

Multimedia Information Security and Forensic Technologies

Chi Man Pun



Department of Computer and Information Science
Faculty of Science and Technology



澳門大學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU

What Is A Watermark?

- A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity.
- A distinguishing mark impressed on paper during manufacture; visible when paper is held up to the light.



What Is Digital Watermarking?

- Digital watermarking is an extension of watermarking concept in the digital world.
- A digital watermark is a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.).



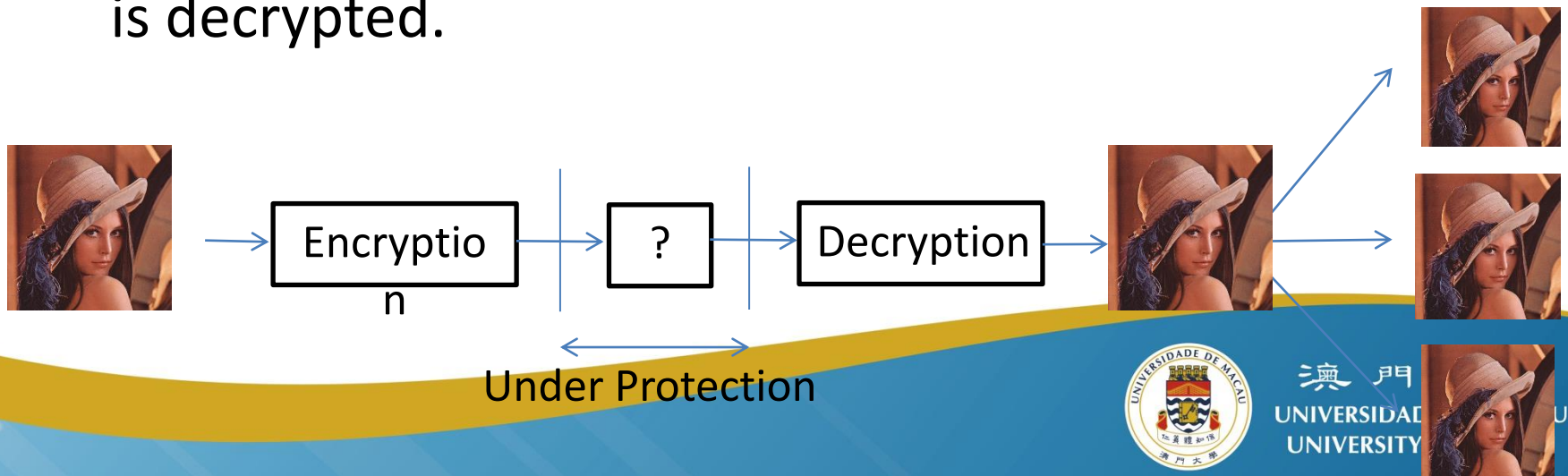
Steganography vs. Watermarking

- The main goal of **steganography** is **to hide** a message m in some audio or video (cover) data d , to obtain new data d' , practically indistinguishable from d , by people, in such a way that an eavesdropper **cannot detect** the presence of m in d' .
- The main goal of **watermarking** is **to hide** a message m in some audio or video (cover) data d , to obtain new data d' , practically indistinguishable from d , by people, in such a way that an eavesdropper **cannot remove or replace** m in d' .



Cryptography vs. Watermarking

- Cryptography is the most common method of protecting digital content and is one of the best developed science.
- However, encryption cannot help the seller monitor how a legitimate customer handles the content after decryption.
- Digital watermarking can protect content even after it is decrypted.



Visible Watermarking

- Visible watermark is a translucent overlaid into an image and is visible to the viewer. Visible watermarking is used to indicate ownership and for copyright protection.



Invisible Watermarking

- Invisible watermark is embedded into the data in such a way that the changes made to the pixel values are perceptually not noticed. Invisible watermark is used as evidence of ownership and to detect misappropriated images.

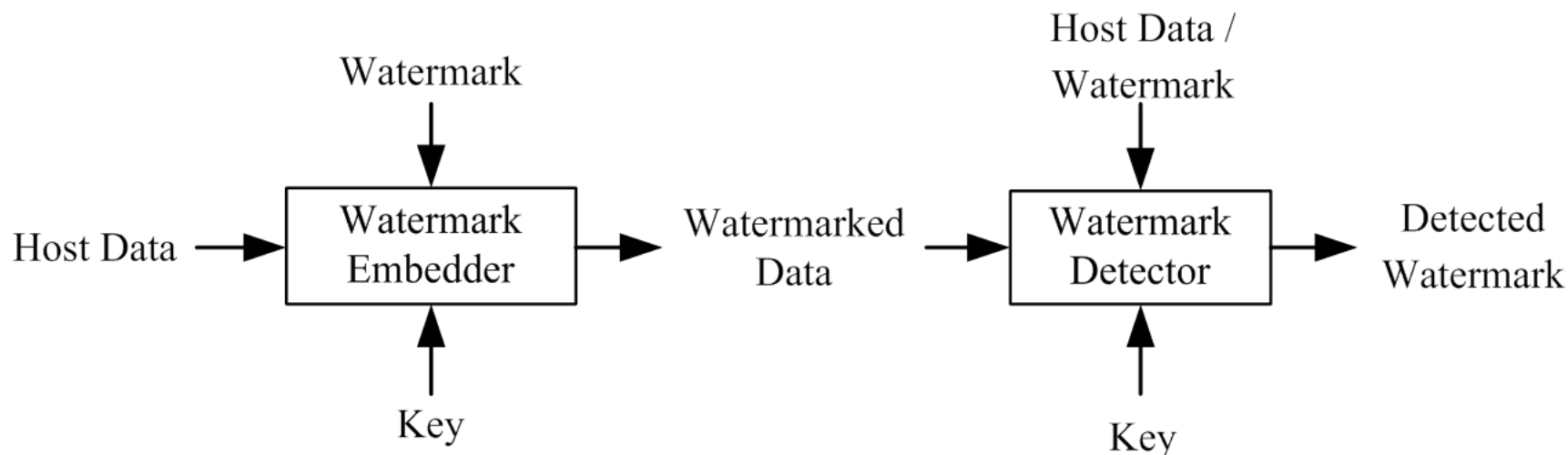


Digital Watermarking Applications

- Authentication
- Copyright Protection
- Database Retrieval and Data Hiding
- Content Description
- Copy and Usage Control



A General Digital Watermarking System



■ Robust Watermarking

- *If the watermarked data is altered, the detected watermark should still well match the watermark.*

■ Fragile Watermarking

- *As long as the watermarked data is slightly modified, the detected watermark should be significantly different from the watermark.*



Examples of Digital Image Watermarking

Original









Watermarked





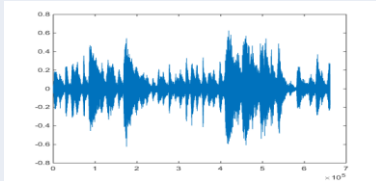
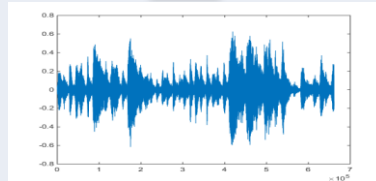


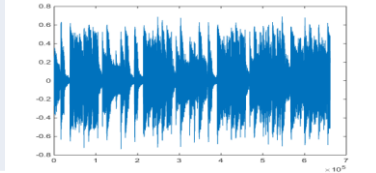
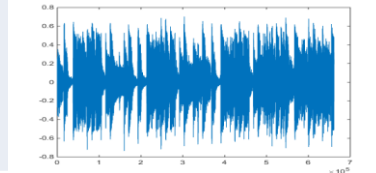


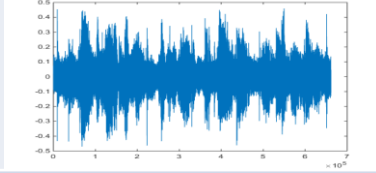
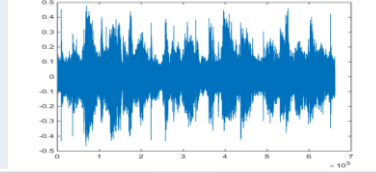


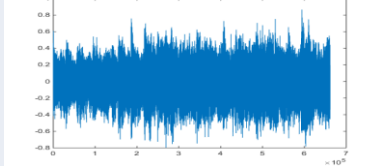
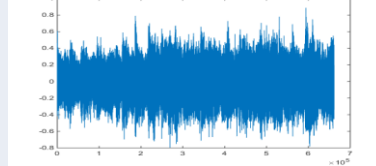
澳門大學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU

Examples of Digital Video Watermarking

	“Carphone”	“Hall”	“Mobile”
Original			
Watermarked			



Examples of Digital Audio Watermarking

Audio Clips	Original	Watermarked
“Danube”		
		
“March”		
		
“Heart”		
		
“Piano”		
		

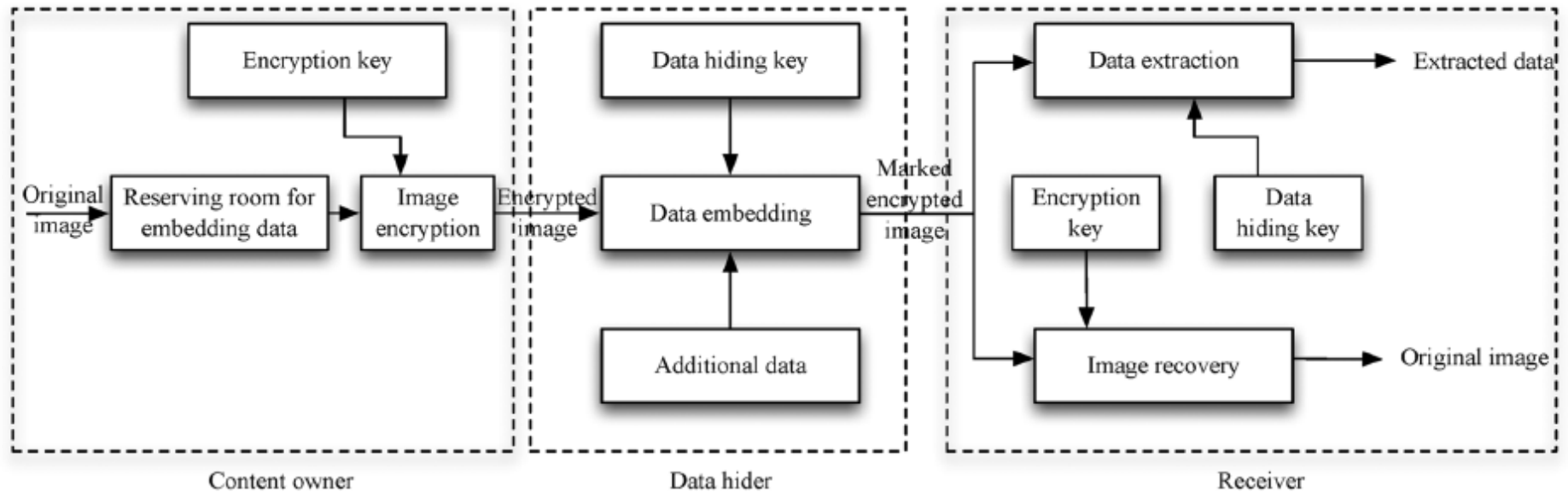


Digital Watermarking / Data Hiding in Encrypted Multimedia

- Enormous streams of real-time valuable data, such as multimedia content, generated from the embedded systems needs to be protected or encrypted to preserve privacy and access control.
- However, encrypted data is usually unintelligible. Hence, it is difficult to extract features without the decryption key.
- It is very useful to manage the encrypted data if we can embed some information in the encrypted domain.



A Reversible Data Hiding System for Encrypted Images



Digital Image Forgery

Seeing is believing ... or is it?



澳門大學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU

Digital Image Forgery



Source image



Tampered image

Easy to be tampered



Digital Image Forgery

- Copy-move forgery
- Splicing forgery

Copy-move Forgery: a part of picture is copied and then pasted onto the same picture to merge to a new image

original image



forgery image



An example of the altered photograph released by Iran and published by western media on July 9, 2008.



澳門大學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU

Splicing Forgery : a part of one picture is copied and then pasted onto the other different picture to merge to a new image

original image



forgery image



The Tourist Guy appeared in a faked photo spread by e-mail shortly after the terrorist attacks of 11 September 2001.



澳門大學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU

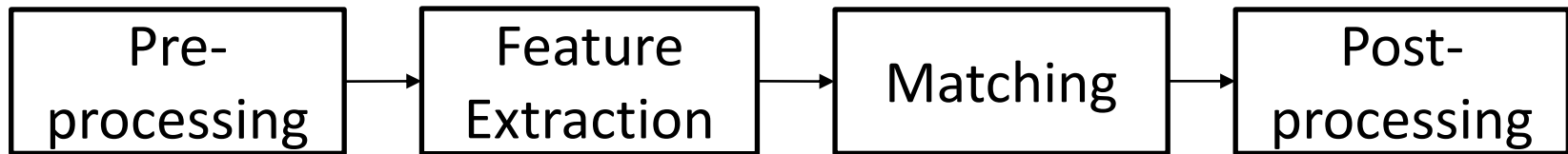
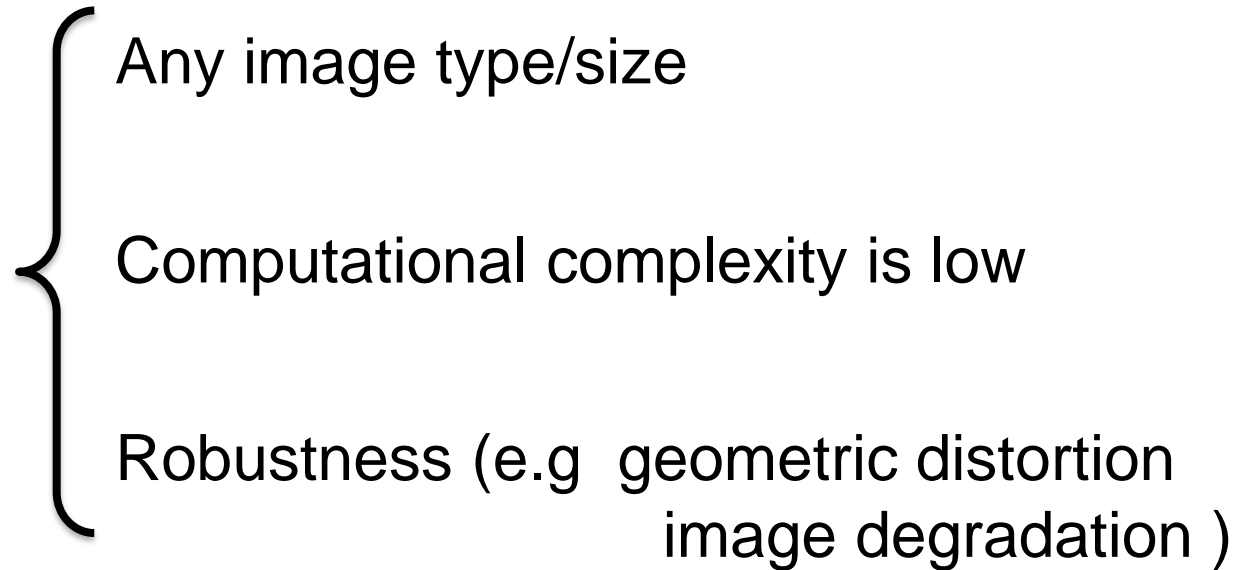
Challenges

- The comprehensiveness of tampering detection
 - » for arbitrary size of the tampered regions
 - » for any position of the tampered regions in the image
- The accuracy of tampering localization
 - » under various content-preserved attacks such as noise, Jpeg compress, low pass filtering, etc.



Copy-Move Forgery Detection(CMFD)

A novel
CMFD

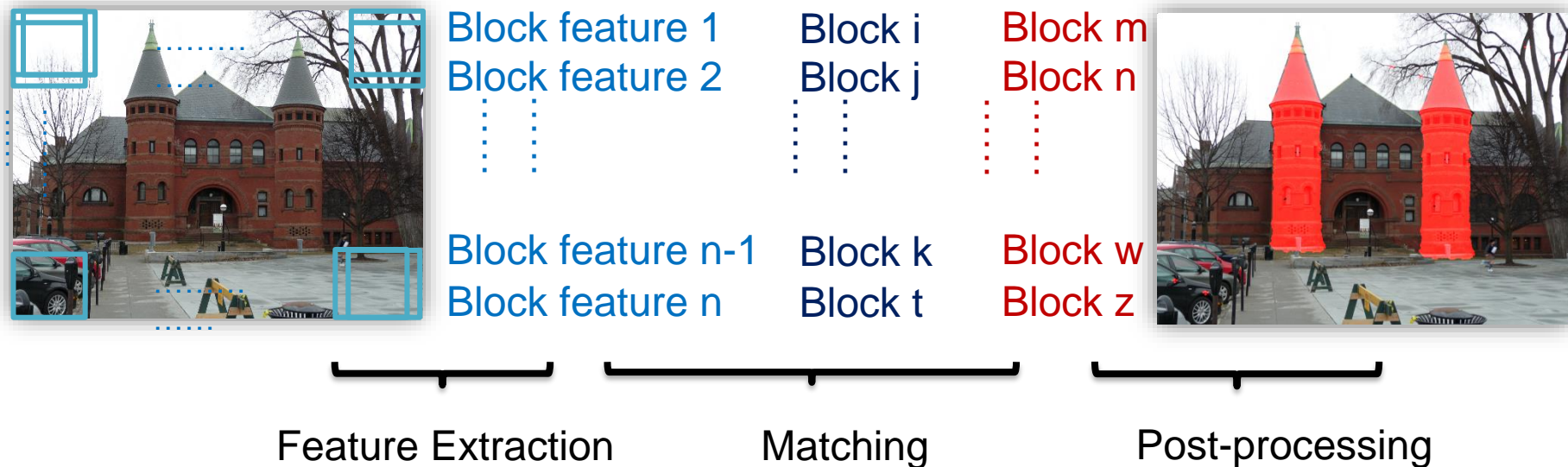


common processing pipeline



- Any image type/size 😊
- Computational complexity 😞
- Robustness 😞

Block-based Detection Method(DCT, DWT, PCA, Zernike and so on)

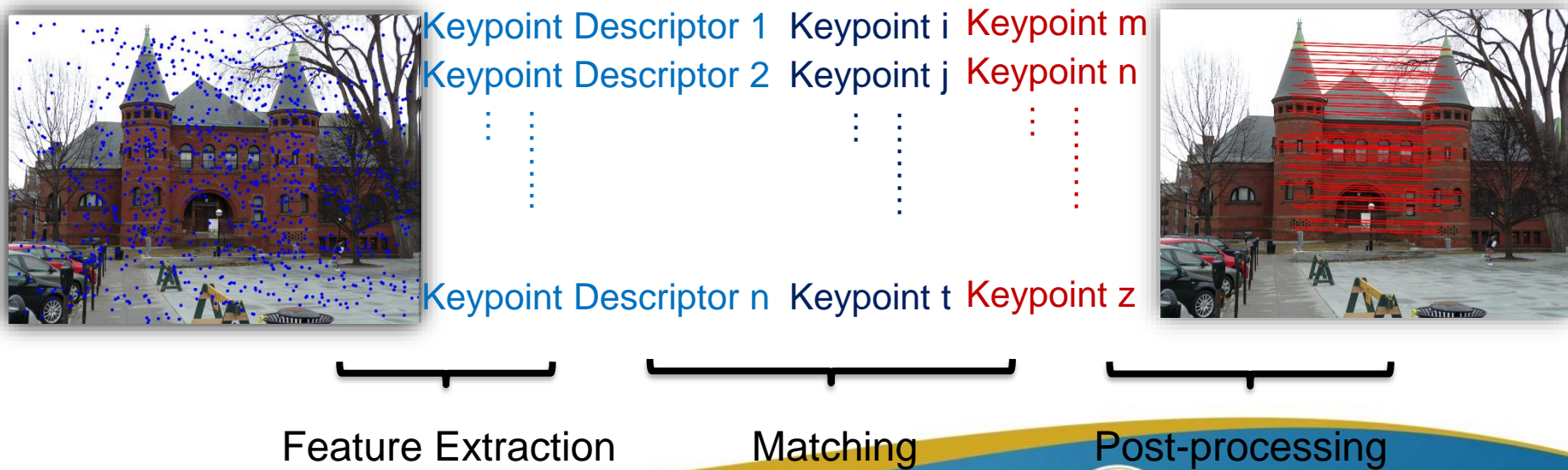


$$\langle (x_i, y_i), (x_j, y_j) \rangle \rightarrow d_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$$



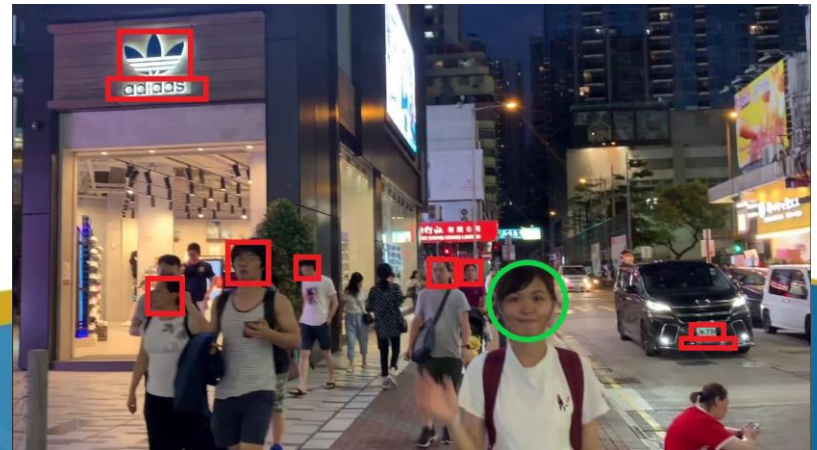
- Any image type/size 😞
- Computational complexity 😊
- Robustness 😊

Keypoint_based Detection Method (SIFT,SURF)



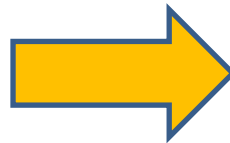
Privacy-sensitive Objects Pixelation for Live Video Streaming

- Objects expose/leak privacy-sensitive information
 - Faces, phone number, car plates, erotic images, trademarks, etc.
 - **But also depends on the scenes.**



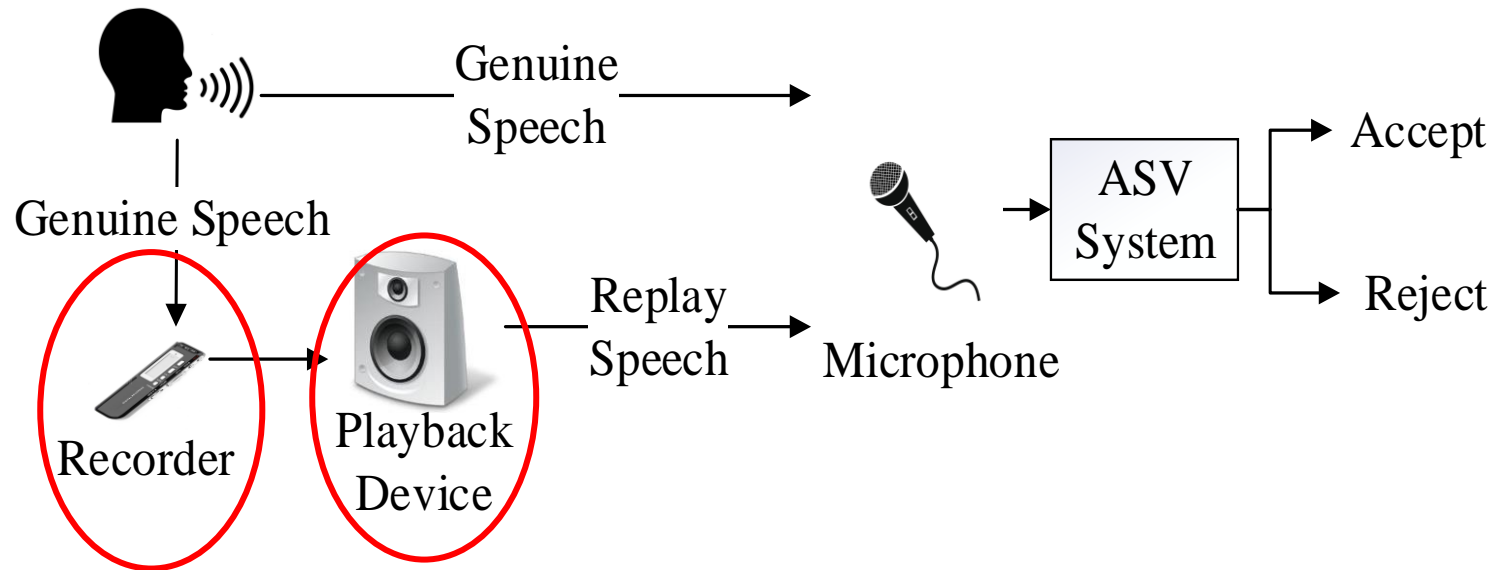
Privacy-sensitive Objects Pixelation for Live Video Streaming

- The process of allocating mosaics on sensitive objects.



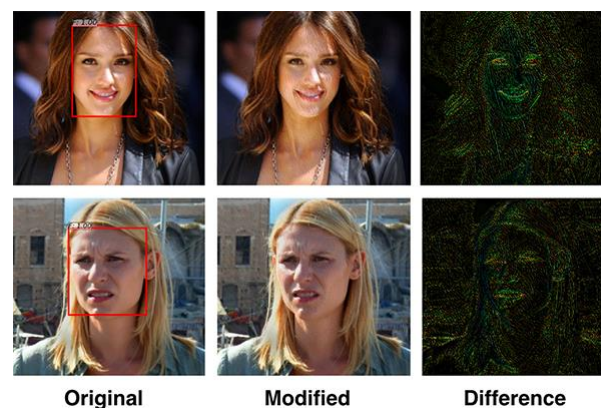
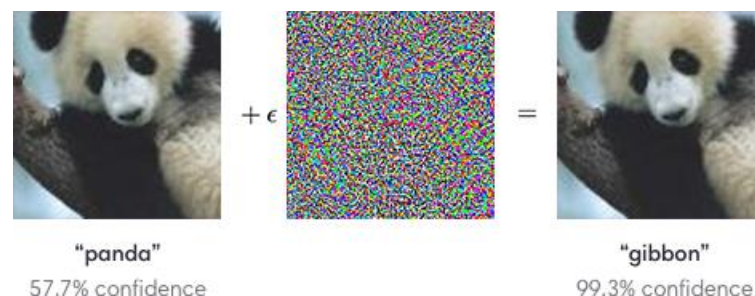
Audio Replay Spoof Attack Detection

- The implementation process of the replay attack



Security and Privacy of Machine Learning

- Adversarial Attacks on Neural Networks;
- Robust Deep Learning;
- Protection of Private Information in Machine Learning Systems.



Thank You!
Q&A



澳門大學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU