Security Issues in Biometric Identification

Anthony Delehanty

University of Minnesota, Morris

Computer Science Senior Seminar
Morris, MN, April 30, 2011

Outline

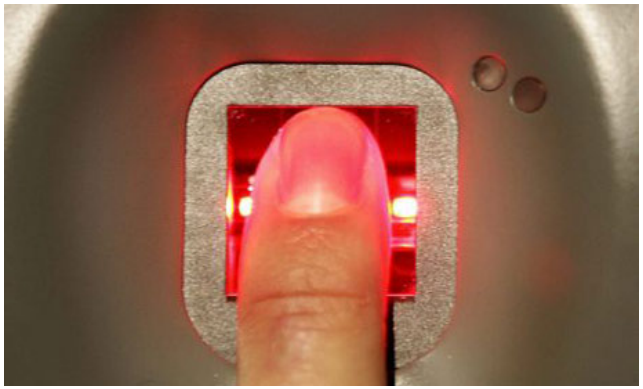
Introduction

- What are Biometrics?
- Benefits and Disadvantages
- Usage

What are biometrics?

Biometrics are traits inherent to an individuals body including:

- DNA
- Fingerprints
- Facial Scans
- Many more



Benefits

Benefits

- Unique: Most biometrics are unique to an individual

Benefits

Benefits

- Unique: Most biometrics are unique to an individual
- Simple: Easy to use

Benefits

Benefits

- Unique: Most biometrics are unique to an individual
- Simple: Easy to use
- Convenient: No need to carry or remember anything extra

Benefits

Benefits

- Unique: Most biometrics are unique to an individual
- Simple: Easy to use
- Convenient: No need to carry or remember anything extra
- Stand-alone: No additional presence is needed.

Disadvantages

Disadvantages

- Intrusive: Many people don't want their biometric information out there

Disadvantages

Disadvantages

- Intrusive: Many people don't want their biometric information out there
- Easily obtainable: It is easy to acquire someone's biometric information

Disadvantages

Disadvantages

- Intrusive: Many people don't want their biometric information out there
- Easily obtainable: It is easy to acquire someone's biometric information
- Limited supply: A person only has so many fingerprints

Disadvantages

Disadvantages

- Intrusive: Many people don't want their biometric information out there
- Easily obtainable: It is easy to acquire someone's biometric information
- Limited supply: A person only has so many fingerprints
- Group size: Some biometrics perform poorly in large groups

Modern Use

Uses

The most commonly used biometric is fingerprints
Biometrics are used for:

- Identification

Modern Use

Uses

The most commonly used biometric is fingerprints
Biometrics are used for:

- Identification
- Authentication

Process

Enrollment

Enrollment is performed the first time a user uses the system

Process

Enrollment

Enrollment is performed the first time a user uses the system

Authentication

Authentication is performed each subsequent time a user uses the system

Vulnerabilities

- Types of failures
- Types of attacks

Types

There are two types of failures in a biometric system:

Types

There are two types of failures in a biometric system:

- Intrinsic failures: Failures due to problems with the hardware or software

Types

There are two types of failures in a biometric system:

- Intrinsic failures: Failures due to problems with the hardware or software
- Failures due to an attack: Failures due to outside interference

Types

There are two types of failures in a biometric system:

- Intrinsic failures: Failures due to problems with the hardware or software
- Failures due to an attack: Failures due to outside interference

Both of these failures can result in false positives and false negatives

Types

There are two types of failures in a biometric system:

- Intrinsic failures: Failures due to problems with the hardware or software
- Failures due to an attack: Failures due to outside interference

Both of these failures can result in false positives and false negatives

- False Positives: When the system incorrectly grants access to an unauthorized person

Types

There are two types of failures in a biometric system:

- Intrinsic failures: Failures due to problems with the hardware or software
- Failures due to an attack: Failures due to outside interference

Both of these failures can result in false positives and false negatives

- False Positives: When the system incorrectly grants access to an unauthorized person
- False Negatives: When the system incorrectly denies access to an authorized person

Types of Attacks

There are three types of attacks on biometric systems:

Types of Attacks

There are three types of attacks on biometric systems:

- Insider attacks:
  An an attack performed by personel involved with the system

Types of Attacks

There are three types of attacks on biometric systems:

- Insider attacks:
  An an attack performed by personel involved with the system
- Physical attacks:
  An attack against the physical scanner

Types of Attacks

There are three types of attacks on biometric systems:

- Insider attacks:
  An an attack performed by personel involved with the system
- Physical attacks:
  An attack against the physical scanner
- Infrastructure attacks:
  An attack against the software

Physical Security and Hardware

Increasing the physical security is not recommended, as it defeats the purpose of using biometric identification

Physical Security and Hardware

Increasing the physical security is not recommended, as it defeats the purpose of using biometric identification

Additional hardware can be added to make a scanner more secure

Physical Security and Hardware

Increasing the physical security is not recommended, as it defeats the purpose of using biometric identification

Additional hardware can be added to make a scanner more secure

These methods on their own are not sufficient

Side Channel Attacks

Side Channel Attacks (SCAs) are attacks based on analysis of the system

Side Channel Attacks

Side Channel Attacks (SCAs) are attacks based on analysis of the system
Shenlin Yang and Ingrid M. Verbauwhede of UCLA [1] designed a system to counter this

Side Channel Attacks

Side Channel Attacks (SCAs) are attacks based on analysis of the system
Shenlin Yang and Ingrid M. Verbauwhede of UCLA [1] designed a system to counter this
As technology has progressed, SCAs are far less common and effective on most systems

Side Channel Attacks

Side Channel Attacks (SCAs) are attacks based on analysis of the system
Shenlin Yang and Ingrid M. Verbauwhede of UCLA [1] designed a system to counter this
As technology has progressed, SCAs are far less common and effective on most systems
A computer will estimate the time it takes to authenticate, and process random data to make up for the difference

Hashing fingerprints

Yang and Verbauwhede's system has another contribution

Hashing fingerprints

Yang and Verbauwhede's system has another contribution

Hashing fingerprints is difficult

Hashing fingerprints

Yang and Verbauwhede's system has another contribution

Hashing fingerprints is difficult

Hashing is the process of reducing a large chunk of data to a smaller one

Hashing fingerprints

Yang and Verbauwhede's system has another contribution

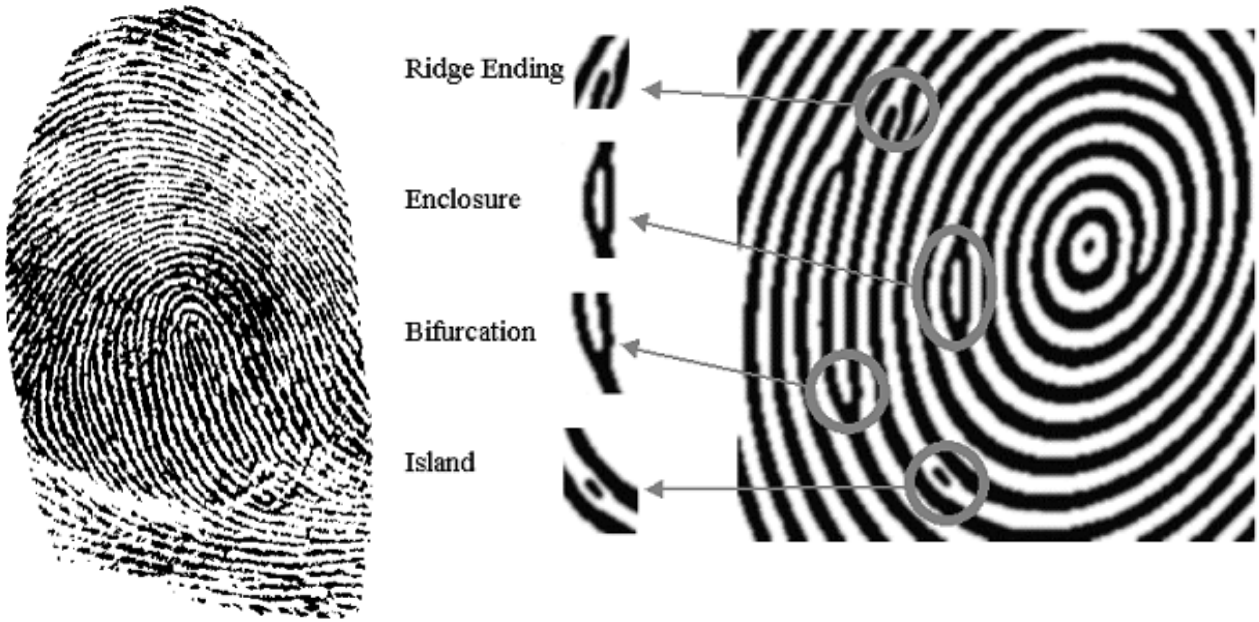
Hashing fingerprints is difficult

Hashing is the process of reducing a large chunk of data to a smaller one

Yang and Verbauwhede used a method of hashing based on minutiae which proved effective
A minutia is a minor detail of the fingerprint, its location and details can be used to identify the fingerprint

Fingerprints

Fingerprint Minutiae



Results

Results

- Used 10 fingerprints of 10 fingers to provide 100 fingerprint images
- Each minutia's neighborhood was determined by the six nearest neighbors
- Three of these neighbors had to match for a minutia to be validated

Results

Results

- Used 10 fingerprints of 10 fingers to provide 100 fingerprint images
- Each minutia's neighborhood was determined by the six nearest neighbors
- Three of these neighbors had to match for a minutia to be validated
- 1% false negatives
- $<$ .01% false positives

Multimodal Systems

A multimodal system is one which uses multiple forms of biometric identification

Multimodal Systems

A multimodal system is one which uses multiple forms of biometric identification

Benefits include:

- Increased security against physical attacks

Multimodal Systems

A multimodal system is one which uses multiple forms of biometric identification

Benefits include:

- Increased security against physical attacks
- More complex data

Multimodal Systems

A multimodal system is one which uses multiple forms of biometric identification

Benefits include:

- Increased security against physical attacks
- More complex data
- Allows for better watermarking and integrity verification systems

Watermarking

What is watermarking?

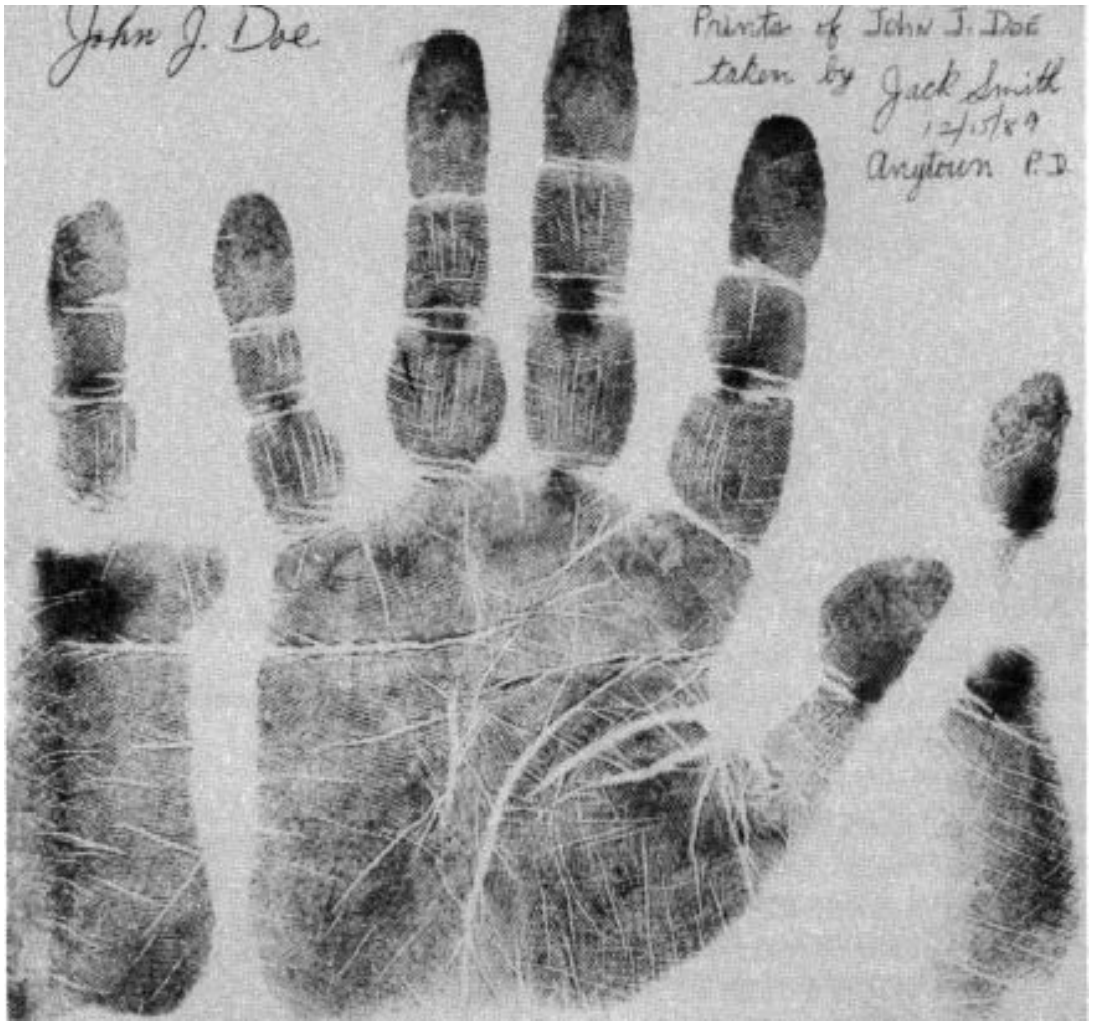
Watermarking is the process of embedding data into an object to verify its authenticity

Watermarking

What is watermarking?

Watermarking is the process of embedding data into an object to verify its authenticity
Sun et al. [2] designed a multimodal system which uses knuckleprints and palmprints

Palmprint


John J. Doe
Prints of John J. Doe
taken by Jack Smith
12/15/89
Anytown P.D.

Results

Results

- 1423 sample images, 73 hands

Results

Results

- 1423 sample images, 73 hands
- 5 samples of each hand formed training set, remaining 1058 was testing set

Results

Results

- 1423 sample images, 73 hands
- 5 samples of each hand formed training set, remaining 1058 was testing set
- Before watermarking: 96.8% recognitiion on knuckleprints, 99.7% on palmprints

Results

Results

- 1423 sample images, 73 hands
- 5 samples of each hand formed training set, remaining 1058 was testing set
- Before watermarking: 96.8% recognitiion on knuckleprints, 99.7% on palmprints
- After watermarking: 96.8% recognition on knuckleprints, 99.8% on palmprints

Results

Results

- 1423 sample images, 73 hands
- 5 samples of each hand formed training set, remaining 1058 was testing set
- Before watermarking: 96.8% recognitiion on knuckleprints, 99.7% on palmprints
- After watermarking: 96.8% recognition on knuckleprints, 99.8% on palmprints
- No decrease in recognition, increase in security

Integrity Verification

What is integrity verification?

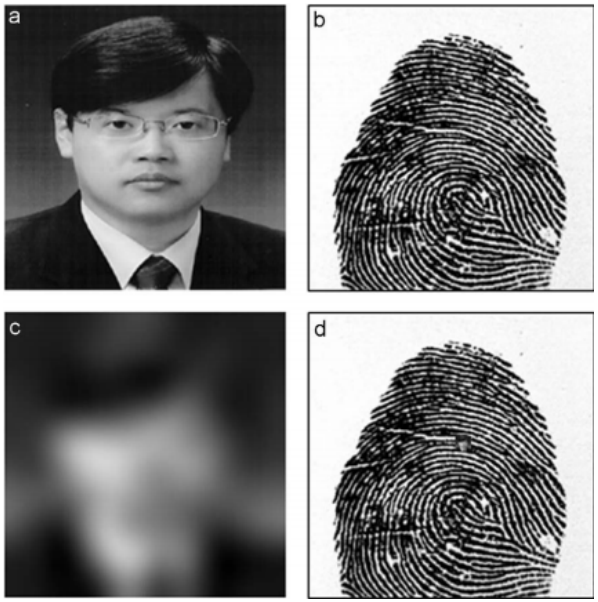
Integrity verification is the process of verifying that the input has not been tampered with

Integrity Verification

What is integrity verification?

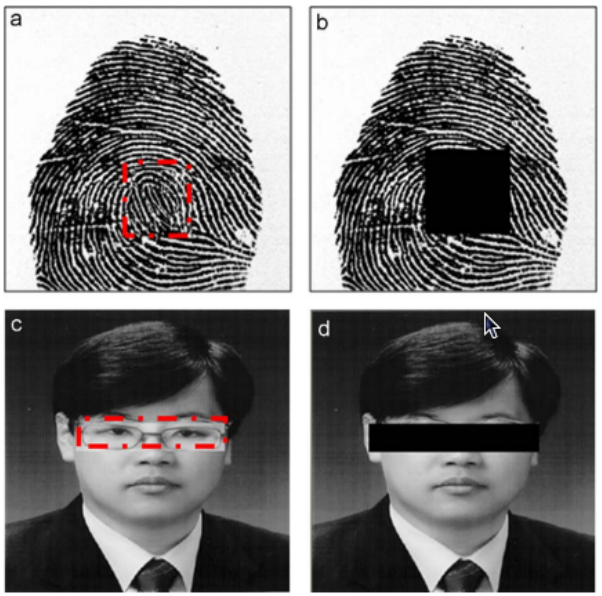
Integrity verification is the process of verifying that the input has not been tampered with

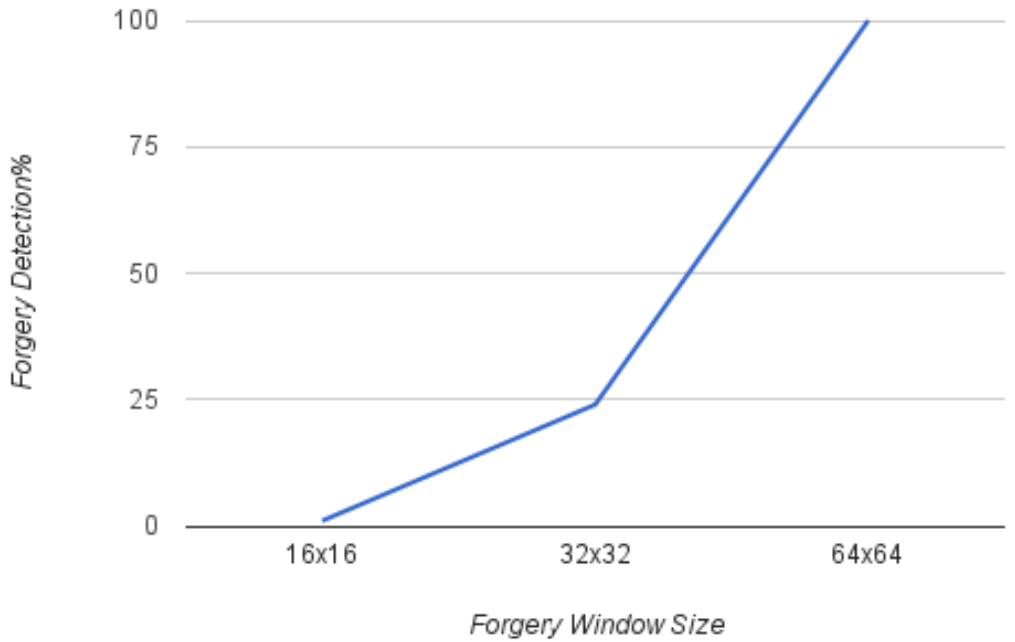
Won-gyum Kim and HeungKyu Lee designed a multimodal system which uses watermarking to verify the integrity of the input



Results

Forgery Detection Rate





Used 1000 forged fingerprint and face image pairs

Conclusions

Conclusions

Fingerprints and Minutiae

Fingerprints and Minutiae

- There are difficulties in hashing fingerprints

Fingerprints and Minutiae

Fingerprints and Minutiae

- There are difficulties in hashing fingerprints
- Hashing minutiae can get around this

Fingerprints and Minutiae

Fingerprints and Minutiae

- There are difficulties in hashing fingerprints
- Hashing minutiae can get around this
- Yang and Verbauwhede achieved the standard of 1% false negatives and .01% false positives

Fingerprints and Minutiae

Fingerprints and Minutiae

- There are difficulties in hashing fingerprints
- Hashing minutiae can get around this
- Yang and Verbauwhede achieved the standard of 1% false negatives and .01% false positives
- In the real world, fingerprints are used on groups far larger than 100, so scalability is unclear

Watermarking

Watermarking

- A multimodal system is more secure than a unimodal system

Watermarking

Watermarking

- A multimodal system is more secure than a unimodal system
- Watermarking provides additional security to a system

Watermarking

Watermarking

- A multimodal system is more secure than a unimodal system
- Watermarking provides additional security to a system
- Watermarking did not lower the effectiveness of the system

Integrity Verification

Integrity Verification

- Integrity Verification is used to validate the authenticity

Integrity Verification

Integrity Verification

- Integrity Verification is used to validate the authenticity
- This system did not work well on small modifications

Integrity Verification

Integrity Verification

- Integrity Verification is used to validate the authenticity
- This system did not work well on small modifications
- It worked very well on larger modifications

Acknowledgements

Acknowledgements

Thank you Elena Machkasova, Rob Jansen, Peter Dolan, James Delehanty, Isaac Sjoblom and Ryan Klawitter for your help in this project.

References

References

1 Yang, Shenlin and Verbauwhede, Ingrid M.: A Secure Fingerprint Matching Technique, 2003

2 Sun, Dongmei; Li, Qiang; Liu, Tong; He, Bing; and Qiu, Zhengding: A Secure Multimodal Biometric Verification Scheme, 2005

3 Kim, Won-gyum and Lee, HeungKyru: Multimodal Biometric Image Watermarking Using Two-stage Integrity Verification, 2009