Digital Image Watermarking

Dr. Asifullah Khan (Associate Professor)

Department of Computer and Information Sciences

Pakistan Institute of Engineering and Applied Sciences

LETS SEE SOME IMAGES

bwin.com

Prominent Approaches; Protection

- Cryptography
- Watermarking
- Steganography

Data Hiding Vs. Cryptography

- **Cryptography**
  - Encryption: translate information into an unintelligible form
  - Decryption: decode to retrieve information
  - Attackers cannot recover the information
- **Data Hiding**
  - Hide information
  - Attackers don’t know where to find the information

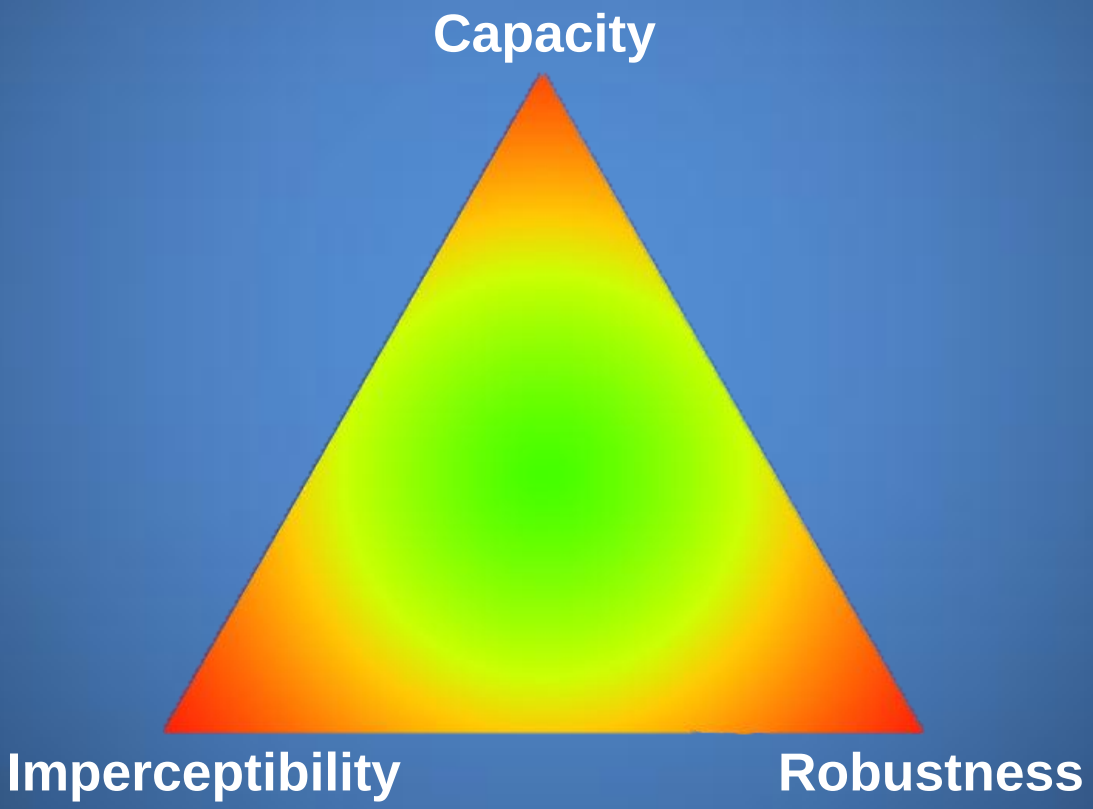
Data Hiding Main Disciplines

- **Steganography**
  - Is the process of secretly embedding information into a data source in such a way that its very existence is concealed.
- **Watermarking**
  - Is the practice of imperceptibly altering a work to embed a message about that work.
  - If copied and redistributed, the embedded information will also be copied and redistributed.

Data Hiding Requirements

- **Imperceptibility**
  - The watermarked and original data source should be perceptually identical.
- **Robustness**
  - The embedded data should survive any signal processing operation the host signal goes through.
- **Capacity**
  - Maximum size limit of the message that can be hidden.

Watermarking Trade-offs



Effective Watermark is

- **Unobtrusive**
  - Watermark should be statistically and visually imperceptible without the compromise on the quality of data.
- **Readily Extractable**
  - Data owner or the control expert can extract the watermark
- **Robust**
  - Watermark should be resistant to the common signal processing techniques, geometrical distortions and to forgery attacks

Effective Watermark is

- **Unambiguous**
  - Extraction of watermark unambiguously recognize the content owner.
- **Innumerable**
  - Large number of watermarks, different from each other, can be generated.

General Data Hiding System

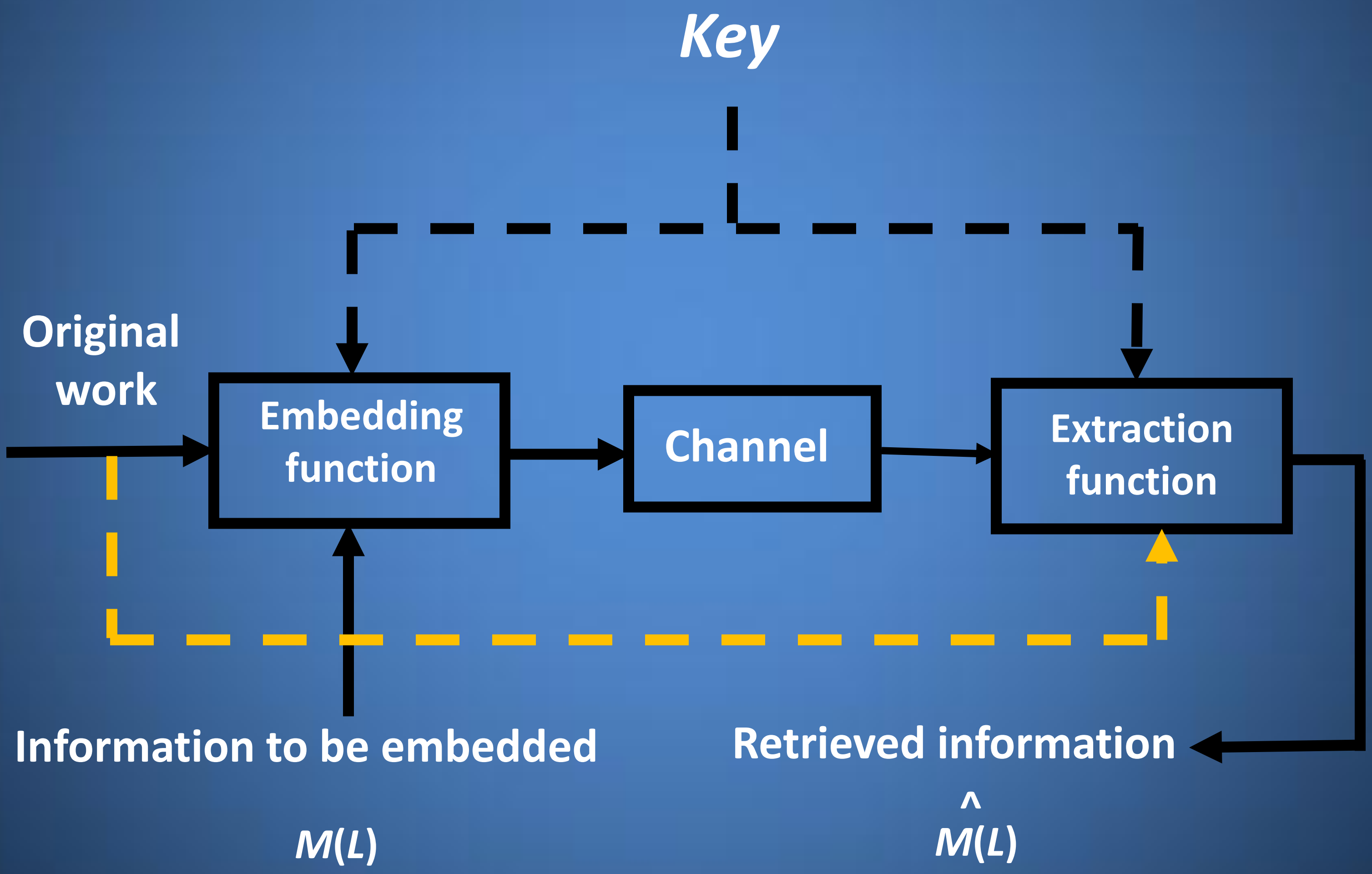


Image Watermarking Example

Original Image

Watermarked Image

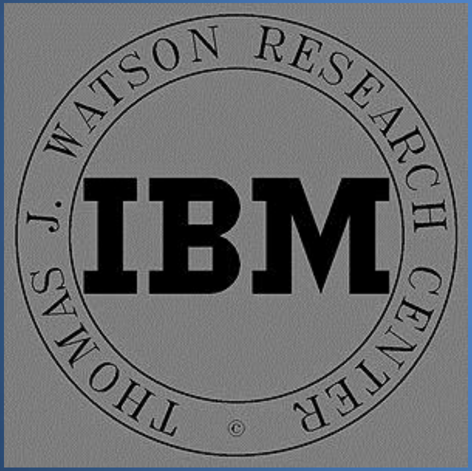
Digital Watermarks Categories

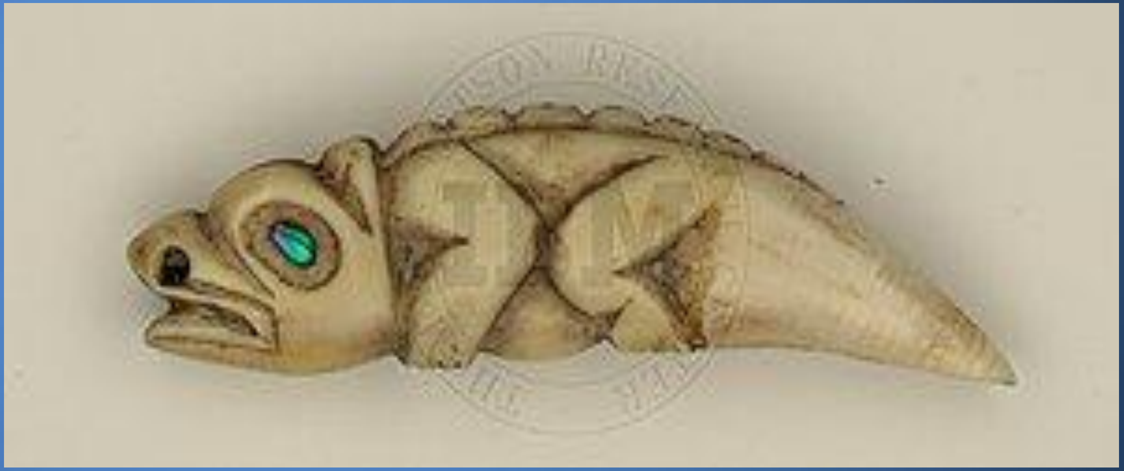
- ROBUST WATERMARK- Used for copyright protection.
  - Requirements: the watermark should permanently intact to the host signal, removing the watermark results in destroying the perceptual quality of the signal.
- FRAGILE WATERMARK- Used for tamper detection or as a digital signature.
  - Requirements: Break very easily under any modification of the host signal.
- SEMI FRAGILE WATERMARK- used for data authentication.
  - Requirements: Robust to some benign modifications, but brake very easily to other attacks.
  - Provides information about the location and nature of attack.

Types of Digital Watermarking on basis of Visibility

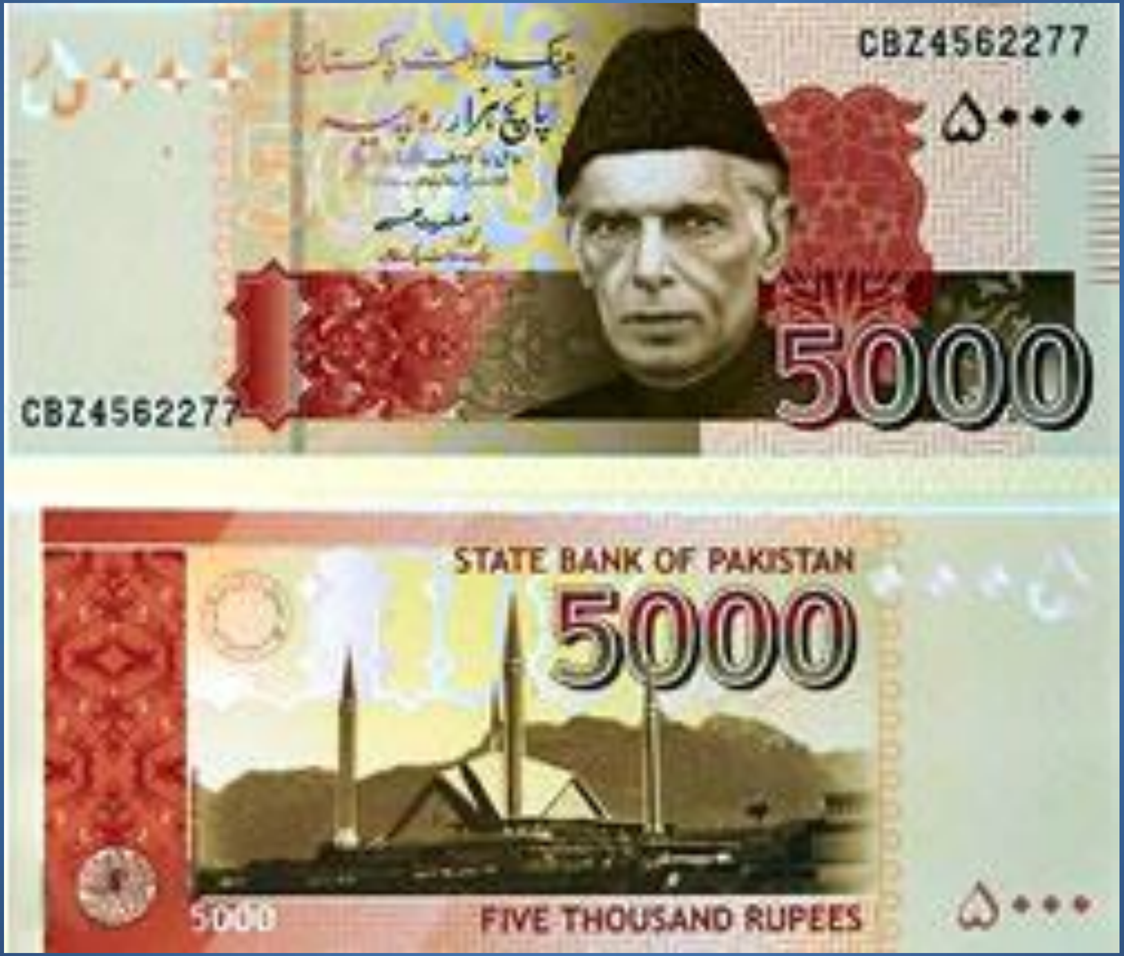
- **Visible Watermarking**
  - The embedded watermark can be seen with naked eye.
  - The embedded information may be a text or a logo that identifies the true owner of the media.
- **Invisible watermarking**
  - The imbedded information cannot be seen with naked eye
  - Although this hidden information can be detected by an extraction mechanism.

Visible Watermarking Example



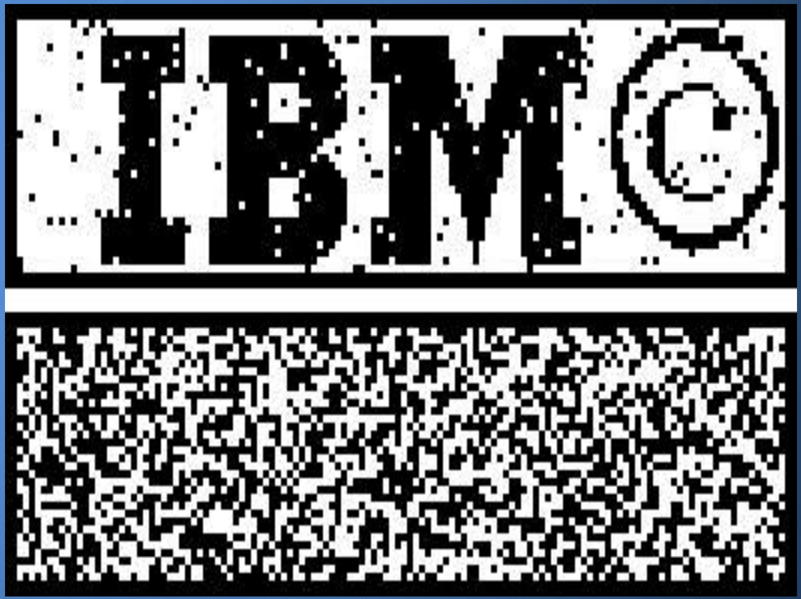


Visible Watermarking Example



Watermarks in Pakistan Currency bills

Invisible Watermarking Example



Invisible Watermarking Example

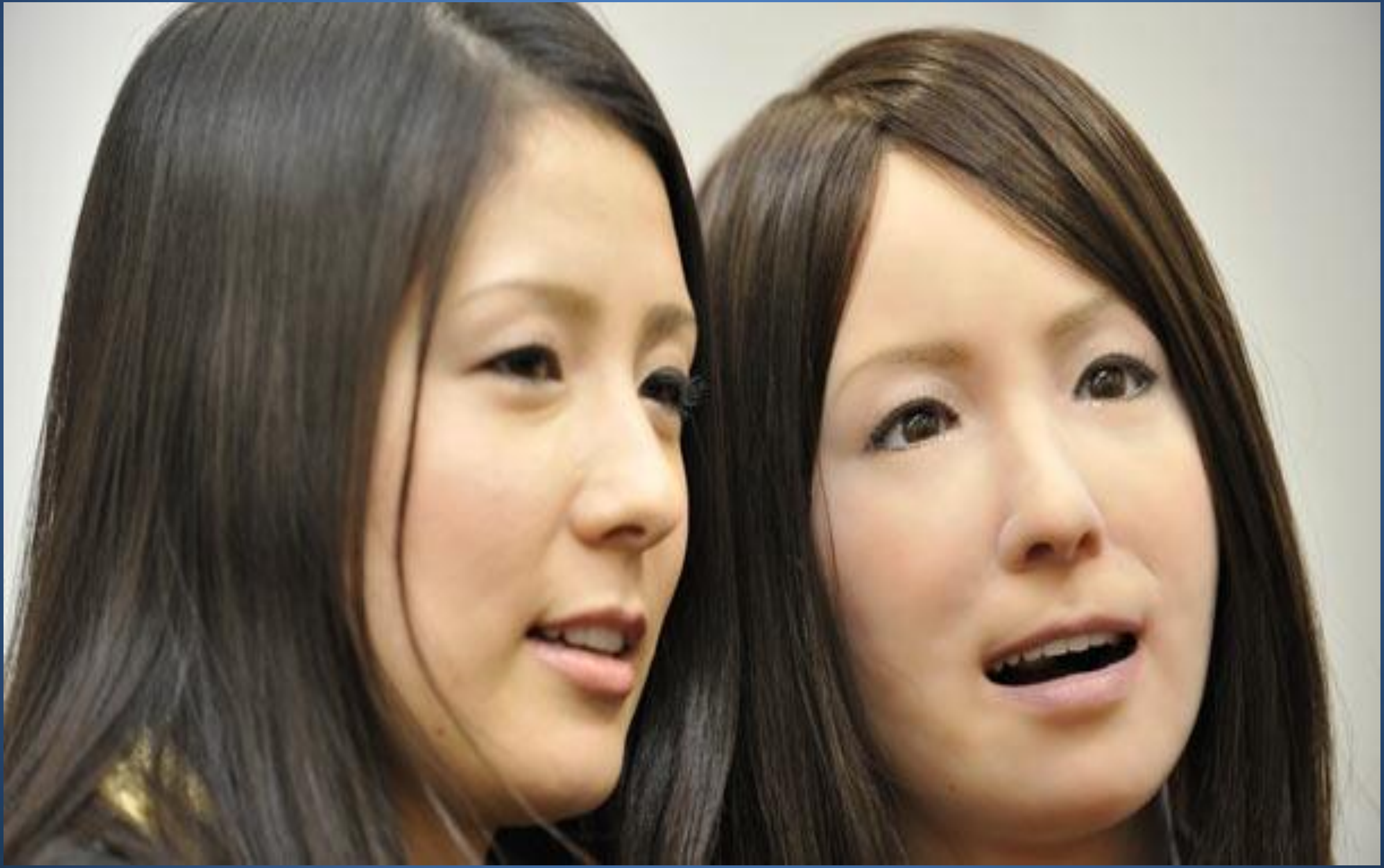
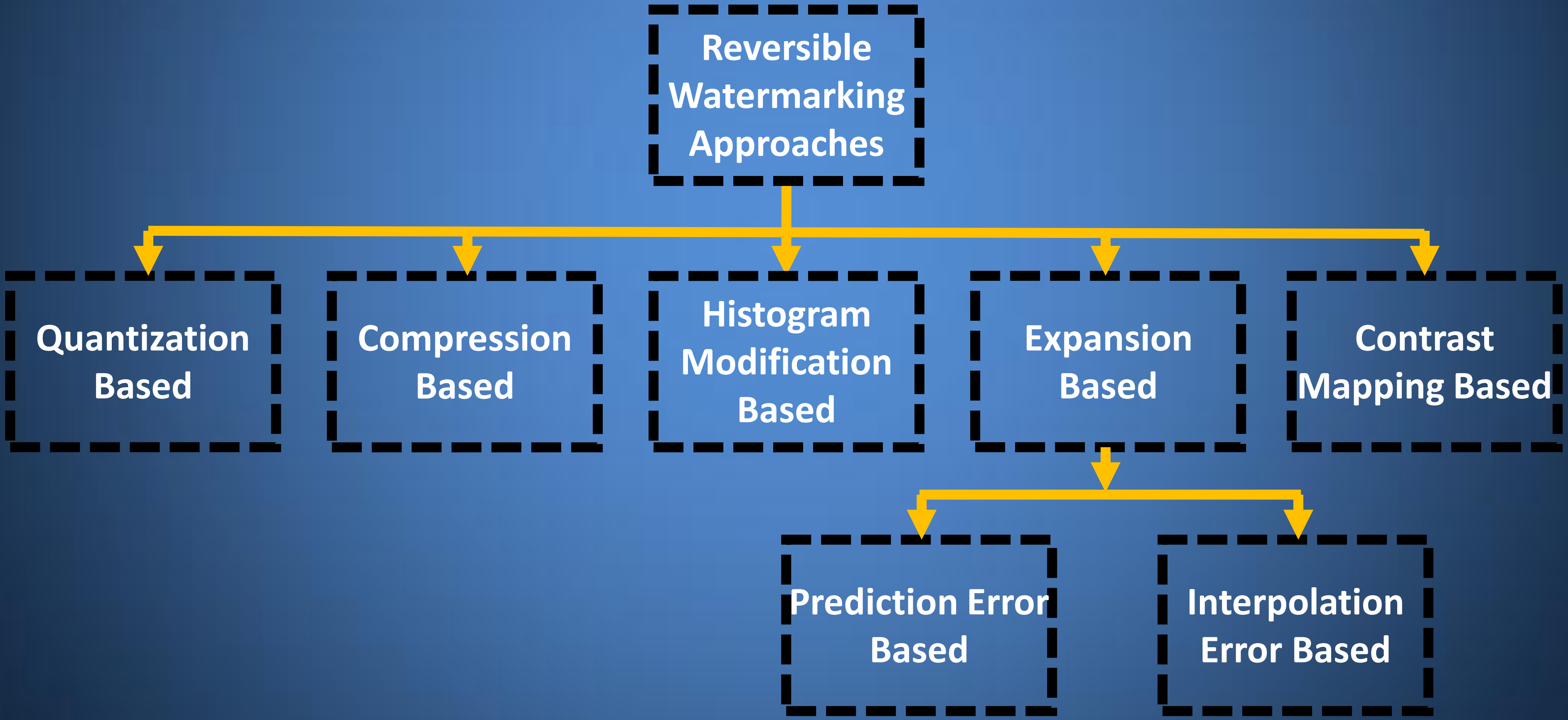
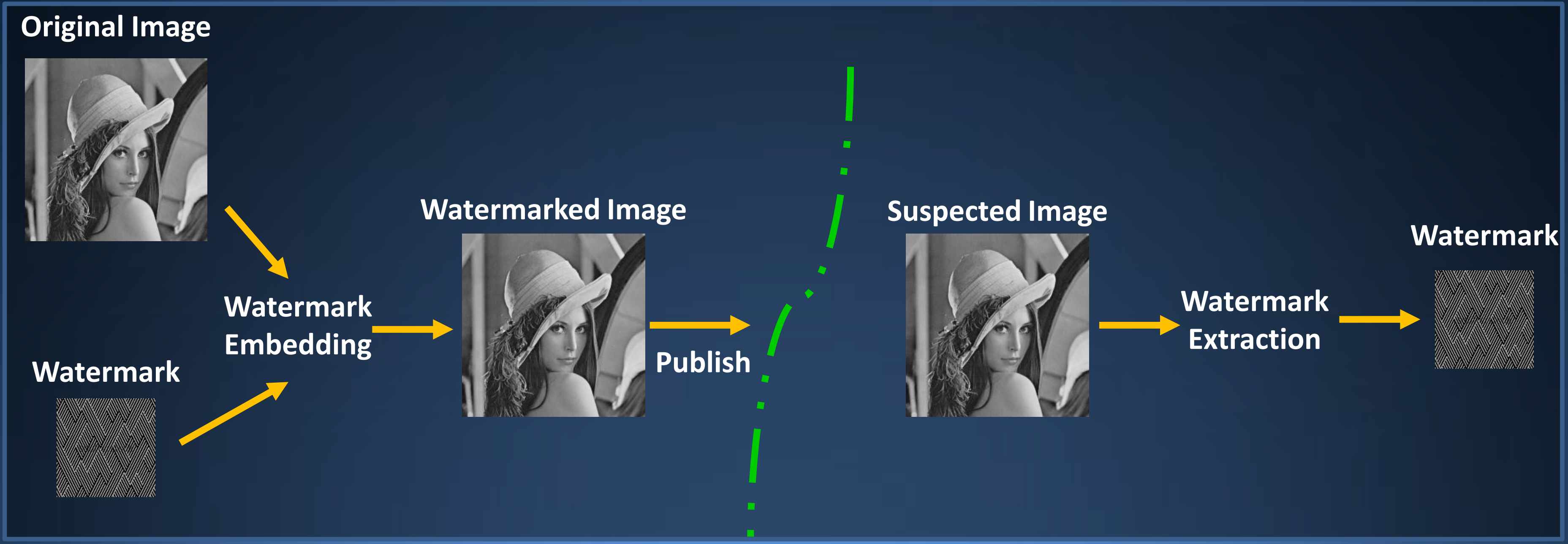


Image of one’s Robot Clone can be stored in his/her own image

Types of Watermarking on Basis of Reversibility





Original Image

Watermark

Watermark Embedding

Watermarked Image

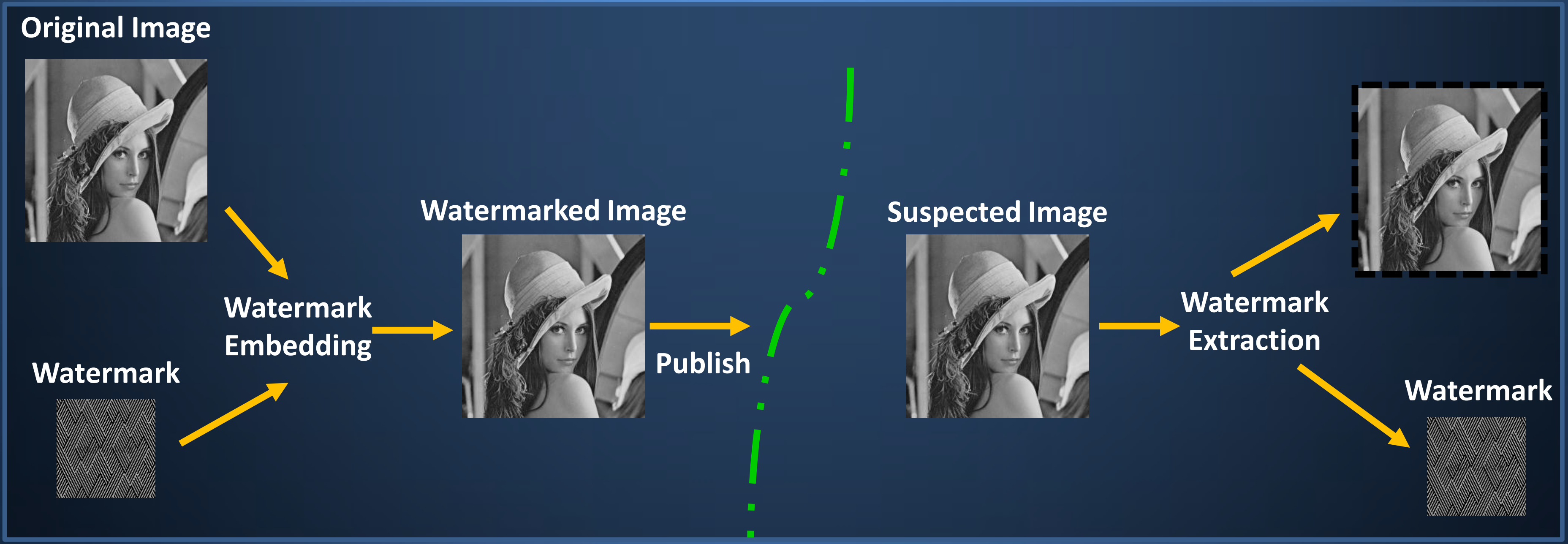
Publish

Suspected Image

Watermark Extraction

Watermark

Conventional Watermarking Scheme



Original Image

Watermark

Watermark Embedding

Watermarked Image

Publish

Suspected Image

Watermark Extraction

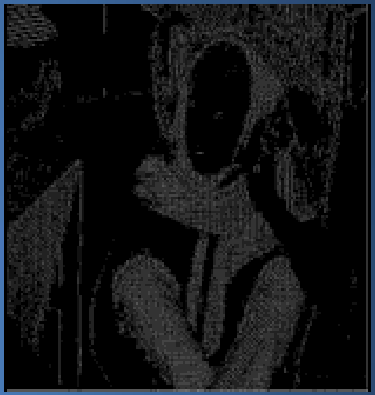
Watermark

Reversible Watermarking Scheme

Reversible Watermarking Example

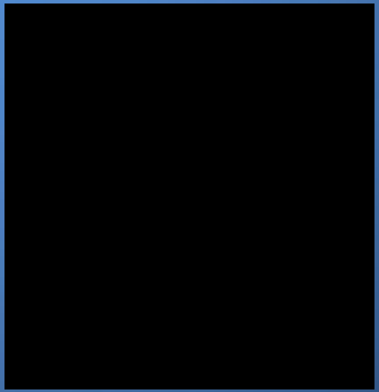
(a) Original Image

(b) Watermarked Image



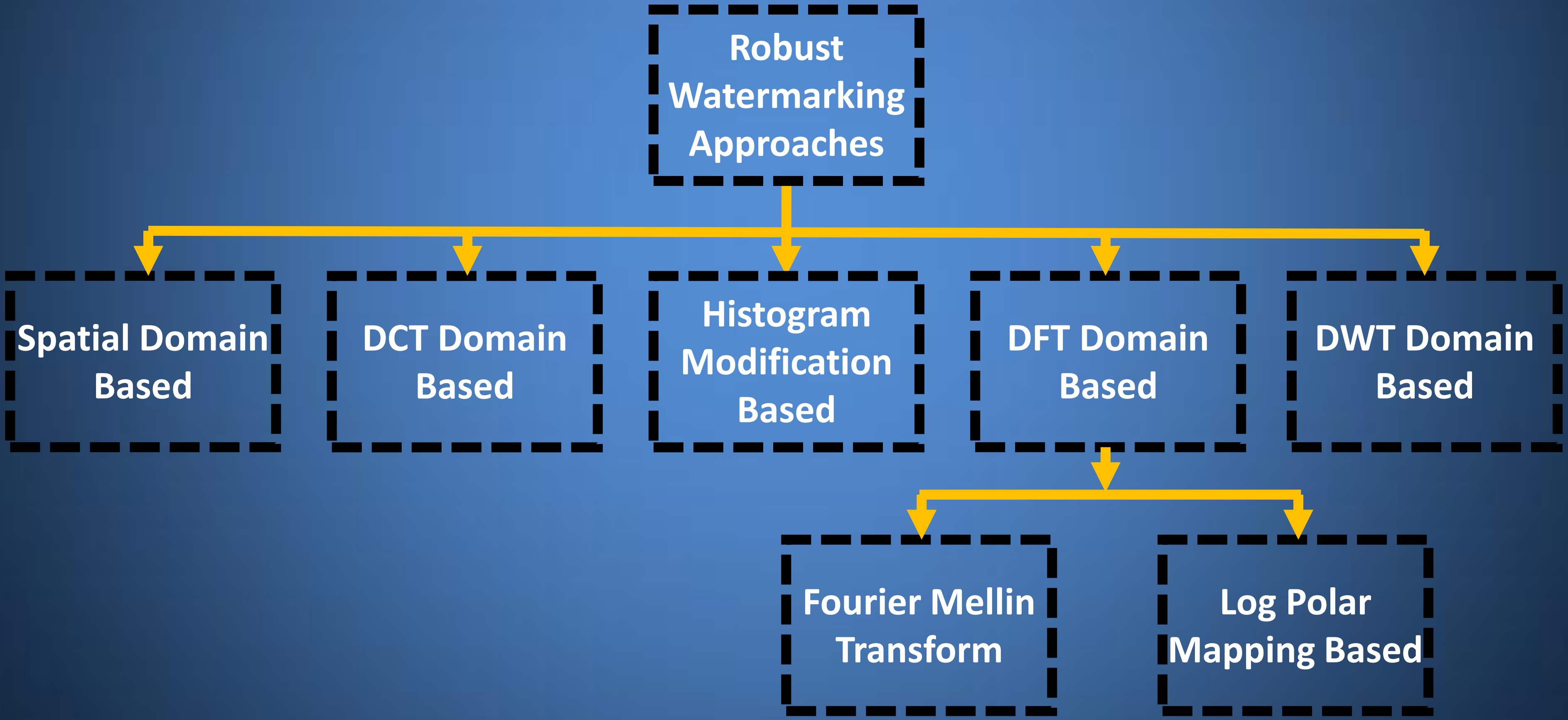
(c) Difference Image

(d) Restored Image



(e) Difference in (a) & (d)

Types of Watermarking on Basis of Robustness



Robust Watermarking Approaches

Spatial Domain Based

DCT Domain Based

Histogram Modification Based

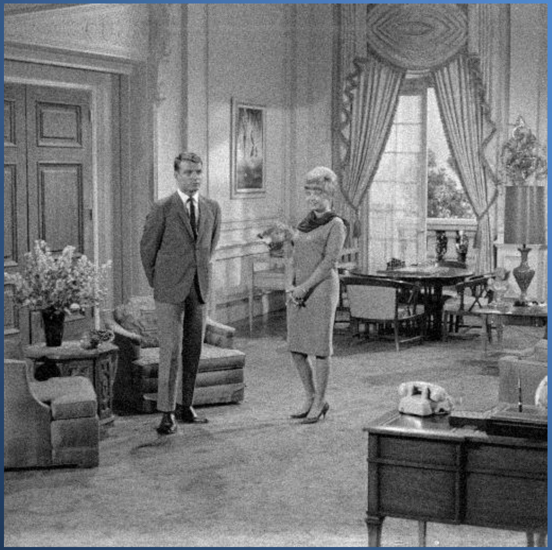
DFT Domain Based

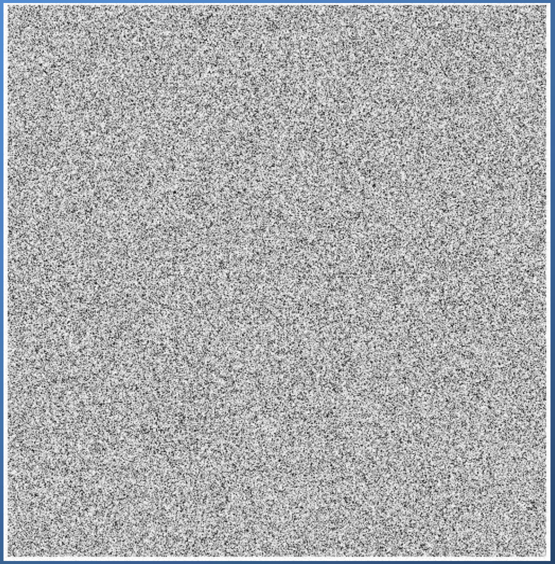
DWT Domain Based

Fourier Mellin Transform

Log Polar Mapping Based

Robust Digital Watermarking (By Khan et al.)





Difference between the watermarked and attacked-watermarked Image

Verification / Detection Methods

- **Non-blind**
  - The watermarking scheme requires the use of the original image.
- **Semi-Blind**
  - The watermarking scheme requires the watermark data and/or the parameters used to embed the data.
- **Blind**
  - If the watermarking scheme does not require the original image or any other data.

Watermark Attacks

- **Friendly attacks:** JPEG compression, filtering, cropping, histogram equalization, additive noise etc.
- **Unfriendly Attacks:** Geometric transformation, rotation, scaling, translation, change aspect ratio, line/frame dropping, affine transformation, unauthorized embedding and detection, etc.
- **Counterfeiting attacks:** Render the original image useless, generate fake original, dead lock problem.
- **Security based Attacks:** Refer to gaining knowledge about the secrets of the watermarking systems, e.g. Key.

Watermark Benchmarking

- There are a number of benchmarking tools which have been created to standardize watermarking system evaluating processes.

Watermark Benchmarking

- **StirMark**
  - StirMark is a benchmarking tool for digital watermarking designed to test robustness
- **CheckMark**
  - CheckMark is a benchmarking suite for digital watermarking developed on Matlab under UNIX and Windows.
- **OptiMark**
  - OptiMark is a benchmarking tool developed to address some deficiencies recognized in Stirmark 3.1.
- **CertiMark**
  - CertiMark is a benchmarking suite developed for watermarking of visual content and a certification process for watermarking algorithms.

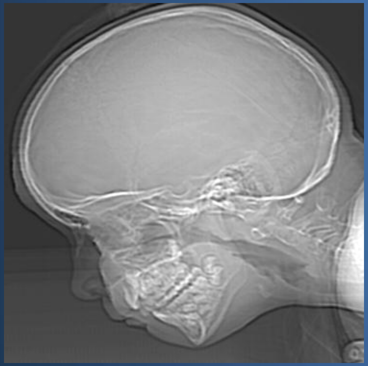
Applications of Watermarking

- **Content Authentication**
  - Tampering is easy in the digital world and the system design should detect it. The system might survive some modification (semi fragile).
- **Copy control**
  - Aim to prevent people from making illegal copies of copyrighted content.
- **Fingerprinting**
  - An owner can embed a watermark into his content that identifies the buyer of the copy (i.e. serial number).
  - If unauthorized copies are found later, the owner can trace the origin of the illegal copies.

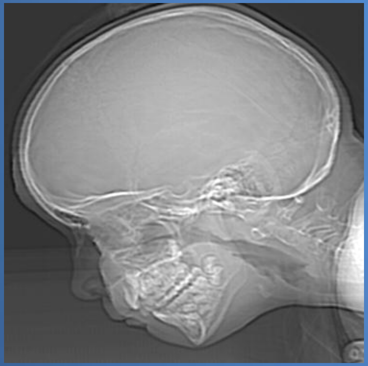
Applications of Watermarking Cont…

- **Broadcast Monitoring**
  - Advertisers want to ensure that they receive all of the air time they purchase from broadcasters (Japan 1997)
- **Ownership Assertion**
  - A rightful owner can retrieve the watermark from his content to prove his ownership.

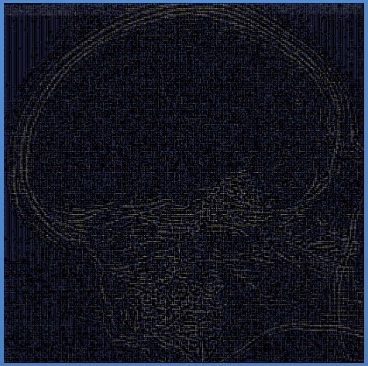
Medical Applications : MRI image Watermarking



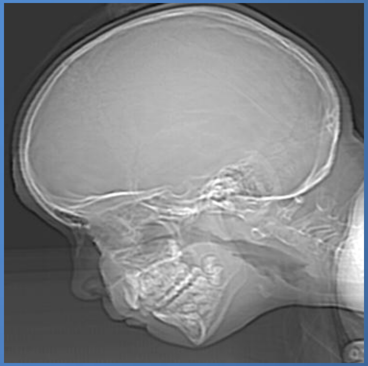
(a) Original Image



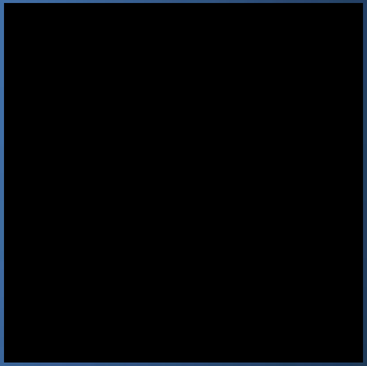
(b) Watermarked



(c) Difference of (a) & (b) With some enhancement technique

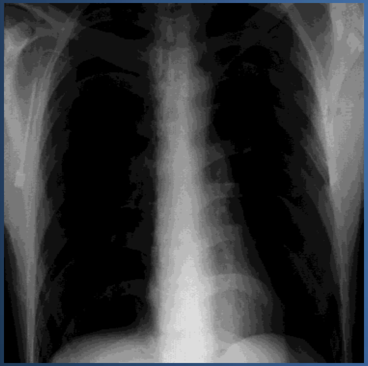


(d) Restored image

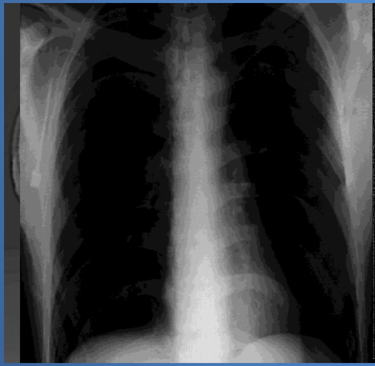


(e) Difference between (a) & (d)

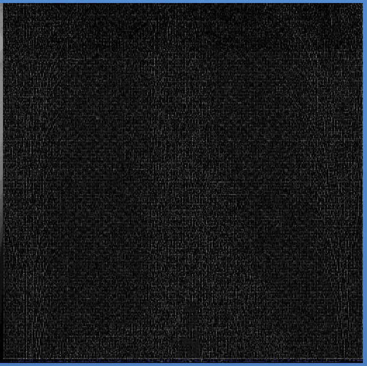
Example : X-ray Image Watermarking



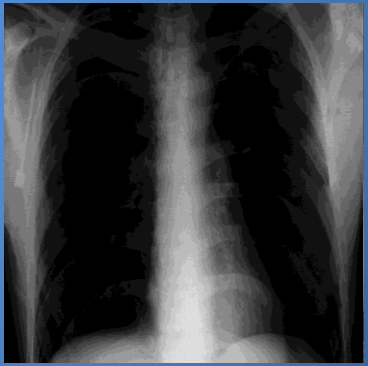
(a) Original Image



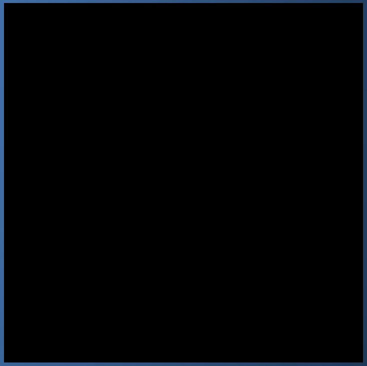
(b) Watermarked



(c) Difference of (a) & (b) With some enhancement technique

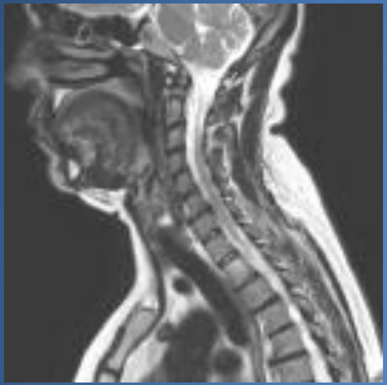


(d) Restored image

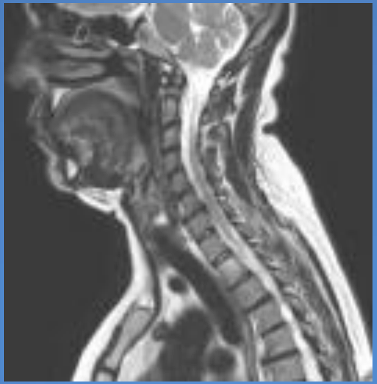


(e) Difference between (a) & (d)

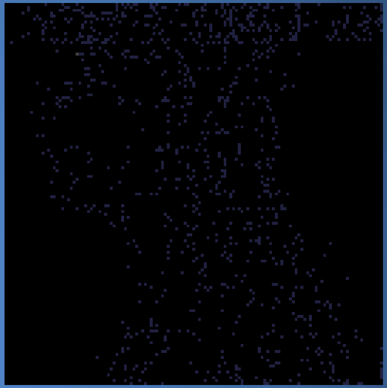
Reversible Watermarking of Spinal Cord Images



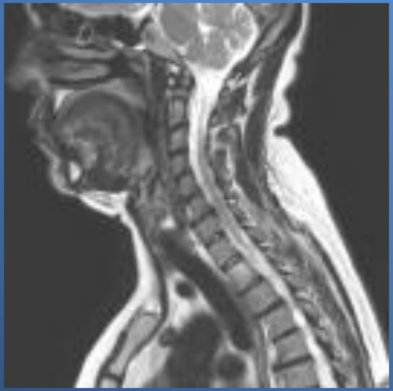
(a)



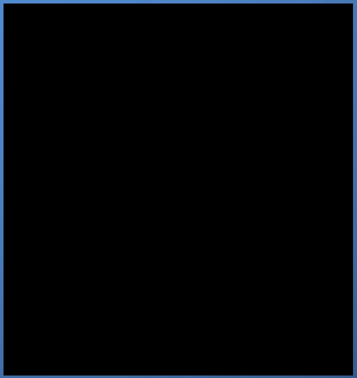
(b)



(c)



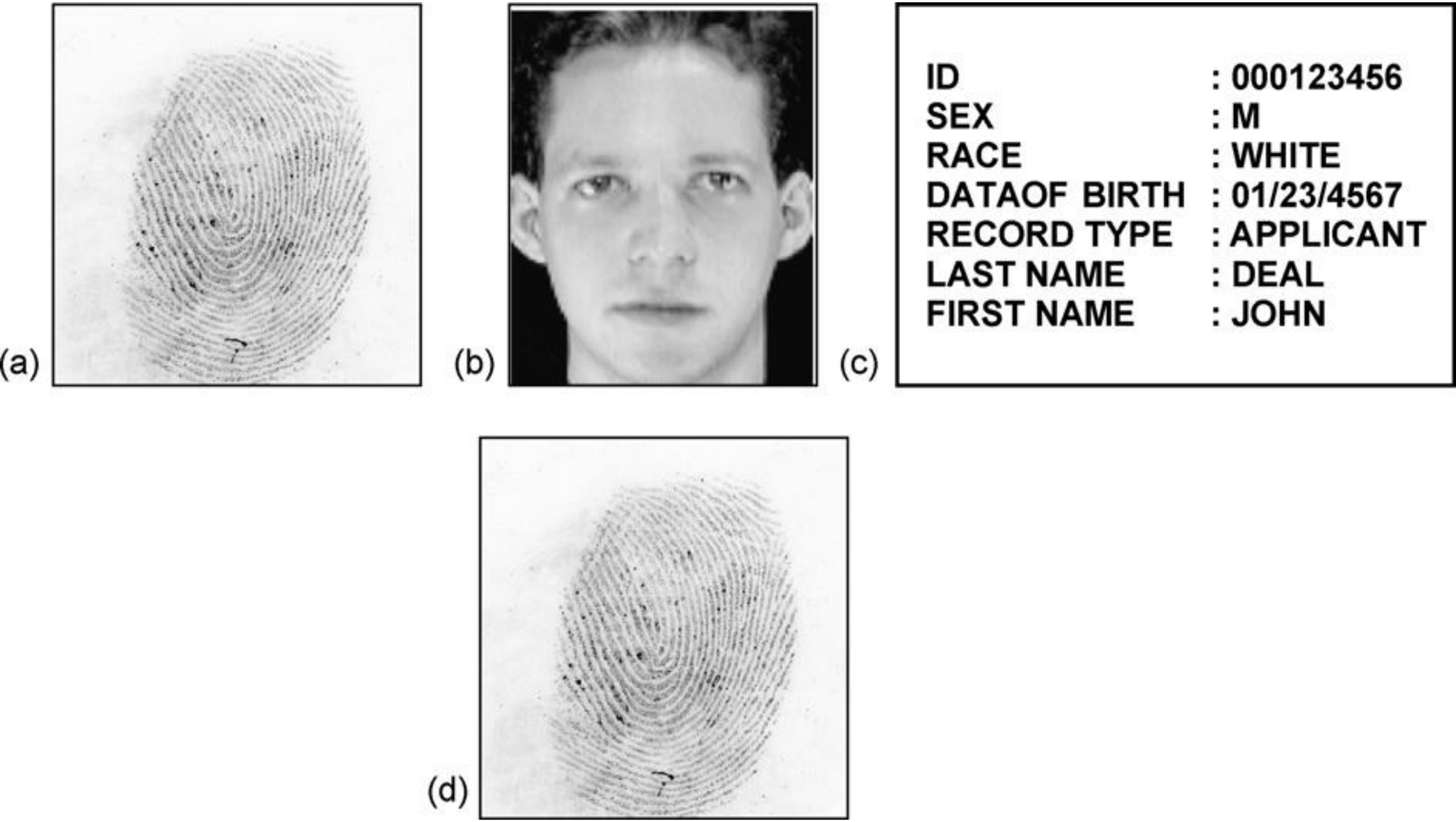
(d)



(e) *SSIM=1*

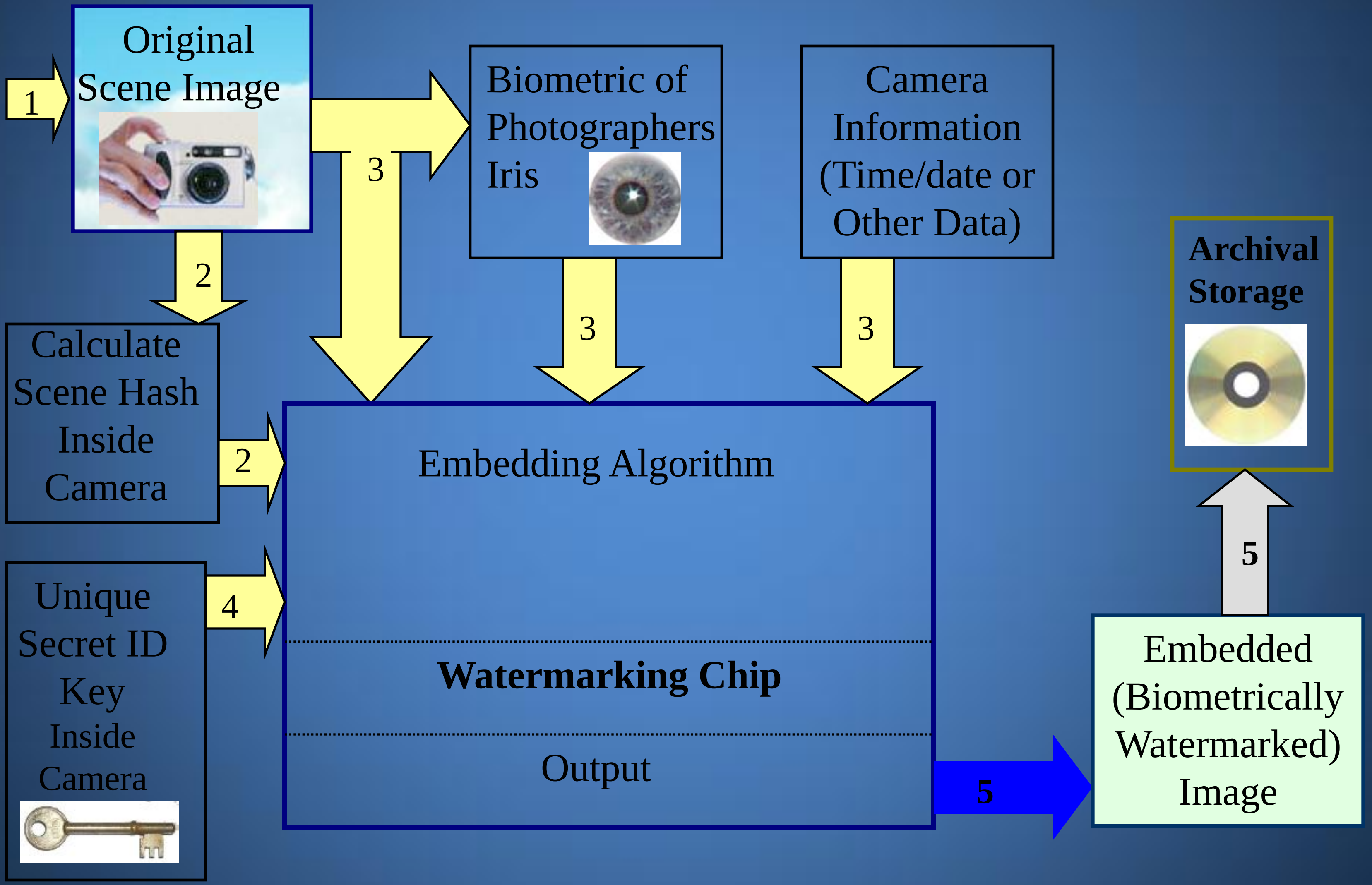
Some Recent Watermarking Applications

- Biometric Watermarking
- Authentication Watermarking
- Robust Watermarking
- Depth Map (3D Information) Embedding
- Secure Digital Camera



ID	: 000123456
SEX	: M
RACE	: WHITE
DATAOF BIRTH	: 01/23/4567
RECORD TYPE	: APPLICANT
LAST NAME	: DEAL
FIRST NAME	: JOHN

Secure Digital Camera (By Fridrich et. al)

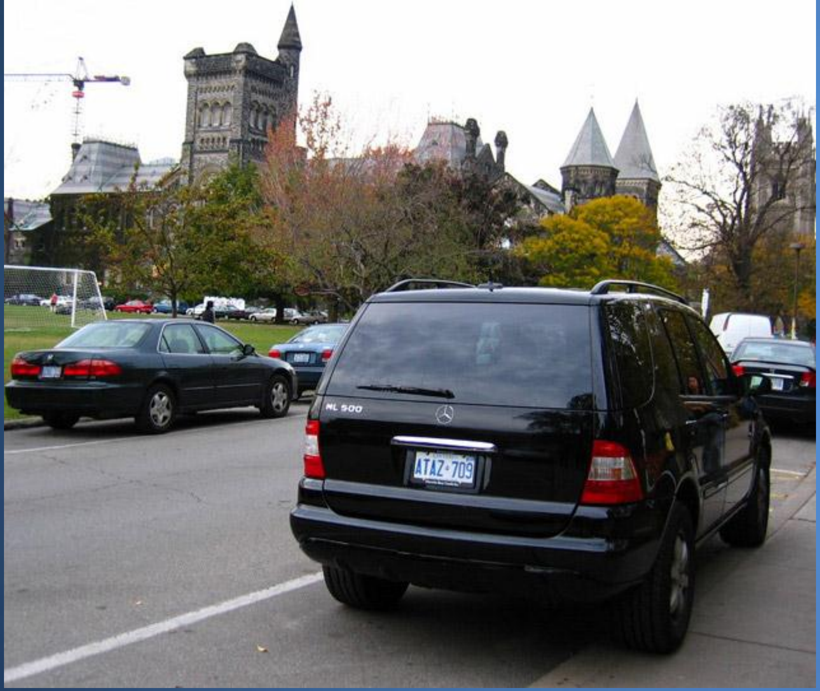


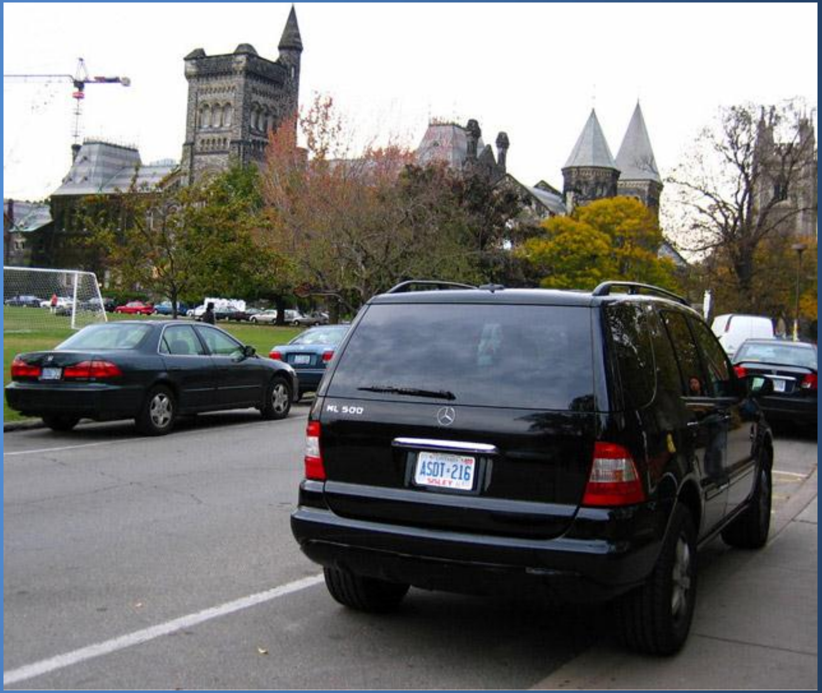
1
Original Scene Image
3
Biometric of Photographers Iris
Camera Information (Time/date or Other Data)
2
3
3
Archival Storage
Calculate Scene Hash Inside Camera
2
Embedding Algorithm
5
Unique Secret ID Key Inside Camera
4
Watermarking Chip
Output
5
Embedded (Biometrically Watermarked) Image

Embedding Scenario

Authentication

Can you tell which one is fake?

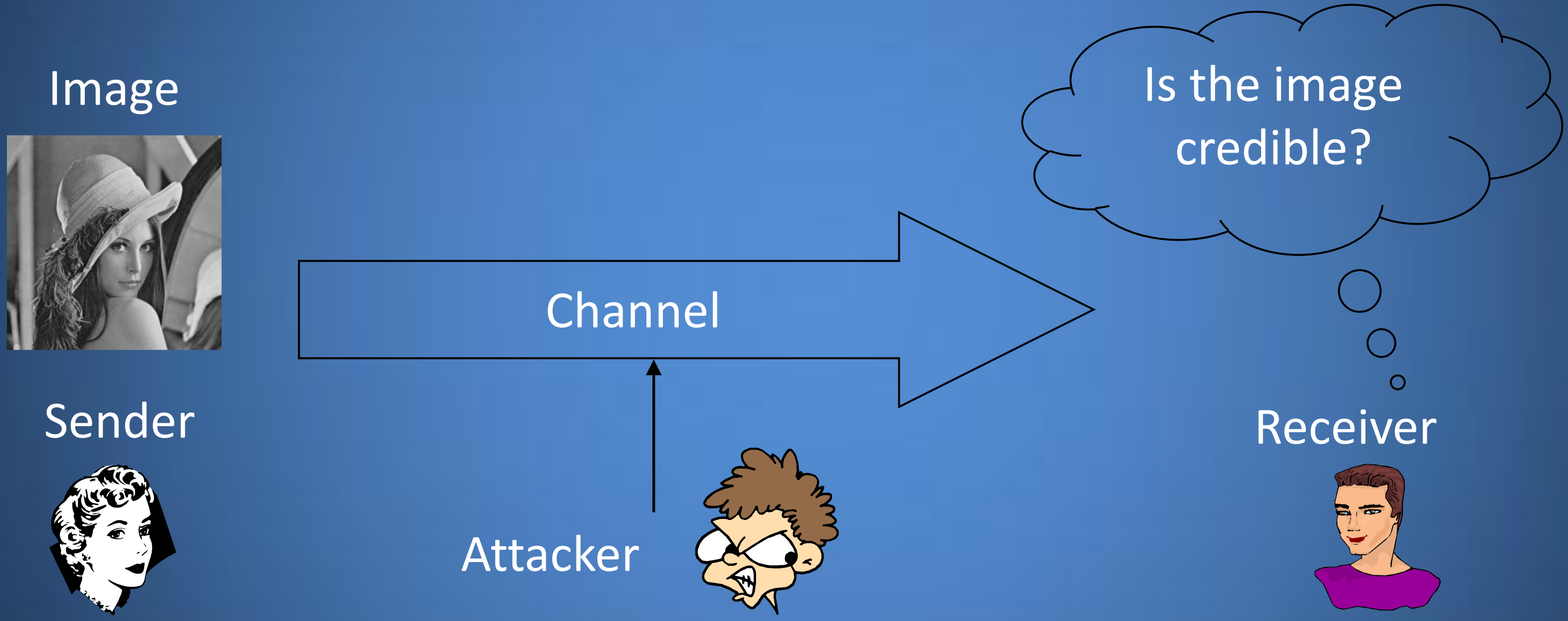




The procedure to validate the integrity of watermarked data, to make sure that the data is not being tampered with.

Authentication

General Model:



Image

Sender

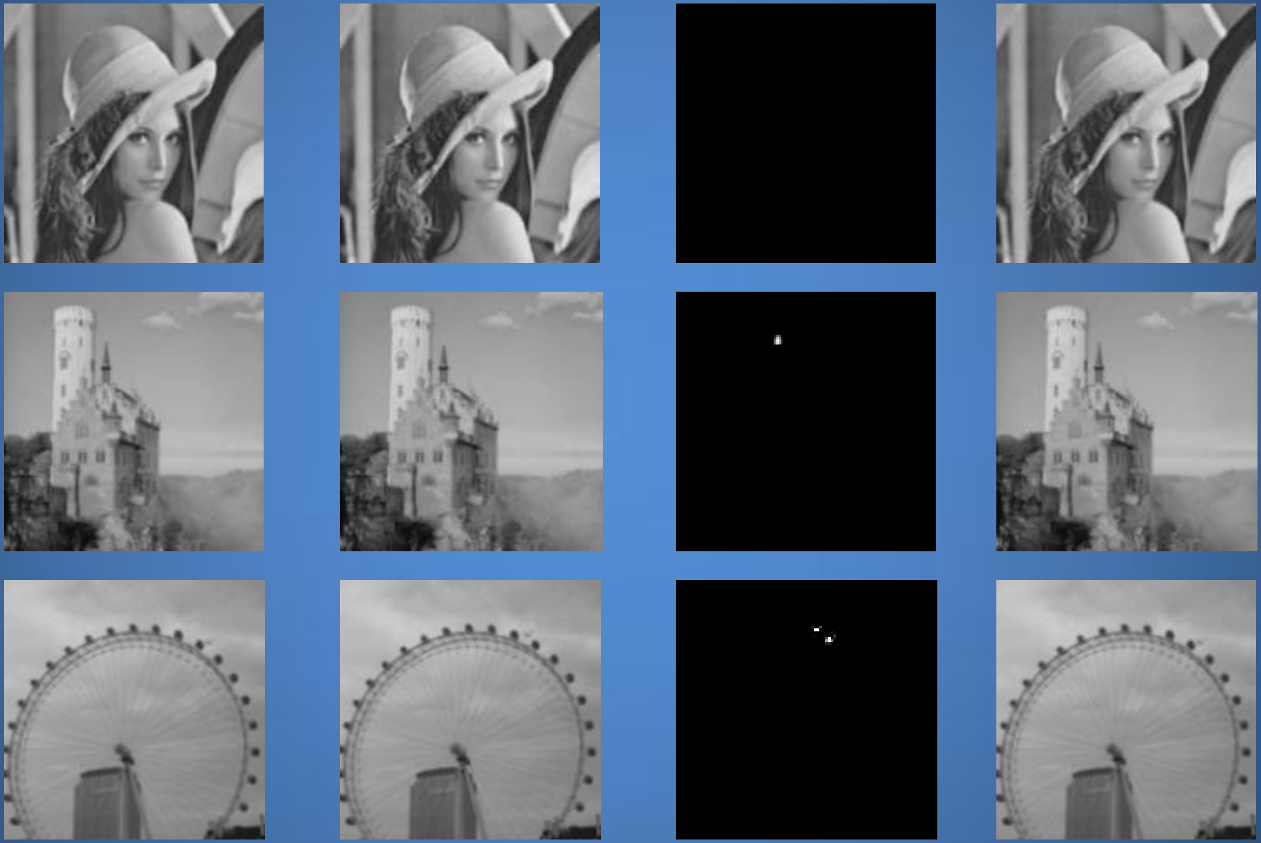
Channel

Attacker

Is the image credible?

Receiver

Experimental Results



1st row Lena (Original, Watermarked, Difference and Recovered), 2nd row and 3rd (Watermarked, tampered, detection and recovered)

THANKS…

Any Questions?