Introduction to Handwritten Signature Verification

Dave Fenton

University of Ottawa

Handwritten signature verification

Presentation overview (altered to remove all signatures):

- **Goal, applications and assumptions**
- Basic concepts in biometrics
- Experimental setup
- Technical difficulties posed by HSV
- Past research and the current state of the art
- Overview of my research

Goal of HSV

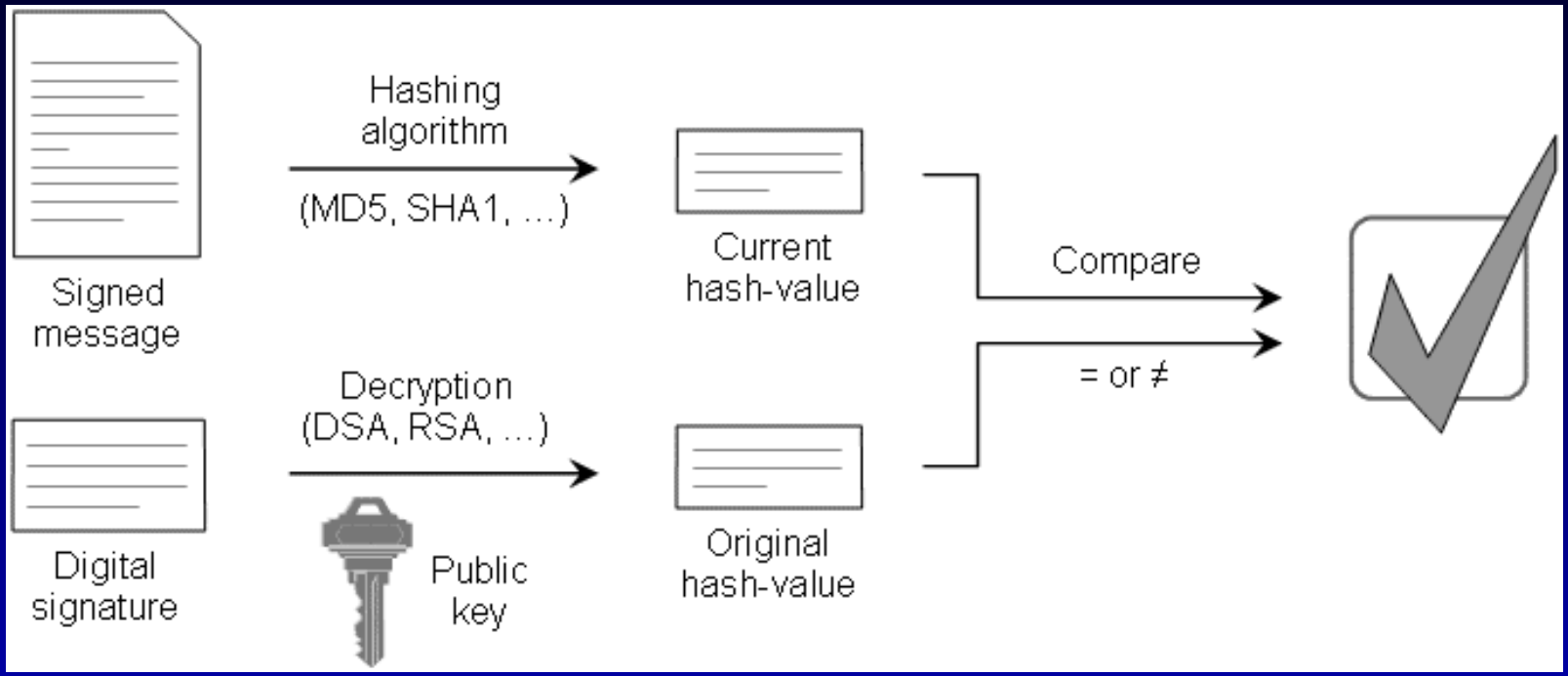
- To verify a person's identity based on the way in which he/she signs his/her name
- Two types of system:
  - Offline systems use static features (the signature image)
  - Online systems use dynamic features (the time series)
- Written passwords are also under consideration

Applications

Principal application: reduce fraud in financial transactions

- Cannot rely on sales staff to visually verify signatures on credit card receipts
- Occasional acceptances of forgeries are allowable
- Rejections of valid signatures may irritate valuable customers
- To date, used mostly for electronic signature of business documents (hash function protects document against alteration)

Document verification



- Apply hash function to document to generate hash code
- If signature is valid, encrypt hash with signer's private key
- Recipient decodes received hash using public key
- If document has been altered, hashes don't match

Applications

Secondary application: access security for buildings or mobile computing devices

- For building security, it would not be tolerable to accept forgeries
- HSV would have to be combined with on-site security staff or other biometric/password/PIN systems
- Already used on some laptops and PDAs

Naïve assumptions

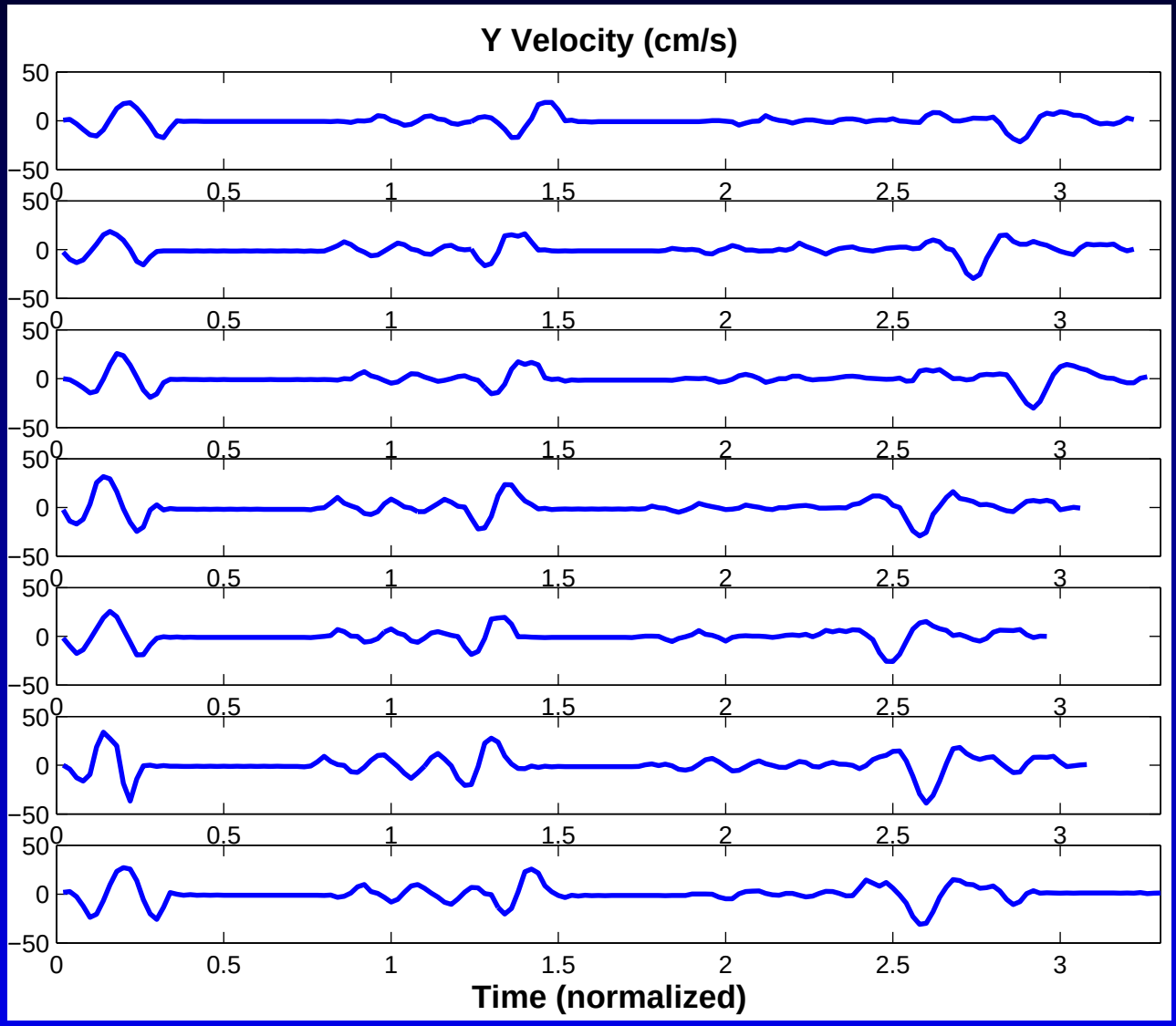
- A person signs his or her name consistently each time
- All signatures contain enough steady features to be reliably verified
- A forger cannot perfectly imitate the dynamic features of a signature
- All a user's passwords can be replaced by his/her signature

Example of consistency – static

Password: “Prejunife”

21 July 2003 2 Sept 2003 24 Sep 2003

Example of consistency – dynamic

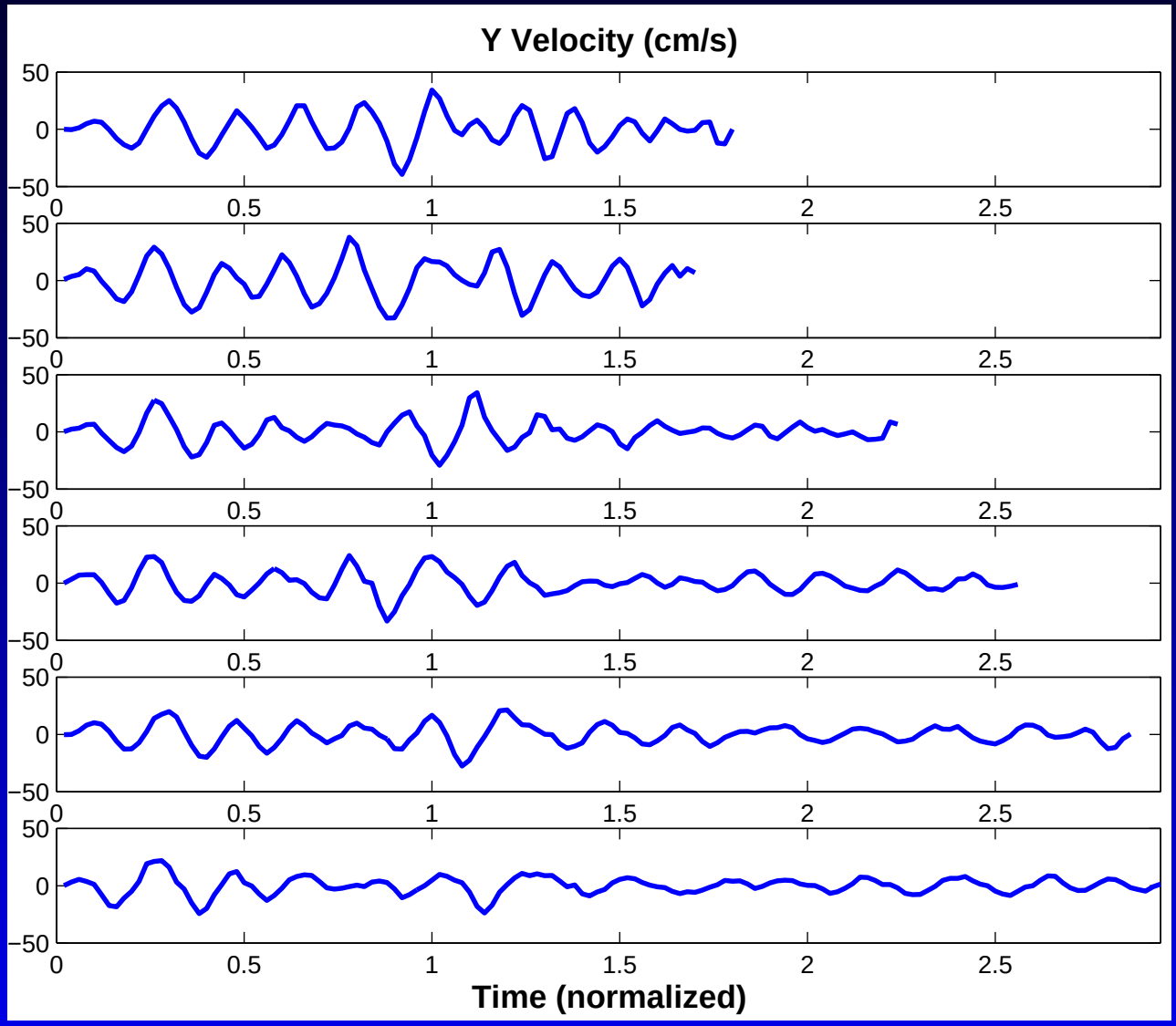


Example of inconsistency – static

Password: “Ingusions”

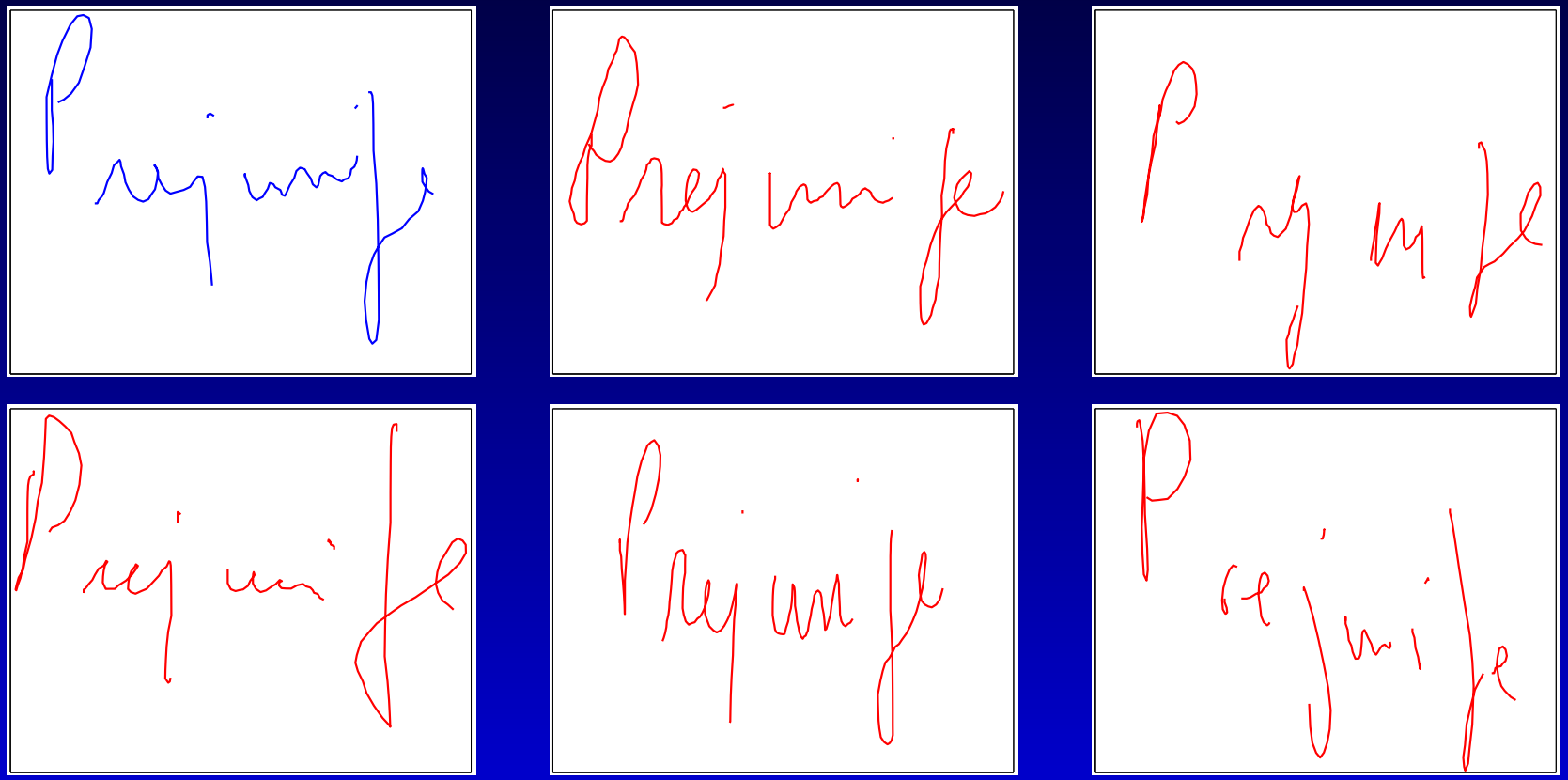
12 Jan 2004 | 18 Mar 2004 | 27 Sep 2004

Example of inconsistency – dynamic

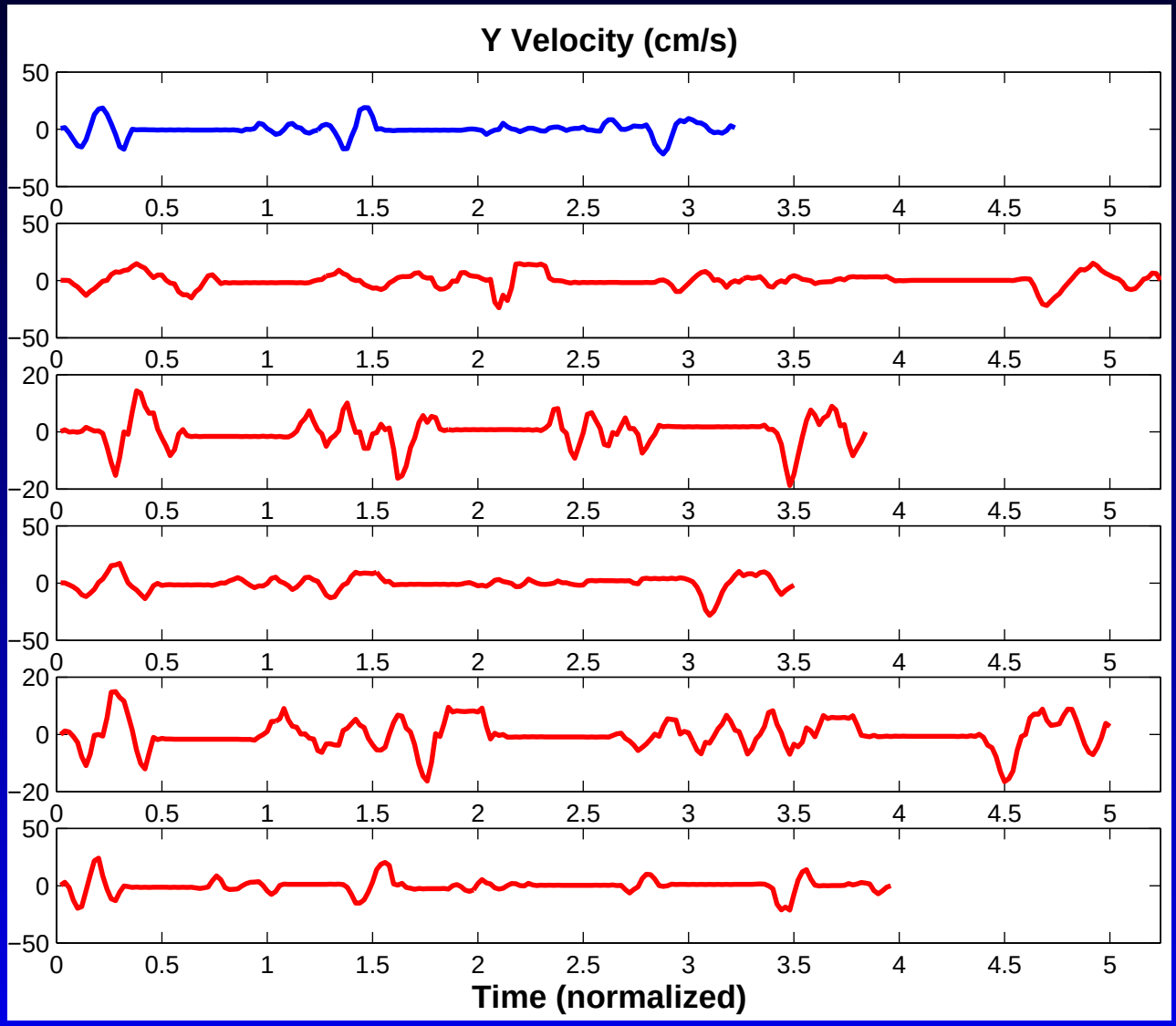


Example of forger ability – static

Password: “Prejunife”



Example of forger ability – dynamic



More realistic assumptions

- Most signers sign their names consistently
- Most signatures contain enough steady features to be reliably verified
- Most forgers cannot reproduce a signature well enough to defeat a good verifier
- It is more difficult to forge both the static and dynamic features of a signature than just the static features

Fallout from broken assumptions

- It may not be possible to verify all signatures reliably
- For any signature, there will probably exist a skilled forger who can forge it competently
- Serious consideration must be given to passwords
  - confidential
  - easily replaced if template compromised
  - can exert some control over the length (quality of features)
  - can *request* the signer to write legibly

Handwritten signature verification

Presentation overview:

- Goal, applications and assumptions
- **Basic concepts in biometrics**
- Experimental setup
- Technical difficulties posed by HSV
- Past research and the current state of the art
- Overview of my research

Basics of biometrics

Physical v. behavioural biometrics:

- A physical biometric makes use of a fixed characteristic of the body (e.g. fingerprints, iris patterns, retina patterns, hand geometry, facial features)
- The most accurate methods are usually perceived as too intrusive.
- A behavioural biometric makes use of personal behaviours which are assumed to be almost invariant (e.g. voice, handwriting, typing, gait)
- Perceived as less intrusive, but less accurate than physical biometrics

Two stages

- 1. *Enrolment*:
  - a user's signature characteristics are learned from a small number of input samples. The resulting information is called the *template*.
  - Typically, 3 – 5 signatures are used
- 2. *Verification* or *recognition*:
  - For verification, a *candidate* signature is compared to the template of a single signer.
  - For recognition, the candidate signature must be compared against many templates.

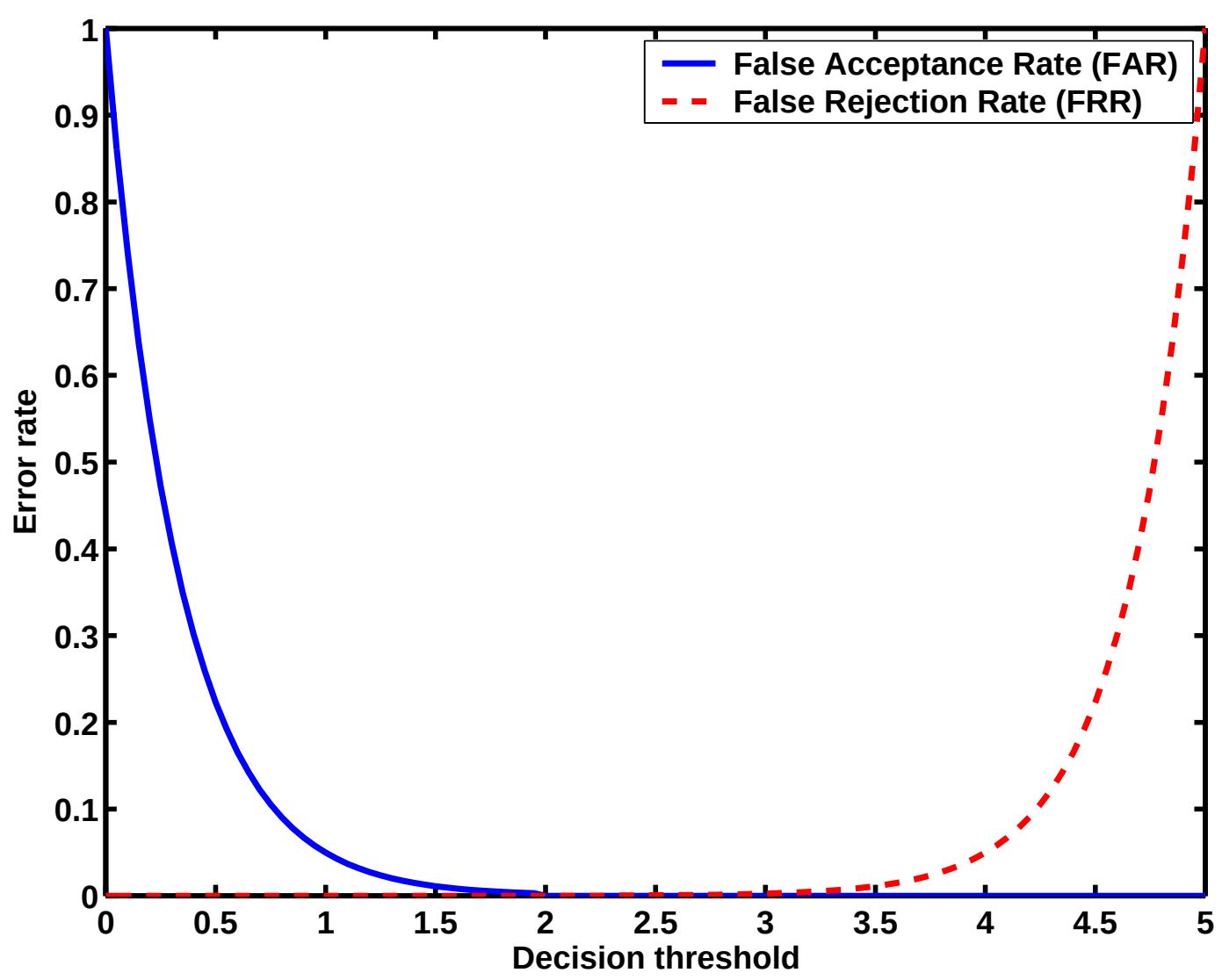
FRR and FAR

- Two error rates are specified:
  - The *False Rejection Rate* (FRR) is the rate at which valid signatures are rejected.
  - The *False Acceptance Rate* (FAR) is the rate at which forged signatures are accepted as valid.
- In many cases, low FRR implies high FAR, and vice-versa
- Current state of the art: FRR and FAR sum to 2 – 5%. Actual numbers may be even worse!

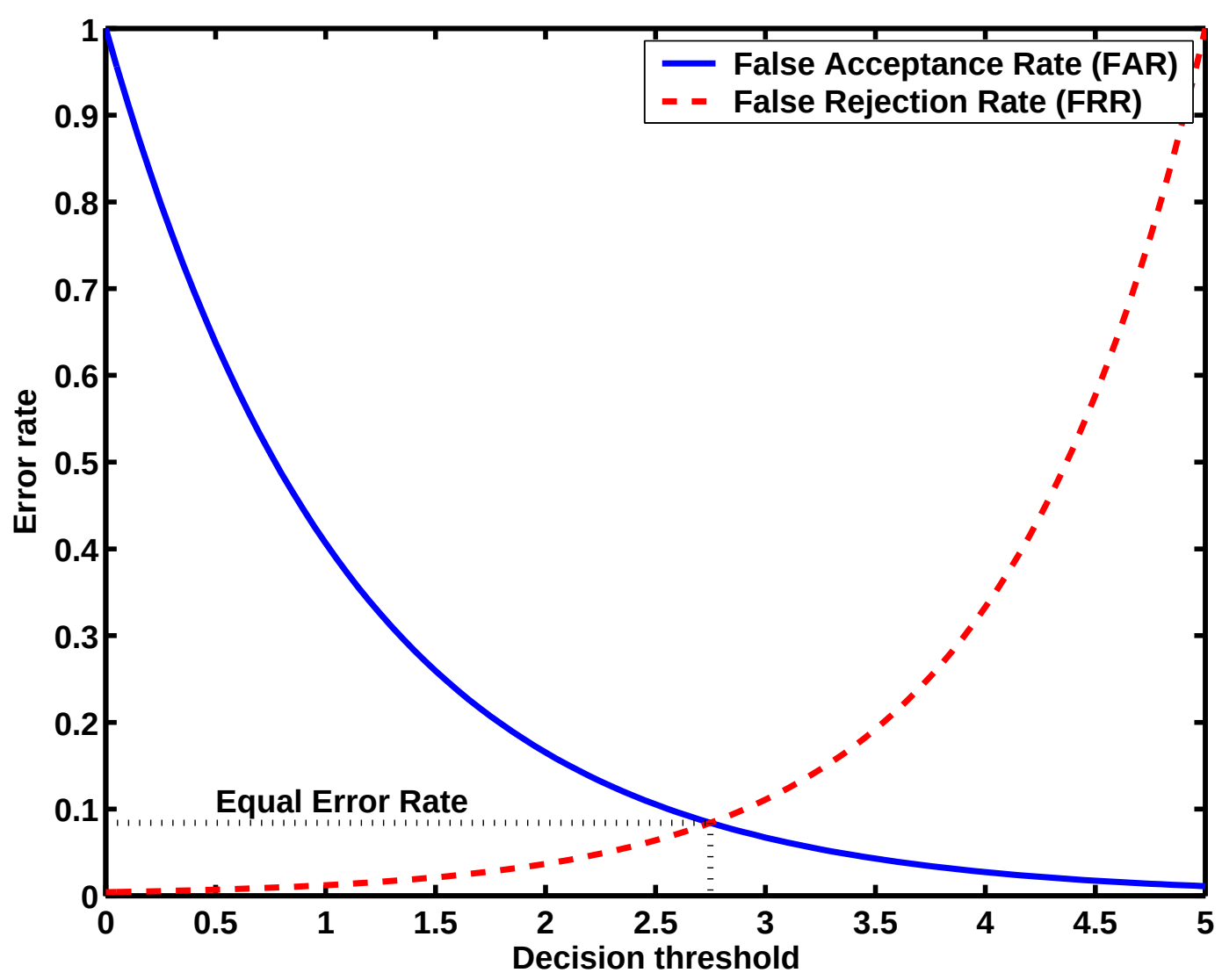
ROC curves

- Most verifiers have a single numerical output. If the output level is above a decision threshold, the signature is accepted as valid, otherwise it is rejected.
- In this case, the FRR and FAR can both be plotted against the decision threshold in a *receiver operating characteristic* (ROC) curve.

Example ROC curves



Example ROC curves

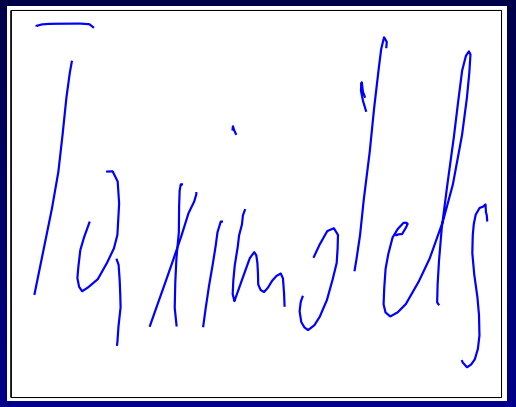


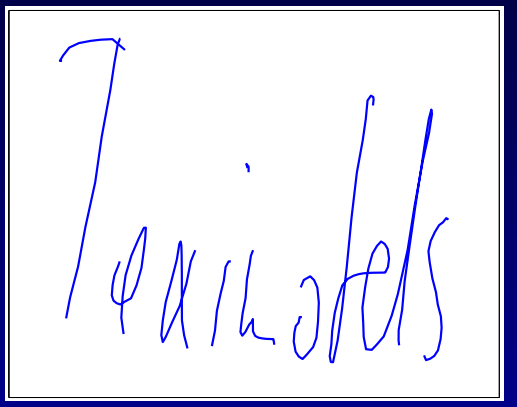
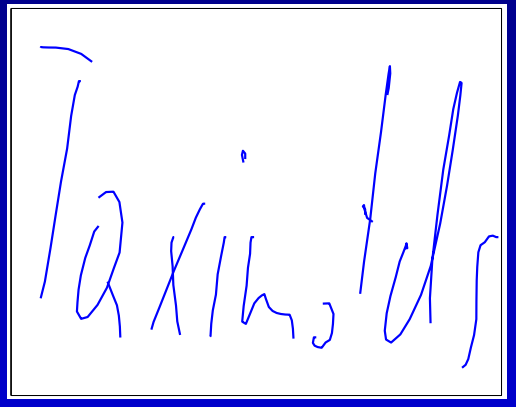
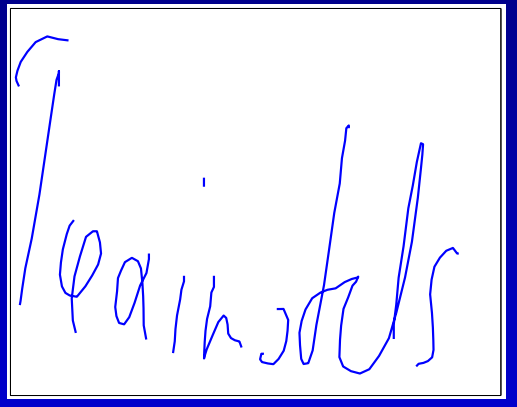
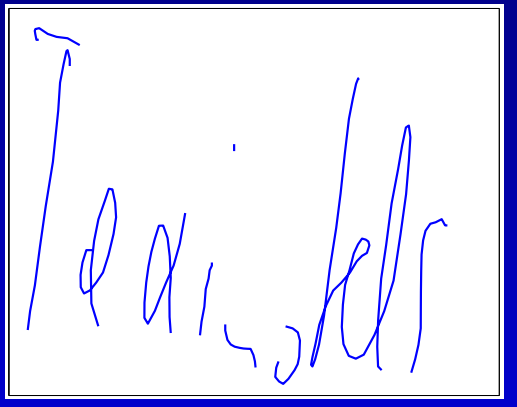
Types of forgery

- *Random*. A random forgery is simply another person's valid signature.
- *Simple*. The forger spells the name correctly, but writes in his own style.
- *Skilled*, or *Knowledgeable*. The forger tries to fully reproduce all the shapes and dynamics of the original signature. In this study, forgers are shown MPEG movies of the original signature.
- The training set consists of a few valid signatures and many random forgeries.
- After training, the verifier is tested against all 3 types of forgery.

Genuine samples

Password: “Taximotels”

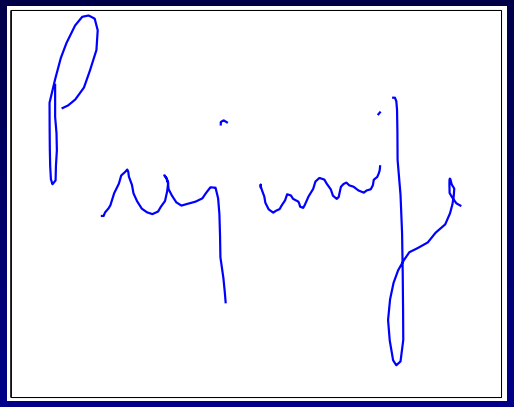


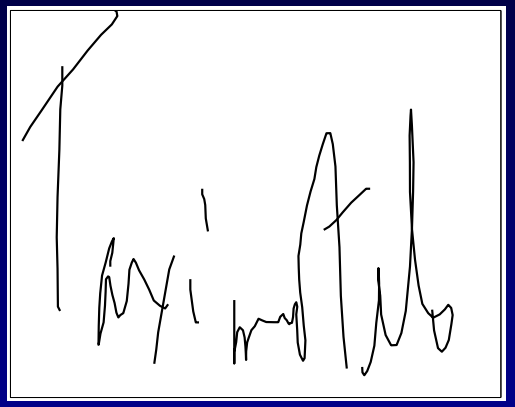





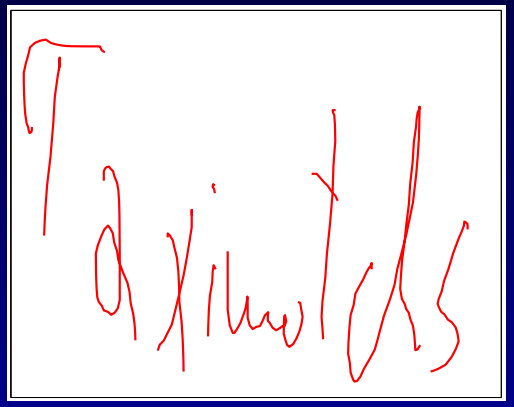
19 Sep 2003 16 Oct 2003 6 Nov 2003

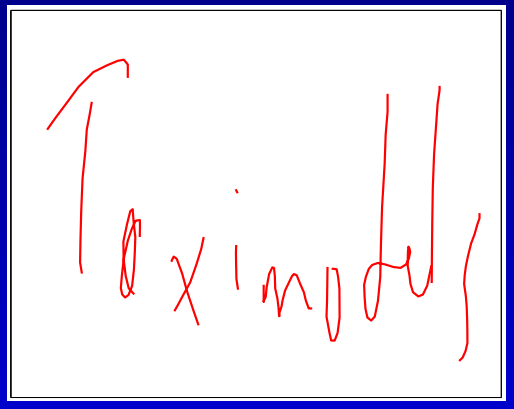
Forgeries

Password: “Taximotels”









Random

Simple

Knowledgeable

Motivations for research

- Despite company claims, error rates are high, and need improvement
- For computing devices with pen inputs (PDAs, tablet PCs), automatic signature verification is a sensible technology
- Signatures are already a widely accepted means of identification

Handwritten signature verification

Presentation overview:

- Goal, applications and assumptions
- Basic concepts in biometrics
- **Experimental setup**
- Technical difficulties posed by HSV
- Past research and the current state of the art
- Overview of my research

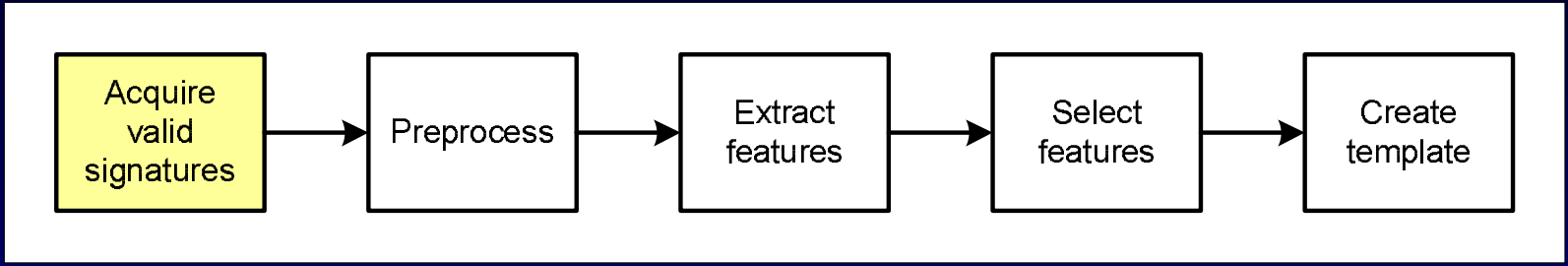
Data collection

- Signatures collected using an Interlink Electronics ePad-ink (100 Hz samp freq)
- Captures X & Y position, pressure, time stamp
- Data collection program written in C++
- Data protected by PGPdisk

Data collection

- Two levels of volunteer:
  - Level 1: one signing session
  - Level 2: three signing sessions
- Each volunteer contributes:
  - 10 samples of genuine signature
  - 10 samples of genuine password
  - Simple forgeries of 2 signatures and 2 passwords
  - Knowledgeable forgeries of a signature and a password

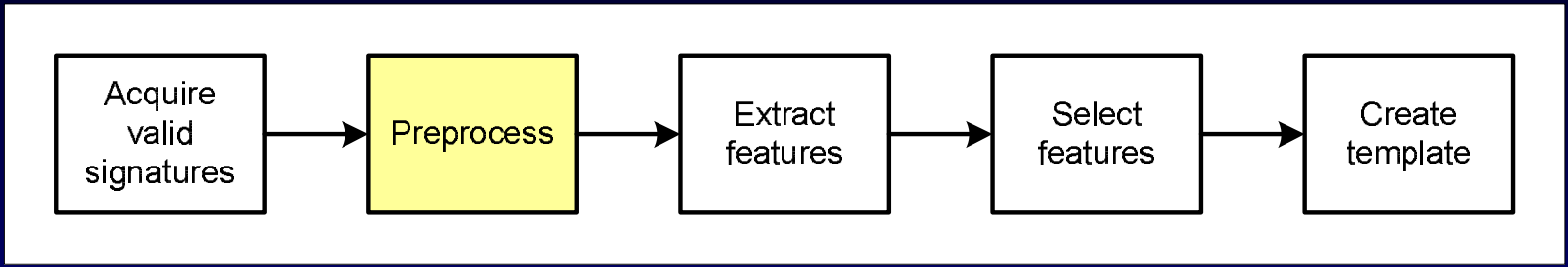
Enrolment



Acquire valid signatures:

- Operational systems typically collect 3 – 5 genuine signatures; academic systems up to 20
- Some use warping and interpolation schemes to "create" extra valid signatures

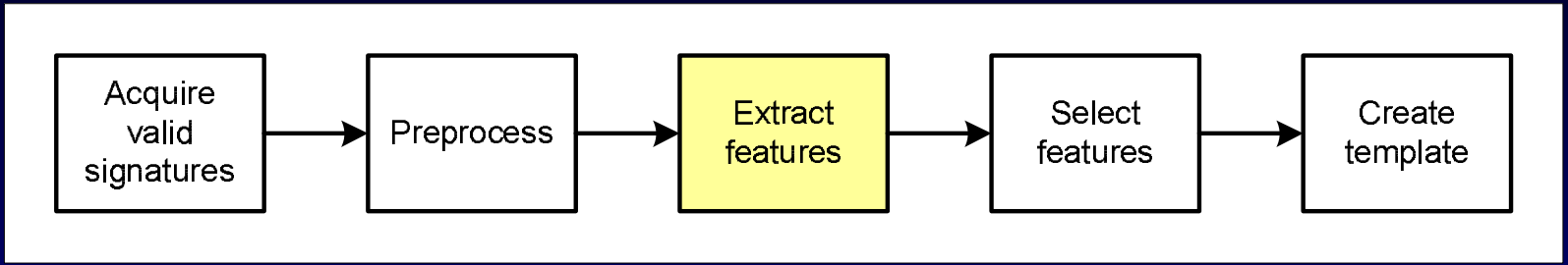
Enrolment



Preprocess:

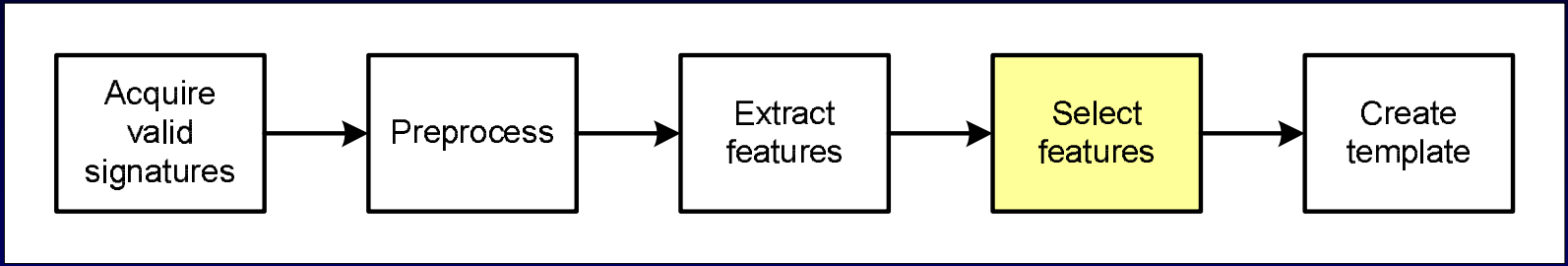
- Concatenate strokes into single time sequence
- Render invariant to:
  - translation: subtract X & Y means
  - rotation: force linear regression line to be horizontal
  - scale: may normalize based on box size or signal power
- Normalization of duration is not carried out at this stage

Enrolment



- May extract hundreds of features. Examples:
  - *Function features*: time series such as velocity or acceleration
  - *Dynamic discrete features*: signing time, number of strokes, pen-down distance, max velocity, mean pressure, time to write longest stroke
  - *Static discrete features*: bounding box, slant

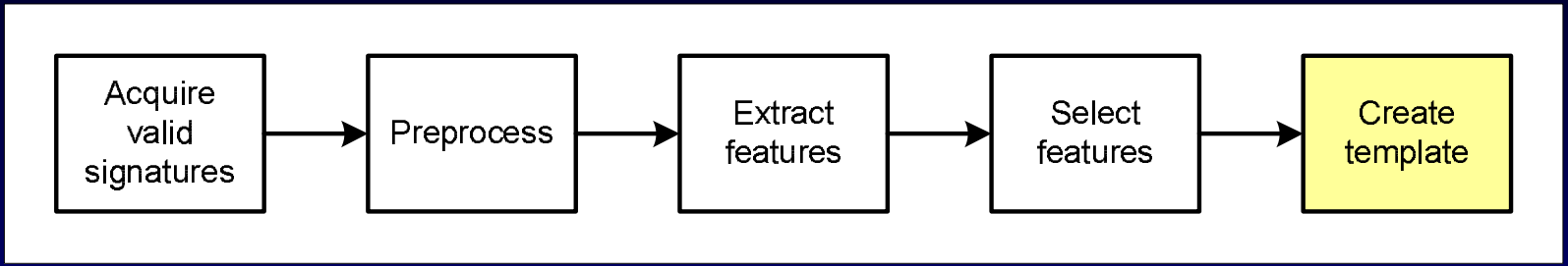
Enrolment



Select features:

- With function features, typically use the same features for each signer
- Not all discrete features are equally informative
- Cost used for feature selection is usually error rate; classifier dependent
- Sequential forward/backward search

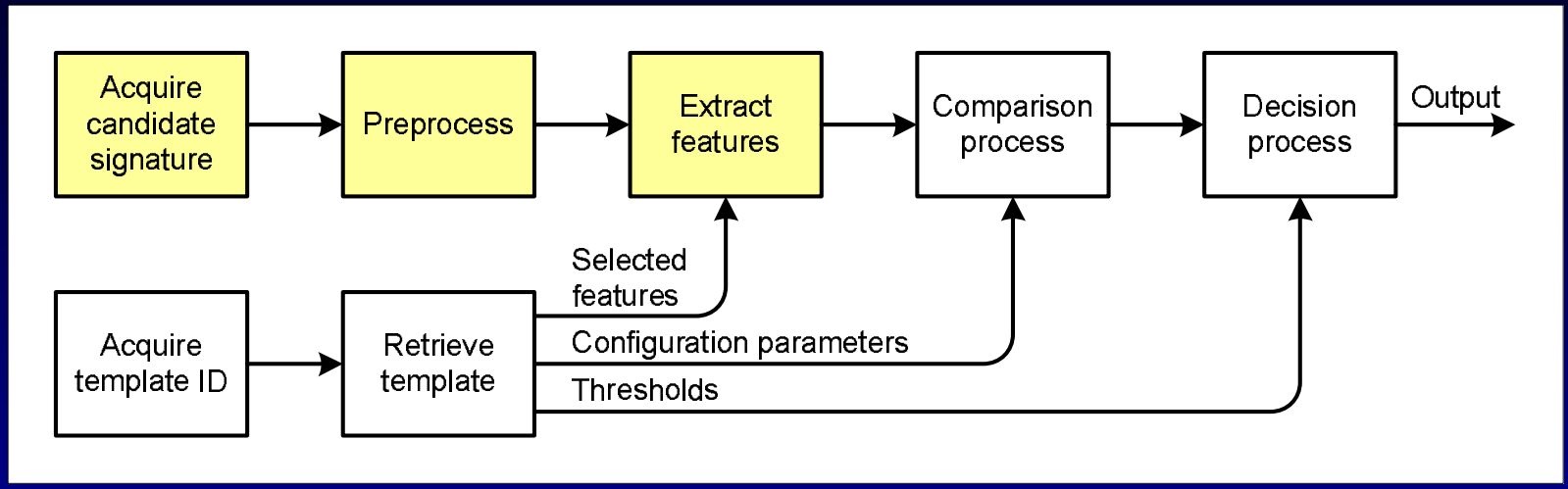
Enrolment



Create template:

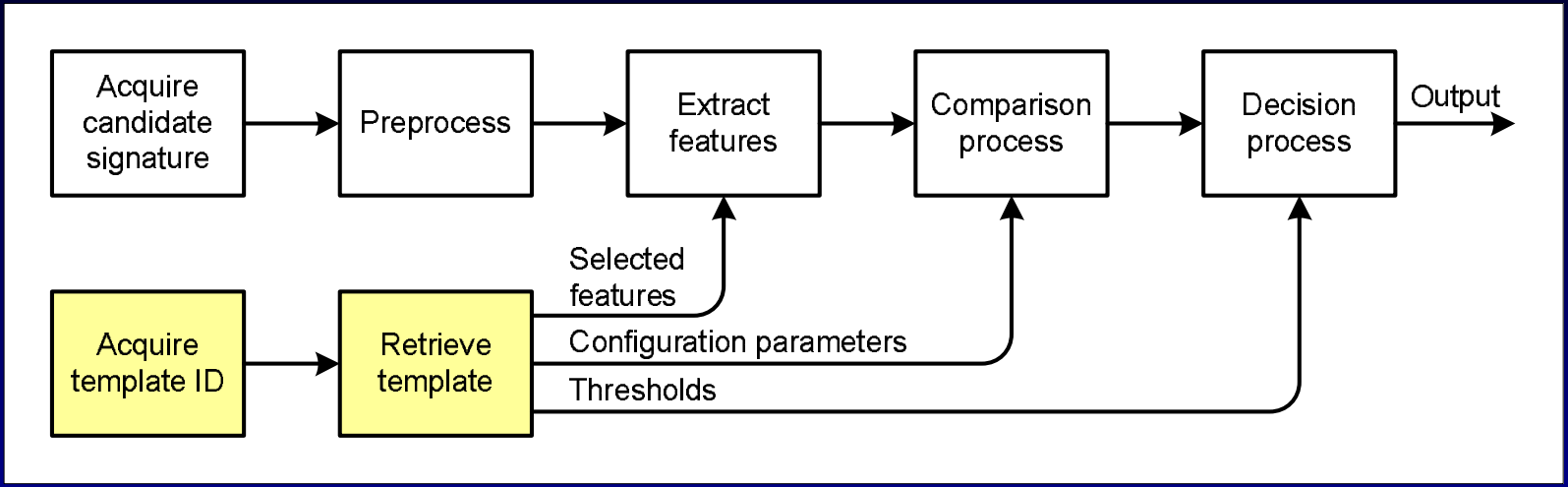
- Best performance so far: keep raw data of multiple signatures
- Bad practice, from security perspective
- Template may also include list of features to keep, best classifier to use, decision thresholds

Verification



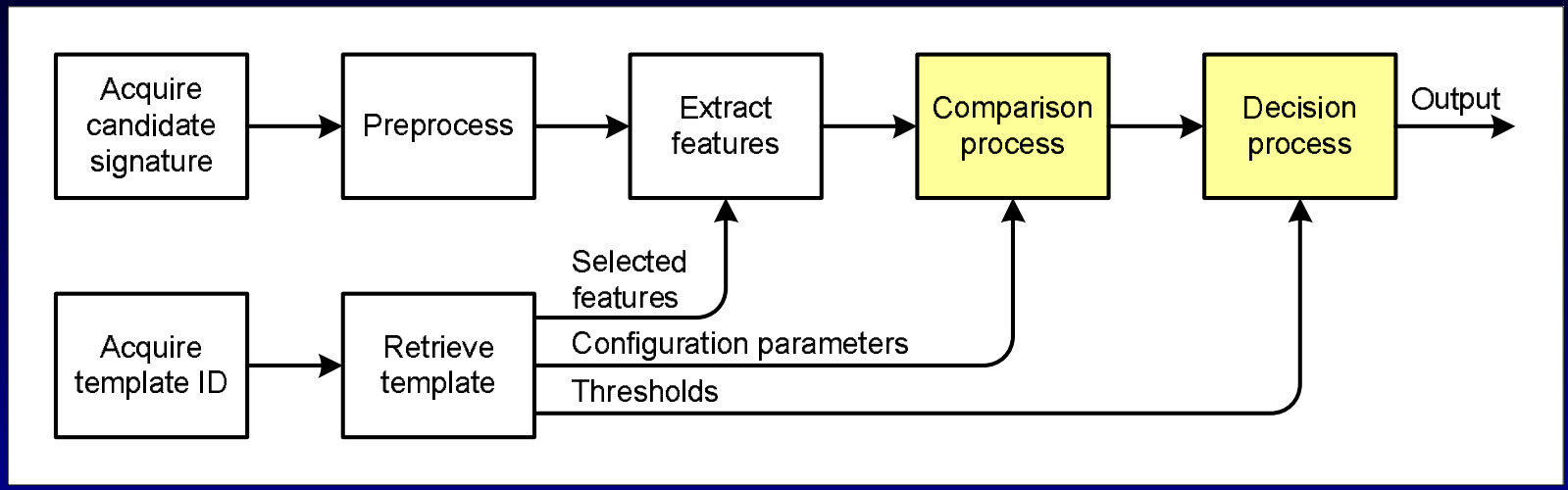
- Initial steps of verification are same as enrolment
- Only selected features need to be extracted

Verification



- Template ID is acquired at same time as candidate signature
- Designated by swipe card, PIN number, etc.
- Template is usually stored in central database, but may also be held on swipe card

Verification



- Many different classifiers have been tried
- May have to combine results from multiple classifiers
- Will be covered in more detail later

Handwritten signature verification

Presentation overview:

- Goal, applications and assumptions
- Basic concepts in biometrics
- Experimental setup
- **Technical difficulties posed by HSV**
- Past research and the current state of the art
- Overview of my research

Technical difficulties

- Physiology of handwriting is not well understood
- Signers not motivated to sign in a careful, invariant manner
- Training sets are sparse and badly imbalanced (few valid signatures)
- No knowledgeable forgeries available for training
- Short, variable signatures often easily forged

Technical difficulties

- No standard database of signatures and forgeries:
  - every researcher uses a different set of amateur forgeries
  - some researchers test only against random forgeries
  - FAR is ill-defined; a low error rate may reflect the forgers' lack of skill rather than the verifier's ability

Technical work-arounds

- Disqualify certain signers during enrolment
- Allow multiple signing attempts
- Allow probationary period with relaxed acceptance criteria (collect more training signatures)
- Use passwords with a certain minimum length

Handwritten signature verification

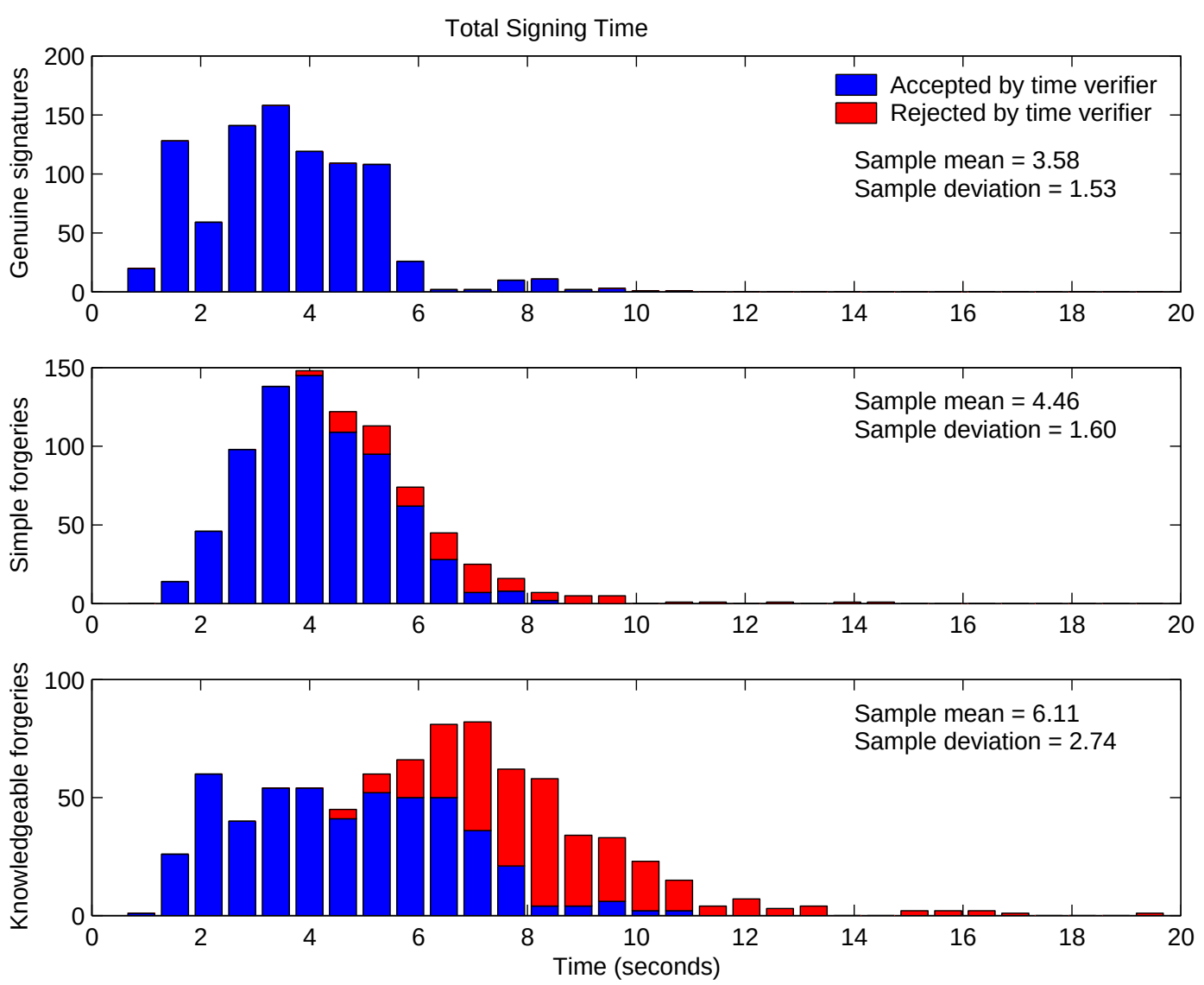
Presentation overview:

- Goal, applications and assumptions
- Basic concepts in biometrics
- Experimental setup
- Technical difficulties posed by HSV
- **Past research and the current state of the art**
- Overview of my research

Past research

- Research has been underway for several decades. Peak activity in mid-1980s to mid-1990s.
- Early ideas are still good performers because they have fewer control parameters
- Between 30 – 60% of forgeries can be detected by a basic time verifier

Time verifier



Classifiers

- Euclidean distance
- weighted linear metrics
- regional correlation
- dynamic time warping (DTW)
- neural networks
- hidden Markov models (HMMs)
- Bayesian belief net

Features used

- Function features (usually position, velocity and pressure)
- Vectors of discrete features
- Features calculated within sliding window (e.g. centre of mass, torque)
- Wavelet coefficients
- LPC coefficients
- Walsh transform of pen-up/pen-down signal
- Pre-defined strokes (HMMs)

Classifier issues

- Time alignment is important if using function features
- With few enrolment signatures, statistical estimates are unreliable
- Lack of training data is a severe problem for learning machines
- Data imbalance is also problematic

State of the art

- In academic studies, more complicated verifiers often achieve better results than simple verifiers
- However, in field use, simple verifiers like DTW often outperform everything else:
  - few adjustable parameters
  - with normalization, can set a single decision threshold for all signers
- Best verifier in public contest: DTW with 5-signature template

State of the art

- Most sophisticated verifier: Plamondon's Sign@metric solution
  - discrete parametric verifier
  - physiological delta-lognormal verifier
  - static feature verifier
  - claimed performance: error rate of 0.0003% among 86,500 people!!
- Other companies that did not take part in public contest: CIC, Cyber-SIGN, SoftPro, Wondernet

Handwritten signature verification

Presentation overview:

- Goal, applications and assumptions
- Basic concepts in biometrics
- Experimental setup
- Technical difficulties posed by HSV
- Past research and the current state of the art
- **Overview of my research**

My research

- Classifier comparison (DTW, NN, SVM, weighted distance metric)
- Techniques to mitigate imbalance of training data
- Re-open debate on the use of passwords
- Data analysis across signing sessions
- Feature selection algorithm that gives preferential treatment to features that are most likely to be stable
- Use of support vector machine

Questions?

To volunteer: please e-mail *d.fenton@ieee.org*