People's Democratic Republic of Algeria

Ministry of Higer Education and Scientific Research

Echahid Cheikh Larbi Tebessi University- Tebessa

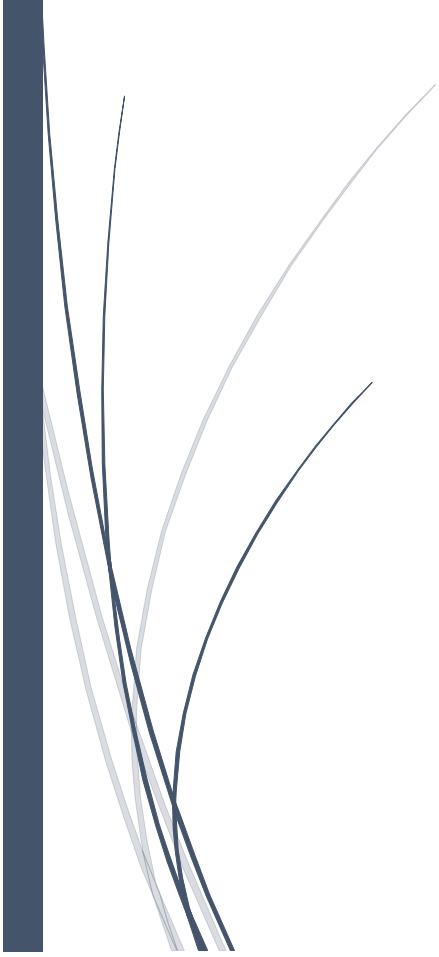
Faculty of Exact Sciences and Natural and Life Sciences

Department of Computer Science

QUALITY AND SECURITY MULTIMEDIA

for the 2nd-year Master's degree in Systems and Multimedia

Dr. Fatima BOUAKKAZ



January 2024

Table of Contents

CHAPTER I: IMAGE QUALITY ---- 1
I.1Introduction ---- 1
I.1.1.Fidelity ... 1
I.1.2.Image Quality ... 1
I.2.Different Types of Degradation ---- 2
I.2.1Blocking Artifacts ... 2
I.2.2. Ringing Artifacts ... 2
I.2.3 Blur ... 2
I.2.4. Noise ... 3
I.3.Image Filtering ---- 5
I.4. Subjective Assessment ---- 5
I.4.1 Key Characteristics ... 6
I.4.2 Influencing Factors ... 6
I.5. Protocols psychosensory subjective evaluation ---- 7
I.5.1 Double Stimulus Continuous Quality Scale (DSCQS) ... 7
I.5.2. Double Stimulus Impairment Scale (DSIS) ... 8
I.5.3. Single Stimulus Continuous Quality Evaluation (SSCQE) ... 8
I.6 Image Databases ---- 10
I.6.2. TID2013 (Tampere Image Database 2013): ... 11
I.6.3. CSIQ (Categorical Subjective Image Quality) Database: ... 11
I.6.4. IVC (Image and Video Communication) Database: ... 11
I.7 Objective Evaluation ---- 12
I. 7.1Full-Reference Methods ... 12
I.7.2. No-Reference Methods ... 12
I.7.3. Reduced-Reference Methods ... 12
I.7.4. most commonly used quantitative metrics include: ... 13
Practical Work 1: Image quality metrics ---- 15
CHAPTER II: IMAGE Security ---- 16
II.1.Introduction ... 16

II.2. Types Of Multimedia Security 16
II.3 Multimedia Encryption 17
II.4. Digital Watermarking: 18
II.4.1 Applications of Watermarking: ----------19
II.4.2.Watermarking Constraints: ----------20
II.5. Digital Watermarking phases 21
II.5.1 Insertion Phase:----------21
II.5.2 Extraction Phase:----------22
II.6.Types of Watermarking based on their level of resistance: 23
II.6.1. Robust Watermarking ----------23
II6.2. Fragile Watermarking ----------23
II.6.3 Semi-Fragile Watermarking ----------24
II.7.Types of Watermarking based on human perception 25
II.7.1. Invisible Watermarking ----------25
II.7. 2Visible Watermarking ----------25
Practical Work 2: Image watermarking using LSB 27
II.8. cryptography Multimedia 28
II.8.1 Definition of Cryptology----------28
II.8.2 Definition of Cryptography----------28
II.8.3 Terminology ----------28
II.9. Symmetric-key Cryptography 30
II.9.1 Advanced Encryption Standard (AES) for Image Encryption:----------30
II.9.2Data Encryption Standard (DES) for Image Encryption: ----------31
II.10.Asymmetric Cryptography RSA (Rivest-Shamir-Adleman) 33
II.11. Applications of Multimedia Cryptography 34
Practical Work 3:Image Encryption Using RSA 36
II.12.Steganography in Multimedia 38
II.12.1Steganography?----------38
II.12.2. Least Significant Bit (LSB) Replacement: ----------38
II.13. Challenges in Multimedia Steganography 38
Practical Work 4 Image Steganography Using LSB (Least Significant Bit) 40
CHAPTR III: CHARACTERIZATION OF THE PROPAGATION CHANNEL ----------41

III.1.Introduction 41
III. 2. Characterization of the Propagation Channel..... 41
III.2.1Factors Affecting the Propagation Channel----------41
II.2.2 Environmental Impacts on Channel Characteristics ----------41
III.2.3.Importance of Characterizing the Channel ----------42
III.3. Closed-loop MIMO Systems..... 42
III.3.1.Multiple-Input Multiple-Output (MIMO) ----------42
III.3.2.Basic Block Diagram of a MIMO System 43
III.3.3.Closed-loop MIMO----------43
III.4. Joint Source-Channel Coding 44
III.5.Multimedia transmission strategies..... 45
III.6.Optimization in Transmission Strategies: 46
III.6.1Key Concepts:----------46
III.6.2.Physical Layer and Its Impact----------46
III.3.7The Relationship Between the Physical Layer and Quality Metrics:..... 47
Practical Work 5: MIMO System Performance Evaluation..... 49
References 52

List of Figures

Figure 1.1. Blocking Artifacts. 2
Figure 1.2. Ringing Artifacts. 2
Figure 1.3. Blur image 3
Figure 1.4. movement blur 3
Figure 1.5.Information loss blur 3
Figure 1.6. (a) original image (b) image with salt-and-pepper noise 4
Figure 1.7. image with gaussian noise 4
Figure 1.8. image with speckle noise 5
Figure 1.9. Double Stimulus Protocol 7
Figure 1.10. Single Stimulus protocol 8
Figure 1.11. Some images Base LIVE 10
Figure 1.12.Some images Base IVC 11
Figure 1.13. Relationship between subjective and objective image quality assessment. 13
Figure 2.1. Types of Security measures 16
Figure 2.2.Types of Security Multimedia 17
Figure 2.3. Watermarking example 18
Figure 2.4. Watermarking Constraints 20
Figure 2.5. Watermarking Insertion phase 22
Figure 2.6. Watermarking Extraction Phase 23
Figure 2.7. Invisible Watermarking. 25
Figure 2.8. Visible Watermarking. 26
Figure 2.9. Multimedia encryption and decryption system. 29
Figure 2.10. Image Encryption Using AES Multimedia encryption and decryption system 31
Figure 2.11. Image Encryption with DES 32
Figure 2.12. Principe of RSA 34
Figure 2.13. Flow of Image Encryption and decryption using RSA 34
Figure 3.1. MIMO System 43
Figure 3.2. Basic Block Diagram of MIMO System 43
Figure 3.3. Open loop MIMO versus Closed loop MIMO System 44

CHAPTER I: IMAGE QUALITY

I.1Introduction

Images play a pivotal role in media, but their effectiveness is highly dependent on their quality. Digital images are susceptible to a multitude of degradations throughout their lifecycle, from acquisition to rendering. These degradations can occur during capture, processing, compression, storage, transmission, and reproduction. In this chapter, we investigate the most common types of degradation that can affect an image.

In this section, we will provide several definitions related to image quality assessment.

I.1.1.Fidelity

Fidelity refers to the degree to which an image reproduction matches its original. To evaluate fidelity, a metric is used to compute the distance between the two images. This distance serves as a numerical representation of the discrepancy between the reproduced image and the original.

I.1.2.Image Quality

Image quality is a general term used by observers to evaluate the inherent quality of an image. It is primarily subjective, meaning that each observer assesses image quality differently. While some may consider an image to be of sufficiently high quality, others with higher standards may perceive it as lacking quality. Image quality is largely determined by resolution and a balance of colors, commonly referred to as contrast. Resolution refers to the amount of detail in an image. Generally, the more detail an image contains, the higher its resolution.

I.2.Different Types of Degradation

I.2.1Blocking Artifacts

The primary source of error in JPEG compression is what is known as blocking artifacts [66]. These artifacts are typically visible at block boundaries and manifest as vertical and horizontal contours.



Figure 1.1. Blocking Artifacts. .

I.2.2. Ringing Artifacts

This degradation is generally due to the quantization of high-frequency coefficients [51]. It manifests as oscillations in the vicinity of high-contrast regions and is often defined as noise around these regions. Wavelets whose support crosses the edge of an object create this type of artifact.



Figure 1.2. Ringing Artifacts.

I.2.3 Blur

An aesthetic effect that results in an imprecise contour .This type of error, which primarily appears in JPEG and JPEG2000 compression, leads to a loss of image sharpness. It is characterized by a blurrier image with more diffused object edges.



Figure 1.3. Blur image .

Furthermore, blur can appear in an image in various ways, namely [51]: **acquisition blur, motion blur, information loss, processing blur, and intentional blur**



Figure 1.4. movement blur .

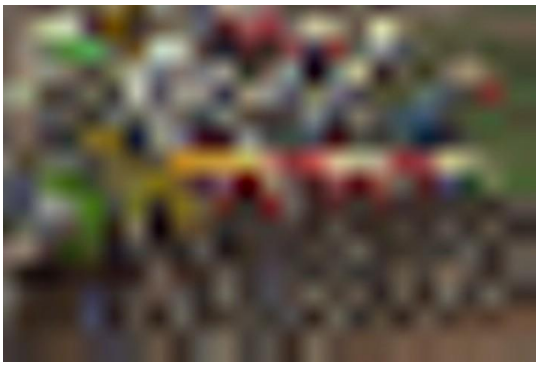


Figure 1.5.Information loss blur .

I.2.4. Noise

Noise is a degradation of an image caused by external interference. When an image is transmitted through satellites, wireless networks, or cables, errors can occur in the image signal. There are different types of noise.

a)Salt-and-pepper noise: It is also called impulse noise, shot noise, or binary noise. This degradation can be caused by sudden, strong disturbances in the image signal. It appears as randomly scattered white or black pixels (or both) on the image (see Figure I.6).



(a) (b)

Figure 1.6. (a) original image (b) image with salt-and-pepper noise .

b) Gaussian noise : Gaussian noise is an idealized form of white noise, caused by random fluctuations in the signal. Adding Gaussian white noise to an image therefore modifies the value of each pixel .



Figure 1.7. image with gaussian noise .

b) Speckle noise : The speckle phenomenon was first observed in 1960 during experiments involving the illumination of objects with a coherent light source, the laser "speckle" in radar images. While Gaussian noise can be modeled by random values added to an image, speckle noise (see Figure

1.8) can be modeled by random values multiplied by pixel values, hence it is also called multiplicative noise. Speckle noise is a significant problem in some radar and ultrasound applications.



Figure 1.8. image with speckle noise .

I.3.Image Filtering

Image filtering is a core task in the field of image processing, aimed at reducing noise in images or datasets. A key requirement for these filtering techniques is their ability to eliminate noise effectively while maintaining the integrity of the image's edges. Traditionally, filtering methods are categorized into two main types: linear and non-linear models.

Linear models are widely used due to their simplicity and computational efficiency. However, they come with significant limitations. One major drawback is their inability to preserve edges, which are essentially abrupt changes or discontinuities in the image. As a result, edges often appear blurred when linear filters are applied.

In contrast, non-linear models offer superior performance in edge preservation compared to linear models. These methods are better equipped to handle discontinuities, making them more effective for tasks where maintaining edge sharpness is critical .

I.4. Subjective Assessment

At present, the most dependable approach for evaluating image quality relies on subjective assessment conducted by human observers. These observers are typically divided into two categories: non-experts and experts. Non-expert viewers often focus on the overall appearance of the image, while expert observers tend to scrutinize finer details more closely.

Subjective evaluation methods generally fall into two main types: reference-based and non-reference

assessments. In reference-based evaluation, observers are provided with standard reference images, which act as benchmarks for their judgments. In contrast, reference-free evaluation requires observers to assess image quality without any reference images for comparison.

Subjective quality assessment relies on human observers to evaluate the quality of images. This approach is considered the most reliable because human perception is the ultimate benchmark for image quality.

I.4.1 Key Characteristics

- Human-Centric: Reflects the actual perception of image quality by viewers.
- Flexible: Can evaluate various aspects of quality, such as sharpness, noise, and color accuracy.
- Time-Consuming: Requires a significant number of observers and controlled experimental conditions

I.4.2 Influencing Factors

Certain factors are taken into account to ensure the reliability of subjective evaluation. These can influence the judgment of observers. The most pertinent are:

a) Observation Distance: The observation distance affects the visibility of a stimulus. This distance is fixed between 4 to 6 times the height of the projected image and must be maintained throughout the test.

b) Screen: It is necessary to calibrate the display device, i.e., the screen, so that it operates under optimal conditions. Without this calibration, the displayed colors may differ from the original stimulus [51].

c) Viewing Conditions: The environment and lighting of the room significantly affect the perception of stimuli (test sequence). High lighting can disturb the observer and thus impair their perception. Conversely, the background color of the room affects the appearance of certain colors.

d) Image Selection: A panel of images with varied visual content and as representative as possible of the scenes related to the intended application should be used.

e) Psychological Factors: To minimize the effects related to the observer's psychological state, it is advisable to start the tests with an initiation session allowing the observer to better understand the test. It is also important to clearly explain the objective of the test and the

protocol to be followed without influencing the participants' judgment. Moreover, it is preferable to conduct numerous short-duration tests (approximately 10 minutes) and varied ones rather than subjecting the observer to long (approximately 30 minutes) and tiring sessions that may lead to hasty and aberrant judgments .

f) **Observers**: It is recommended to have a panel of observers as large as possible, at least fifteen individuals. They can be experts or novices, depending on the theme of the evaluation campaign. Before each session, observers will be selected for their normal or corrected-to-normal visual acuity and normal color vision. The observer must thus have a visual acuity of 10/10 for both eyes with or without correction. The observer panel chosen depends on both the types of treatment to be evaluated and the nature of the study to be conducted. Several criteria must therefore be taken into account when selecting this panel, such as age but also sociocultural, professional origin, etc. Thus, the evaluation campaign can be conducted on a panel of the type "European women aged 30 to 40 or Asian men over 60" .

I.5. Protocols psychosensory subjective evaluation

There are essentially three main common families of subjective evaluation defined by the ITU : Double Stimulus Continuous Quality Scale (DSCQS), Double Stimulus Impairment Scale (DSIS), and Single Stimulus Continuous Quality Evaluation (SSCQE).

I.5.1 Double Stimulus Continuous Quality Scale (DSCQS)

This method is employed to evaluate the quality of images that have been altered or degraded during transmission through a communication channel. The ***Double Stimulus Impairment Scale (DSIS)*** operates in a cyclic manner, where the evaluator is first shown an unimpaired reference image, followed by the same image in its impaired form. The evaluator is then asked to rate the impaired image while considering the reference.

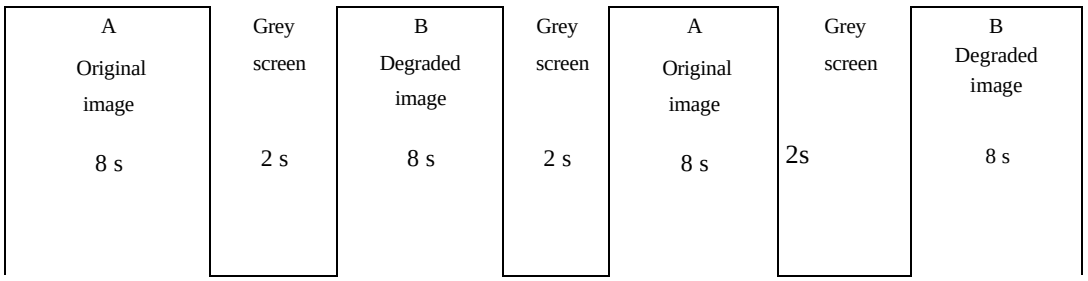


Figure 1.9. Double Stimulus Protocol .

Table 1.1 provides an example of a 5-level rating scale used to evaluate the quality of an image.

Table 1.1: Example of a Rating Scale

Quality	Rating	Description
Excellent	5	Imperceptible
Good	4	Perceptible but not annoying
Fair	3	Slightly annoying
Poor	2	Annoying
Bad	1	Very annoying

I.5.2. Double Stimulus Impairment Scale (DSIS)

Similar to the DSCQS method, each trial in the Double Stimulus Impairment Scale (DSIS) consists of a pair of stimuli: the reference and the test. However, in DSIS, the stimuli are always presented in the same order: the reference first, followed by the test. Observers compare the two stimuli and rate the degradation of the test stimulus relative to the reference using a 5-level impairment scale. Only one vote is cast per DSIS trial.

I.5.3. Single Stimulus Continuous Quality Evaluation (SSCQE)

Instead of viewing pairs of short, separate sequences, observers watch a program typically lasting 20-30 minutes that has been processed by the test system. The reference is not shown (Single Stimulus Continuous Quality Evaluation, SSCQE). Using a slider, observers continuously evaluate the perceived quality in real-time on a DSCQS scale ranging from bad to excellent (see Figure 2.2).

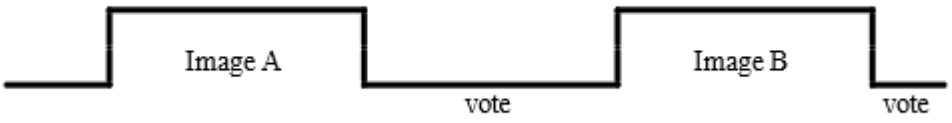


Figure 1.10. Single Stimulus protocol .

A rating scale used to evaluate image quality is provided in Table 2.2. These scales can range from 1 to 5 or even up to 100.

Table 1.2: Image Quality Evaluation Scale.

Quality
Excellent
Good
Fair
Poor
Bad

In the subjective evaluation procedure, several points need to be emphasized. First, the number of observers must be sufficiently large to ensure statistical confidence in image quality experiments. Second, the results of the subjective test are influenced by the experimental conditions, which means that the viewing conditions should be designed to closely align with practical viewing conditions. Additionally, there are several other procedural elements to consider, such as the selection of observers, reference conditions, signal sources for test scenes, the timing of the presentation of various test scenes, and the selection of a range of test scenes.

a) MOS: Mean Opinion Score

Once the tests are completed, the goal is to determine the average quality. A score is assigned to each image by combining the scores from all observers. This score, called the Mean Opinion Score (MOS), is calculated using the following formula:

$$MOS(i) = \frac{1}{N}\sum_{j=1}^{N} Note_i(j)$$

Where N is the number of observers, and ***Note ij*** is the score given by observer jj for the degradation ii of the image.

b) Confidence Interval

To reduce the impact of potential errors, a confidence interval is often associated with each MOS (Mean Opinion Score). It is typically set at 95% and is given by the following relation:

$$e_j = 1.95\frac{\sigma_j}{\sqrt{N}}$$

$$[MOS(i) - e_j, MOS(i) + e_j]$$ Where and

$$\sigma_j = \sqrt{\frac{\sum_{k=1}^{N}\left(Note_i(k) - MOS(k)\right)^2}{N-1}}$$

I.6 Image Databases

Several image databases have been proposed in the field of image quality assessment. In this section, we present the six most widely used image databases in the literature. For each database, we describe the types of images included and the protocols used for subjective evaluation. In the field of image quality assessment (IQA), several image databases have been developed to serve as benchmarks for evaluating and comparing different IQA algorithms. These databases typically contain images with various types and levels of distortions, along with corresponding subjective quality scores provided by human observers. Here are some of the most widely used image databases in IQA:

I.6.1LIVE Image Quality Assessment Database:

- Developed by the Laboratory for Image and Video Engineering (LIVE) at the University of Texas at Austin.
- Contains 29 reference images and 779 distorted images with five types of distortions: JPEG compression, JPEG2000 compression, white noise, Gaussian blur, and fast fading.
- Includes subjective qua lity scores in the form of Difference Mean Opinion Scores (DMOS).



Figure 1.11. Some images Base LIVE .

I.6.2. TID2013 (Tampere Image Database 2013):

- Contains 25 reference images and 3000 distorted images with 24 types of distortions.
- Each distortion type is applied at different levels of severity.
- Includes Mean Opinion Scores (MOS) from human observers.

I.6.3. CSIQ (Categorical Subjective Image Quality) Database:

- Developed at Oklahoma State University.
- Contains 30 reference images and 866 distorted images with six types of distortions: JPEG compression, JPEG2000 compression, global contrast decrements, additive pink noise, Gaussian blur, and additive white noise.
- Includes subjective quality scores in the form of DMOS.

I.6.4. IVC (Image and Video Communication) Database:

- Developed by the Image and Video Communication (IVC) group at the University of Nantes.

- Contains 10 reference images and 185 distorted images with four types of distortions: JPEG compression, JPEG2000 compression, LAR coding, and blur.

- Includes subjective quality scores in the form of MOS.



Figure 1.12.Some images Base IVC .

These databases are essential for the development and validation of IQA algorithms, as they provide a standardized set of images and subjective quality scores that can be used to compare the performance of different methods. Researchers often use these databases to train and test their algorithms, ensuring that they can generalize well to a variety of image distortions and quality levels. The table 1.3 gives a comparison between LIVE and IVC databases:

Table 1.3:compariton LIVE &IVC Data Base.

Feature	LIVE Database	IVC Database
Full Name	LIVE Image Quality Assessment Database	IVC Image Quality Database
Purpose	Benchmarking IQA algorithms with diverse distortions	Testing IQA methods with controlled distortions
Types of Distortions	JPEG, JPEG2000, Gaussian blur, white noise, fast-fading artifacts	JPEG, JPEG2000, additive noise, blur
Dataset Size	Larger, with greater variety and diversity	Smaller, focusing on specific distortions
Subjective Ratings	Includes real-world subjective quality ratings	High-quality subjective ratings
Use Case	Broad-spectrum IQA validation	Targeted IQA testing for specific distortion types

I.7 Objective Evaluation

In short, objective quality measurement (as opposed to subjective quality evaluation by human observers) aims to determine image quality algorithmically. The goal of objective quality assessment research is to design algorithms whose quality predictions align with the subjective evaluations of human observers.

Image quality assessment methods can be classified into three broad categories:

I. 7.1Full-Reference Methods

In these methods, the algorithm has access to a perfect version of the image, which it uses to compare with the degraded version. The perfect version is typically obtained from a high-quality acquisition device and is later degraded by compression or transmission errors.

I.7.2. No-Reference Methods

In these methods, the algorithm only has access to the distorted signal and must estimate its quality without any knowledge of the perfect version. Since no-reference methods do not require reference information, they can be used in any application where quality measurement is needed.

I.7.3. Reduced-Reference Methods

In these methods, partial information about the perfect version is available. A side channel exists through which some reference information can be provided to the quality assessment algorithm. Reduced-reference algorithms use this partial reference information to judge the quality of the distorted signal.

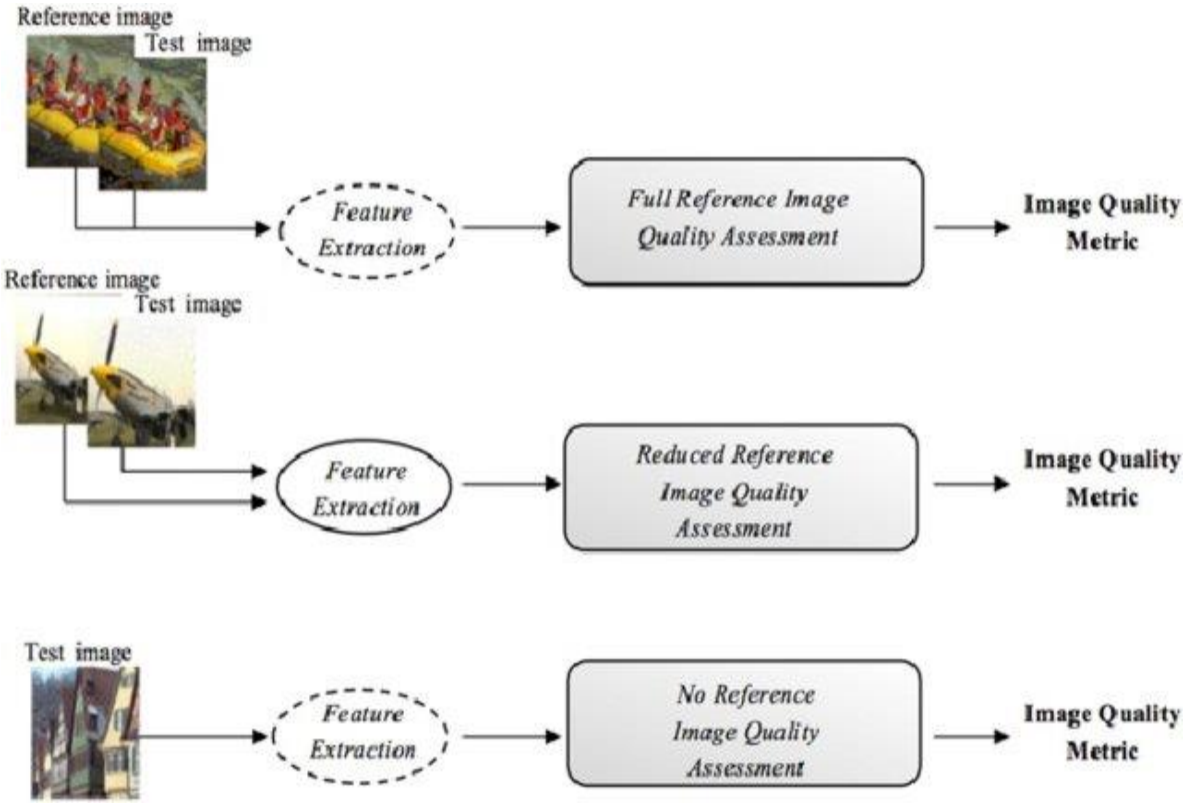


Figure 1.13. Relationship between subjective and objective image quality assessment. .

I.7.4. most commonly used quantitative metrics include:

- **Mean Squared Error (MSE):** is a commonly used metric in regression tasks to measure the average squared difference between the predicted values and the actual values. It provides a way to quantify the accuracy of a model by penalizing larger errors more heavily due to the squaring of the differences.

• **MSE(Mean Square Error)**

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2$$

$\hat{y}_i$: Predicted output value

y_i : Actual (expected) output value

- **Peak Signal-to-Noise Ratio (PSNR):** Peak Signal-to-Noise Ratio (PSNR) is a widely used objective

metric in image quality assessment. It measures the quality of a reconstructed or compressed image compared to its original, uncompressed version. The higher the PSNR value, the better the quality of the reconstructed image.

$$PSNR = 20 \log_{10} \left(\frac{MAX_f}{\sqrt{MSE}} \right)$$

- **MAX**: The maximum possible pixel value of the image (e.g., 255 for 8-bit images).
- **MSE**: Mean Squared Error between the original and reconstructed images, which quantifies the average squared differences between corresponding pixels.- And others.

Practical Work 1: Image quality metrics

In this practical work, we will calculate three common image quality metrics—Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Signal-to-Noise Ratio (SNR)—to compare two images: an original image and a distorted or processed version of it. These metrics are widely used in image processing to evaluate the quality of images after compression, noise addition, or other forms of degradation. This practical work provides a foundation for understanding and applying image quality metrics in various image processing tasks.

1. Objectives

- Calculate MSE, PSNR, and SNR between two images.
- Understand the mathematical formulas and their significance.
- Implement the calculations using Python.

Step 1: Load the Images

First, we need to load the original and distorted images. We will assume the images are grayscale (single channel) for simplicity. If the images are in color, we can convert them to grayscale or calculate the metrics for each channel separately. Uses python function

original_image = cv2.imread('original_image.png', cv2.IMREAD_GRAYSCALE)

distorted_image = cv2.imread('distorted_image.png', cv2.IMREAD_GRAYSCALE)

Step 2: Calculate Mean Squared Error (MSE)

MSE measures the average squared difference between the original and distorted images. A lower MSE indicates better quality. **calculate_mse(original, distorted):**

Step 3: Calculate Peak Signal-to-Noise Ratio (PSNR)

PSNR is a measure of the peak error between the original and distorted images. It is usually expressed in decibels (dB). A higher PSNR indicates better quality. **calculate_psnr(original, distorted):**

Step 4: Calculate Signal-to-Noise Ratio (SNR)

SNR measures the ratio of the signal power to the noise power. A higher SNR indicates better quality. use

calculate_snr(original, distorted);

CHAPTER II: IMAGE SECURITY

II.1.Introduction

Multimedia has become an integral part of our everyday lives, with its usage growing rapidly. The amount of multimedia data generated and shared is significantly larger compared to traditional text-based information. However, the protocols used for multimedia communication often come with their own set of vulnerabilities. As networked multimedia systems continue to expand, the demand for safeguarding digital media has become increasingly critical. This is especially true when it comes to protecting and enforcing intellectual property rights. Without effective security measures, sharing images or videos on public networks exposes them to risks such as theft and unauthorized modifications.

Security measures can be broadly categorized into three main types:

- **Computer Security**: Focuses on protecting data stored on a computer system.
- **Network Security**: Ensures the safety of data while it is being transmitted across networks.
- **Content Security**: Aims to protect intellectual property rights.Ensures the authenticity and trustworthiness of digital content.



Figure 2.1. Types of Security measures .

II.2. Types Of Multimedia Security

Digital multimedia, including audio, video, and still images, faces a wide range of security challenges. For content creators and providers, preventing unauthorized distribution or alteration of their materials is a top priority. On the other hand, end-users want assurance that the content they

download is free from viruses and obtained from legitimate sources. To address these concerns, various security tools such as Encryption and Digital Branding are commonly used.

Among the most widely adopted techniques for securing multimedia are Watermarking ,Cryptography and Steganography. These methods serve different purposes:

- **Watermarking**: Embeds identifiable information into the multimedia content to prove ownership or authenticity.
- **Cryptography:** Protects data by converting it into a format that is unreadable without a decryption key.
- **Steganography**: Hides information within other data, making it invisible to unauthorized users.

Applications of steganography and watermarking extend beyond security. They can be used for feature location (identifying specific components within a dataset), captioning, time-stamping, and tamper-proofing (verifying that the original content has not been altered). These techniques play a crucial role in ensuring the integrity, authenticity, and protection of digital multimedia in various contexts.

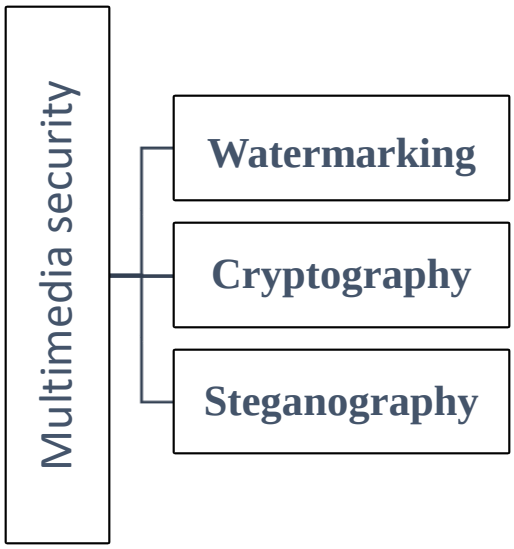


Figure 2.2.Types of Security Multimedia .

II.3 Multimedia Encryption

Multimedia encryption is a critical aspect of securing digital content such as audio, video, and images. It focuses on protecting multimedia data from unauthorized access, tampering, and misuse

during transmission or storage. The primary goals of cryptography in the context of multimedia security are:

- **Confidentiality:** Ensuring that multimedia content is accessible only to authorized parties. Encryption transforms the data into an unreadable format, which can only be decrypted by someone with the correct key. This prevents unauthorized users from accessing or understanding the content.
- **Data Integrity:** Guaranteeing that the multimedia content has not been altered or tampered with during transmission or storage. Cryptographic techniques, such as hash functions, can be used to verify that the data remains unchanged from its original form.
- **Authentication:** Confirming the identity of the sender or the source of the multimedia content. This ensures that the data comes from a legitimate and trusted source, preventing impersonation or fraud.
- **Non-repudiation:** Preventing parties from denying their involvement in a transaction or communication involving multimedia.

II.4. Digital Watermarking:

Digital watermarking involves embedding copyright or verification data into digital files, including audio, video, images, or documents. The embedded data, called the watermark, consists of bits that may include information like the creator's name or ownership details. This method is inspired by the historical practice of marking physical documents and currency.



Figure 2.3. Watermarking example .

II.4.1 Applications of Watermarking:

Watermarking has several important applications, including:

- **Copyright Protection**: is a key application of digital watermarking, where an identifying mark is embedded in a document to link it to its creator or legal owner. In disputes, the watermark can prove ownership. It must be robust enough to resist attacks aimed at erasing it, hindering its detection, or creating ambiguity in ownership claims.
- **Data Integrity**: Data integrity in watermarking involves embedding a mark in an image to authenticate the document or prove its content hasn't been altered. Fragile watermarks are used for strict authentication, becoming undetectable if any data in the document is changed.
- **Document Indexing**: through watermarking involves embedding a unique identifier into digital content for each author. This enables searching for watermarked content online. When web pages are scanned for the watermark, any matches can be flagged, notifying the content owner to take action.
- **Fingerprinting** : through watermarking refers to the unique traits of an object that distinguish it from others. It is used to trace authorized users who violate licensing agreements by illegally distributing copyrighted material. The embedded information often includes client-specific details, such as a unique client ID number.Here's a table give for each application of watermarking an example.

Table.2.1: Watermarking application's examples

Application	Example
Copyright Protection	A photographer embeds their name or copyright information in a photo. If used without permission, the watermark proves ownership.
Data Integrity	A government document is watermarked. If altered, the watermark becomes undetectable, indicating tampering.
Document Indexing	A researcher embeds a unique identifier in their paper to track its usage. If the paper is posted on an unauthorized site, the researcher is notified.

Fingerprinting	An eBook publisher adds a unique client ID to each copy. If the eBook is shared illegally online, the watermark helps trace the original purchaser.

II.4.2.Watermarking Constraints:

Digital watermarking involves balancing trade-offs between payload capacity, transparency, and robustness. These trade-offs are shaped by the specific needs of different applications. Watermarking systems are designed to meet these requirements, taking into account the inherent characteristics of the technology. Figure II.4 highlights the key requirements of digital watermarking.

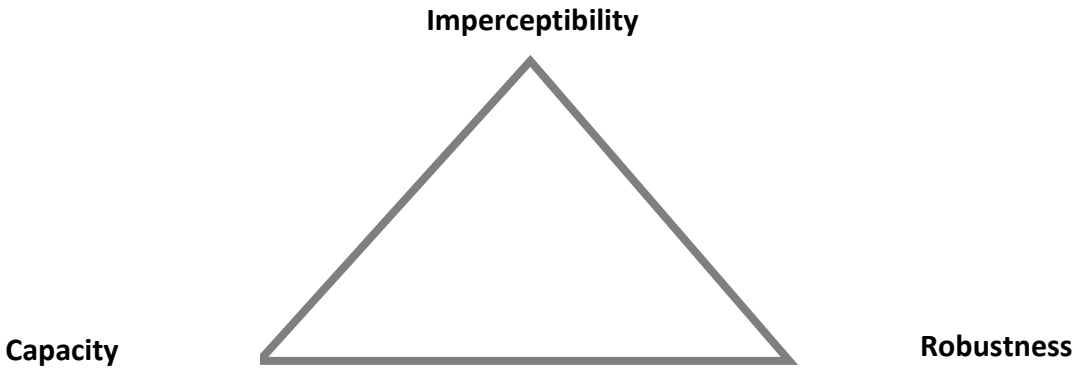


Figure 2.4. Watermarking Constraints .

- **Capacity:** is the amount of hidden data, typically measured in bits. This capacity is related to the number of messages that can be embedded through the encoding algorithm. As the size of the host data increases, more watermark bits can be embedded, thus directly increasing the payload capacity.
- **Imperceptibility:** refers to how much distortion is introduced when embedding a watermark. It is evaluated through two key measures: fidelity, which compares the similarity between the original and watermarked objects, and quality, which assesses the acceptability of the watermarked object through an independent test. Both fidelity and quality are used to evaluate the imperceptibility of the watermark.
- **Robustness:** This aspect can be divided into two parts: robustness and security are two key aspects of watermarking, often confused with each other. Robustness refers to the watermark's ability to endure transformations like geometric changes (e.g., rotation, cropping) or alterations

in image characteristics (e.g., color or saturation). It also includes resilience to frequency-based degradations, such as lossy compression or filtering. Security in watermarking refers to the watermark's resistance to malicious attacks, where attackers try to remove or decode the watermark. These attackers are often assumed to know the algorithm used and may attempt to uncover the key through detailed analysis of the watermarking method.

II.5. Digital Watermarking phases

Watermarking consists of two fundamental phases: insertion phase and extraction phase

II.5.1 Insertion Phase:

The inputs for the watermarking insertion are the watermark, the original data, and the key. The watermark can be a sequence of numbers, a binary bit sequence, or even an image. The key is used to enhance the security of the watermarking system. The output of the insertion process is the watermarked data.The general diagram for watermark insertion (watermarking) typically includes the following steps:

- **Inputs:** Watermark (W): This could be a sequence of numbers, a binary bitstream, or an image. Original data (I): The digital content (image, audio, video, etc.) that will be watermarked. Key (K): This is used to improve the security of the watermarking process.
- **Process:** The watermark (W) is embedded into the original data (I) using the key (K). The process aims to modify the content in such a way that the watermark is imperceptible or minimally noticeable, depending on the type of watermarking (robust, fragile, etc.).
- **Output:** The output is the watermarked data, which is the original data (I) with the watermark (W) embedded into it. The watermarked content is visually (or audibly) similar to the original but now contains the hidden watermark.

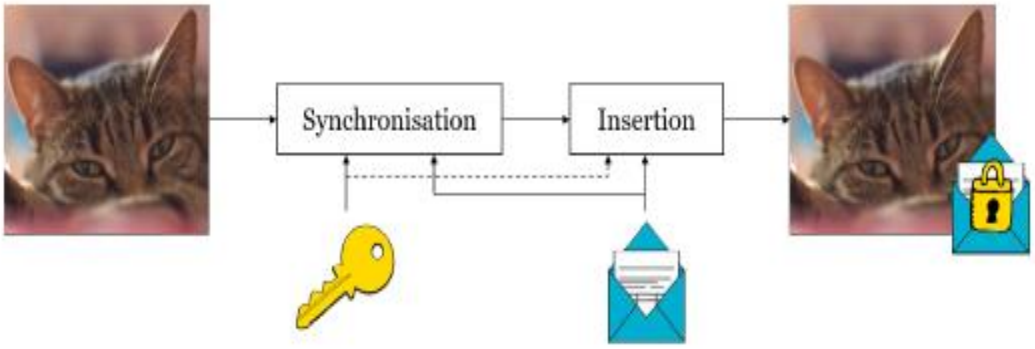


Figure 2.5. Watermarking Insertion phase .

II.5.2 Extraction Phase:

The process of watermark extraction in watermarking typically follows these steps:

- **Input Watermarked Data**: The process starts with the watermarked data (image, audio, video, or document) that has had the watermark embedded during the insertion phase.
- **Watermark Extraction Algorithm**: The watermarked data is processed using an extraction algorithm that is designed to retrieve the watermark. The algorithm applies various techniques based on the type of watermarking scheme (e.g., blind or non-blind, robust or fragile).
- **Key (if necessary):** In some watermarking schemes, a key (such as a secret key) may be required to extract the watermark. In blind watermarking, the key is not needed for extraction, but in non-blind schemes, it is essential.
- **Watermark Output:** The watermark, which can be a sequence of bits, numbers, or an image, is extracted and provided as the output. If the watermark is embedded properly, it will match the original watermark used during the insertion phase.
- **Comparison (optional):** The extracted watermark can be compared with the original watermark to verify the data integrity, ownership, or authenticity of the content.

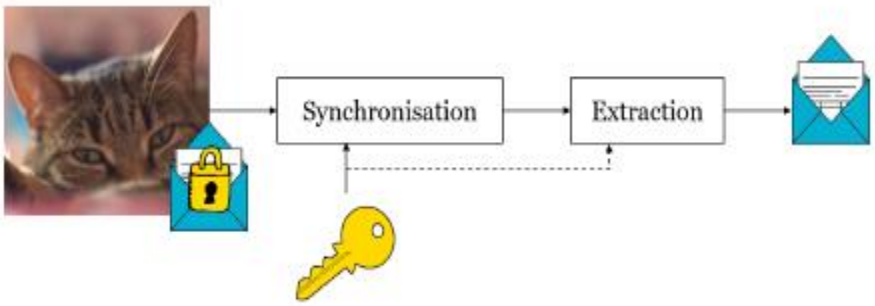


Figure 2.6. Watermarking Extraction Phase .

This process ensures that the embedded watermark can be retrieved and verified, ensuring the protection, tracking, or authenticity of digital content.

II.6.Types of Watermarking based on their level of resistance:

Watermarking schemes can be categorized into three main types based on their level of resistance to alterations and attacks. These types are: Robust Watermarking, Fragile Watermarking and Semi-Fragile Watermarking. Each type serves different purposes and is designed to withstand specific levels of modification or attack.

II.6.1. Robust Watermarking

- **Purpose**: Designed to resist both intentional and unintentional modifications to the document.
- **Resistance**: Highly resistant to a wide range of attacks, including compression, filtering, cropping, rotation, scaling, and noise addition.
- **Applications:** Copyright protection (to prove ownership of digital content).,Digital rights management (DRM) and Tracing the source of illegal copies.
- **Characteristics:** The watermark remains detectable even after significant alterations. Often embedded in the frequency domain (e.g., DCT, DWT) for better resilience. Requires a trade-off between robustness and imperceptibility.

II6.2. Fragile Watermarking

- **Purpose:** Designed to be highly sensitive to any modifications, making it ideal for detecting tampering or unauthorized changes.
- **Resistance:** Not resistant to alterations; the watermark is destroyed or altered if the

document is modified.

- **Applications:** Integrity verification (to detect if a document has been tampered with). Authentication of digital content. Ensuring the originality of sensitive documents (e.g., legal or medical records).
- **Characteristics:** The watermark is embedded in a way that any change to the document will affect it. Often used in the spatial domain (e.g., pixel-level modifications). There are three types of watermarking schemes categorized by their level of resistance.

II.6.3 Semi-Fragile Watermarking

- **Purpose**: A hybrid approach that is resistant to certain types of modifications (e.g., compression) but sensitive to others (e.g., malicious tampering).
- **Resistance:** Resists legitimate, non-destructive operations (e.g., lossy compression) but detects malicious alterations.
- **Applications:** Distinguishing between acceptable modifications (e.g., compression) and malicious tampering. Authenticating content while allowing for some processing.
- **Characteristics** :Balances the properties of robust and fragile watermarking. Useful in scenarios where some modifications are expected but tampering must be detected.

The next table Table II.2 gives a comparison of Watermarking Types

Table.2.2: Comparison of Watermarking Types

Feature	Robust Watermarking	Fragile Watermarking	Semi-Fragile Watermarking
Resistance	High resistance to attacks	No resistance to alterations	Resists some modifications
Sensitivity	Insensitive to changes	Highly sensitive to changes	Sensitive to malicious changes
Use Case	Copyright protection, DRM	Integrity verification	Authentication, tamper detection
Embedding Domain	Frequency domain (e.g., DCT)	Spatial domain (e.g., pixels)	Hybrid (frequency/spatial)

Trade-off	Robustness vs. imperceptibility	Fragility vs. tamper detection	Balance of robustness/sensitivity

II.7.Types of Watermarking based on human perception

Watermarking can also be classified i.e., whether the watermark is visible or invisible to the human eye or ear. This classification depends on how the watermark is embedded in the digital content (image, audio, video, or text) and whether it is designed to be perceptible or imperceptible to humans.

II.7.1. Invisible Watermarking

Invisible watermarks are embedded in such a way that they cannot be perceived by humans under normal viewing or listening conditions. They are hidden within the content and require specialized tools or algorithms to detect or extract them.

- **Characteristics:**
  - Imperceptible: The watermark does not alter the visual or auditory quality of the content.
  - Robustness: Often designed to be robust against modifications and attacks.
  - Detection: Requires specific software or keys to extract the watermark.
- **Applications :**
  - Copyright protection (e.g., proving ownership without affecting the content's appearance).
  - Digital rights management (DRM).
  - Tamper detection and content authentication.
- **Examples:**
  - Embedding a watermark in the frequency domain of an image (e.g., using DCT or DWT).
  - Hiding a watermark in the least significant bits (LSB) of pixel values in an image.
  - Embedding an inaudible watermark in an audio file.

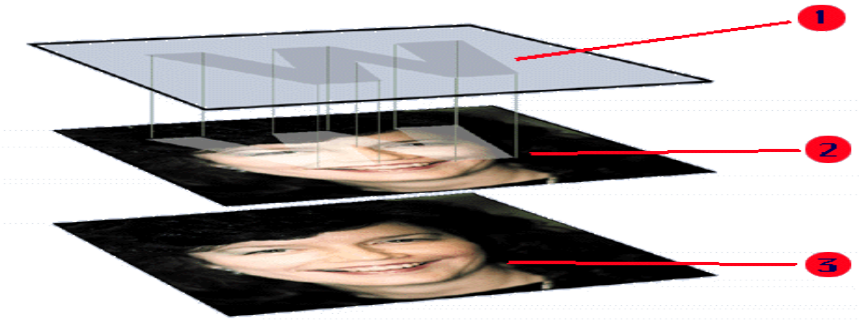


Figure 2.7. Invisible Watermarking.

II.7. 2Visible Watermarking

Visible watermarks are intentionally designed to be perceptible to humans. They are often overlaid on the content in a way that is clearly visible or audible, serving as a deterrent against unauthorized use.

- **Characteristics:**
  - Perceptible: The watermark is clearly visible or audible.
  - Transparency: While visible, it is often designed to not completely obstruct the content.
  - Purpose: Acts as a deterrent or provides immediate identification of ownership.
- **Applications:**
  - Branding (e.g., adding a logo or text to images or videos).
  - Demonstrating ownership (e.g., "Sample" or "Proof" watermarks on preview content).
  - Preventing unauthorized use by making the content less appealing for redistribution.
- **Examples:**
  - A semi-transparent logo overlaid on an image or video.
  - Text watermarks (e.g., "Copyright" or "Do Not Copy") displayed on documents or videos.
  - Audio watermarks, such as a voiceover stating ownership or usage rights.

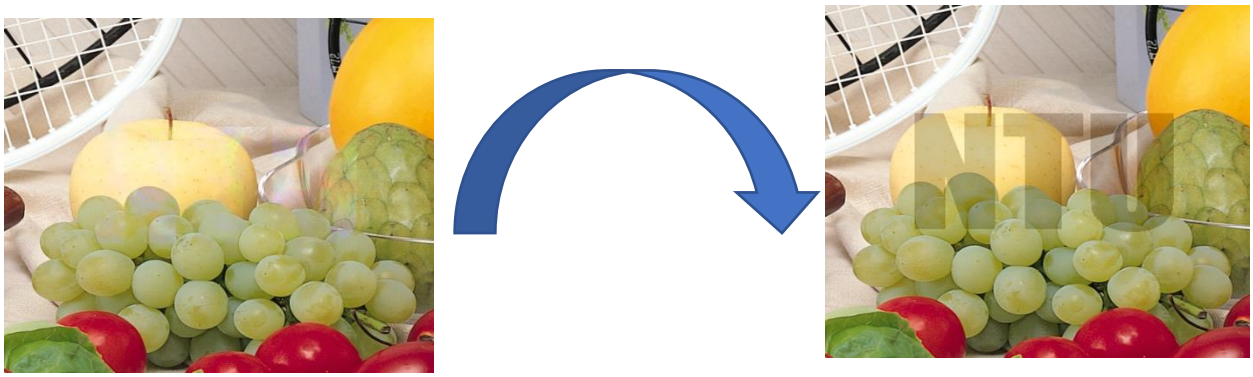


Figure 2.8. Visible Watermarking.

The digital watermarking is a critical technology for protecting digital content in an era where intellectual property breaches are increasingly common. It begins by defining digital watermarking as the process of embedding copyright or verification data into digital files, such as audio, video, images, or documents. The watermark, which can include information like the creator's name or ownership details, serves as a tool for monitoring content usage and managing its distribution.

Practical Work 2: Image watermarking using LSB

Exercise 01:

1. Encode "hello everyone" using the shift caesar cipher and the key K = 9
2. Decode "IUSVX KYYOUT GBKI VKXZK" knowing that it was created by a Caesar cipher with K=6

Exercise 02:

1. Using the LSB Method the last two bits to hide a message in an image, the image cover is :

   a. X = [132,127,205 , 212 ;
   250, 212 , 102 , 55 ;
   205 ,145, 115,45 ;
   200, 0 ,118 ,76 ;
   41 ,122 ,100 ,127 ;
   101,41 ,78 ,198 ;
   95,46 ,178 ,254]

2. In this image cover hide the secret message "ALEGRIA" in the case using the LSB method with the last two bits (each line contains one character)
3. Using the LSB method with the last four bits (each line contains two characters) to hide a message in a concealment image we obtained the following stego image Y:

196	**204**	**4**	**249**
245	**193**	**100**	**69**

To help you, here is the ASCII alphabet code:

ASCII BINARY ALPHABET

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1010111
L	1001100	Y	1011001
M	1001101	Z	1011010

II.8. cryptography Multimedia

Cryptography plays a critical role in securing multimedia data, such as images, videos, and audio files, against unauthorized access and tampering. With the proliferation of digital media, the need for robust cryptographic techniques in multimedia applications has become increasingly significant. This lesson provides an in-depth exploration of cryptology in the context of multimedia, including its principles, methods, and applications. The material is designed for students and professionals seeking to understand how cryptographic techniques are applied to protect multimedia data.

II.8.1 Definition of Cryptology

Cryptology is a compound word derived from Greek: “kryptos”, meaning "secret," and “logy, meaning "science." It is the science of secrecy and has only recently been recognized as such. Cryptology encompasses both cryptography (secret writing) and cryptanalysis (the analysis of secret writing). It can be described as an ancient art and a modern science: ancient because Julius Caesar used it, and it appears in the Old Testament in the form of the Atbash cipher; modern because it has only been a topic of scientific research since the 1970s.

II.8.2 Definition of Cryptography

The term cryptography originates from two Greek words: “kryptos” (secret) and “graphein”(writing). Cryptography is the art of hiding information to make it unintelligible. It encompasses techniques used to encrypt messages.The process of encryption uses a key called the encryption key, while decryption relies on a key known as the decryption key

II.8.3 Terminology

Key terms used in cryptography include:

- **Cryptology:** A mathematical science that encompasses both cryptography and cryptanalysis.
- **Cryptography:** The study of methods to securely send data over a specific medium.
- **Ciphertext:** The encrypted text produced after applying encryption to plaintext.
- **Plaintext**: The original message intended for encryption.
- **Encryption**: A process that transforms data (text, messages, etc.) into an unreadable format

for anyone other than the creator and intended recipient.

- **Decryption**: The process of converting ciphertext back into plaintext.
- **Cryptanalysis**: Contrary to cryptography, cryptanalysis aims to retrieve plaintext from ciphertext by identifying weaknesses in the algorithms used.
- **Cryptosystem**: A cryptosystem consists of a cryptographic algorithm, all possible keys, and the protocols that enable its operation
- **Key**: A parameter used in cryptographic operations (encryption or decryption). There are two main types of keys:
    - **Symmetric keys**: Used for both encryption and decryption, enabling symmetric or secret-key encryption.
    - **Asymmetric keys**: Used in public-key encryption, where different keys are applied for encryption and decryption.

Multimedia encryption and decryption system is illustrated in Figure

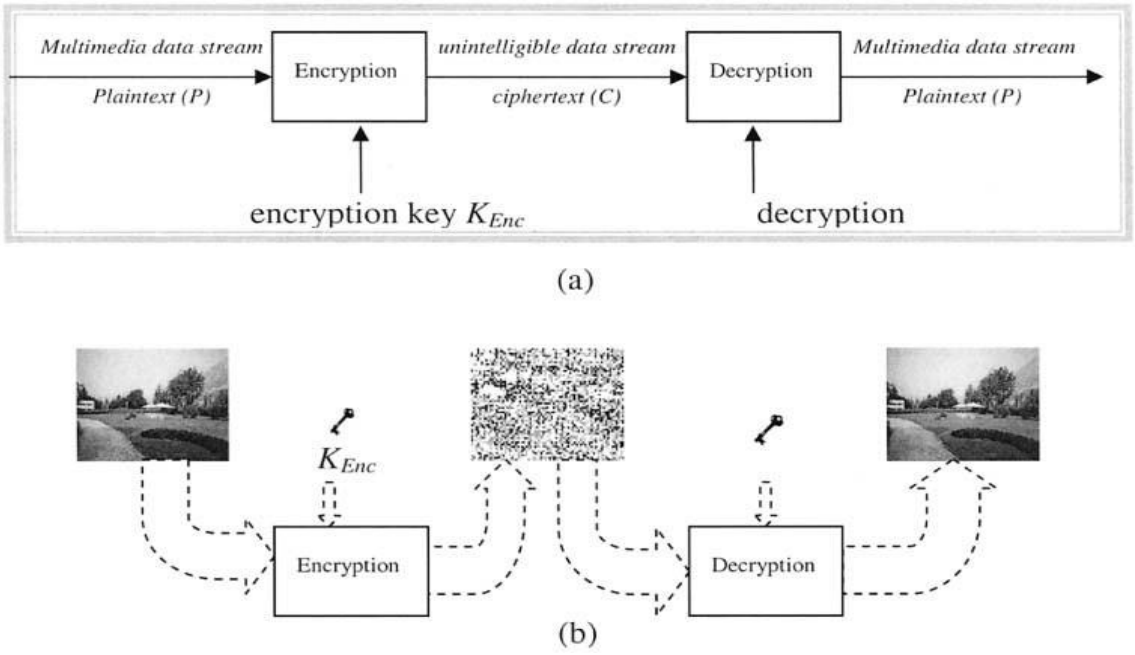


Figure 2.9. Multimedia encryption and decryption system.

II.9. Symmetric-key Cryptography

Symmetric key cryptography uses a single key for both encryption and decryption. It is widely used in multimedia applications due to its efficiency and speed. Common symmetric algorithms include:

II.9.1 Advanced Encryption Standard (AES) for Image Encryption:

The Advanced Encryption Standard (AES) is widely used for securing digital data, including image encryption. AES operates on fixed-size blocks of data (128 bits) using symmetric-key cryptography, which makes it efficient and secure for multimedia applications, such as image encryption. Below is a detailed explanation of how AES can be applied to encrypt images:

- **Overview of AES** : AES is a symmetric encryption algorithm that encrypts data in blocks of 128 bits using keys of 128, 192, or 256 bits. It follows a series of transformation rounds based on the key length: 10 rounds for 128-bit keys,12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

- **Main operations** :Each round consists of four main operations:
  - **SubBytes:** A non-linear substitution step using an S-box.
  - **ShiftRows:** A transposition step where each row of the state is shifted cyclically.
  - **MixColumns:** A mixing operation combining the columns of the state matrix.
  - **AddRoundKey:** A bitwise XOR operation with the round key.

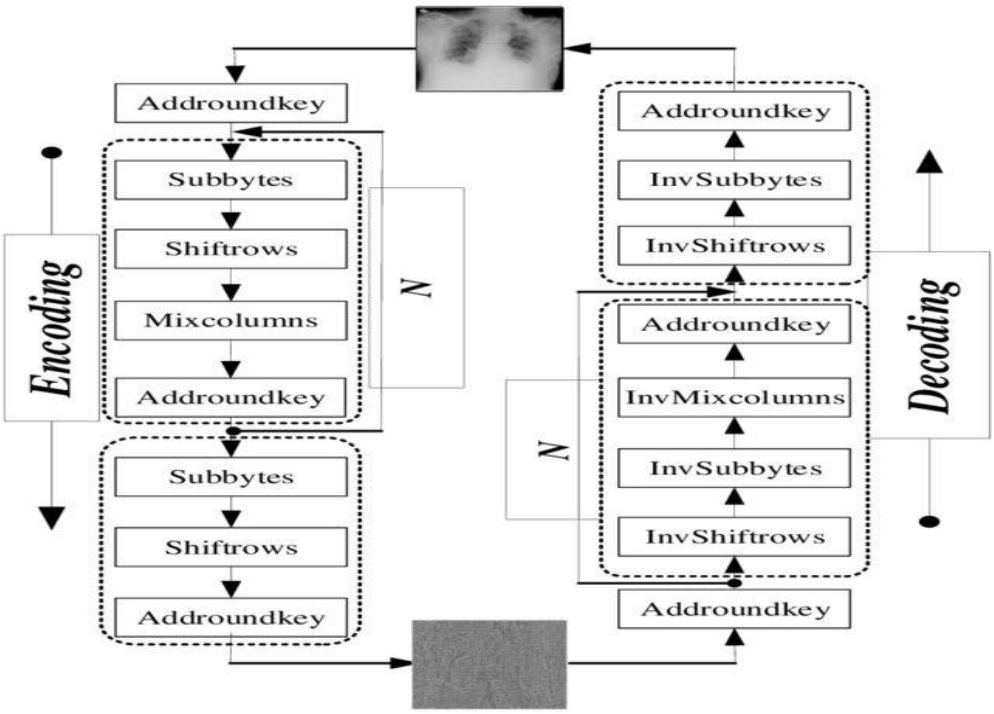


Figure 2.10. Image Encryption Using AES Multimedia encryption and decryption system

II.9.2Data Encryption Standard (DES) for Image Encryption:

The Data Encryption Standard (DES) is one of the earliest and most well-known symmetric encryption algorithms. Developed in the 1970s, DES was widely adopted for securing sensitive data, including images, before being gradually replaced by more advanced algorithms like AES (Advanced Encryption Standard). Despite its limitations, DES remains a foundational algorithm in cryptography and is still used in certain applications. DES was designed to provide confidentiality for digital data, including images. While it is no longer considered secure for highly sensitive applications due to its short key length (56 bits). While DES is no longer recommended for high-security applications, it can still be used in certain scenarios:

- **Educational Tools**: DES is often used in cryptography courses to demonstrate encryption principles.
- **Legacy Systems**: Some older systems, such as embedded devices or industrial equipment, may still use DES for image encryption.
- **Low-Security Applications**: In cases where security is not a critical concern, DES can provide basic encryption for images.

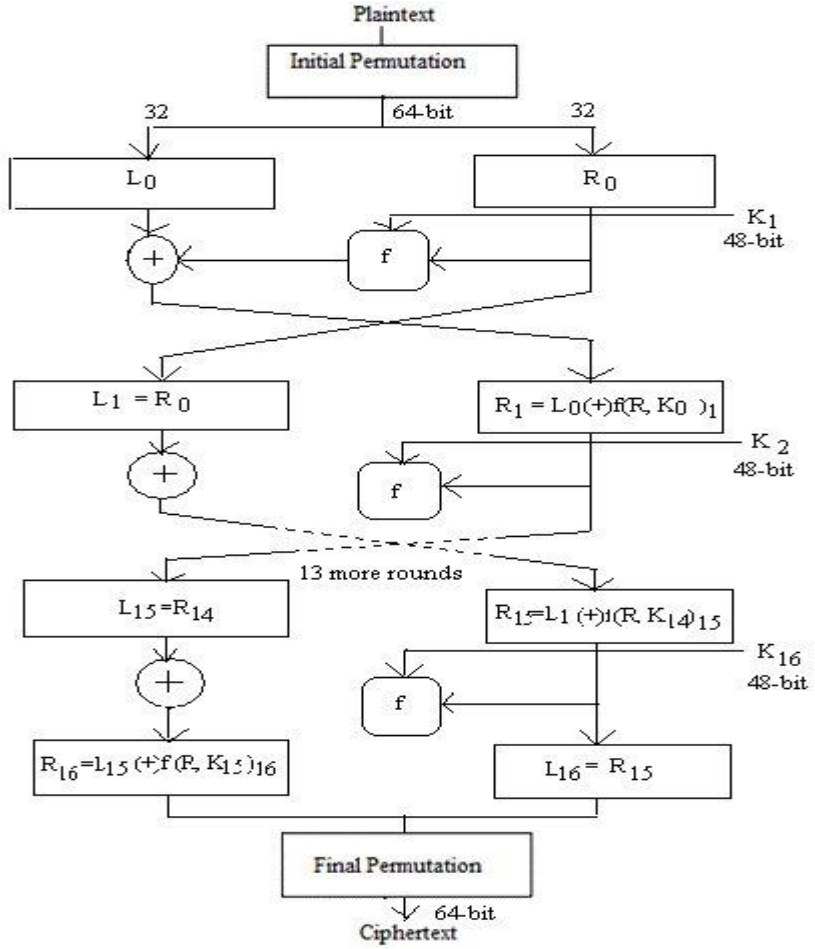


Figure 2.11. Image Encryption with DES

Table a detailed comparison table for AES and DES when applied to image encryption:

Feature	AES (Advanced Encryption Standard)	DES (Data Encryption Standard)
Key Size	128, 192, or 256 bits	56 bits
Block Size	128 bits	64 bits
Number of Rounds	10 (128-bit key), 12 (192-bit key), 14 (256-bit key)	16 rounds
Security	Very high due to larger key size and more rounds.	Moderate, vulnerable to brute force due to small key size.
Performance	Faster on modern processors due to optimized implementation.	Slower compared to AES.
Algorithm Structure	Substitution-permutation network.	Feistel network.
Key Scheduling	Complex and robust key expansion algorithm.	Relatively simple key schedule, vulnerable to attacks.
Computational Overhead	Higher due to complex operations but efficient on hardware.	Lower computational complexity but less secure.
Resistance to Attacks	Resistant to linear and differential cryptanalysis.	Vulnerable to cryptanalysis and brute force.

Image Quality Impact	Maintains image quality with minimal artifacts.	Slightly more susceptible to visual artifacts.
Use in Practice	Widely used for secure applications including multimedia encryption.	Largely replaced by AES due to stronger security.
Flexibility	Supports multiple key lengths for various security requirements.	Fixed key length, limited flexibility.
Suitability for Images	Better suited for real-time and high-security image encryption.	Suitable for basic encryption but less secure for sensitive images.

- AES is generally preferred for image encryption due to its robust security, support for larger key sizes, and faster performance on modern hardware.
- DES, while historically significant, is now considered outdated and less secure, making it suitable only for less critical or legacy applications.

Symmetric key cryptography is particularly suitable for encrypting large multimedia files, such as videos, where speed and computational efficiency are critical.

II.10.Asymmetric Cryptography RSA (Rivest-Shamir-Adleman)

Asymmetric key cryptography uses a pair of keys—a public key for encryption and a private key for decryption. It is often used for secure key exchange and digital signatures in multimedia systems.

RSA (Rivest–Shamir–Adleman) is an asymmetric cryptographic algorithm that uses a pair of keys (public and private) for encryption and decryption. While it is widely used for securing text and digital signatures, applying RSA to image encryption poses unique challenges and requires specific adaptations. Below is an explanation of how RSA can be applied to encrypt images, along with its limitations and considerations. Figure I.4 illustrates the fundamental principle of the RSA method.

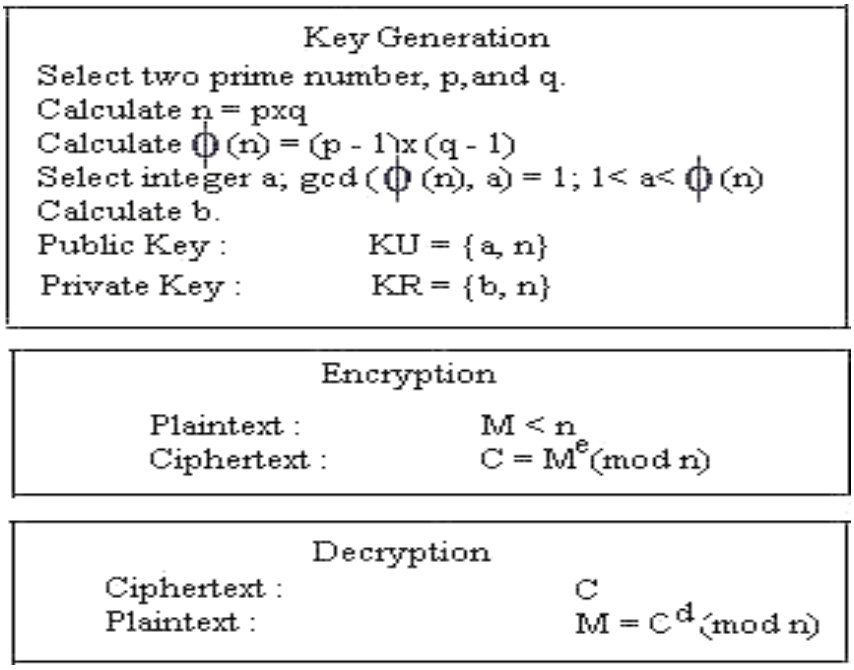


Figure 2.12. Principe of RSA

The figure 2.13 illustrate the flow chart of image encrypt encryption and decryption using RSA.

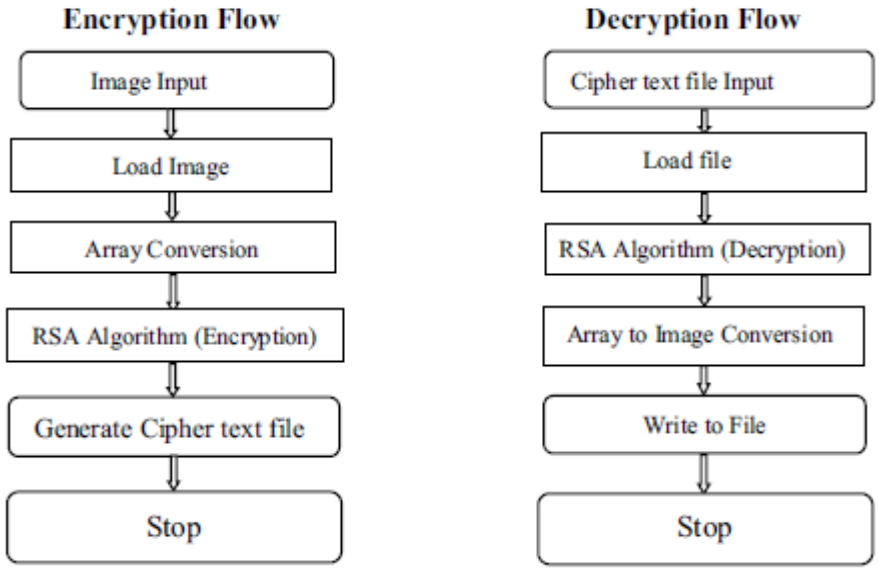


Figure 2.13. Flow of Image Encryption and decryption using RSA

Asymmetric cryptography is particularly useful for securing multimedia content in applications like video conferencing and digital rights management (DRM).

II.11. Applications of Multimedia Cryptography

- **Digital Rights Management (DRM):** DRM systems use cryptographic techniques to

protect copyrighted multimedia content, such as movies, music, and e-books, from unauthorized distribution and piracy.

- **Secure Video Conferencing**: Encryption ensures that video and audio streams in video conferencing applications remain confidential and tamper-proof, protecting sensitive communications.

- **Medical Imaging**: In healthcare, cryptographic techniques secure medical images and videos, ensuring patient privacy and compliance with regulations like HIPAA.

- **Military and Surveillance**: Multimedia cryptography is used to secure sensitive visual and audio data in military and surveillance applications, preventing unauthorized access and tampering.

- **Social Media and Cloud Storage**: Encryption and watermarking protect multimedia content shared on social media platforms and stored in cloud environments, safeguarding user privacy and intellectual property.

Cryptographic techniques play a vital role in securing multimedia content in an increasingly digital world. From symmetric and asymmetric encryption to digital watermarking and steganography, these methods ensure the confidentiality, integrity, and authenticity of multimedia data. As technology continues to evolve, so too must the cryptographic techniques used to protect it. By addressing current challenges and embracing emerging trends, we can build a more secure future for multimedia applications. - Ensures only authorized users can access or distribute multimedia content.

Practical Work 3:Image Encryption Using RSA

1) Detailed Example RSA Key calculation

- Choose two prime numbers: p = 7 and q = 19.
- Compute n = p * q = 7 * 19 = 133.
- Compute m = (p - 1) * (q - 1) = 6 * 18 = 108.
    - Choose **e** such that it is coprime with **m** (GCD(e, m) = 1):
    - GCD(2, 108) = 2 → Not coprime ,GCD(3, 108) = 3 → Not coprime.
    - GCD(4, 108) = 4 → Not coprime ,GCD(5, 108) = 1 → e = 5 (valid choice).
- Determine "d" such that "d * e" mod m = 1;
    - This means d = (1 + k * m) / e➔ for some integer k.
    - Try values of "k":
        - k = 0**: d = 1/5 → Not an integer.
        - k = 1**: d = 109/5 → Not an integer.
        - k = 2**: d = 217/5 → Not an integer.
        - **k = 3**: d = 325/5 = 65 → **d = 65** (valid choice).
- **Public Key: (n = 133, e = 5).**
- **Private Key: (n = 133, d = 65).**

2)Encryption and Decryption with RSA

- Given: n = 133, e = 5, d = 65.
- Suppose we want to transmit the message x = 6.

Encryption:

- Compute y = **x^e** mod n. ;y = 6^5 mod 133. Encrypted message: **y = 62.**

- Decryption:

- Compute x = y^d mod n. ; x = 62^65 mod 133.
- Simplify using modular exponentiation:
- Break down 62^65 mod 133:
- Compute 7502 mod 133 = 6.

- Decrypted message: **x = 6.**

This example demonstrates the RSA algorithm for key generation, encryption, and decryption. The original message is successfully recovered after decryption, confirming the correctness of the process.

3) Image Encryption Using RSA

This practical work (TP) is designed to help students understand and implement the RSA algorithm for image encryption. The goal is to encrypt an image using RSA, transmit the encrypted image, and then decrypt it to recover the original image. This TP will cover key generation, encryption, and decryption processes.

Objective

- Implement the RSA algorithm to encrypt and decrypt an image.
- Understand the steps involved in RSA key generation, encryption, and decryption.
- Gain hands-on experience with modular arithmetic and cryptographic techniques.

Tools and Prerequisites

- Programming Language: Python (recommended due to its simplicity and libraries).
- Basic Knowledge: RSA algorithm. , Modular arithmetic,Python programming.

Steps for the TP

1. Key Generation like the precedent example
2. Image Encryption: Load the image and convert the image into a pixel matrix and encrypt each pixel value using the public key (n, e). Save the encrypted pixel values as a new image.
3. Image Decryption: Load the encrypted image and convert the encrypted image into a pixel matrix. Decrypt each pixel value using the private key (n, d). Reconstruct the original image from the decrypted pixel values.
4. Verification: Compare the original image and the decrypted image to ensure they are identical. Analyze the encryption and decryption process for correctness.

This TP provides a hands-on approach to learning RSA encryption and its application in securing images. It encourages students to explore cryptographic concepts and develop problem-solving skills.

II.12.Steganography in Multimedia

Steganography is the art and science of hiding information within other non-secret data, such as images, audio, or video files, without altering the perceptible quality of the carrier medium. Unlike cryptography, which focuses on making data unreadable, steganography aims to conceal the very existence of the data. This makes it a powerful tool for secure communication, copyright protection, and digital watermarking.

In this section, we will explore steganography in multimedia, focusing on techniques for hiding data in images, audio, and video, as well as their applications and challenges.

II.12.1Steganography?

Steganography involves embedding secret information (e.g., text, images, or audio) into a carrier file (e.g., an image, audio, or video) in such a way that the presence of the hidden data is undetectable to the human eye or ear. The carrier file is called the **cover medium**, and the file containing the hidden data is called the stego medium.Images are the most common medium for steganography due to their widespread use and the availability of redundant data that can be manipulated without noticeable changes.

II.12.2. Least Significant Bit (LSB) Replacement:

The LSB of each pixel's color channel (e.g., red, green, blue) is replaced with a bit of the secret message.For example: In an 8-bit grayscale image, the LSB of each pixel can be modified to store 1 bit of the secret message.

- Advantages: Simple and easy to implement.
- Disadvantages: Vulnerable to statistical analysis and noise.

II.13. Challenges in Multimedia Steganography

- **Capacity vs. Robustness**: increasing the amount of hidden data often reduces the robustness of the stego medium against compression or noise.
- **Detection and Analysis**: Advanced steganalysis techniques can detect the presence of hidden data by analyzing statistical anomalies in the stego medium.
- **Compression and Format Conversion**: Lossy compression (e.g., JPEG, MP3, MPEG) can destroy hidden data, making it difficult to recover.
- **Real-Time Processing**:- Embedding and extracting data in real-time (e.g., live video streams) requires efficient algorithms and hardware.

Steganography in multimedia is a powerful technique for secure communication, digital

watermarking, and covert surveillance. By hiding data in images, audio, or video files, steganography ensures that the presence of the hidden information remains undetectable. While challenges such as capacity, robustness, and detection exist, ongoing research and technological advancements are addressing these issues. As multimedia continues to dominate digital communication, steganography will play an increasingly important role in ensuring data security and privacy.

CHAPTR III: CHARACTERIZATION OF THE PROPAGATION CHANNEL

III.1.Introduction

This chapter provides a comprehensive understanding of key technologies that impact the quality of multimedia content transmission. It explores advanced techniques such as **propagation channel characterization**, **MIMO systems**, and **joint source-channel coding**. The course emphasizes how to optimize transmission strategies by considering both the content being transmitted and the characteristics of the channel, ultimately improving the overall multimedia quality in various real-world applications like video streaming, telecommunication, and real-time communication systems.

III. 2. Characterization of the Propagation Channel

A propagation channel describes the path through which electromagnetic signals travel from the sender (transmitter) to the receiver. The quality of the propagation channel significantly influences the signal strength, clarity, and reliability of the communication. Physical phenomena such as interference, fading, and path loss can degrade the signal, creating challenges in maintaining high-quality transmission. Therefore, understanding the propagation channel is essential for enhancing multimedia transmission in real-world conditions.

III.2.1Factors Affecting the Propagation Channel

- **Interference:** Interference occurs when overlapping signals disrupt the original signal, often leading to reduced clarity or performance. This is common in environments with multiple communication devices.
- **Fading**: Fading refers to variations in signal strength caused by obstacles, environmental factors, or the multiple paths signals take to reach the receiver (multipath propagation).
- **Multipath fading:** When signals arrive via different paths, they may combine constructively or destructively.
- **Shadowing:** Obstacles like walls or buildings can block or weaken the signal.
- **Path Loss**:As signals propagate, they lose power due to distance, atmospheric conditions, and medium characteristics. This is especially significant over long distances, such as in rural or open areas.

II.2.2 Environmental Impacts on Channel Characteristics

Indoor Settings:

- In indoor environments, signals encounter walls, furniture, and objects, causing reflection, refraction, and scattering.
- Materials like concrete, metal, and glass further contribute to attenuation.

Urban Areas

- Urban settings are characterized by dense buildings and infrastructure, leading to increased multipath propagation and signal degradation.
- The presence of numerous devices and networks increases interference, which can reduce communication quality.

Rural Areas

- In rural environments, signals often have a clearer line of sight (LOS), resulting in less interference from obstacles.
- However, the greater distances between transmitters and receivers can lead to higher path loss, making it necessary to use stronger transmitters or additional relay stations.

III.2.3.Importance of Characterizing the Channel

By analyzing and characterizing propagation channels, engineers can design more efficient communication systems. For instance:

- Optimizing network designs for 5G and IoT to ensure reliable performance in diverse environments.
- Developing adaptive systems that adjust to fading, interference, or changing environmental conditions.
- Enhancing signal processing techniques for multimedia applications, such as video streaming and online gaming, to improve user experience.

Understanding the nuances of the propagation channel helps to address challenges and leverage opportunities in modern communication networks.

III.3. Closed-loop MIMO Systems

III.3.1.Multiple-Input Multiple-Output (MIMO)

systems use multiple antennas at both the transmitter and receiver ends to improve signal quality and capacity. This is especially beneficial in wireless communication systems, such as Wi-Fi and 4G/5G

networks, because it increases the amount of data that can be transmitted without requiring additional bandwidth.

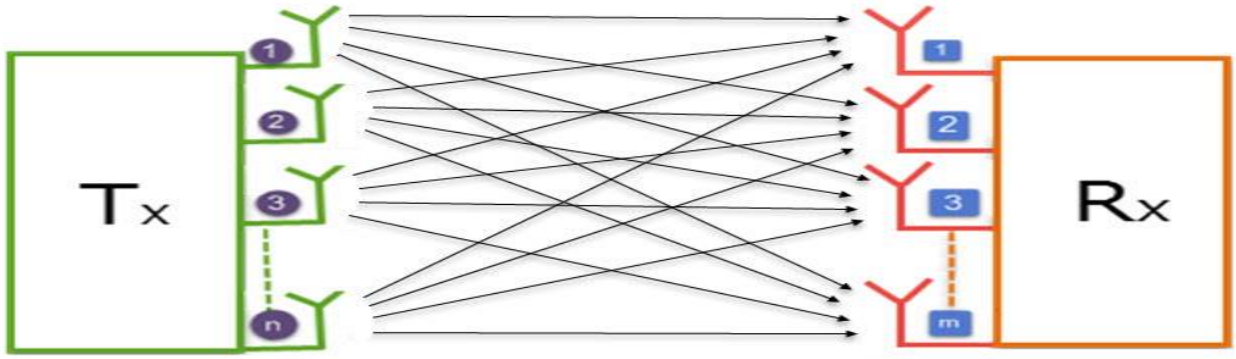


Figure 3.1. MIMO System

III.3.2.Basic Block Diagram of a MIMO System

A MIMO system processes information bits through encoding, interleaving, and symbol mapping (e.g., QAM). A space-time encoder then generates spatial data streams, which are mapped to transmit antennas via precoding. The transmitted signals propagate through the channel and are received by an antenna array. The receiver reverses these operations, including space-time decoding and deinterleaving, to recover the original data.

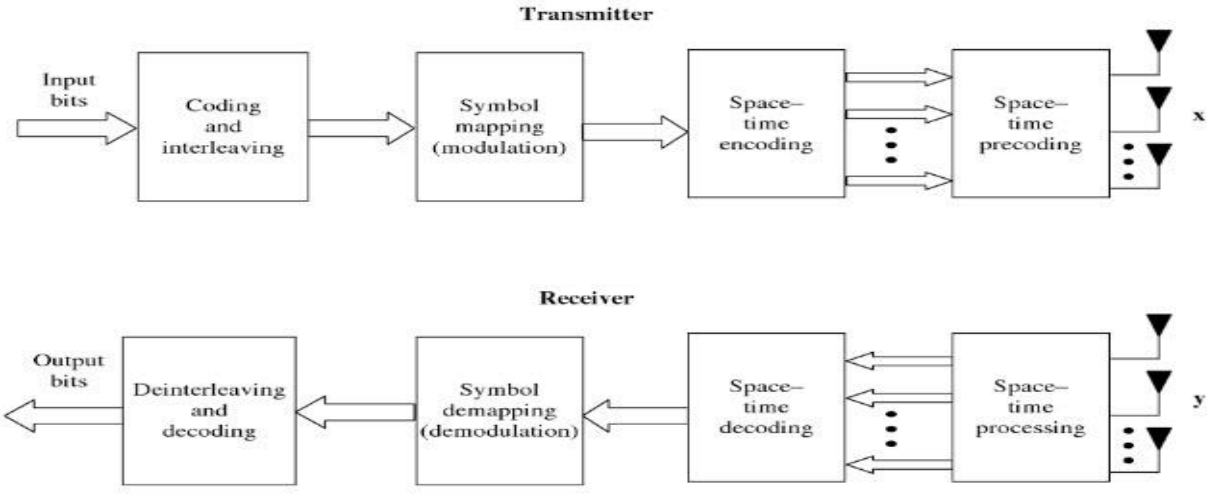


Figure 3.2. Basic Block Diagram of MIMO System

III.3.3.Closed-loop MIMO

Closed-loop MIMO systems use feedback from the receiver to adjust transmission parameters, such as the antenna configuration or the power used in the transmission. This feedback ensures that the system adapts dynamically to changing channel conditions. The Channel State Information (CSI)

provides crucial details about the channel's current state, allowing the system to optimize its transmission strategies.

Closed-loop MIMO is particularly beneficial in multimedia communication where high data rates and low latency are crucial, like video streaming and real-time gaming. The system can adjust its transmission methods in real-time to optimize the quality and minimize transmission errors.

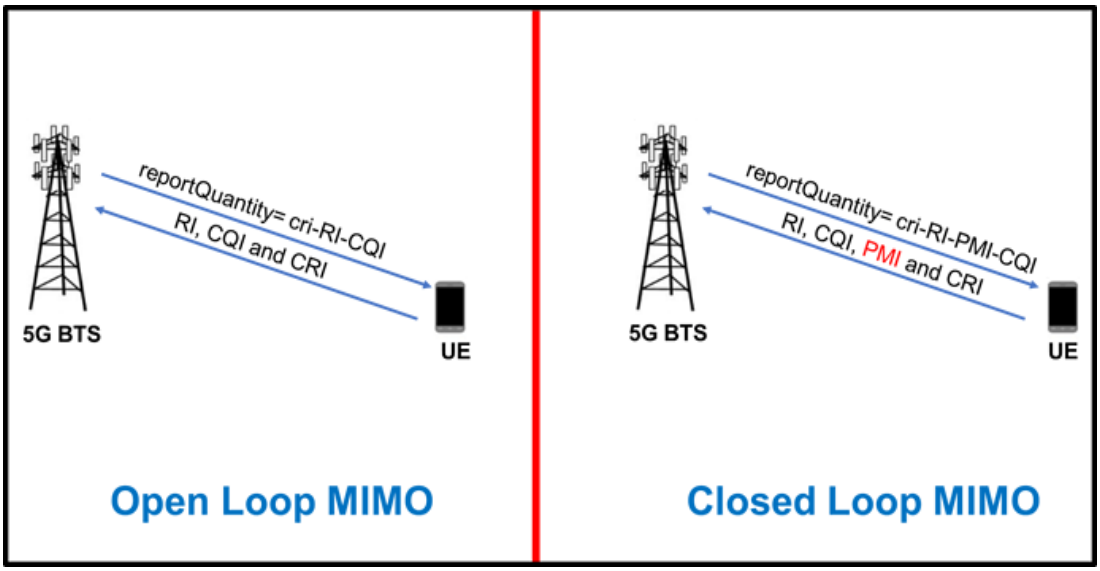


Figure 3.3. Open loop MIMO versus Closed loop MIMO System

III.4. Joint Source-Channel Coding

- **Source coding** (compression) reduces the amount of data that needs to be transmitted without losing significant information (e.g., using codecs for audio/video).
- **Channel coding** (error correction) ensures that the data is transmitted reliably, even in the presence of noise or interference in the channel.

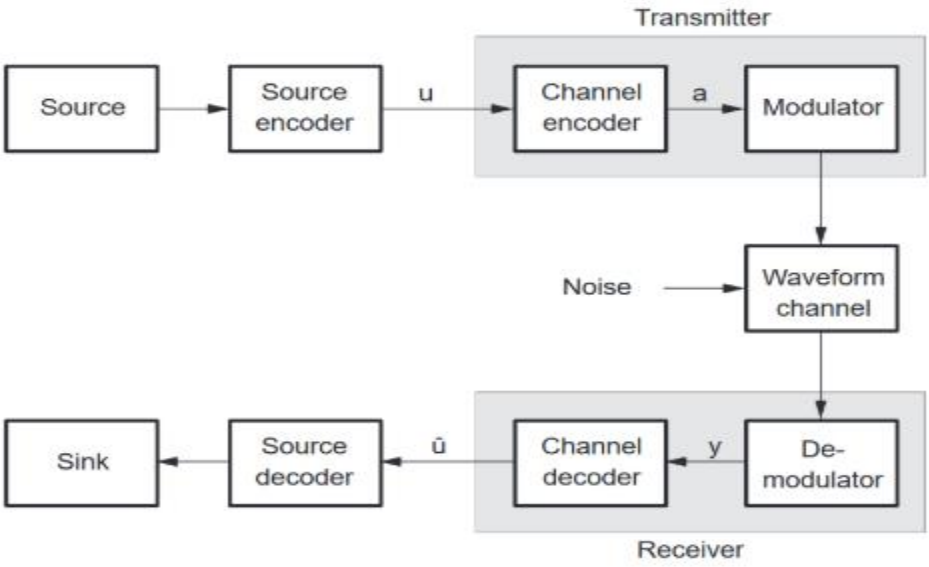


figure diagram of joint source-channel coding.

JSCC optimizes both the source and the channel coding at the same time. By considering both compression and error correction simultaneously, JSCC enables more efficient transmission, especially in situations with low bandwidth or high error rates. The advantage of JSCC is that it dynamically balances data compression and error correction based on channel conditions.

JSCC is particularly useful in scenarios like real-time video streaming or mobile video calls, where bandwidth is limited, and data losses can significantly degrade quality. The combined approach ensures minimal data loss while maintaining a good quality experience for the end-user.

III.5.Multimedia transmission strategies

To transmit multimedia (such as audio, video, or data) efficiently, considering both the nature of the content being transmitted and the characteristics of the transmission channel (like bandwidth, latency, and reliability). The goal is to optimize the use of resources, ensure high-quality transmission, and minimize delays or losses during the transfer.

- **Content-Aware Transmission Strategies :**Not all types of multimedia content need the same treatment. For example, a fast-moving action scene in a video requires different transmission priorities compared to a still image. Content-aware strategies can dynamically adjust encoding rates and error correction based on the complexity and importance of the content being transmitted.
- **Exploiting the Transmission Channel :**Adaptive transmission techniques adjust the transmission rate based on the current quality of the channel. For example, when signal conditions are good,

higher data rates can be used to transmit higher-quality content, and when the channel quality is poor (e.g., low signal strength), the system can reduce the transmission rate to avoid errors.

- **Transmission Strategies for Different Types of Multimedia :**For **video streaming**, adaptive bitrate streaming ensures smooth playback even in fluctuating network conditions by adjusting video quality based on available bandwidth. For **audio streaming**, it may involve dynamic range control and noise reduction to enhance quality in noisy environments.

III.6.Optimization in Transmission Strategies:

In communication systems, optimizing the way information is transmitted is crucial for achieving the best performance given the constraints of the system and the specific requirements of the application. The phrase "Introduction to optimization for defining optimal transmission strategies relative to the intended application" refers to the use of mathematical and computational techniques to determine the most efficient way to transmit data while meeting the performance needs of a given application.

III.6.1Key Concepts:

- **Optimization** involves using methods such as mathematical modeling, algorithms, and simulations to select the best parameters for transmitting data. For example, optimizing parameters like power, modulation schemes, and coding strategies can lead to more efficient and reliable communication.
- The **intended application** refers to the specific use case of the communication system, such as video streaming, voice calls, or data transfer, each of which has its own performance requirements. For instance, video streaming may prioritize high throughput and low latency, while voice calls may focus on minimizing bit errors and maintaining clarity.

III.6.2.Physical Layer and Its Impact

The **physical layer** is the lowest layer in the OSI model of communication systems. It includes the hardware components, such as antennas, transmitters, and receivers, as well as the actual transmission of signals through the medium (e.g., radio waves, fiber optics, etc.).

This layer plays a crucial role in determining the quality of the transmission because it directly influences how signals are sent and received. Factors like signal strength, noise, and interference are primarily governed by the physical layer.

- **Quality Metrics:** The physical layer's performance is evaluated using several quality metrics, which help measure the effectiveness of the transmission. These include:
- **Bit Error Rate (BER):** BER is a key metric for determining the reliability of data transmission. It represents the ratio of bits received in error to the total number of bits transmitted. A lower BER indicates better transmission quality and fewer errors.
- **Throughput (Data Rate):** Throughput measures the rate at which data is successfully transmitted over a communication channel, usually in bits per second (bps). It directly affects how fast an application can send or receive data, and optimizing throughput is critical for applications like video streaming and file transfers.
- **Peak Signal-to-Noise Ratio (PSNR):** PSNR is a measure of the quality of the received signal relative to the noise in the channel. It is particularly important in multimedia applications such as image and video transmission, where high PSNR values are associated with clearer, higher-quality content. PSNR is calculated based on the signal's peak power and the noise power, where a higher ratio indicates less distortion and better quality.

III.3.7The Relationship Between the Physical Layer and Quality Metrics:

The **physical layer** affects all of these quality metrics. For example:

- **Signal Strength:** The strength of the transmitted signal can influence the BER, throughput, and PSNR. A stronger signal typically reduces BER (fewer errors) and can improve throughput and PSNR.
- **Noise and Interference:** These can degrade the signal quality, leading to a higher BER, reduced throughput, and lower PSNR. The physical layer must handle noise efficiently using techniques like error correction, modulation, and coding.
- **Channel Conditions:** The type of transmission channel (e.g., wired vs. wireless) and its characteristics (e.g., bandwidth, propagation delay) can also impact all three metrics. For instance, wireless channels may experience more interference and noise than wired ones, leading to higher BER and lower throughput.

The physical layer of a communication system directly impacts key quality metrics such as BER, throughput, and PSNR, and understanding this relationship is crucial for improving system performance and meeting application requirements. By applying optimization techniques, one can

fine-tune the transmission parameters to maximize efficiency and minimize errors and distortions, leading to better overall communication quality.

Practical Work 5: MIMO System Performance Evaluation

Objective: To implement and evaluate the performance of MIMO systems in improving signal quality and bandwidth efficiency.

Task:

Implement a basic MIMO system using Python, MATLAB, or another simulation platform. The system should use multiple antennas at both the transmitter and receiver.

Simulate different MIMO configurations (e.g., 2x2, 4x4) and evaluate the improvements in signal quality and bandwidth efficiency using metrics like capacity and bit error rate (BER).

Analyze the advantages of closed-loop MIMO versus open-loop MIMO.

Deliverables: A report with MIMO system simulations, comparing the performance of various MIMO configurations, and discussing the impact of feedback and CSI on system efficiency.

:To implement a basic MIMO (Multiple-Input, Multiple-Output) system using a simulation platform like Python or MATLAB, here's a step-by-step approach.

Set Up the Simulation Environment

- Choose a simulation platform: MATLAB, Python (using libraries like `numpy`, `scipy`, `matplotlib`), or other simulation tools like Simulink.
- Install necessary libraries (Python): `numpy`, `matplotlib`, `scipy`, `comm` (for communication system functions).
- Define the simulation parameters such as frequency, signal power, noise power, etc.

Define MIMO System Parameters

- **Number of Antennas**: Define the number of antennas at both the transmitter (Tx) and receiver (Rx). For example, for a 2x2 MIMO, you'll have 2 antennas at Tx and 2 antennas at Rx.
- **Channel Model**: Choose a channel model (e.g., Rayleigh fading, Rician fading, AWGN channel).
- **Modulation Scheme**: Select a modulation scheme (e.g., QPSK, 16-QAM).
- **Signal-to-Noise Ratio (SNR)**: Define the SNR range to evaluate system performance.

Generate Transmit Signal

- **Transmit Data Generation**: Create a random data stream to be transmitted (e.g., random bits).
- **Modulate the Data**: Apply modulation (e.g., QPSK, 16-QAM) to the data to prepare it for transmission.

```
# Example in Python

data = np.random.randint(0, 2, size=(n, 1))  # Random bits

mod_data = qpsk_mod(data)  # Apply QPSK modulation
```

Create MIMO Channel Model

- **Define Channel Matrix**: Create a random MIMO channel matrix (e.g., H matrix) that models the transmission environment. This could be Rayleigh fading or other types of fading.

```
# Channel matrix H (2x2 for 2x2 MIMO)
H = np.random.randn(2, 2) + 1j * np.random.randn(2, 2)
```

- **Channel Effects**: Apply the channel matrix to the transmitted signal to simulate the signal propagation.

```
transmitted_signal = np.dot(H, mod_data)  # Apply channel matrix
```

Add Noise and Disturbance

- **Add Noise**: Add Gaussian noise to the received signal to simulate real-world interference (AWGN noise).

```
noise = np.sqrt(1/(2*SNR)) * (np.random.randn(*transmitted_signal.shape) + 1j *
np.random.randn(*transmitted_signal.shape))
received_signal = transmitted_signal + noise
```

Implement MIMO Receiver

- **Channel Estimation**: For closed-loop MIMO, estimate the channel at the receiver using feedback from the transmitter. In open-loop MIMO, no feedback is used.
- **Signal Detection**: Use algorithms like Zero-Forcing (ZF) or Minimum Mean Square Error (MMSE) for signal detection at the receiver.

```
# Zero-Forcing receiver (ZF)
H_inv = np.linalg.pinv(H)  # Compute pseudo-inverse of H
received_data = np.dot(H_inv, received_signal)  # Detect signal
```

Demodulate the Signal

- **Demodulation**: Apply the reverse of the modulation process (e.g., QPSK demodulation) to recover the transmitted data.

```
demod_data = qpsk_demod(received_data)  # Demodulate the received data
```

Compute Performance Metrics

- **Capacity Calculation**: Use the Shannon capacity formula to compute the channel capacity and evaluate bandwidth efficiency.

```
# Shannon capacity
capacity = np.log2(np.linalg.det(np.eye(N) + (SNR / N) * np.dot(H, H.T)))
```

- **Bit Error Rate (BER)**: Compare the transmitted data with the demodulated data and compute the Bit Error Rate (BER).

```
BER = np.sum(data != demod_data) / len(data)
```

Simulate Different MIMO Configurations

- Simulate various MIMO configurations (e.g., 2x2, 4x4, etc.), and repeat steps 3-8 for each configuration.
- **Evaluate Performance**: Plot the BER vs SNR and compare the results for different configurations.

```
# For 4x4 MIMO, change the dimensions of H, etc.
H_4x4 = np.random.randn(4, 4) + 1j * np.random.randn(4, 4)
```

Analyze the Advantages of Closed-loop vs Open-loop MIMO

- **Closed-loop MIMO**: Feedback is used for channel state information (CSI) from the receiver to the transmitter, allowing for better adaptation (e.g., beamforming, power control).
- **Open-loop MIMO**: No feedback; transmission is based on assumptions or random channel matrices.
- **Compare Performance**: Compare the BER and capacity of closed-loop and open-loop MIMO systems. Closed-loop systems typically provide better performance by adapting to changing channel conditions.

```
# For closed-loop MIMO, implement feedback-based algorithms like beamforming.
```

Visualize Results

- **Plot the Results**: Generate plots to visualize performance (e.g., BER vs. SNR, capacity vs. SNR) for each MIMO configuration and closed-loop/open-loop systems.

```
import matplotlib.pyplot as plt
plt.plot(SNR_values, BER_values)
plt.xlabel('SNR (dB)')
plt.ylabel('Bit Error Rate (BER)')
plt.title('BER vs SNR for MIMO Configurations')
plt.show()
```

REFERENCES

- **Image Quality Metrics (PSNR, MSE, SSIM, etc.)**:
  - **Wang, Z., & Li, Q. (2011).** *Information content weighting for perceptual image quality assessment*. IEEE Transactions on Image Processing, 20(5), 1185-1199.
  - **Gao, L., & Zhang, L. (2014).** *Image quality assessment: From quality evaluation to optimization*. Journal of Visual Communication and Image Representation, 25(1), 51-59.
  - **Liu, X., & Sun, X. (2017).** *A novel full-reference image quality assessment method based on local structure information*. Signal Processing: Image Communication, 55, 84-94.
  - **Zhu, S., & Zhang, L. (2020).** *Single image super-resolution with multi-scale wavelet-based features for perceptual quality evaluation*. Journal of Electronic Imaging, 29(5), 053022.
- **Watermarking Techniques (LSB, DCT, DWT):**
  - **Yang, J., & Zhang, X. (2012).** *A new image watermarking scheme using DCT and DWT*. International Journal of Computer Science and Network Security, 12(7), 70-74.
  - **Khan, I. A., & Ali, S. (2015).** *A hybrid watermarking scheme based on LSB and DCT for copyright protection*. Journal of Multimedia, 10(3), 268-274.
  - **Hussain, A., & Soni, P. (2018).** *A comprehensive survey on digital image watermarking techniques: Algorithms and applications*. Journal of King Saud University - Computer and Information Sciences, 30(5), 597-617.
  - **Liu, B., & Sun, X. (2021).** *A robust image watermarking method using discrete wavelet transform and singular value decomposition*. International Journal of Computer Applications, 174(2), 1-6.
- **Cryptography (AES, DES, RSA, etc.):**
  - **He, Q., & Wang, Z. (2015).** *A new approach to AES encryption with dynamic key generation*. Journal of Cryptology, 28(4), 1014-1037.
  - **Feldman, J., & Rogers, B. (2016).** *Practical RSA encryption and decryption using private key infrastructure*. International Journal of Applied Cryptography, 4(2), 72-81.
  - **Sharma, V., & Ghai, S. (2017).** *A comprehensive survey on encryption algorithms: AES, RSA, DES*. International Journal of Computer Applications, 165(3), 12-16.
  - **Hassan, S., & Alabdulwahab, S. (2020).** *A comparative analysis of AES and RSA cryptosystems for multimedia data security*. Security and Privacy, 3(2), e116.

- **Steganography (LSB-based, Challenges in Multimedia Steganography)**:
  - **Gupta, A., & Gupta, S. (2012).** *A review on image steganography techniques*. International Journal of Computer Applications, 49(13), 26-29.
  - **Ahmed, F., & Al-Khatee, S. (2015).** *An advanced LSB-based steganography technique for robust multimedia data hiding*. Journal of Electronic Science and Technology, 13(2), 103-109.
  - **Bharati, A., & Kumar, M. (2016).** *Multimedia steganography and cryptography techniques: A survey*. International Journal of Computer Applications, 142(1), 1-6.
  - **Yin, Z., & Zhang, Z. (2020).** *Challenges and improvements in multimedia steganography: A survey and future directions*. Multimedia Tools and Applications, 79(29), 21499-21532.

- **MIMO Systems (Open-loop vs. Closed-loop, CSI, Performance Evaluation)**:

- **Chiani, M., & Guo, X. (2010).** *Performance analysis of MIMO systems with partial channel state information*. IEEE Transactions on Communications, 58(2), 540-546.
- **Kim, H., & Lee, W. (2015).** *A study on closed-loop MIMO for future wireless communication systems*. IEEE Transactions on Wireless Communications, 14(4), 1955-1966.
- **Marzetta, T. L., & Vucic, I. (2017).** *Noncooperative MIMO systems with imperfect channel state information*. IEEE Transactions on Signal Processing, 65(11), 2954-2967.
- **Zhang, H., & Zhang, J. (2021).** *A review on MIMO systems with open and closed-loop feedback in 5G and beyond*. IEEE Access, 9, 130755-130773.

- **Propagation Channel Characterization (Fading, Interference, Path Loss, Environmental Impacts):**

- ***Matz, G., & Huber, M. (2011).*** Fundamentals of wireless propagation and interference modeling. *IEEE Transactions on Communications, 59(9), 2765-2775.*
- ***Zhao, M., & Sinha, S. (2013).*** Wireless channel modeling for interference mitigation in MIMO systems. *IEEE Transactions on Wireless Communications, 12(5), 2345-2355.*
- ***Gao, X., & Li, S. (2015).*** A survey of MIMO propagation channel models: Theory and applications. *International Journal of Antennas and Propagation, 2015, 352392.*
- ***Tan, S., & Li, J. (2020).*** Channel modeling for 5G and beyond: Interference, fading, and environmental impacts. *IEEE Transactions on Vehicular Technology, 69(3), 3062-3072*.