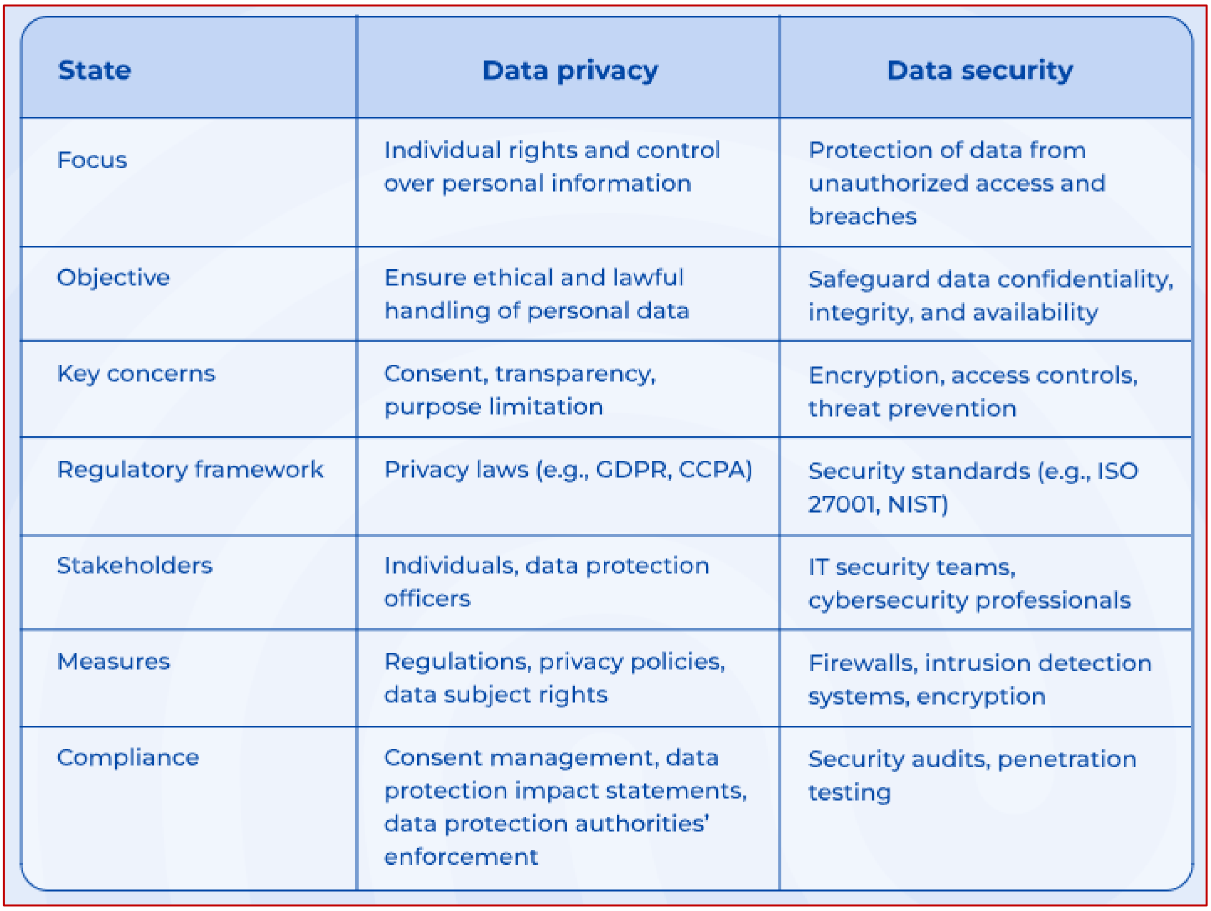
Biometric systems utilize unique physical or behavioral traits for authentication, making them a reliable method for securing multimedia content. This method serves as a strong defense against fraud, significantly reducing the chances of identity theft or unauthorized access to sensitive data associated with multimedia platforms. For instance, biometric verification, through mechanisms such as fingerprint or facial recognition, ensures that only authorized users can access digital assets, enhancing overall data security.



Data Security and Privacy

The implementation of biometric solutions is not only about enhancing security but also about upholding user privacy. With stringent regulations governing the handling of biometric data, organizations are required to obtain consumer consent and provide clear notices about data usage. This compliance helps build trust among users, enabling a secure multimedia environment where personal data is treated with utmost confidentiality.


Data Privacy
Data Security
Governing how data is collected, shared and used
Protecting data from internal and external attackers



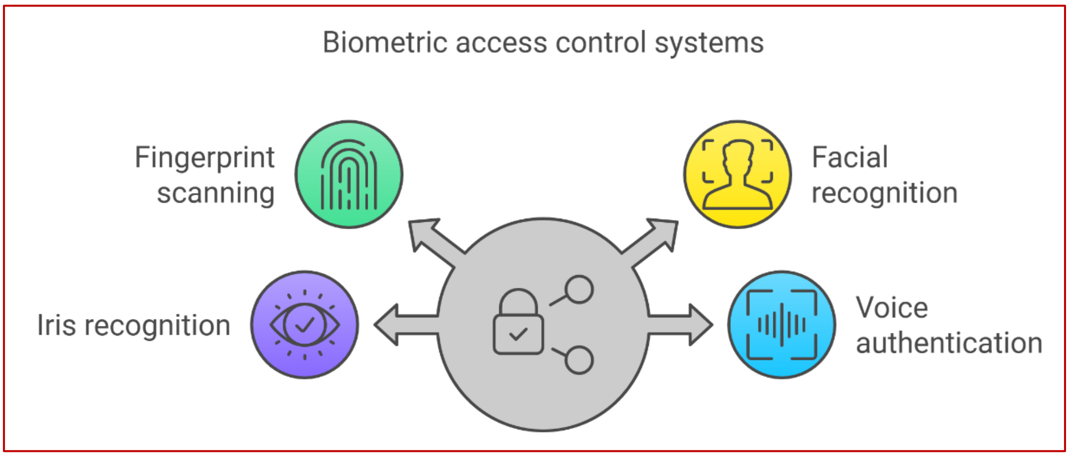
State	Data privacy	Data security
Focus	Individual rights and control over personal information	Protection of data from unauthorized access and breaches
Objective	Ensure ethical and lawful handling of personal data	Safeguard data confidentiality, integrity, and availability
Key concerns	Consent, transparency, purpose limitation	Encryption, access controls, threat prevention
Regulatory framework	Privacy laws (e.g., GDPR, CCPA)	Security standards (e.g., ISO 27001, NIST)
Stakeholders	Individuals, data protection officers	IT security teams, cybersecurity professionals
Measures	Regulations, privacy policies, data subject rights	Firewalls, intrusion detection systems, encryption
Compliance	Consent management, data protection impact statements, data protection authorities' enforcement	Security audits, penetration testing

Biometric Applications in Multimedia Security

Biometric technology finds numerous applications in multimedia security, including:

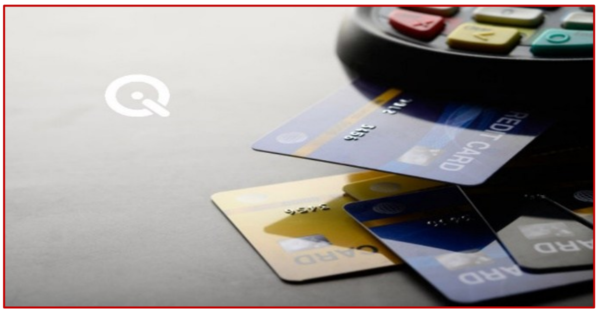
Access Control

In security systems, biometric authentication strengthens access control measures. For instance, organizations often utilize biometric systems for granting access to confidential multimedia files, ensuring that only individuals with verified identities can view or manipulate sensitive content. This is particularly important in sectors like finance and healthcare, where multimedia data may include sensitive personal information.



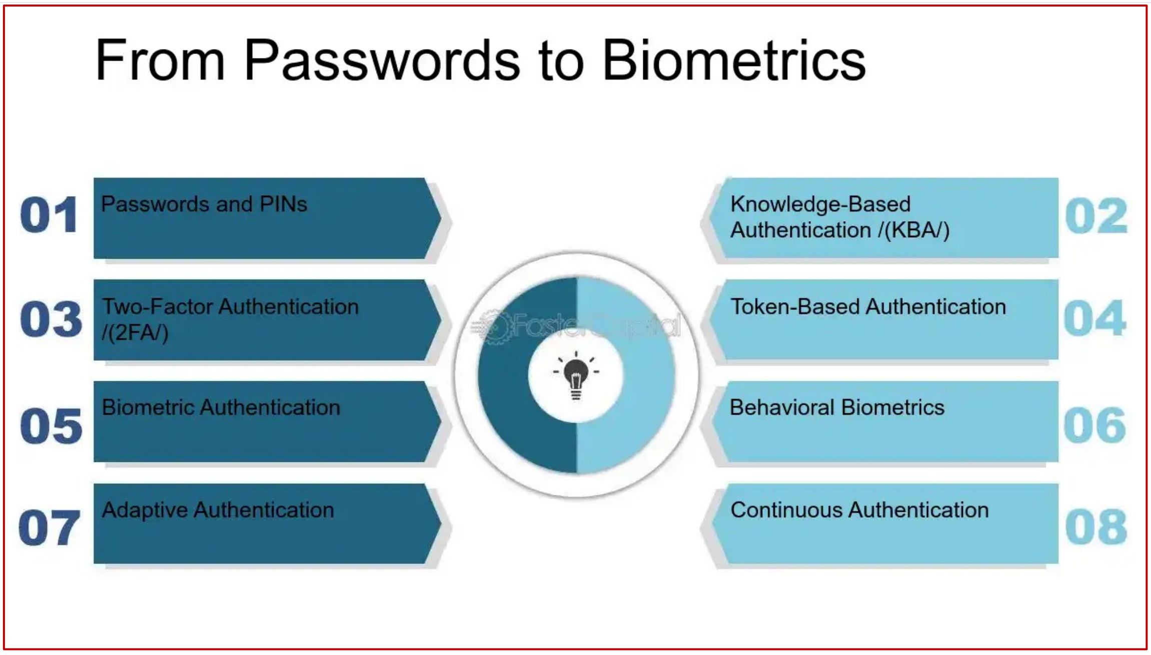
Secure Transactions

In financial services, the secure management of biometric data is critical for safeguarding multimedia transactions. Biometric authentication provides an added layer of security during transactions involving multimedia content, such as video conferencing or online banking, thereby ensuring that the user engaged in the transaction is indeed the authorized individual.



Enhancing User Experience

Moreover, biometric authentication can significantly enhance user experience by facilitating passwordless access to multimedia applications. By using biometric identifiers, users can seamlessly access their multimedia content without the need to remember complex passwords, thus improving both security and convenience.



From Passwords to Biometrics

01 Passwords and PINs

02 Knowledge-Based Authentication /(KBA/)

03 Two-Factor Authentication /(2FA/)

04 Token-Based Authentication

05 Biometric Authentication

06 Behavioral Biometrics

07 Adaptive Authentication

08 Continuous Authentication

1. Passwords and PINs:

2. knowledge-Based authentication (KBA): To enhance security, KBA asks users for information only they should know. This could include personal details or answers to pre-selected security questions. While more secure than passwords alone, KBA can still be compromised through social engineering or data breaches.

3. Two-Factor Authentication (2FA):

4. Token-Based Authentication: Tokens, both physical (like a key fob) and digital (like a software token), generate codes that users enter alongside their passwords. These tokens provide a dynamic element to the authentication process, making it harder for unauthorized users to gain access.

5. Biometric Authentication: The latest frontier in authentication technology, biometrics use unique physical characteristics, such as fingerprints, facial recognition, or iris scans, to verify identity. The use of biometrics has been popularized by smartphones and laptops, offering a high level of security combined with ease of use. For example, Apple's introduction of Touch ID and Face ID revolutionized phone security by making biometric authentication mainstream.

6. Behavioral Biometrics: Going beyond physical traits, behavioral biometrics analyze patterns in user behavior, such as typing rhythm or mouse movements, to create a profile that is incredibly difficult to replicate. This method is still emerging but promises a future where authentication is almost invisible to the user.

7. Adaptive Authentication: This method uses a variety of contextual factors, such as location, device, or time of access, to determine the level of authentication needed. For example, accessing a service from a known device in a familiar location might require less stringent authentication than from an unknown device or location.

8. Continuous Authentication: The future may hold a shift towards continuous authentication, where the system constantly verifies the user's identity through a combination of biometric and behavioral factors, ensuring that the authenticated user is still the one interacting with the system.

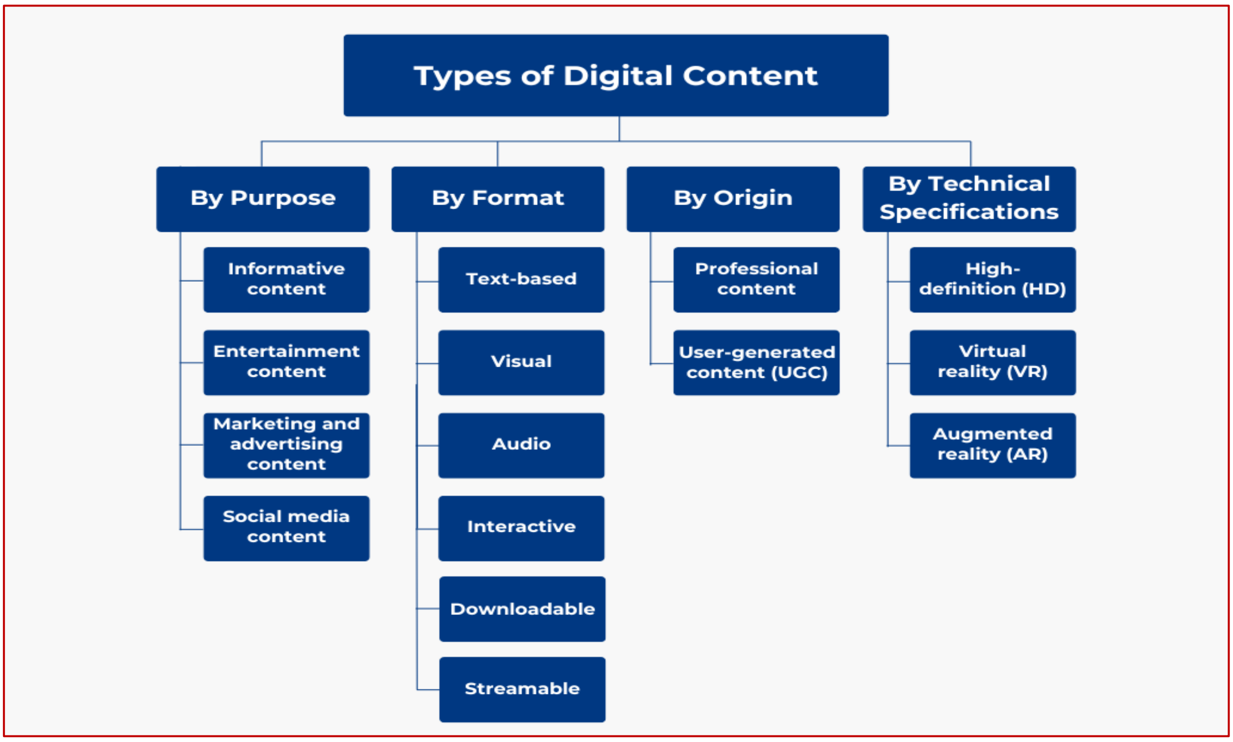
Applications of Biometrics in Multimedia Security

Overview of Biometric Applications

Biometric technology is increasingly being utilized to enhance security in multimedia environments, offering robust solutions for identification and authentication. These technologies leverage unique physiological or behavioral characteristics of individuals, such as fingerprints, facial recognition, and iris scans, to secure multimedia content and access control systems.

Enhanced Security in Digital Content

Digital content is anything you can see, hear, or interact with on a computer or an electronic device. It’s not a physical object you can hold but rather information stored electronically. Biometric authentication plays a crucial role in protecting digital media from unauthorized access and piracy. By utilizing biometric data, content providers can ensure that only authorized users can access their multimedia files, significantly reducing the risk of digital rights violations. For instance, biometric systems can be integrated into streaming services and digital libraries to authenticate users before granting access to premium content, thereby safeguarding intellectual property.



Types of Digital Content

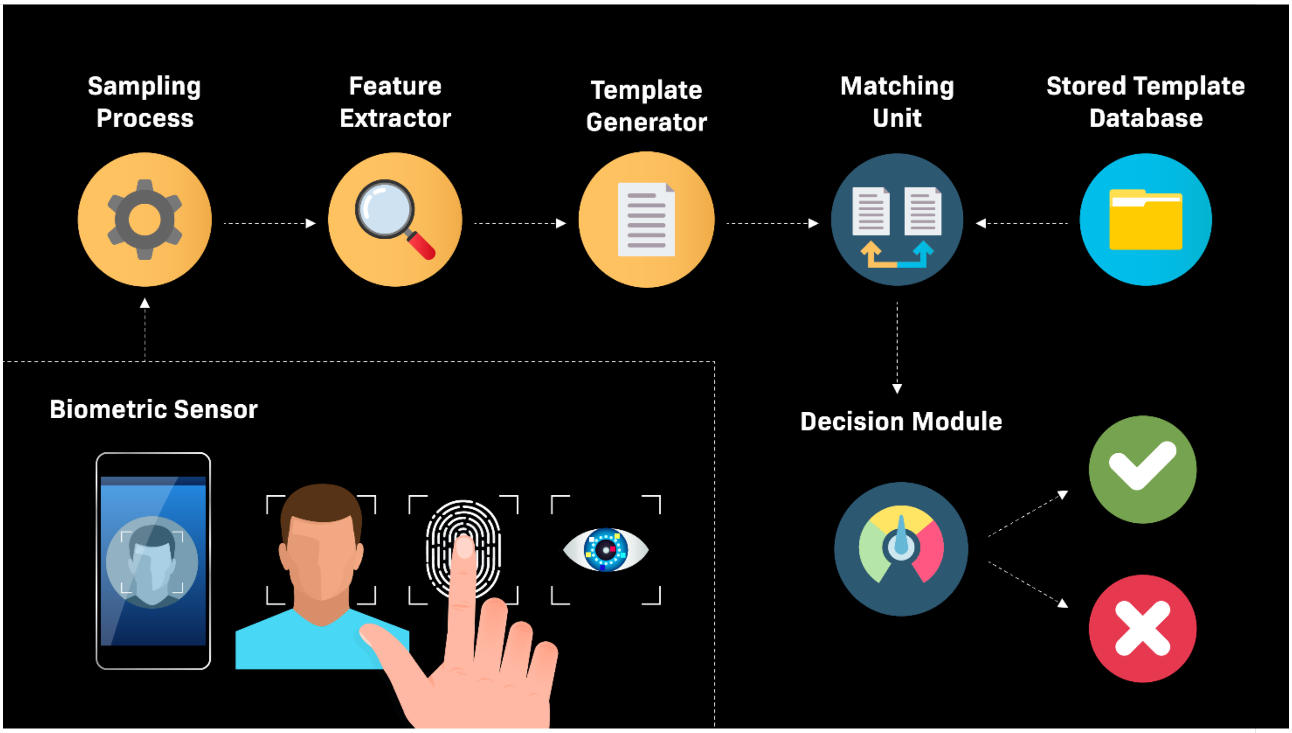
- By Purpose
  - Informative content
  - Entertainment content
  - Marketing and advertising content
  - Social media content
- By Format
  - Text-based
  - Visual
  - Audio
  - Interactive
  - Downloadable
  - Streamable
- By Origin
  - Professional content
  - User-generated content (UGC)
- By Technical Specifications
  - High-definition (HD)
  - Virtual reality (VR)
  - Augmented reality (AR)

Mobile Device Security

With the proliferation of smartphones and tablets, biometric technology has become an integral part of multimedia security. Modern devices commonly feature biometric authentication methods, such as fingerprint sensors and facial recognition, to secure applications and multimedia files. Users can unlock their devices and access sensitive content through these biometric systems, providing a seamless and secure experience. This convenience encourages wider adoption and fosters trust among users regarding the protection of their personal data.

Mobile security is a system of security software and habits that keeps your data out of the hands of hackers, scammers, and identity thieves. While it's tempting to think that only politicians, financial institutions, and big tech companies need enhanced security, everyone needs protection.

Elements of Mobile Security	
Security Software	**Security Practices**
• Anti-malware • VPNs • Remote wiping • Parental controls • Password manager • Encrypted backups	• Strong passwords • Device passcodes • 2FA (two-factor authentication) • Updated OS and apps • **Biometrics**



Biometric Authentication in Payment Systems

Biometric technology is also crucial in securing mobile payment systems that often involve multimedia transactions. By using biometric verification methods, such as fingerprint or facial recognition, users can authorize payments while enjoying a secure transaction process. This adds an additional layer of security, particularly in e-commerce, where the risk of fraud is heightened. The integration of biometrics into payment systems not only enhances security but also streamlines the user experience, making transactions faster and more efficient.

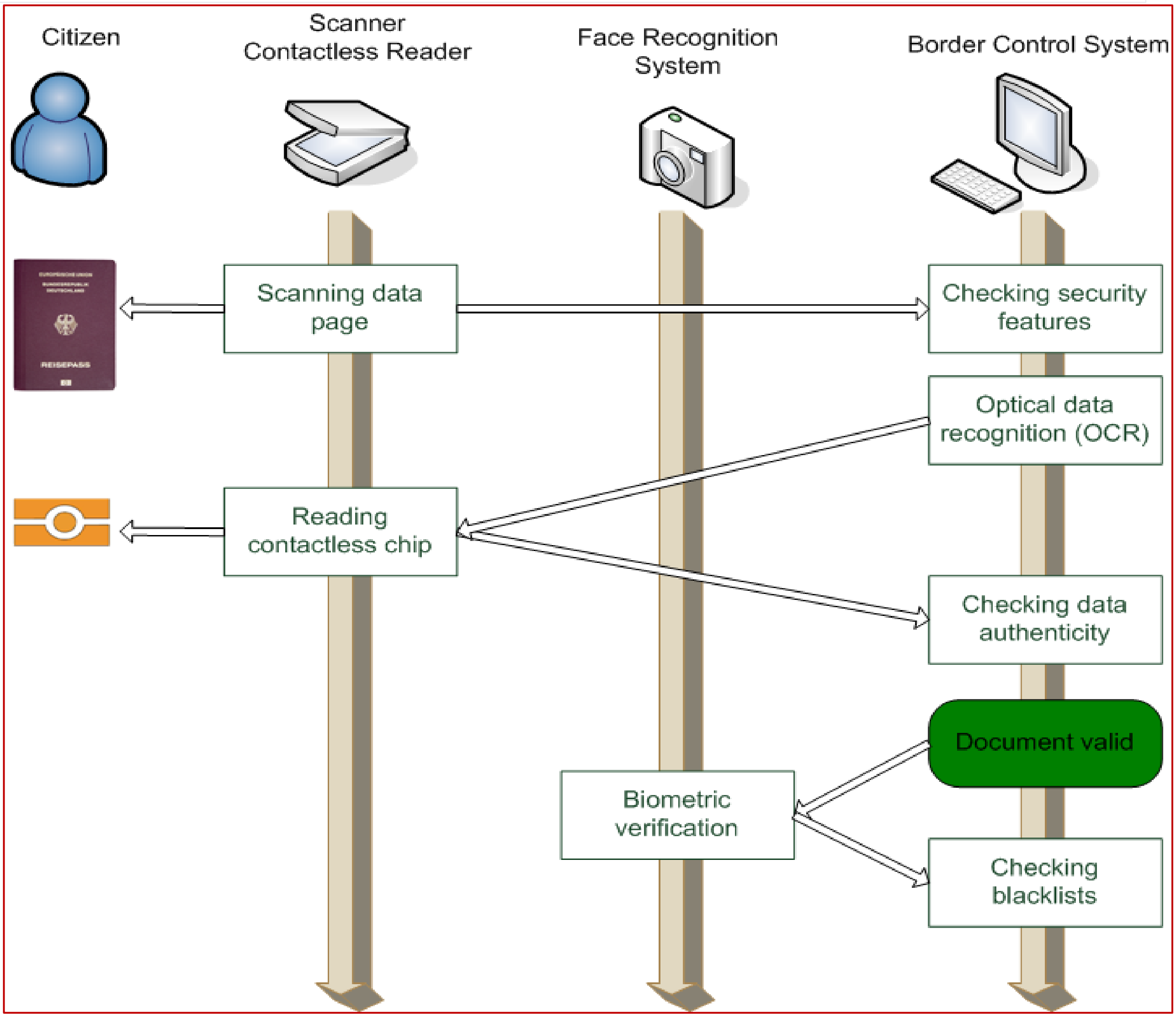
Applications in Healthcare

In healthcare, biometric systems are used to protect sensitive patient data and ensure that only authorized personnel can access medical records and multimedia patient information. Biometric identification methods, including facial recognition and fingerprint scans, can help healthcare professionals verify patient identities and manage access to confidential information. This application reduces the risk of data breaches and enhances patient privacy in multimedia contexts.

Border Control and Immigration

Biometrics are essential in enhancing security at borders and during immigration processes. By using facial recognition and iris scanning, authorities can verify the identities of travelers, preventing illegal entry and ensuring that multimedia records, such as passport photos, match the individuals crossing borders. This application not only strengthens national security but also facilitates smoother travel experiences for legitimate travelers.

Automated border control systems (**ABC**) or **eGates** are automated self-service barriers which use data stored in a chip in biometric passports along with a photo or fingerprint taken at the time of entering the eGates to verify the passport holder's identity.



Advantages of Biometrics

Biometric technology offers several significant advantages that enhance security and improve user experience in various applications.

Enhanced Security

Biometric systems offer enhanced security over traditional authentication methods such as passwords or swipe cards. Since biometrics rely on physical traits that are inherently difficult to replicate, they provide a higher level of security against unauthorized access. Multimodal biometric systems, which use multiple biometric traits, further strengthen security by requiring simultaneous validation of different identifiers, thereby complicating attempts to bypass the system.

Cost-effectiveness

While the initial setup of biometric systems may involve significant investment, they can lead to long-term cost savings. The reduction of security breaches and fraud can mitigate potential losses, while streamlined processes can improve operational efficiency in sectors such as banking, healthcare, and law enforcement.

Unique Identification

One of the primary benefits of biometric systems is their ability to provide unique identification based on individual physical characteristics. Biometrics such as fingerprints, facial recognition, and iris scans are distinctive to each person, making them a reliable form of identification for security purposes. This uniqueness significantly reduces the risk of impersonation and identity fraud.

User Experience

The implementation of biometric systems can greatly improve user experience. Biometric authentication is generally faster and more convenient than traditional methods, as users do not need to remember passwords or carry access cards. When designed effectively, biometric systems can offer intuitive interfaces and quick processing times, fostering higher acceptance among users.

Privacy Enhancement

In certain contexts, biometric systems can enhance privacy by providing a secure method of identification that minimizes the need to share sensitive personal information. For example, using biometric verification in financial transactions can offer an additional layer of security, thereby reducing the need for extensive personal data storage.

Adaptability and Integration

Biometric technology is adaptable and can be integrated into various systems across different sectors, including public security, healthcare, and financial services. This versatility allows for the development of customized solutions that meet specific security needs while improving overall system performance.

Challenges and Limitations

Biometric systems, while offering enhanced security and convenience, face several significant challenges and limitations that can impact their effectiveness and ethical implementation.

Privacy Concerns

The collection and storage of biometric data raise serious privacy issues. Individuals may not fully comprehend how their biometric information will be used, stored, and potentially shared, leading to feelings of mistrust and unease. Informed consent, a critical aspect of ethical data handling, often becomes contentious in the realm of biometrics, as many organizations may collect data without sufficiently informing individuals about associated risks. This lack of transparency can result in coercive environments where users feel pressured to provide biometric data in exchange for access to services, thereby undermining the genuineness of their consent.

Technological Limitations

Biometric systems are also subject to various technological constraints. Issues such as inaccuracies in recognition, environmental factors, and the potential for spoofing can hinder their reliability. For instance, biometric systems may fail to recognize individuals due to changes in appearance or external conditions affecting the data capture process. Moreover, advanced techniques for capturing biometric information covertly raise the stakes, as unauthorized collection becomes easier and more widespread.

Security Risks

The inherent nature of biometric data poses unique security challenges. Unlike passwords, which can be changed if compromised, biometric data such as fingerprints or facial recognition features cannot be altered. This irreversibility makes stolen biometric data particularly valuable and dangerous, as exemplified by significant breaches like the 2015 US Office of Personnel Management incident, which exposed the biometric data of millions. The risk of such data being used maliciously increases as biometric technologies evolve and become more integrated into everyday applications.

Ethical and Regulatory Compliance

Organizations deploying biometric technologies must navigate a complex landscape of ethical considerations and regulatory requirements. Failure to adequately assess the practices of third parties involved in biometric data handling, provide proper training for employees, or conduct ongoing monitoring can lead to violations of ethical standards and legal frameworks, as highlighted by the Federal Trade Commission's policy statements. Such oversights not only jeopardize consumer trust but can also result in significant legal repercussions for organizations.

Societal Implications

The broad implementation of biometric systems raises societal concerns regarding surveillance and profiling. The potential for increased monitoring can lead to a climate of fear and distrust among individuals, particularly if such technologies are misused by governments or corporations for invasive tracking and profiling based on biometric data. This issue is compounded by the ethical implications of data misuse, which can disproportionately affect marginalized groups.

Future Trends in Biometrics

As biometric technology continues to evolve, several trends are emerging that promise to enhance security and convenience across various sectors. These trends are driven by advancements in artificial intelligence (AI), machine learning (ML), and secure data storage solutions.

Integration of AI and Biometrics

The integration of biometric systems with AI technologies is set to revolutionize the field of identity verification. AI-powered biometric systems can significantly improve accuracy and reliability by utilizing ML algorithms that allow systems to adapt over time. This capability enables these systems to recognize patterns and anomalies, making them highly effective in real-world applications such as security checks and access control. Moreover, the ability to adapt to changes in user behavior adds an extra layer of security, making it increasingly difficult for potential threats to bypass these systems.

Multi-modal Biometrics

Future advancements in biometric technology are likely to see the rise of multi-modal biometric systems, which combine various forms of biometric data, such as fingerprint recognition, facial recognition, and iris scans. By leveraging multiple biometric traits, these systems can enhance verification accuracy and security, thereby reducing the chances of false positives and negatives. This holistic approach not only boosts security but also improves user convenience, allowing for seamless authentication across different platforms and devices.

Behavioral Biometrics

Another significant trend is the development of behavioral biometrics, which analyzes patterns in user behavior, such as typing speed, mouse movements, and even gait. These systems provide an additional layer of security that complements traditional biometric methods. By continually monitoring user behavior, organizations can identify unusual activity that may indicate a security breach, thereby enhancing overall system integrity.

Secure Biometric Data Storage

With the growing importance of biometric data, the need for secure storage solutions is more critical than ever. Blockchain technology is emerging as a promising candidate for securing biometric data, as it offers decentralized ledgers that enhance privacy and security. Biometric data stored on a blockchain is immutable and can only be accessed with the user's consent, ensuring both data integrity and user control. This trend could address many privacy concerns associated with traditional centralized databases, making it a vital development in the field.

Applications in Everyday Life

The application of biometric technology is expanding beyond traditional security and identification contexts to include mobile payment systems, healthcare, and even retail environments. For instance, biometric authentication is increasingly being integrated into contactless payment methods, allowing users to authorize transactions with their fingerprints. Additionally, facial recognition technology is being employed in healthcare settings for patient identification and management, enhancing both security and efficiency.

Part TWO:

- **Image and Video Encryption Techniques.**
- **Steganography fundamentals and applications.**
- **Watermarking techniques.**
- **Define key terms such as cracker, penetration tester, firewall, and authentication**

BY

PROF. DR. BASHAR ALESAWI

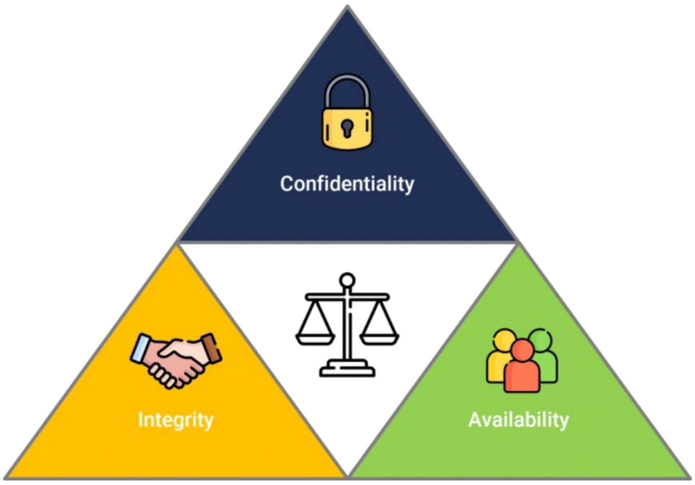
Basic Concepts in Data Security

Multimedia communication plays an important role in multiple areas of today’s society, including politics, economics, industries, militaries, entertainment, etc. It is of the 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, etc. Due to the rapid growth and widespread use of information and communication technologies, Internet services demand better methods of protecting computers, data, and information.

Data security is the protection of programs and data in computers and communication systems against unauthorized modification, destruction, disclosure or transfer whether accidental or intentional.

Data Security Core Principles

The three core principles of data security also referred to as information security are confidentiality, integrity and availability. Below is CIA Triad diagram:



Confidentiality

Protecting the information from disclosure to unauthorized parties. It means that sensitive data or information belonging to an organization or government should not be accessed by or disclosed to unauthorized people. Such data include employees’ details, classified military information, business financial records etc.

Integrity

Integrity of information refers to protecting information from being modified by unauthorized parties. This means that data should not be modified without owner's authority. This term covers two related concepts:

- **Data integrity**: Assures that information and programs are changed only in a specified and authorized manner.
- **System integrity**: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability

Availability of information refers to ensuring that authorized parties are able to access the information when needed. The information must be available on demand. This means that any information system and communication link used to access it must be efficient and functional. An information system may be unavailable due to power outages, hardware failures, unplanned upgrades or repairs.

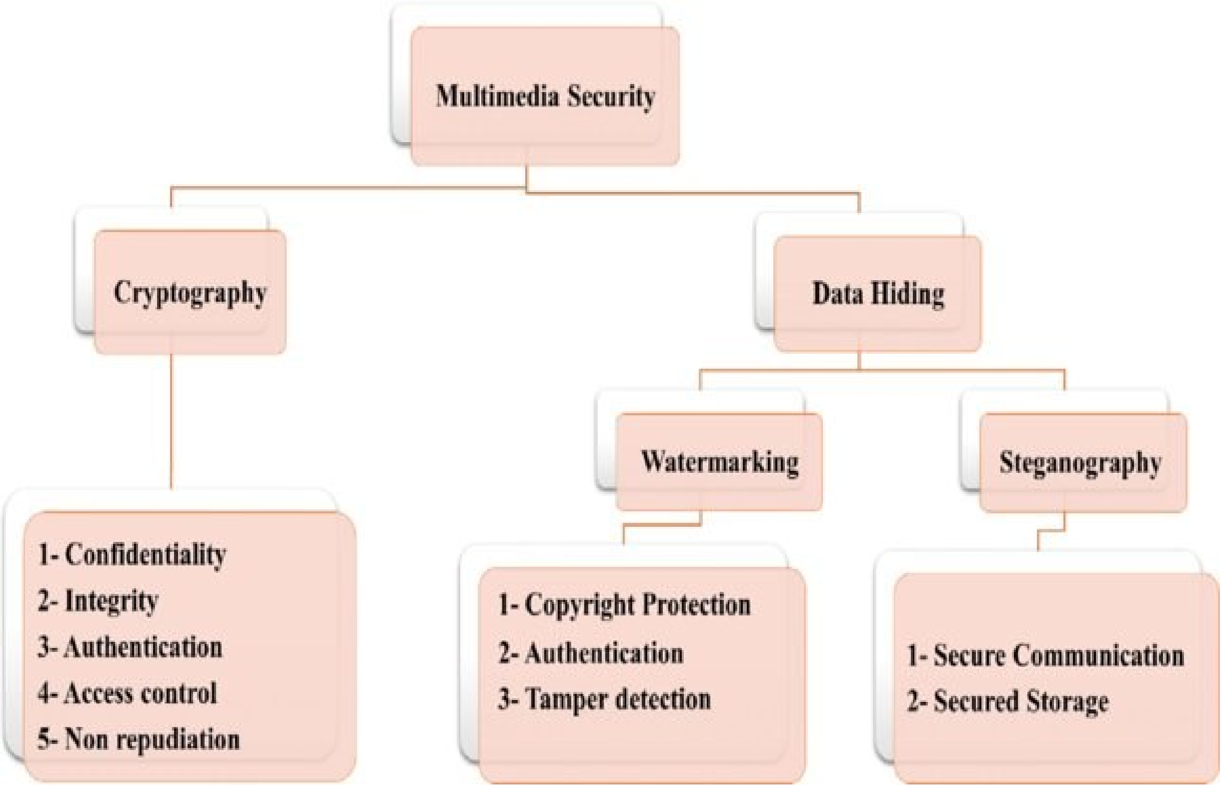
Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:

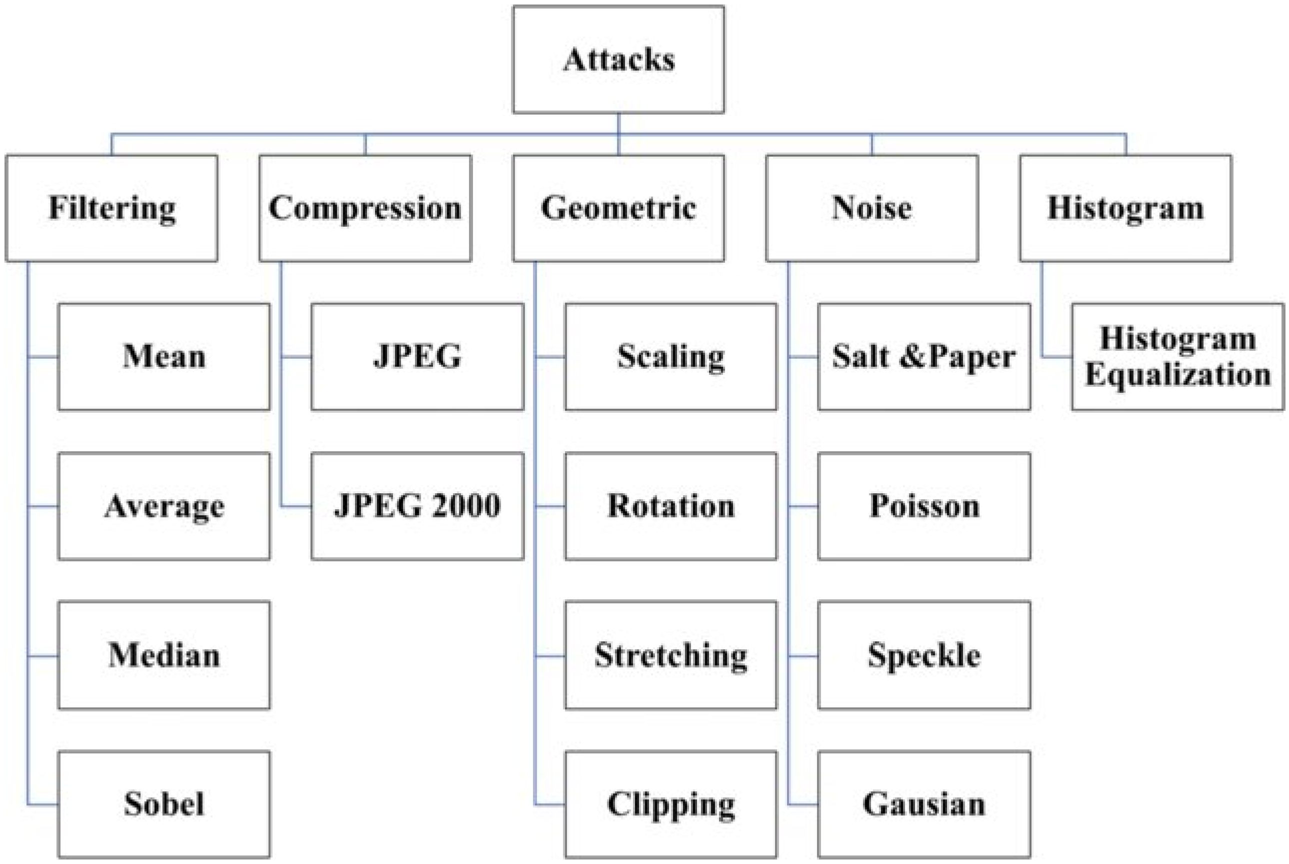
Authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability

The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party.


Multimedia Security
Cryptography
Data Hiding
Watermarking
Steganography
1- Confidentiality
2- Integrity
3- Authentication
4- Access control
5- Non repudiation
1- Copyright Protection
2- Authentication
3- Tamper detection
1- Secure Communication
2- Secured Storage


Attacks
Filtering
Compression
Geometric
Noise
Histogram
Mean
Average
Median
Sobel
JPEG
JPEG 2000
Scaling
Rotation
Stretching
Clipping
Salt &Paper
Poisson
Speckle
Gausian
Histogram Equalization

Security Architecture

The OSI security architecture is useful to managers as a way of organizing the task of providing security. The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined:

- Security attack: Any action that compromises the security of information owned by an organization.
- Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Security Attack:

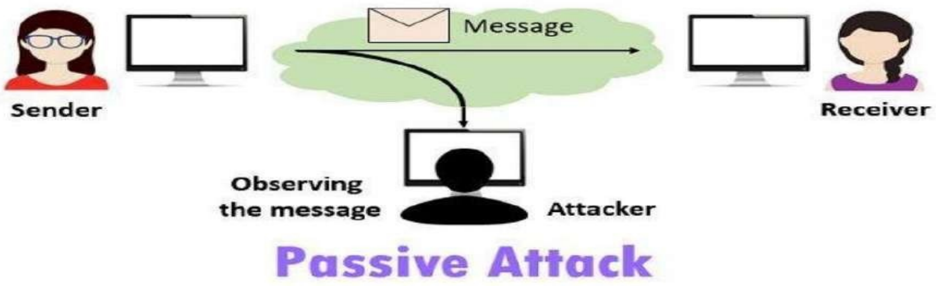
- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often threat & attack used to mean same thing
- have a wide range of attacks and can focus on two generic types of attacks: passive and active.

Passive attacks: which attempt to gather or make use of information from the system but does not affect system resources. By eavesdropping on, or keeping track of transmissions to:

- obtain message contents or
- monitor traffic flows

- Are difficult to detect because they do not involve any alteration of the data.

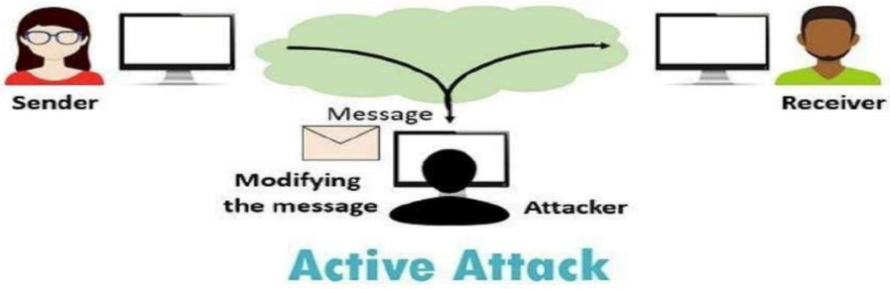
- However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.



Active attacks: which attempt to alter system resources or affect their operation. By modification of data stream to:

- replay previous messages
- modify messages in transit
- denial of service

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.



Denial of Service, A "denial-of-service" attack is an attempt by attackers to prevent legal users of a service from using that service. Examples include

- Flooding the network to overloading the servers
- Disrupting connections between systems
- attempts to prevent a particular individual from accessing a service

Security service: Some services, such as:

1. Authentication

It is a verification of the identity of the user. Some methods of authentication are:

- **User ID and passwords**. The system compares the given password with a stored password. If the two passwords match, then the user is authentic.
- **Swipe card**, which has a magnetic strip embedded, which would already contain your details, so that no physical data entry takes place or just a PIN is entered.
- **Digital certificate**, an encrypted piece of data which contains information about its owner, creator, generation and expiration dates, and other data to uniquely identify a user.
- **Biometrics** - retinal scanners and fingerprint readers. Parts of the body are considered unique enough to allow authentication to computer systems based on their properties.

2. Access Control

Access control is the security methodology that allows access to information based on identity. Users who have been given permission or keys to information can access it otherwise, access is denied.

3. Encryption-Based Access Control (Privacy) private key

The key used to decode public key messages that must be kept private. A totally different way to control access is to simply encrypt data using public key encryption. Access to the encrypted data is given to those who want it, but it's worthless to them unless they have the private key required to decode it.

Scenario: Encryption-Based Access Control in Multimedia Security

Scene 1: Alice Grants Bob Access to Encrypted Multimedia Files

⚲ *Location: Alice's Security Office*

◇ **Bob:** "Hey Alice, I need access to the 'Project Falcon' video documentation and AI-generated image datasets. I'm working on the multimedia security module this week."

◇ **Alice:** "Sure, Bob. Since these multimedia assets are sensitive, they are protected using **Selective Multimedia Encryption** and **Access Control Watermarking**. I'll generate a decryption key linked to your role."

◇ **(Alice uses a Digital Rights Management (DRM) system to generate a decryption key for Bob. The key is bound to Bob's user ID and device.)**

◇ **Alice:** "I've assigned you a cryptographic key to decrypt the video and image datasets. The files are encrypted using **AES-256 encryption** for secure storage and **Secure Streaming Encryption (SSE)** for online playback."

◇ **Bob:** "Got it! So, even if someone downloads the video files, they can't play them without the right decryption key, right?"

◇ **Alice:** "Exactly. Also, if any unauthorized copy is made, our system embeds an **invisible forensic watermark** to trace the leak."

Scene 2: Bob Tries to Access a Restricted Video

⚲ *Location: Bob's Workstation*

◇ **(Bob logs into the company's secure multimedia portal and attempts to stream a high-security video file, but access is denied.)**

◇ **System Alert:** "Access Denied! You do not have the required decryption key to view this multimedia content."

◇ **Bob:** "Hmm… I can access AI-generated images, but not the confidential training videos. Makes sense!"

◇ **(Bob contacts Alice.)**

◇ **Bob:** "Hey Alice, I can't open some videos in the repository. Are they encrypted separately?"

◇ **Alice:** "Yes, those videos are protected using **Hierarchical Encryption-Based Access Control**. Only employees with 'Senior Developer' or 'Security Analyst' roles can decrypt them."

◇ **Bob:** "That's a great way to prevent unauthorized access. So, even if someone downloads them, they remain encrypted?"

◇ **Alice:** "Yes, and even if they somehow bypass encryption, an **AI-powered deepfake detection system** ensures that unauthorized modifications are flagged instantly."

Scene 3: Attempted Multimedia Piracy & Unauthorized Streaming

📍 *Location: A Hacker's Workspace*

◇ **(A hacker obtains Bob's old login credentials through a phishing attack and tries to download the confidential videos.)**

◇ **Hacker (thinking):** "If Bob had access before, I should be able to use his credentials to get the videos and decrypt them."

◇ **(The hacker logs in and tries to stream a confidential training video but sees a watermark on the screen.)**

◇ **Watermark Message:** "User: Bob | Device ID: 192.168.1.10 | Location: Unknown"

◇ **Hacker:** "What?! This video is tagged with a forensic watermark? If I leak this, it will be traced back to Bob's account!"

◇ **(The hacker tries to bypass the watermark by screen recording, but the AI-based screen capture detection system activates.)**

◇ **System Alert:** "Unauthorized screen recording detected. Streaming has been disabled!"

◇ **Hacker:** "Damn! This encryption-based access control is too advanced!"

Scene 4: Alice Detects the Security Breach

📍 *Location: Alice's Security Dashboard*

◇ **(Alice receives an alert from the Multimedia Security AI system.)**

◇ **AI Alert:** "Unauthorized login attempt detected from an unrecognized device. Possible credential theft!"

◇ **Alice:** "That's strange… Bob's login was used from an unknown location. Let's analyze the forensic watermark on the accessed video."

◇ **(Alice checks the system logs and confirms that the hacker used stolen credentials but failed to remove the watermark.)**

◇ **Alice:** "Nice try, hacker! The forensic watermark confirms the unauthorized access. I'll revoke Bob's key and investigate further."

Scene 5: Security Measures & AI-Powered Protection

📍 *Location: Alice's Incident Response Team Meeting*

◇ **Alice:** "A hacker tried to access confidential videos using Bob's old credentials. Luckily, our encryption-based access control prevented any leaks."

◇ **Cybersecurity Analyst:** "The forensic watermarking and AI-based screen capture detection worked perfectly! Even if the hacker recorded the video, we would have traced the source."

◇ **Alice:** "Yes! We'll also implement **Zero Trust Security**, requiring multi-factor authentication (MFA) before streaming any sensitive multimedia content."

◇ **Security Manager:** "Great work, Alice! This proves that **encryption-based multimedia security** is critical for protecting confidential images, videos, and AI-generated media."

Final Takeaways

☑ **Selective Multimedia Encryption:** Ensures that only authorized users can decrypt and access multimedia content.

☑ **Secure Streaming Encryption (SSE):** Prevents unauthorized downloads or offline access.

☑ **Forensic Watermarking:** Embeds an invisible identifier to trace leaks.

☑ **AI-Based Screen Capture Detection:** Detects and blocks unauthorized recording attempts.

☑ **Zero Trust Security Model:** Requires MFA and device-based authentication for secure access.

Security mechanisms:

Security mechanisms are technical tools and techniques that are used to implement security services. A mechanism may operate independently or in conjunction with others to offer a certain service.

Image and Video Encryption Techniques

Introduction

Today, we'll dive into the fascinating world of image and video encryption techniques, a critical area in multimedia security. With the explosion of digital media—think social platforms, streaming services, and telemedicine—the need to protect visual data from unauthorized access has never been more pressing. Unlike text encryption, where data is often sequential and uniform, images and videos present unique challenges: high redundancy, large data sizes, and real-time processing requirements. Our goal today is to explore the principles, algorithms, and emerging trends in this field. We'll cover classical methods, chaotic systems, transform-based techniques, and modern approaches like deep learning-based encryption. Let's get started.

1. Why Encrypt Images and Videos?

Before we jump into techniques, let's establish the "why." Images and videos carry sensitive information—medical scans, surveillance footage, personal photos, or proprietary video content. Traditional encryption methods like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) were designed for text and struggle with multimedia due to:

- **High data volume**: A single 1080p frame is ~6MB uncompressed.
- **Redundancy**: Adjacent pixels or frames are highly correlated.
- **Real-time needs**: Video streaming demands low-latency encryption.

Thus, we need specialized techniques that balance security, speed, and format preservation. Let's define encryption formally:

Given plaintext P (image/video data), a key K, and an encryption function E, we produce ciphertext C=E(P,K) C = E(P, K)C = E(P, K), where P is recoverable only with the correct decryption key D(C,K)=PD(C, K) = PD(C, K) = P.

2. Classical Encryption Techniques

Let's start with foundational methods adapted for images and videos.

2.1 Substitution and Permutation

The simplest approach is to treat pixel values as numbers and apply substitution (changing values) or permutation (shuffling positions). For an 8-bit grayscale image with pixel values $P(x,y) \in [0,255]$

Substitution: Replace $P(x,y)$ with $S(P(x,y))$ using a key-driven lookup table.

Permutation: Scramble pixel positions using a key-based mapping, e.g., $(x,y) \rightarrow (x',y')$.

Algorithm 1: Basic Pixel Permutation

```
Input: Image I (M × N), Key K
Output: Encrypted Image I_enc
1. Generate permutation sequence S from K (e.g., using a PRNG)
2. For each pixel (x, y) in I:
   - Map (x, y) to new position (x', y') using S
   - I_enc(x', y') = I(x, y)
3. Return I_enc
```

Limitations: Low security against statistical attacks—histograms remain unchanged in permutation, and substitution alone doesn't disrupt spatial correlation.

2.2 Block Cipher Adaptation (e.g., AES)

AES, a symmetric block cipher, can encrypt image/video data by dividing it into 128-bit blocks. For an RGB image:

- Flatten pixel values into a 1D array.
- Pad if necessary, then apply AES in modes like CBC (Cipher Block Chaining).

Problem: AES ignores spatial correlation, and its computational cost scales poorly with video data. Compression (e.g., JPEG, H.264) before encryption also complicates format-preserving encryption.

3. Chaos-Based Encryption

Now, let’s explore a powerful paradigm: chaotic systems. Chaos offers pseudo-randomness, sensitivity to initial conditions, and ergodicity—ideal for encryption.

3.1 Chaos Theory Basics

A chaotic map, like the logistic map, is defined as:

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n), \quad x_n \in [0,1], \quad r \in [3.57, 4]$$

Small changes in x0 or r produce vastly different sequences, making it a natural key space.

3.2 Algorithm: Chaotic Image Encryption

Algorithm 2: Logistic Map Encryption

Input: Image I (M × N), Initial value x_0, Parameter r

Output: Encrypted Image I_enc

1. Generate chaotic sequence X = {x_1, x_2, ..., x_{M×N}} using logistic map
2. Sort X to get permutation indices P
3. Permute I’s pixels using P
4. XOR each pixel with a quantized chaotic value (e.g., floor (x_i × 255))
5. Return I_enc

3.3 Video Extension

For videos, apply chaos frame-by-frame or use 3D chaotic maps (e.g., Lorenz system) to scramble spatiotemporal data. Key advantage: High diffusion and confusion (Shannon’s principles).

Security: Resists statistical attacks (flat histogram) and brute-force (large keyspace).

Drawback: Computational overhead for real-time video.

4. Transform-Based Encryption

Next, let’s leverage signal processing with transform-domain encryption.

4.1 Discrete Cosine Transform (DCT)

Used in JPEG/MPEG, DCT concentrates energy in low-frequency coefficients. Encrypt only significant coefficients:

$$DCT(I) = C, \quad C(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(x,y) \cos\left(\frac{\pi u(2x+1)}{2M}\right) \cos\left(\frac{\pi v(2y+1)}{2N}\right)$$

- Encrypt top-left k×k coefficients with AES or chaotic substitution.
- Inverse DCT reconstructs a scrambled image.

4.2 Selective Encryption for Video

In H.264, encrypt I-frame DCT coefficients or motion vectors. This preserves compression while obscuring content.

Trade-off: Partial encryption reduces security but boosts speed.

---

5. Modern Approaches: Deep Learning

Finally, let’s touch on cutting-edge methods using neural networks.

5.1 Adversarial Encryption

Train a generator G to encrypt images/videos into a noise-like domain, with a discriminator D ensuring perceptual obscurity. Only authorized decoders with the key can reconstruct:

$$I_{enc} = G(I,K), \quad I_{dec} = D(I_{enc}, K) \approx I$$

5.2 Homomorphic Encryption

Encrypt images/videos to allow processing (e.g., CNN inference) in the encrypted domain. Expensive but revolutionary for cloud security.

You can See This simple HE code here (BMN):

6. Evaluation Metrics

How do we assess these techniques?

- **Security**: Keyspace size, resistance to differential attacks (NPCR, UACI).
- **Quality**: PSNR (Peak Signal-to-Noise Ratio) between original and decrypted data.
- **Speed**: Encryption/decryption time (critical for video).

Example: Chaos-based methods often achieve NPCR > 99%, PSNR ≈ ∞ (lossless), but lag in speed vs. selective DCT.

1. Keyspace Size (حجم فضاء المفتاح)

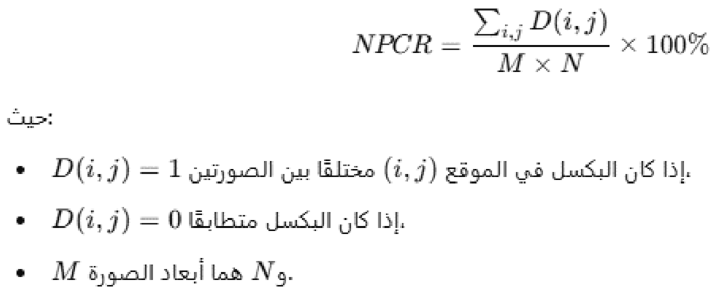
يُشير إلى العدد الكلي للمفاتيح الممكنة التي يمكن استخدامها في نظام التشفير. كلما كان فضاء المفتاح أكبر، زادت صعوبة تنفيذ هجوم القوة الغاشمة.(Brute-force attack)

المتطلبات الأمنية لحجم فضاء المفتاح:

- يُفضل أن يكون حجم فضاء المفتاح **أكبر من** 2^{100} لضمان أمان كافٍ.
- يُستخدم غالبًا 128-bit AES، أو 256-bit في تشفير الصور والفيديو، مما يعطي فضاء مفتاح 2^{128} أو 2^{256}.
- بعض خوارزميات التشفير الفوضوية (Chaotic Encryption) تعتمد على معاملات أولية عالية الدقة يمكن أن تزيد من حجم فضاء المفتاح.

2. NPCR (Number of Pixels Change Rate)

يُستخدم NPCR لقياس مدى تأثير تغيير بسيط في الصورة الأصلية على الصورة المشفرة.



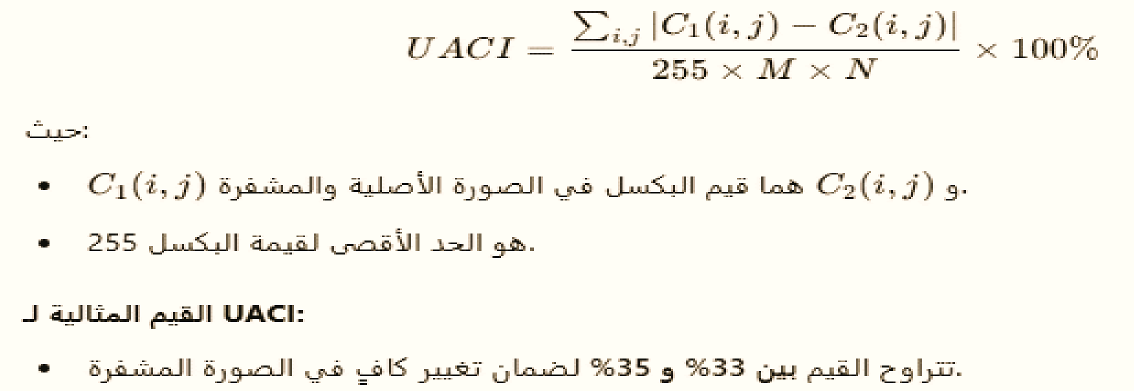
$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%$$

حيث:

- $D(i,j) = 1$ إذا كان البكسل في الموقع (i,j) مختلفًا بين الصورتين.
- $D(i,j) = 0$ إذا كان البكسل متطابقًا.
- M و N هما أبعاد الصورة.

القيم المثالية لـ NPCR: يجب أن يكون **أعلى من 99%** لضمان حساسية عالية تجاه التغيرات الطفيفة في الصورة الأصلية.

3.UACI (Unified Average Changing Intensity)



$$UACI = \frac{\sum_{i,j} |C_1(i,j) - C_2(i,j)|}{255 \times M \times N} \times 100\%$$

حيث:

- $C_1(i,j)$ و $C_2(i,j)$ هما قيم البكسل في الصورة الأصلية والمشفرة.
- 255 هو الحد الأقصى لقيمة البكسل.

القيم المثالية لـ UACI:

- تتراوح القيم بين 33% و 35% لضمان تغيير كافٍ في الصورة المشفرة.

7. Challenges and Future Directions

- Real-Time Video: 4K/8K streaming demands ultra-fast algorithms.
- Compression Compatibility: Encryption must coexist with codecs.
- Quantum Threats: Post-quantum multimedia encryption is uncharted.

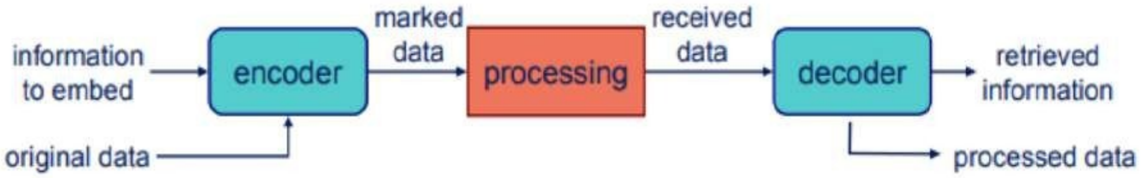
Research Idea: Can we design a hybrid chaos-DCT-deep learning system for 8K video at 60fps?

My BMN python Code here

Information Hiding

Information Hiding

Information Hiding: Communication of information by embedding it in and retrieving it from other digital data. Depending on application we may need process to be robust and secure, etc. we use hide data Because you want to protect it from malicious use, copy protection (Digital Watermarks), or because you do not want anyone to even know about its existence Covert communication (Steganography).



Where can we hide?

- **Media**
  - ✦ Video
  - ✦ Audio
  - ✦ Still Images
  - ✦ Documents
- **Software**
- **Hardware designs**

The Needed to Data Hiding

- ✦ Covert communication using images.
- ✦ Ownership of digital images, authentication, copyright
- ✦ Adding captions to images, additional information.

Steganography

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information. The word steganography is derived from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write) defining it as “hidden writing”.

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

Steganography can be used to hide almost any type of digital content, including text, image, video or audio content; the data to be hidden 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 cover data stream. If not encrypted, the hidden text is commonly processed in some way in order to increase the difficulty of detecting the secret content.

Watermark

Digital watermarking is the method of embedding data into digital multimedia content. This is used to verify the credibility of the content or to recognize the identity of the digital content's owner. A watermark is a “secret message” that is embedded into a “cover message”. Usually, only the knowledge of a secret key allows us to extract the watermark.

Why we use Watermark?

- ✦ Ownership assertion.
- ✦ Fingerprinting.
- ✦ Copy prevention or control.
- ✦ Content protection (visible watermarks).
- ✦ Authentication.

Wait for 3rd part SoooooN