Biometric Authentication using Online Signature

Claudia Tinnirello, PhD student

University of Trento
Department of Mathematics

Outline

Introduction

An example of authentication scheme

Performance analysis and possible improvements

Outline

Introduction

An example of authentication scheme

Performance analysis and possible improvements

Outline

Introduction

An example of authentication scheme

Performance analysis and possible improvements

Identification plays a fundamental role in an increasingly interconnected society.

There are three broad identification modes, based on

1. something you *know*;
2. something you *have*;
3. something you *are*.

$\rightarrow$ biometric recognition

Identification plays a fundamental role in an increasingly interconnected society.

There are three broad identification modes, based on

1. something you *know*;
2. something you *have*;
3. something you *are*.

→ biometric recognition

Identification plays a fundamental role in an increasingly interconnected society.

There are three broad identification modes, based on

1. something you *know*;
2. something you *have*;
3. something you *are*.

→ biometric recognition

Identification plays a fundamental role in an increasingly interconnected society.

There are three broad identification modes, based on

1. something you *know*;
2. something you *have*;
3. something you *are*.

→ biometric recognition

Identification plays a fundamental role in an increasingly interconnected society.

There are three broad identification modes, based on

1. something you *know*;
2. something you *have*;
3. something you *are*.

→ biometric recognition

Identification plays a fundamental role in an increasingly interconnected society.

There are three broad identification modes, based on

1. something you *know*;
2. something you *have*;
3. something you *are*.

→ biometric recognition

Handwritten Signature

The signature is captured using a digital table like

It extracts from the signature some information like: time stamp, pressure, coordinates x and y, ...

$\Rightarrow$ velocity, acceleration ...

Handwritten Signature

The signature is captured using a digital table like

It extracts from the signature some information like: time stamp, pressure, coordinates x and y, ...
$\Rightarrow$ velocity, acceleration ...

POSITIVE ASPECTS:

- people are familiar with the use of signatures in their daily life;
- analysis requires no invasive measurements.

NEGATIVE ASPECTS:

- an individual signature is never entirely the same and can vary substantially over an individual's lifetime.

POSITIVE ASPECTS:

- people are familiar with the use of signatures in their daily life;
- analysis requires no invasive measurements.

NEGATIVE ASPECTS:

- an individual signature is never entirely the same and can vary substantially over an individual's lifetime.

POSITIVE ASPECTS:

- people are familiar with the use of signatures in their daily life;
- analysis requires no invasive measurements.

NEGATIVE ASPECTS:

- an individual signature is never entirely the same and can vary substantially over an individual's lifetime.

POSITIVE ASPECTS:

- people are familiar with the use of signatures in their daily life;
- analysis requires no invasive measurements.

NEGATIVE ASPECTS:

- an individual signature is never entirely the same and can vary substantially over an individual's lifetime.
- A user's biometric cannot be changed like a password.

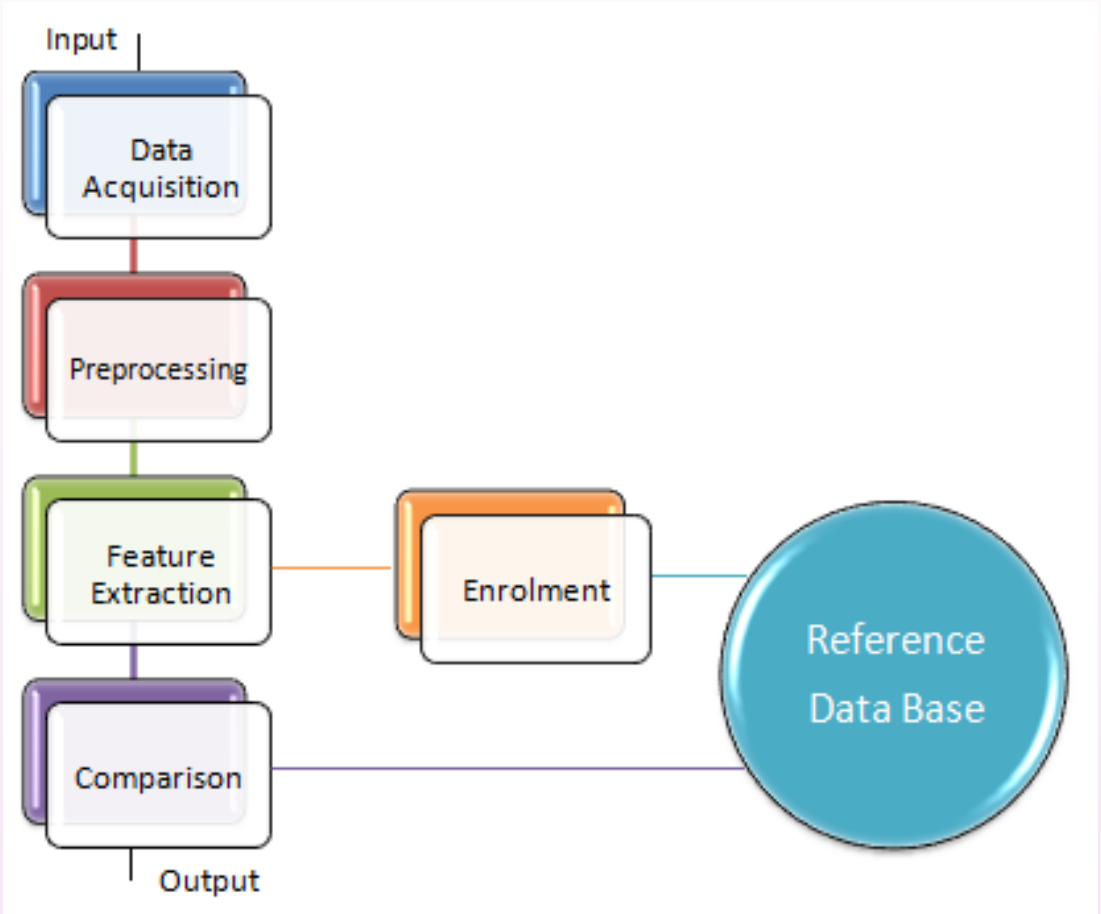
POSITIVE ASPECTS:

- people are familiar with the use of signatures in their daily life;
- analysis requires no invasive measurements.

NEGATIVE ASPECTS:

- an individual signature is never entirely the same and can vary substantially over an individual's lifetime.
- A user's biometric cannot be changed like a password.

Typical Verification Process



Our Algorithm

The algorithm consists of 3 main steps

1. **Training**: step necessary to compute time thresholds and the values used during the binarization phase;
2. **Enrollment**: the steps the algorithm follows when a new user is enrolled into the system;
3. **Authentication**: the steps the algorithm follows when a user needs to verify his gesture.

Our Algorithm

The algorithm consists of 3 main steps

1. **Training**: step necessary to compute time thresholds and the values used during the binarization phase;
2. **Enrollment**: the steps the algorithm follows when a new user is enrolled into the system;
3. **Authentication**: the steps the algorithm follows when a user needs to verify his gesture.

Our Algorithm

The algorithm consists of 3 main steps

1. **Training**: step necessary to compute time thresholds and the values used during the binarization phase;
2. **Enrollment**: the steps the algorithm follows when a new user is enrolled into the system;
3. **Authentication**: the steps the algorithm follows when a user needs to verify his gesture.

Training

For this step we need a training database, representative of the population we want to enrol into the system.

The tablet extracts some or all of the following data per gesture:

- spatial coordinates X and Y ;
- a time-stamp, T;
- pressure, P;
- event type, E
- event ID - different touch events have different ID when they are simultaneously in contact with the device.

Training

For this step we need a training database, representative of the population we want to enrol into the system.

The tablet extracts some or all of the following data per gesture:

- spatial coordinates X and Y ;
- a time-stamp, T;
- pressure, P;
- event type, E
- event ID - different touch events have different ID when they are simultaneously in contact with the device.

Training

For this step we need a training database, representative of the population we want to enrol into the system.

The tablet extracts some or all of the following data per gesture:

- spatial coordinates X and Y ;
- a time-stamp, T;
- pressure, P;
- event type, E
- event ID - different touch events have different ID when they are simultaneously in contact with the device.

Feature Extraction

Starting from this data, we computed a total of 63 features for each gesture.

ID	Description	ID	Description	ID	Description
1	Number of Sample	19,21,23,25	Y Local Acceleration	49	Height
2	Time Duration	26-27	X and Y Absolute Mean Velocity	50	Y Maximum
3	Aspect Ratio	28-29	X and Y Initial Value	51	Y Minimum
4-5	X and Y Areas	30-31	X and Y Final Value	52	Y Mean
6	X Mean Velocity	32-35	Statistic Moments $M_{1,1}$,$M_{1,2}$,$M_{2,1}$, $M_{0,3}$	53	Pressure Mean
7	X Mean Acceleration	37-40	X Local Area	54	Pressure Maximum
8	Y Mean Velocity	41-44	Y Local Area	55	Pressure Minimum
9	Y Mean Acceleration	45	Width	56-57	X and Y Maximum Velocity
10,12,14,16	X Local Velocity	46	X Maximum	58-61	Pressure Local Area
11,13,15,17	X Local Acceleration	47	X Minimun	62	X Peak Number
18,20,22,24	Y Local Velocity	48	X Mean	63	Y Peak Number

Training

From the training database we calculate the following values:

- *four time thresholds* th_1, th_2, th_3, th_4 (Time Threshold Control);
- *three medians* m_1, M, m_2 for each feature (Binarization process)

Training

From the training database we calculate the following values:

- *four time thresholds* th_1, th_2, th_3, th_4 (Time Threshold Control);
- *three medians* m_1, M, m_2 for each feature (Binarization process)

Training

From the training database we calculate the following values:

- *four time thresholds* th_1, th_2, th_3, th_4 (Time Threshold Control);
- *three medians* m_1, M, m_2 for each feature (Binarization process)

Enrollment

- 5 biometric measurements are recorded for each user;
- The mean time duration T is compared to the four time thresholds computed during the training stage, obtaining `Fascia_temp`.
- For each feature the median value is compared to m_1, M, m_2 in order to assign it one of the following strings $\{1011, 1111, 0111, 0101\}$ obtaining the vector B.

  The same process is applied to each of the five feature vectors, obtaining the vectors b_1, b_2, b_3, b_4, b_5

Enrollment

- 5 biometric measurements are recorded for each user;
- The mean time duration T is compared to the four time thresholds computed during the training stage, obtaining `Fascia_temp`.
- For each feature the median value is compared to m_1, M, m_2 in order to assign it one of the following strings $\{1011, 1111, 0111, 0101\}$ obtaining the vector B.

  The same process is applied to each of the five feature vectors, obtaining the vectors b_1, b_2, b_3, b_4, b_5

Enrollment

- 5 biometric measurements are recorded for each user;
- The mean time duration T is compared to the four time thresholds computed during the training stage, obtaining `Fascia_temp`.
- For each feature the median value is compared to m_1, M, m_2 in order to assign it one of the following strings $\{1011, 1111, 0111, 0101\}$ obtaining the vector B.

The same process is applied to each of the five feature vectors, obtaining the vectors b_1, b_2, b_3, b_4, b_5

Enrollment

- 5 biometric measurements are recorded for each user;
- The mean time duration T is compared to the four time thresholds computed during the training stage, obtaining `Fascia_temp`.
- For each feature the median value is compared to m_1, M, m_2 in order to assign it one of the following strings $\{1011, 1111, 0111, 0101\}$ obtaining the vector B.

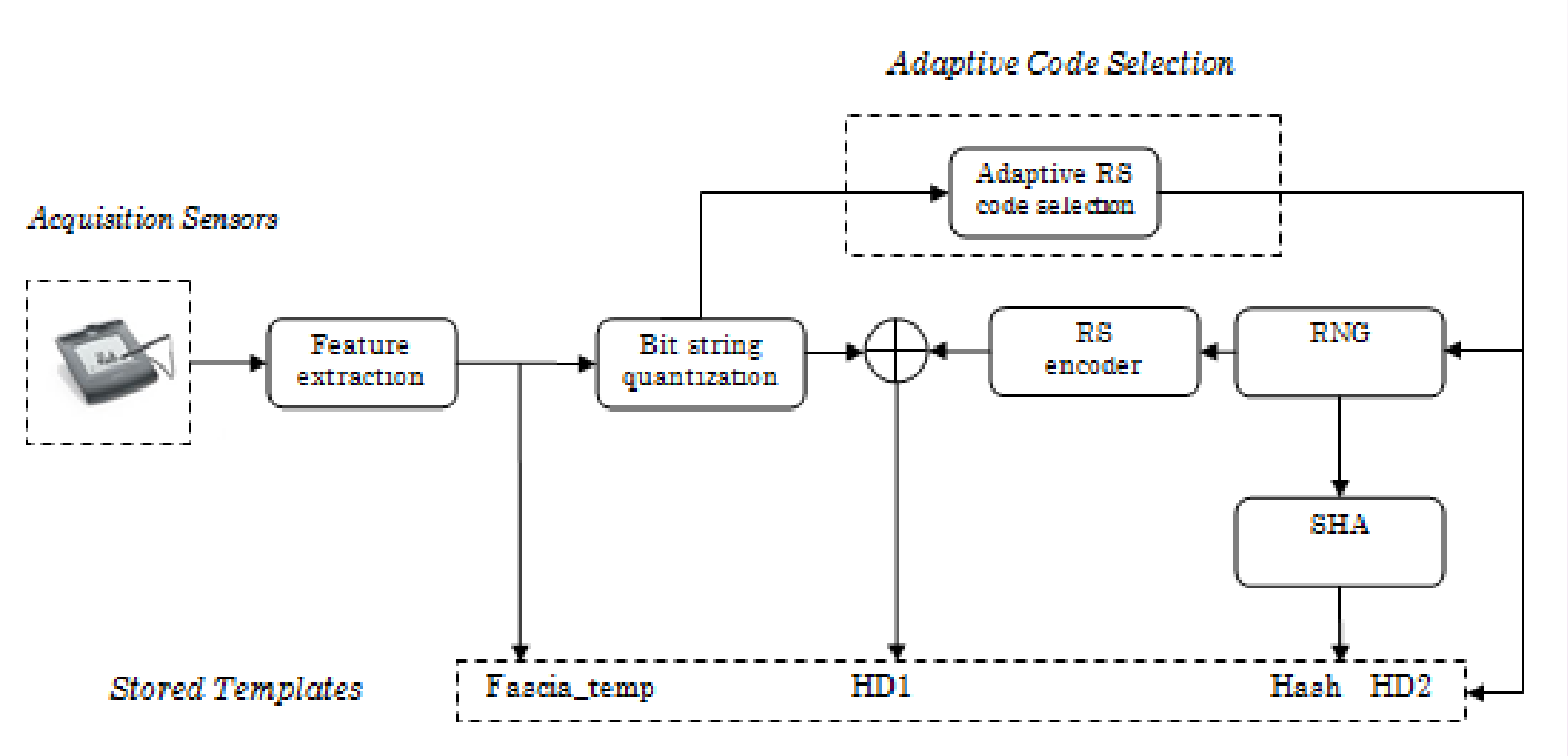
  The same process is applied to each of the five feature vectors, obtaining the vectors b_1, b_2, b_3, b_4, b_5

Enrollment

- 5 biometric measurements are recorded for each user;
- The mean time duration T is compared to the four time thresholds computed during the training stage, obtaining `Fascia_temp`.
- For each feature the median value is compared to m_1, M, m_2 in order to assign it one of the following strings $\{1011, 1111, 0111, 0101\}$ obtaining the vector B.

  The same process is applied to each of the five feature vectors, obtaining the vectors b_1, b_2, b_3, b_4, b_5

Enrollment


Adaptive Code Selection
Adaptive RS code selection
Acquisition Sensors
Feature extraction
Bit string quantization
RS encoder
RNG
SHA
Stored Templates
Fascia_temp
HD1
Hash
HD2

Stored templates

The system saves the following data:

- m_1, M, m_2
- HD_1, the sum between the binarized vector B and the code word obtain for each user s
- HD_2, the correction capability vector
- Hash
- `Fascia_temp`

Stored templates

The system saves the following data:

- m_1, M, m_2
- HD_1, the sum between the binarized vector B and the code word obtain for each user s
- HD_2, the correction capability vector
- Hash
- `Fascia_temp`

Authentication

The authentication process is organized into two steps:

1. Time threshold control
2. Feature analysis

Authentication

The authentication process is organized into two steps:

1. Time threshold control
2. Feature analysis

Time threshold control

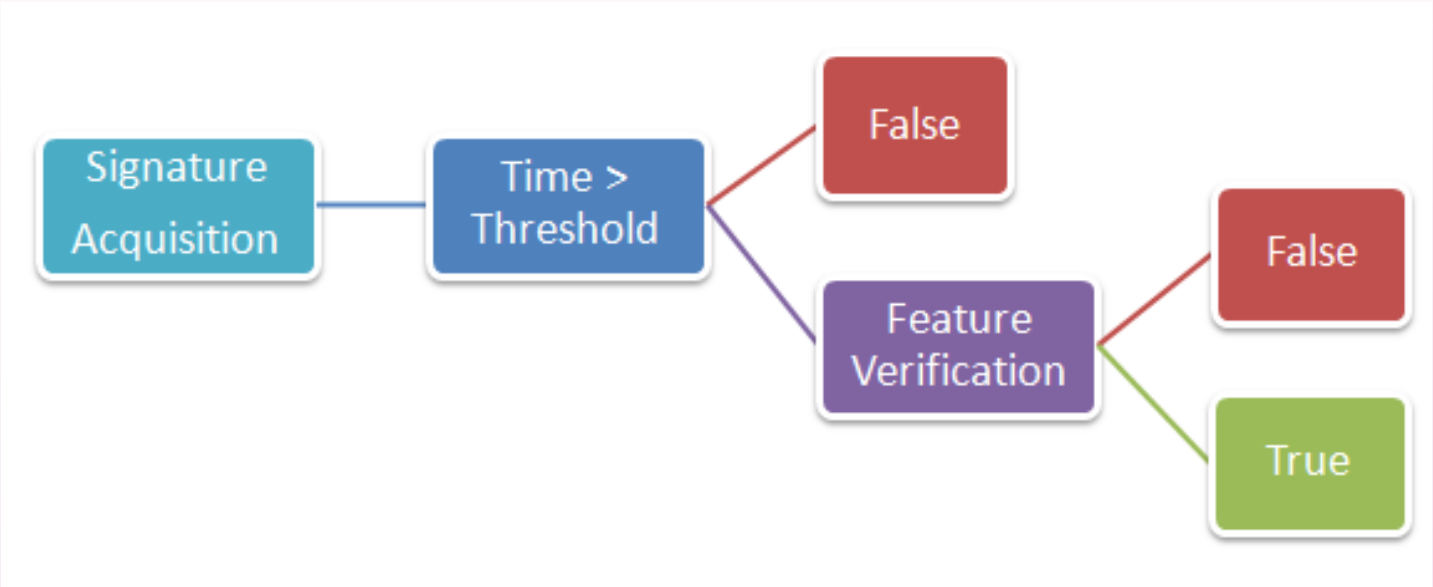
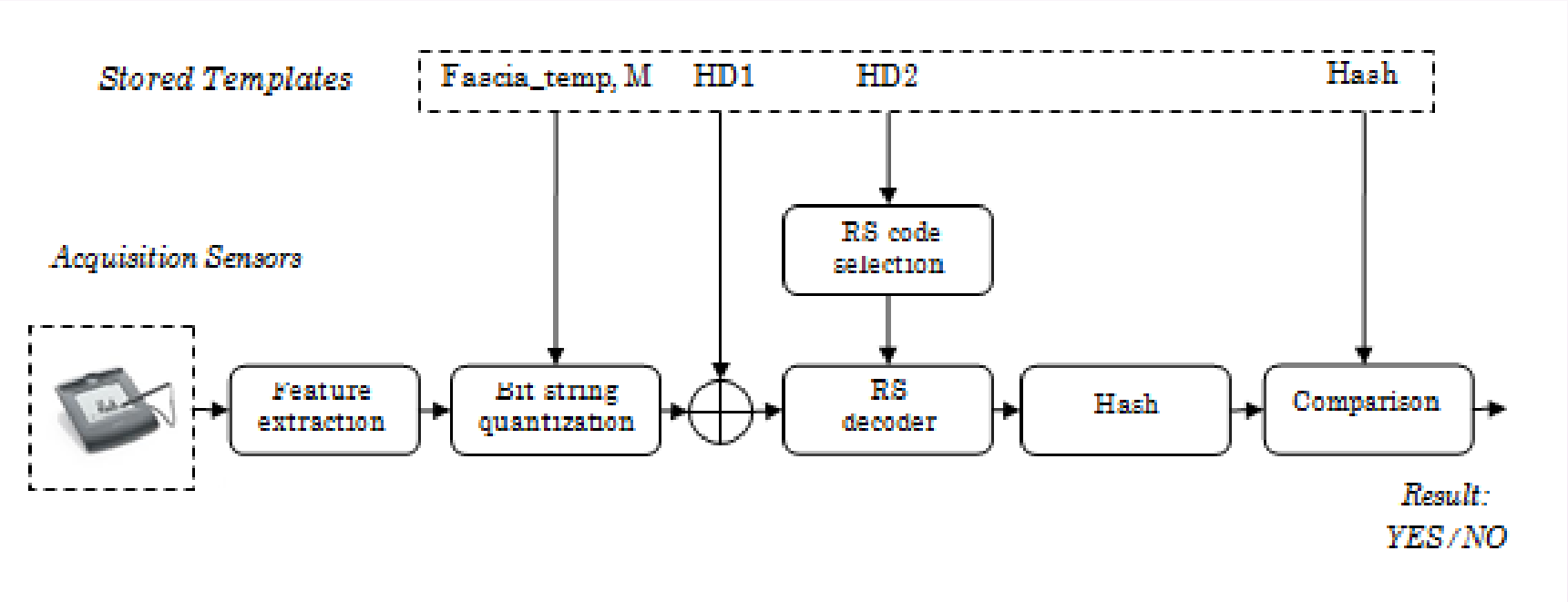


Figure : Scheme representing how the time threshold will be used.

Feature analysis



Performance Evaluation

Evaluating a verification system requires the analysis of two types of errors:

1. **False Acceptance Rate** (**FAR**): rate of incorrectly accepted forgeries
2. **False Rejection Rate** (**FRR**): rate of genuine signatures that are incorrectly rejected by the system

Results

Different choices of *time thresholds* and *code correction capability* lead to different percentages.

Allowing the user to have a *second* signature attempt in case the first one fails to authenticate, the best results achieved with the used database are:

$$\text{FAR} = 1.91\% \qquad \text{FRR} = 6.66\%$$

Results

Different choices of *time thresholds* and *code correction capability* lead to different percentages.

Allowing the user to have a *second* signature attempt in case the first one fails to authenticate, the best results achieved with the used database are:

$$\text{FAR} = 1.91\% \qquad \text{FRR} = 6.66\%$$

Possible improvements

Many modifications are possible that can enhance the performance of the previous algorithm.
For example, one can change

- the extracted set of features;
- the encoding scheme;
- the binarization process

(in order to test your new verification scheme you could need a database containing genuine and forgery signatures).

Thank you for attention!