Image security and biometrics: A review

Ion Marqués and Manuel Graña

Computational Intelligence Group, University of the Basque Country

HAIS'2012, Salamanca, Spain

eman ta zabal zazu

Universidad
del País Vasco

Euskal Herriko
Unibertsitatea

Outline

Introduction

Image security

Biometrics and image security

Conclusion

Outline

Introduction

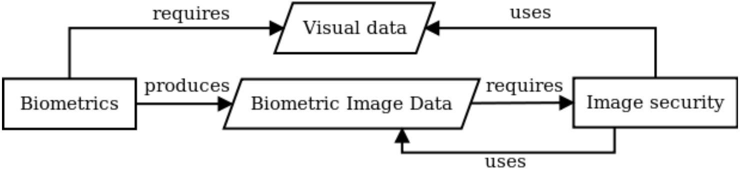
Image security

Biometrics and image security

Conclusion

Biometrics ⟷ Image security

- **Interplay** between these two research areas:



Outline

Introduction

Image security

Biometrics and image security

Conclusion

Image security

- Image security's **goals** are to ensure:
  1. The *authenticity* and/or ownership of the image creator or sender.
  2. The *integrity* of the image data, and the ability to know if the image has been altered.
  3. *Privacy*, in terms of content and/or ownership of the data.

  The developed methods must also usually compel *performance* requirements (speed, memory usage, etc.), *usability* criteria (user-friendliness, no expertise requirements,etc.) and other features that could be necessary.

Watermarking

- **Applications**: *Ownership assertion*, *data integrity* and *fingerprinting*.
- Watermarking algorithms must have a proper **tradeoff** between
  - *Fidelity:* The higher, the more difficult to notice visually.
  - *Capacity:* Amount of data that a watermark can hold.
  - *Robustness*: Resilience to passive distortions.

Watermarking

- Recent targets:
  - Focusing on specific domain of image data (e.g. Image forgery prevention, image forensics)
  - Copyright protection.
  - Lossles or lossy-to-lossless applications (e.g. Medical imaging, arts storage)

Watermarking

- Recent targets:
  - Focusing on specific domain of image data (e.g. Image forgery prevention, image forensics)
  - Copyright protection.
  - Lossles or lossy-to-lossless applications (e.g. Medical imaging, arts storage)
- Recent techniques:
  - Watermarking of **fused** biometric data.
  - **3D** data watermarking.
  - **Extractable** watermarks.
  - Ability to **recover** the original image.

Image cryptography

- Classic cryptography is centered on text data.
- Nowadays more research is focused on **image data**.

Image cryptography

- Classic cryptography is centered on text data.
- Nowadays more research is focused on **image data**.

- The idea is to use the **visual information** as the different components that form a **cryptosystem**. Furthermore, it is desirable that the procedure does not require additional optical hardware.
- For example, Hartley or Fourier or Mellin transform can be a public key and some phase distribution the private key.

Image cryptography

Other aspect of cryptography is **Visual Cryptography:**

- The idea is to divide visual information into meaningless trunks and divide them between users.
- The image can only be reconstructed if all the parts are overlaid in a certain way, hopefully without loss of information.
- These methods don't require keys because the human visual system decrypts the data.

Steganography

- The science that involves hiding and communicating secret data in a multimedia carrier like images or video is called steganography. Its goal is to hide the very existence of the secret data.

Steganography

- The science that involves hiding and communicating secret data in a multimedia carrier like images or video is called steganography. Its goal is to hide the very existence of the secret data.
- This is a key feature in applications like medical image sharing, which handle private data.

Steganography

- Most algorithms work on spatial or frequency domain.
- The fusion of both domains has lead to better results.
- Some approaches try to hide the data and enhance the image quality at the same time.
- Recent trends focus also on 3D steganography algorithms.

Outline

Introduction

Image security

Biometrics and image security

Conclusion

Biometrics: Introduction

- Biometric algorithms and procedures should conform a system which **ensures the identity of the target** using biological traits: Fingerprint, face image, DNA sequence, voice, walking gaits, etc.

Biometrics: Introduction

- Biometric algorithms and procedures should conform a system which **ensures the identity of the target** using biological traits: Fingerprint, face image, DNA sequence, voice, walking gaits, etc.

- Most of biometric systems require strong security. Therefore, they usually make use of **watermarking**, **cryptography** and **steganography**.

Biometric systems: Properties

- *Universality*: Applicable to every human.
- *Distinctiveness*: Any two subject's biometric features must be sufficiently distinguishable.
- *Permanence*: The biometric features should be persistent over time. Obtaining or verifying them should not induce changes in the user's biometric features.
- *Collectability*: The features can be measured quantitatively.
- *Performance*: Accuracy, speed, low resource usage and invariability to environmental factors are desirable.
- *Acceptance*: It is important to measure the social acceptance of a certain biometric characteristic.
- *Security*: Biometric systems should ensure authenticity, integrity, privacy and resistance to attacks and forgery.

Biometric methods ⟷Imaging techniques

Technique	Image-based method?	Involvement of image techniques	
	(image type)	Acquisition	Verifc./identific.
Face recognition	Yes (visual)	Yes	Yes
Ear recognition	Yes (visual)	Yes	Yes
Thermography	Yes (infrared)	Yes	Yes
Palmprint/fingerprint	Yes (scan)	Yes	Yes
Iris	Yes (visual)	Yes	Yes
Retinal scan	Yes (infrared)	Yes	Yes
Geometry (e.g. hand)	Yes (scan)	Yes	Yes
Gait	Yes (video)	Yes	Yes
EHF image (e.g thorax)	Yes (EHF)	Yes	Yes
Dental	Sometimes	Sometimes	Sometimes
Signature, keystroke	No	Sometimes	Sometimes
Voice	No	No	Sometimes
Odor	No	No	No
DNA	No	No	No

Image based biometrics

- Face recognition. Recent approaches:
  - Lattice computing, frequency based methods. Soft biometrics used to enhance these hard biometrics.
  - Use of infrared data, 3D data, etc.

Image based biometrics

- Face recognition. Recent approaches:
  - Lattice computing, frequency based methods. Soft biometrics used to enhance these hard biometrics.
  - Use of infrared data, 3D data, etc.
- Iris recognition (is more obtrusive, pupils dilate, there are reflections, people wear contact lenses):
  - Fusing different techniques (e.g. Gabor filters and DCT) leads to systems less sensitive to poor quality data.

Image based biometrics

- There are other image based biometrics like palmprint recognition, hand geometry, dental biometrics, ear biometrics, millimetre-wave scans, etc.

Image based biometrics

- There are other image based biometrics like palmprint recognition, hand geometry, dental biometrics, ear biometrics, millimetre-wave scans, etc.
- **Multi-modal (or hybrid) biometrics** is another current research area:
  - Extract and fuse features from different sources like faces and palmprints.
  - Build classifier ensembles using different feature types on each classifier.

Biometric image security

- The use of biometric features like face images or fingerprints to enhance classic cryptographic or watermarking systems is a promising approach.

Biometric image security

- The use of biometric features like face images or fingerprints to enhance classic cryptographic or watermarking systems is a promising approach.
- This research topic open some concerns: What happens if the biometrics of a subject are stolen? What is the proper balance between performance and robustness? What biometric approach should we use in terms of proper universality, distinctiveness, social acceptance, etc.?

Biometric image security

- One of the approaches is to secure biometric images via **encryption** techniques.
- The challenge of bio-cryptography is to implement *cancelable* biometrics, which can be described as the application of non-invertible and repeatable modifications to the original biometric templates.

Biometric image security

- One of the approaches is to secure biometric images via **encryption** techniques.
- The challenge of bio-cryptography is to implement *cancelable* biometrics, which can be described as the application of non-invertible and repeatable modifications to the original biometric templates.

- **Steganography** and **watermarking** are also being employed on biometric data security. This techniques allows embedding large amounts of biometric information within an image.
- Steganography can be employed to embed biometric images into publicly transmitted images.
- Multimodal biometric image watermarking is also a promising research area.

Outline

Introduction

Image security

Biometrics and image security

Conclusion

Conclusion

- Computer vision and imaging sciences are closely related to biometrics. The interplay between both research areas is continually evolving.
- Old biometric systems which relied on human visual verification are being displaced by the superior analyzing capabilities of computers.
- Image data has become an asset to protect, and we also use imaging techniques to secure data.
- Thus, new computational advances in steganography, watermarking or pattern recognition boost the development of secure and effective biometric systems.
- One of the big challenges is to build secure systems using hybrid or fused biometric data.

Thank you for your attention.

www.ehu.es/ccwintco