Egyptian Atomic Energy Authority
Nuclear Research Center
Department of Nuclear Reactors
First Egyptian Research Reactor

Biometrics security and privacy protection

Prepared by:

AHMED ASAKER
“Nuclear Research Center, Department of Nuclear
Reactors, Inshas, P.O. Box 13759,
Atomic Energy Authority, Cairo, Egypt”

OSAMA ZAHRAN
Department of Electronics and Electrical Communication Engineering,
Faculty of Electronic Engineering
Menoufia University, Menoufia, Egypt

The scope

- The scope of this work is to provide an overview of various methods that used for preserving the privacy and security of the individual's biometrics data including:

  - ➢ Encryption techniques
  - ➢ Visual cryptography
  - ➢ Biometric watermarking
  - ➢ Steganography
  - ➢ Cancellable biometrics, and
  - ➢ Hybrid methods

physical protection system

- Physical security at nuclear facilities is an important licensing and design consideration.
- The ultimate objective of the physical protection system (PPS) is to prevent the accomplishment of unauthorized overt or covert actions to nuclear facilities and nuclear materials.
- Access Control Systems are one of the main pillars of physical protection

What is the Purpose of an Access Control System?

- To prevent unauthorised persons from gaining access to all or part of a given area.
- To allow access of authorised people to given area.

Automatic ACS Equipment (minimum requirements)

- Method of identification.
- Controllable door lock or release.
- Controller.
- Appropriate power supply.
- Communications between the items.
- Method of exit .

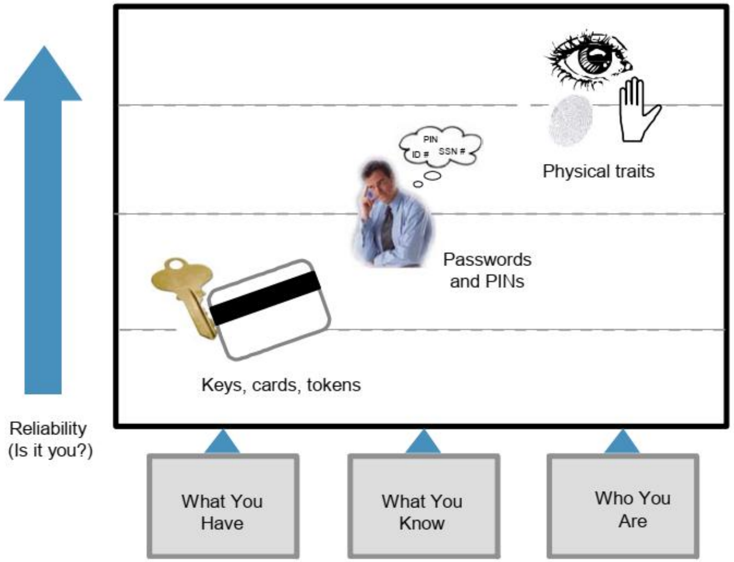
Identification technology

- Identifying people methods fall into three main categories of increasing reliability and increasing equipment cost

❖ What you have

❖ What you know

❖ Who you are



Individual Characteristics for Biometrical Identification of a Person

- Hand outline (HandKey)
- Fingerprint
- Retina
- Voice
- Iris

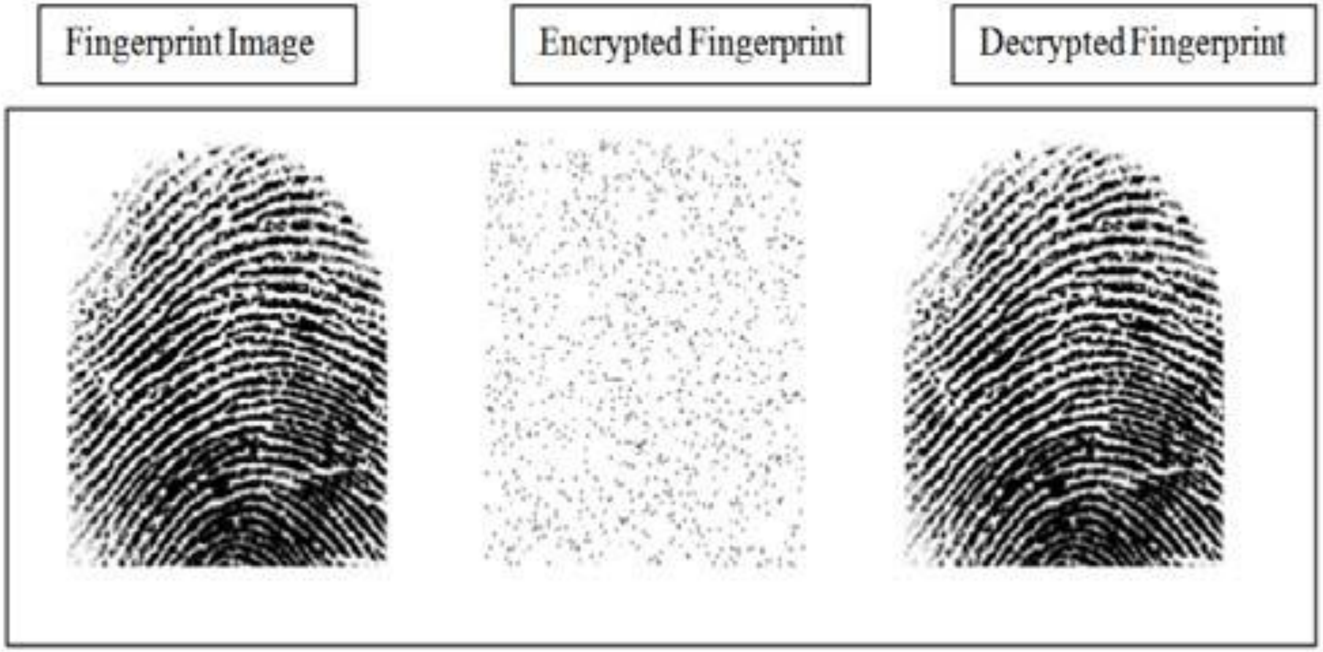
biometrics security and privacy concerns

- Biometrics cannot be revoked or canceled
- Biometrics is not secret.
- Cross application invariance and cross-matching

- So biometrics definitely is sensitive data and therefore should be properly protected.

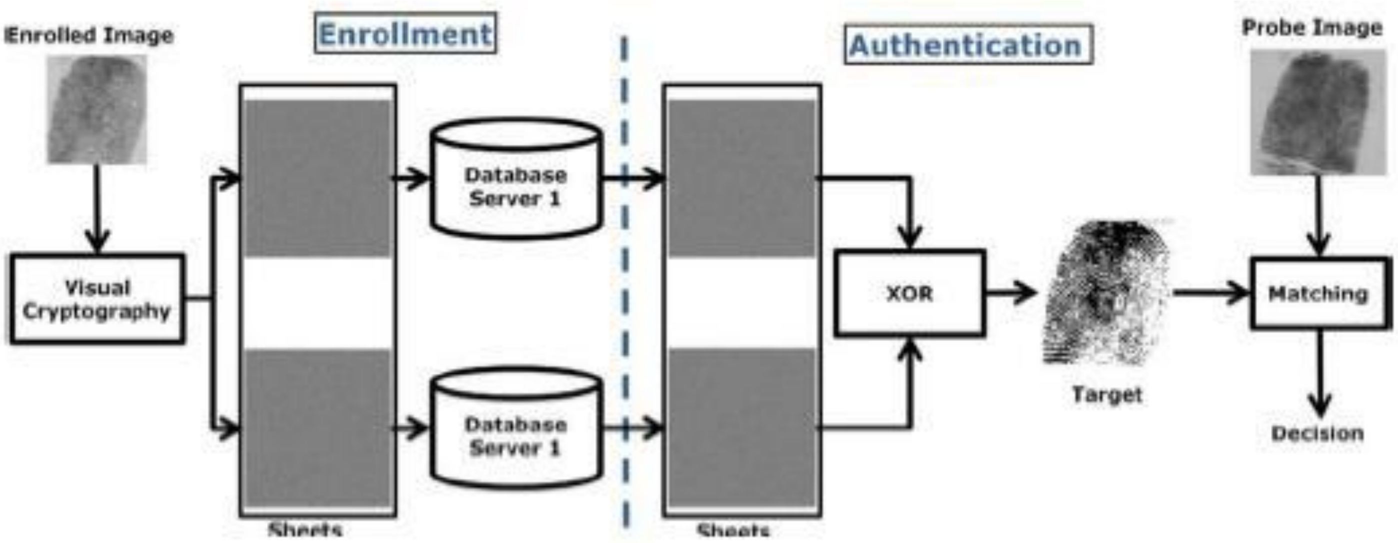
Biometrics security and privacy protection strategies

1- Encryption techniques



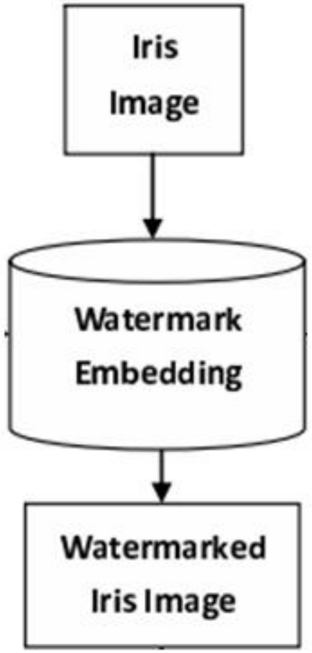
Security Schemes for Biometric securing

2- Visual Cryptography Technique



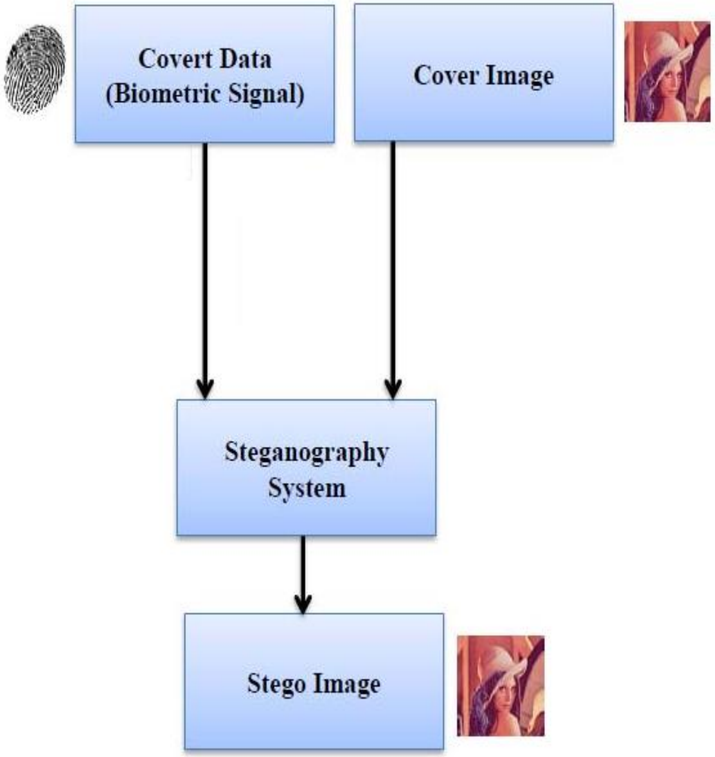
Security Schemes for Biometric securing

3- Biometric watermarking



Security Schemes for Biometric securing

4- Steganography Techniques



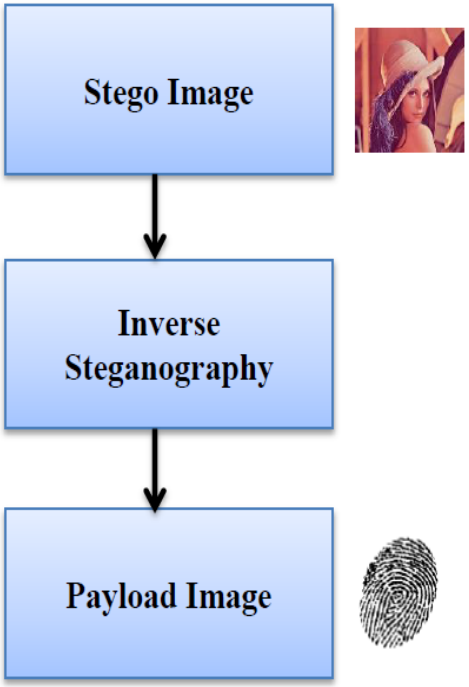
Covert Data (Biometric Signal)

Cover Image

Steganography System

Stego Image

Embedding Algorithm



Stego Image

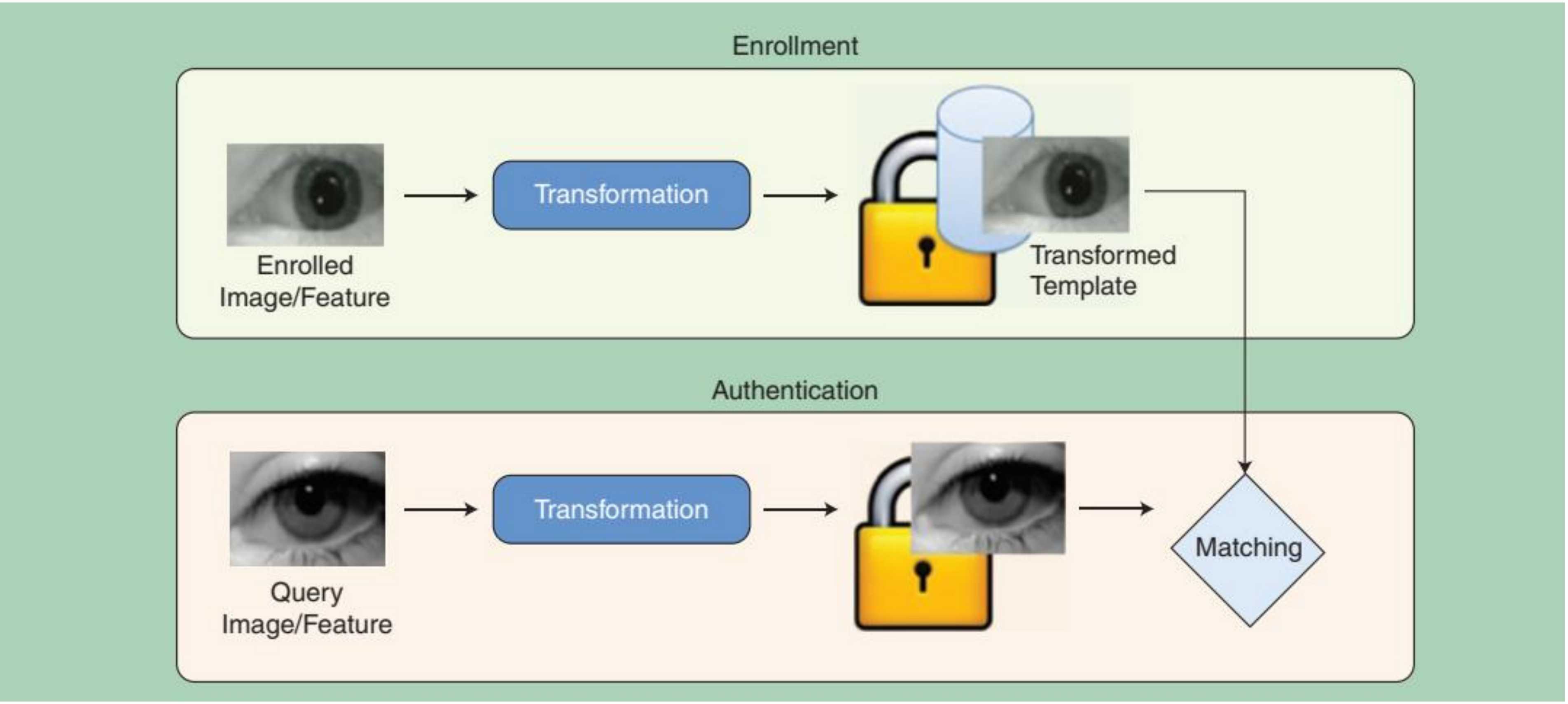
Inverse Steganography

Payload Image

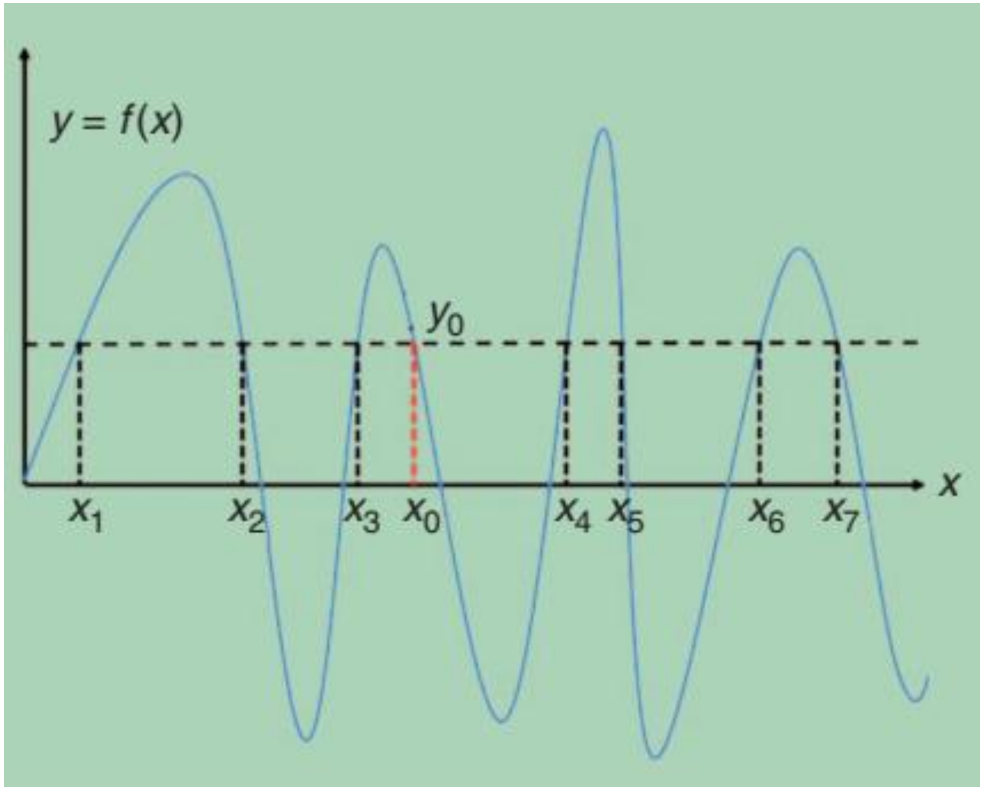
Extraction Algorithm

Security Schemes for securing Biometric data

5- Cancelable biometric

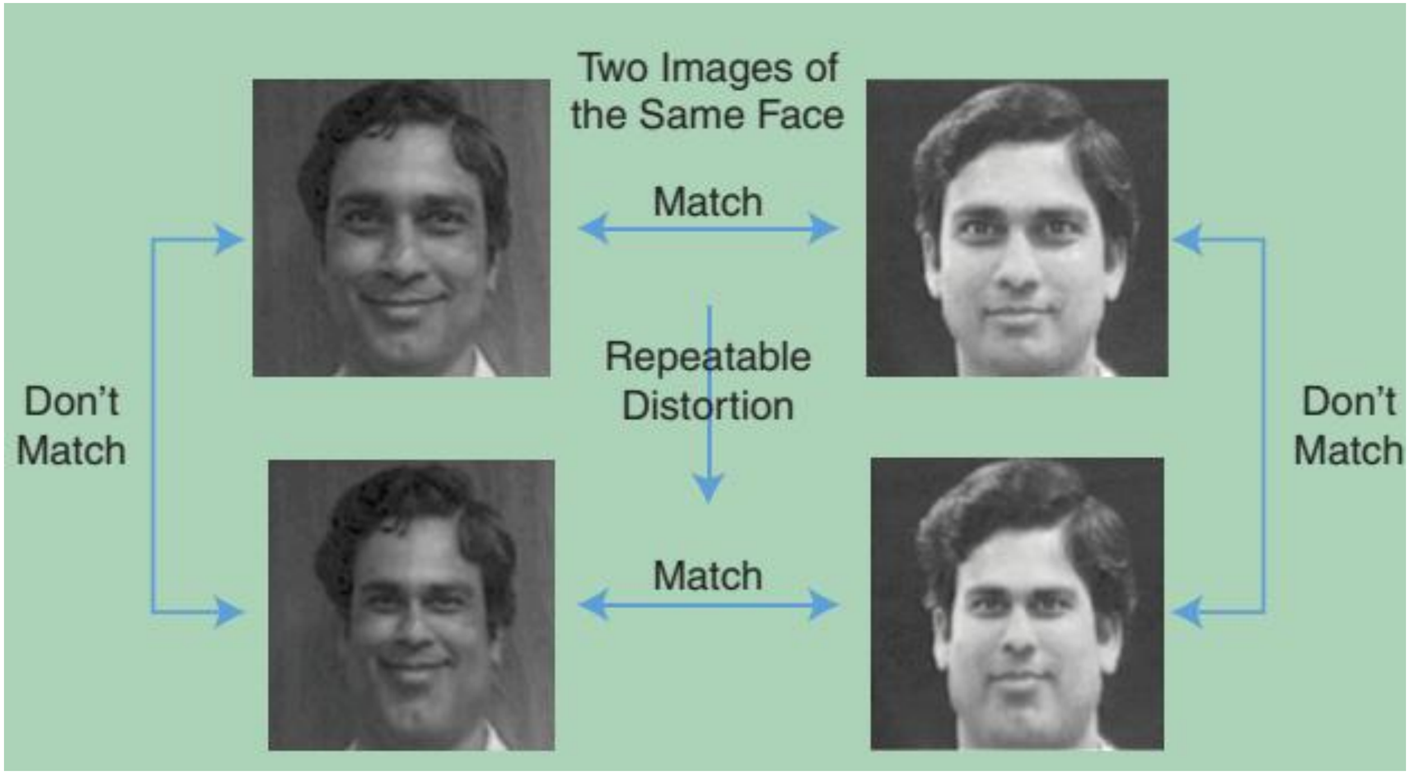


Cancelable biometric example applied in the feature domain for fingerprint biometric



Feature-domain nonlinear transformation example for fingerprint biometrics. each minutiae (feature) position is transformed using a noninvertible function.

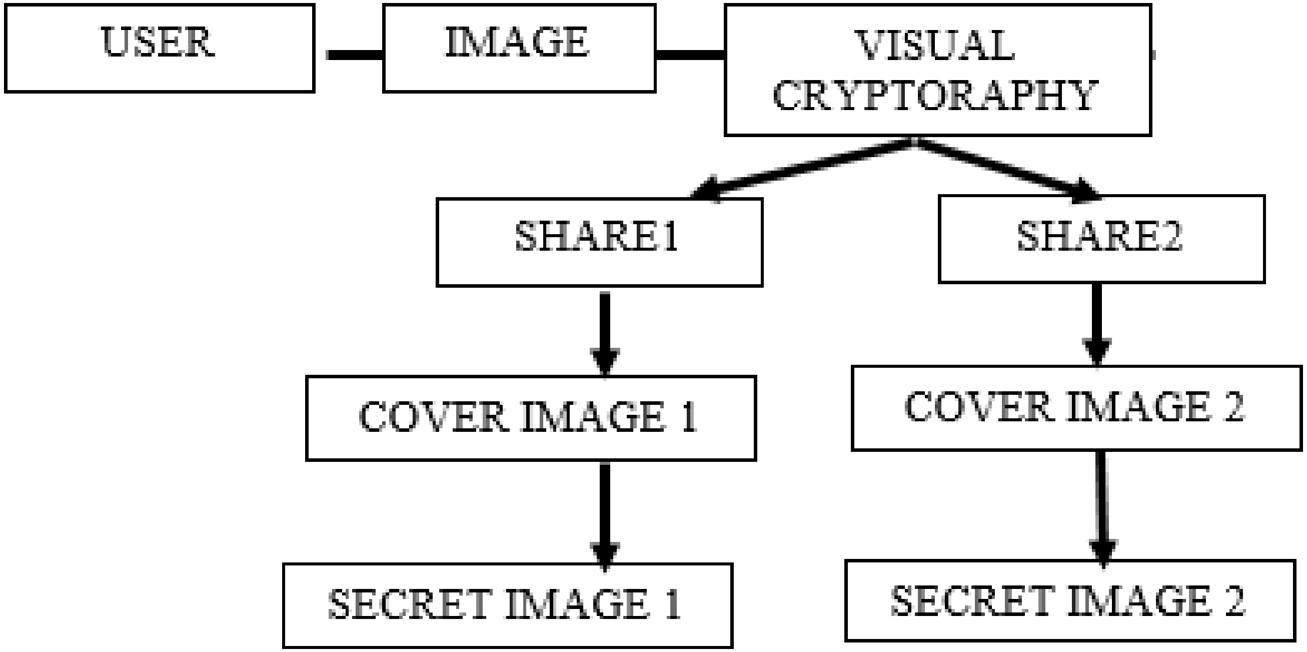
Cancelable biometric example applied in the signal domain for face biometric.



Security Schemes for Biometric securing

6- Hybrid methods

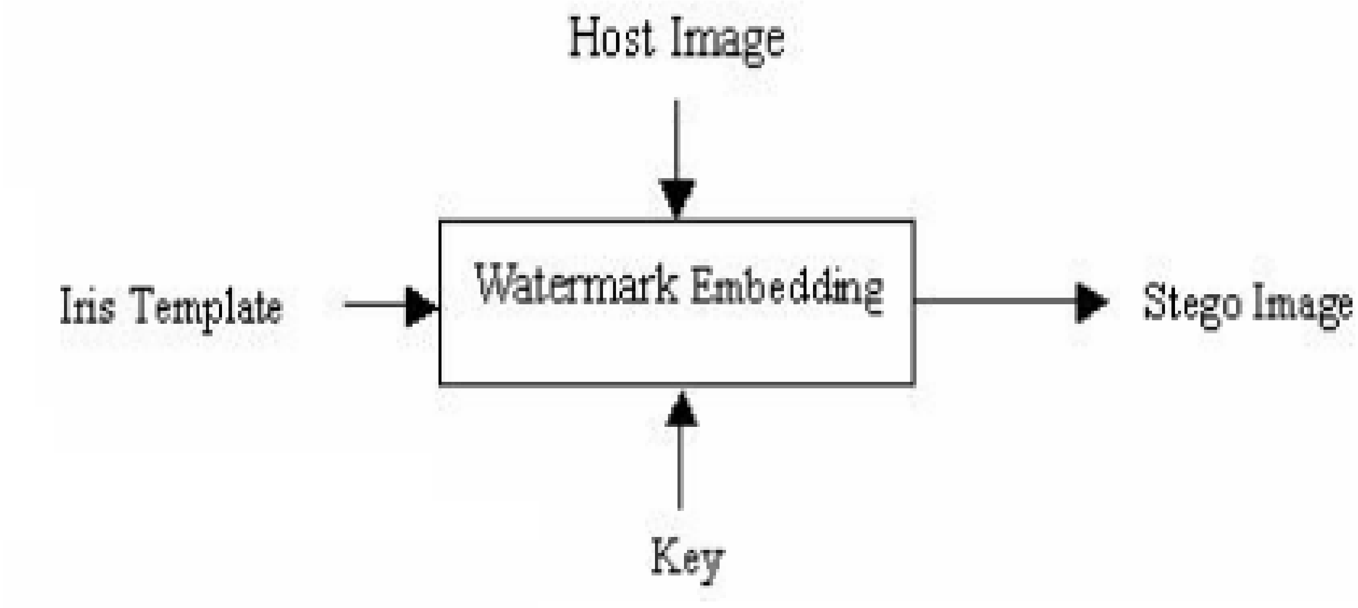
Combination of Visual Cryptography and Steganography



Security Schemes for Biometric securing

6- Hybrid methods

Combination of watermarking and steganography scheme



Conclusion

- Nowadays, biometric technologies provide a reliable solution for identity verification problem that allows restriction access to confidential data via unauthorized users.
- With the widespread deployment of biometric systems in various applications, there is an increasing concern that biometric technologies can be compromised and misused by any attacker.
- So, biometrics definitely is sensitive data and therefore it should be properly secured.
- This article presented a review of recent protection schemes developed for preserving the privacy and security of biometrics data which included encryption techniques, visual cryptography technique, watermarking, stegnography, cancellable biometrics and hybrid methods.
- cancellable biometric scheme has been widely recognized as one of the desirable solutions towards more secure biometrics.

Thank you for your attention