DIGITAL WATERMARKING IN MODULAR ARITHMETIC AND CRYPTOGRAPHY

Presentation by:

Farcas Amalia

Hognogi Ana-Maria Cristina

Moldovan Andrei-Bogdan

INTRODUCTION TO DIGITAL WATERMARKING

A process to embed hidden information into digital media.

Example: Protect intellectual property, verify authenticity, and prevent tampering.
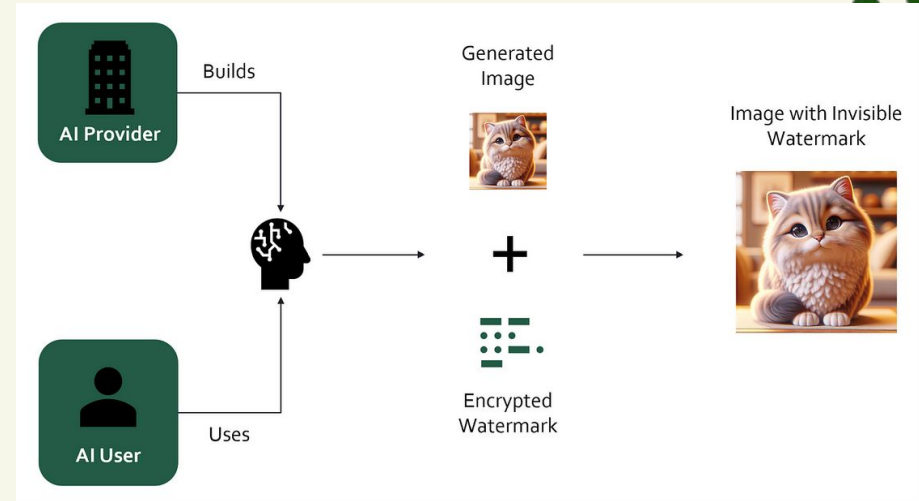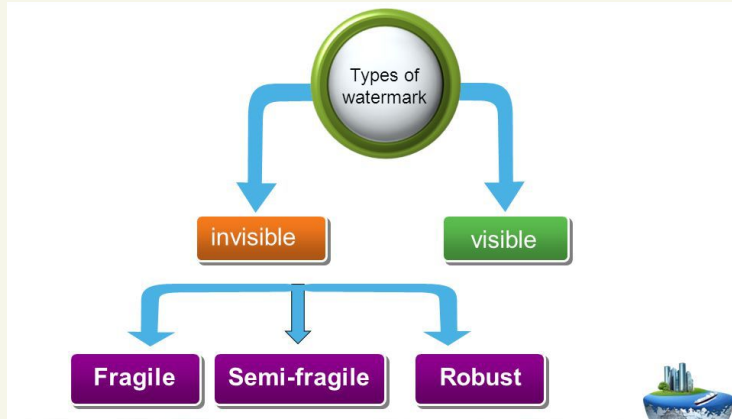
IMPORTANCE OF DIGITAL WATERMARKING

Protection against piracy and unauthorized use.

Ensures ownership, integrity, and traceability.
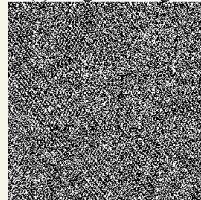
TYPES OF WATERMARKING

Types of watermark

invisible

visible

Fragile Semi-fragile Robust

AI Provider — Builds — Generated Image

AI User — Uses

Encrypted Watermark

Image with Invisible Watermark

TECHNIQUES: SPATIAL VS. FREQUENCY DOMAINS

(a) Original Image
(b) Tampered Image
(c) Extracted Watermark
(d) Decompressed Image

SPATIAL DOMAIN

Directly modifies pixel values.

Watermark bits (-1,1)
Spreading with chip-rate
Modulation
X
Scaling
DCT
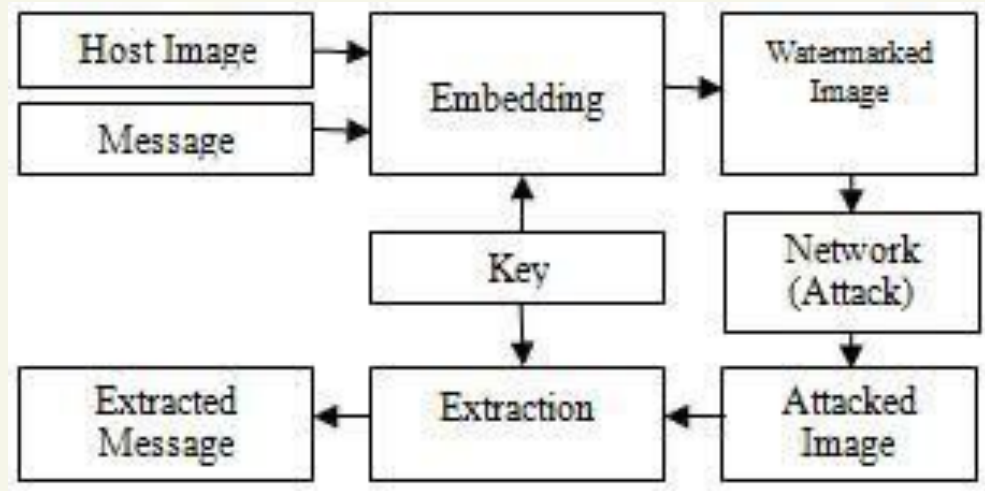DCT coefficients
DCT
IDCT
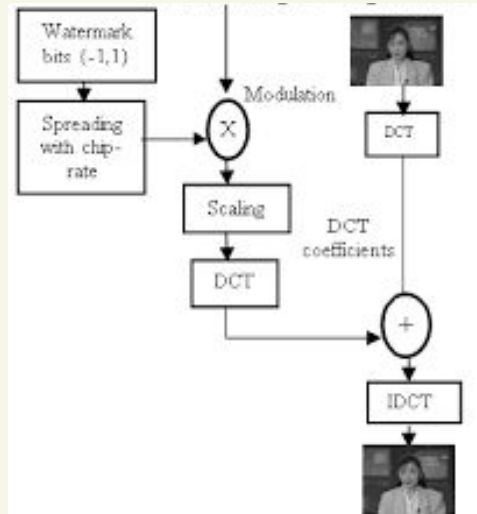
FREQUENCY DOMAIN

Embeds watermarks in transformed media (e.g., DCT, FFT).

MODULAR ARITHMETIC IN WATERMARKING

Modular arithmetic helps securely embed and detect watermarks.

Formula: (W = (M + K) \mod N),

where: M - Media data, K - Key, N - Modulus.

# CRYPTOGRAPHIC TECHNIQUES IN WATERMARKING

SYMMETRIC KEY WATERMARKING:

- Fast and efficient.
- Uses shared secret keys (e.g., AES encryptiON).
- Suitable for applications requiring speed and simplicity.

PUBLIC KEY WATERMARKING:

- Provides enhanced security with asymmetric cryptography (e.g., RSA).
- Uses a private-public key pair for embedding and verifying watermarks.
- Ideal for scenarios needing authentication and integrity verification.

HASH FUNCTIONS:

- Used for content verification and tamper detection.
- Ensures the integrity of the embedded watermark.
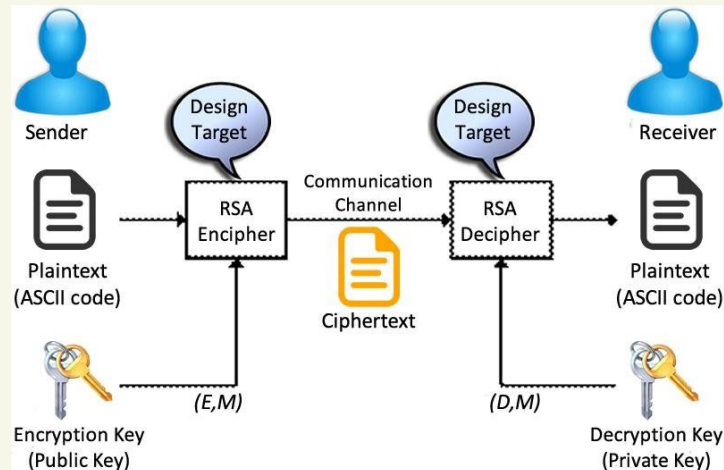

```
# RSA Key Generation
public_key, private_key = generate_RSA_keys()

# Watermark Embedding
encrypted_watermark = encrypt(public_key, watermark_data)
content_with_watermark = embed(content, encrypted_watermark)

# Watermark Extraction and Verification
extracted_watermark = extract(content_with_watermark)
original_watermark = decrypt(private_key, extracted_watermark)
```

STEP-BY-STEP EXAMPLE: WATERMARKING AN IMAGE

STEPS TO EMBED A WATERMARK:

1. Select a pixel from the image (P).
2. Apply the formula: P′ = (P + K) mod 256, where KKK is the watermark value.
3. Save the watermarked image.

```python
from PIL import Image

# Load image and watermark key
image = Image.open('original_image.png')
pixels = image.load()
K = 50  # Example watermark value

# Embed watermark
for x in range(image.width):
    for y in range(image.height):
        P = pixels[x, y][0]  # Select the red channel (example)
        P_prime = (P + K) % 256
        pixels[x, y] = (P_prime,) + pixels[x, y][1:]

# Save watermarked image
image.save('watermarked_image.png')
```
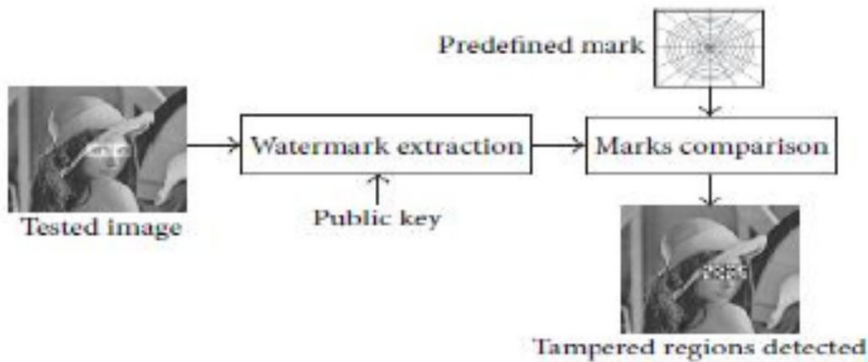

(a)   (b)

WATERMARK DETECTION AND EXTRACTION

DETECTION PROCESS:

1. Use modular inverse or direct comparison to detect and extract the watermark.
2. Formula: W = (P′ − K) mod N, where:
   - P′: Watermarked pixel.
   - K: Watermark key.
   - N: Range of pixel values (e.g., 256 for 8-bit images).

**Fig 2**: Embedding and Extraction process in Secured environment

CHALLENGES IN DIGITAL WATERMARKING

Digital watermarks must remain imperceptible yet robust against various attacks.

Attacks: Digital watermarks face several challenges, including:
- Compression (e.g., JPEG)
- Noise addition
- Cropping

Trade-offs: Robustness vs. visibility: Balancing the visibility of watermarks with their robustness against removal or alteration is crucial.
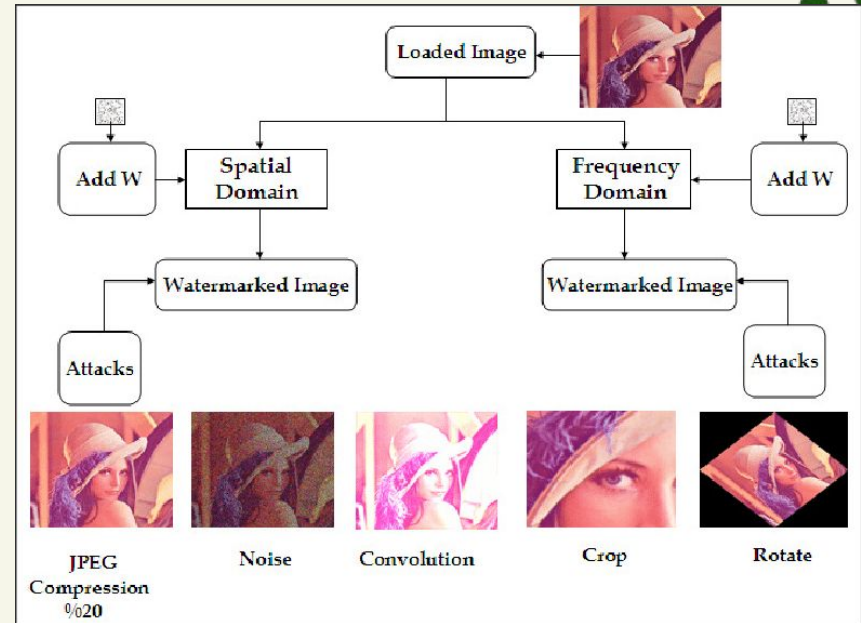
APPLICATIONS OF DIGITAL WATERMARKING

Digital watermarking protects content across media (videos, images, audio), banking (digital signatures), and content ownership (logos, PDFs). Major platforms like Netflix, Shutterstock, and Adobe use watermarks to prevent unauthorized use and verify authenticity.

NETFLIX EXAMPLE

Netflix uses an interesting version of digital watermarking named Forensic Watermarking. In short, Forensic Watermarking inserts pieces of information such that they can track illegal distribution of content. When a copyright holder discovers illegally distributed content, they can detect the watermark, track the user and take legal action against them.

# ADVANTAGES OF DIGITAL WATERMARKING

- It safeguards copyright by clearly identifying content ownership
- Maintains data integrity by detecting unauthorized alterations
- Enables traceability by tracking how and where digital content is used and distributed.

SUMMARY

Digital watermarking technology relies on cryptographic techniques and modular arithmetic to embed hidden information within digital content. This technology serves multiple critical purposes: it helps fight digital piracy, provides clear proof of content ownership, and ensures data protection. The process involves two main steps: embedding the watermark into the original content and later detecting it to verify authenticity or ownership.

CONCLUSION

As digital threats continue to evolve, watermarking remains a crucial tool for protecting intellectual property and ensuring content authenticity in our increasingly digital world. The mathematical approach ensures robust protection while maintaining the integrity of the original content
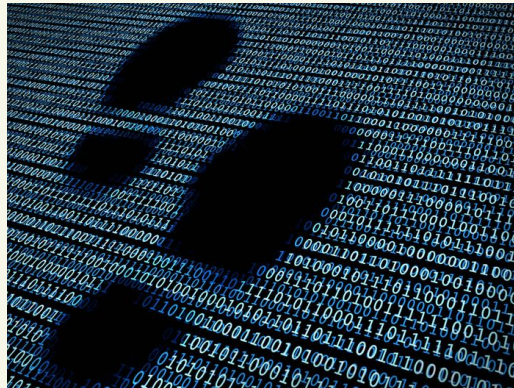
BIBLIOGRAPHY

https://www.researchgate.net/figure/Example-of-a-digital-watermark-A-random-noise-pattern-is-added-to-the-image-in-the_fig1_315116341

https://medium.com/pallycon/how-netflix-protects-contents-part-2-33c1b60002a3

https://www.digitalguardian.com/blog/digital-watermarking#:~:text=Digital%20watermarking%20involves%20embedding%20a,it%20contains%20source%20tracking%20code.

https://slideplayer.com/slide/3927563/

https://www.geeksforgeeks.org/digital-watermarking-and-its-types