



Biometrics in the Real World

Dr. Paul A. Watters

Division of Information and
Communication Sciences



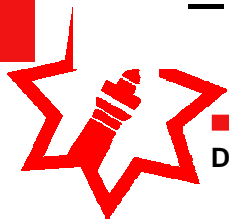
Overview

- The problem of proving identity
 - In real-world applications ...
 - Using physiological and behavioural characteristics ...
- Two different requirements
 - Are enrolled and target the same? (validation)
 - What is the identity of the target(s)? (verification)
 - Which one is best for different applications?
- Where are we at?
 - Going beyond the “how” to “what, when, where, why”
- Biometrics research at Macquarie



Proving Identity

- Modern living relies more on proof of identity
 - Driving a car: Driver's License
 - Travelling overseas: Passport
 - Bank account: Driver's License + Passport
 - Law enforcement: Identifying criminals and terrorists
- Identity is currently very hard to prove
 - Birth certificate doesn't contain any verifiable proof of identity, such as DNA extract
 - How to enrol reliably? What about "legacy" subjects?
 - Policies unlikely to change due to privacy concerns
 - How to protect integrity of this data?
 - How to store it securely?



Identification: Four Types

- Validation: Is this the same person that enrolled?
 - Not necessary to “prove” identity
- Verification (1-1): Is this person who they say they are?
- Verification (1-many): Is this person a member of a known group?
- Verification (many-many): Does anyone in this set of people belong to any of these groups?
- Which of these feasible in real-time?
 - What applications only require validation versus verification?



Authentication

- Verifying identity at point of access
 - 1st factor: Something you know (password)
 - 2nd factor: Something you have (certificate/SecurID)
 - 3rd factor: Something you are (biometric identifier)
- Problems...
 - You can forget your password (and/or it can be guessed or copied if reused)
 - You can lose your certificate/SecurID (and/or it can be stolen)
 - But you **shouldn't** be able to deny your identity...
 - The 3rd factor facilitates non-repudiation
 - Guessability eliminated – all biometrics equally secure



Data Problems

- Biometric matching uses templates
 - Gathered from subject during enrolment; stored in a database
 - Database record can be tampered with
 - Data can be stolen by Trojan horse
 - Biometric data can be “lifted” from physical environment
 - Data can be fabricated
 - How can data be revoked?

Possibilities for Fraud

Making an Artificial Finger **directly from** a Live Finger

How to make a gummy finger



Pour the liquid into the mold.



Put it into a refrigerator to cool.



The gummy finger

It takes around 10 minutes.

Source: Tsutomu Matsumoto



Biometric Identifiers

- The main biometric identifiers
 - DNA (unique; unchanging; very difficult to obtain)
 - Iris (unique; unchanging; somewhat difficult to obtain)
 - Fingerprints (unique; unchanging; difficult to obtain)
 - Face (variable uniqueness; changing; easy to obtain)
 - Physiological characteristics vs behavioural traits
 - Data content of a fingerprint vs pressure on a pad
 - Effective combination?

An Example: Face Recognition

- Face recognition
 - DNA/iris/fingerprint all require subject co-operation/contact
 - Subjects may not even know they are being identified
 - Many commercially available systems
- Applications
 - Finding missing children in a shopping mall
 - Identifying criminals/terrorists “in the act”

Face Identification

- How do we know whether a natural scene contains a face?
 - Essential if enrolment and testing locations are different (resolution, lighting, camera angle etc)
 - Required for real-time scanning (e.g., security systems)
 - Current approaches are slow for even small images
 - Colour Histogram Approach: 9s for 256x384
 - Support Vector Machine: 8s for 1280x1024

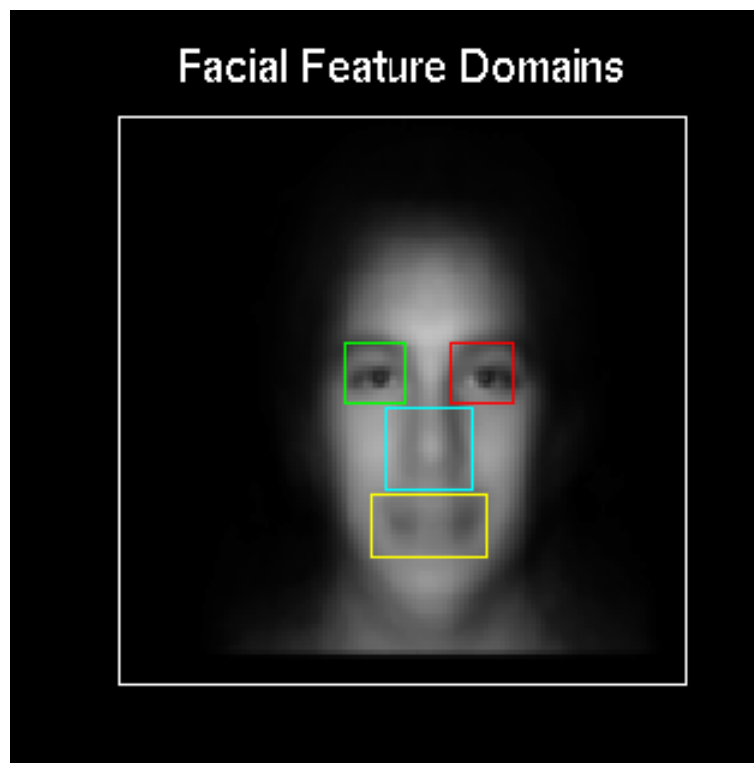


Feature Extraction

- Once you've found a face
 - Identify local features of interest in the face, e.g., eyes, nose, etc
 - Create template through data reduction
 - Matching score generated from target template compared to enrolled template (or set of all templates...)
 - Does matching score exceed threshold? (Validation)
 - Which enrolled template has the greatest match for the target? (Verification)
 - NB: More distinctive faces are more likely to be correctly recognised than someone with “average” features



Local Features



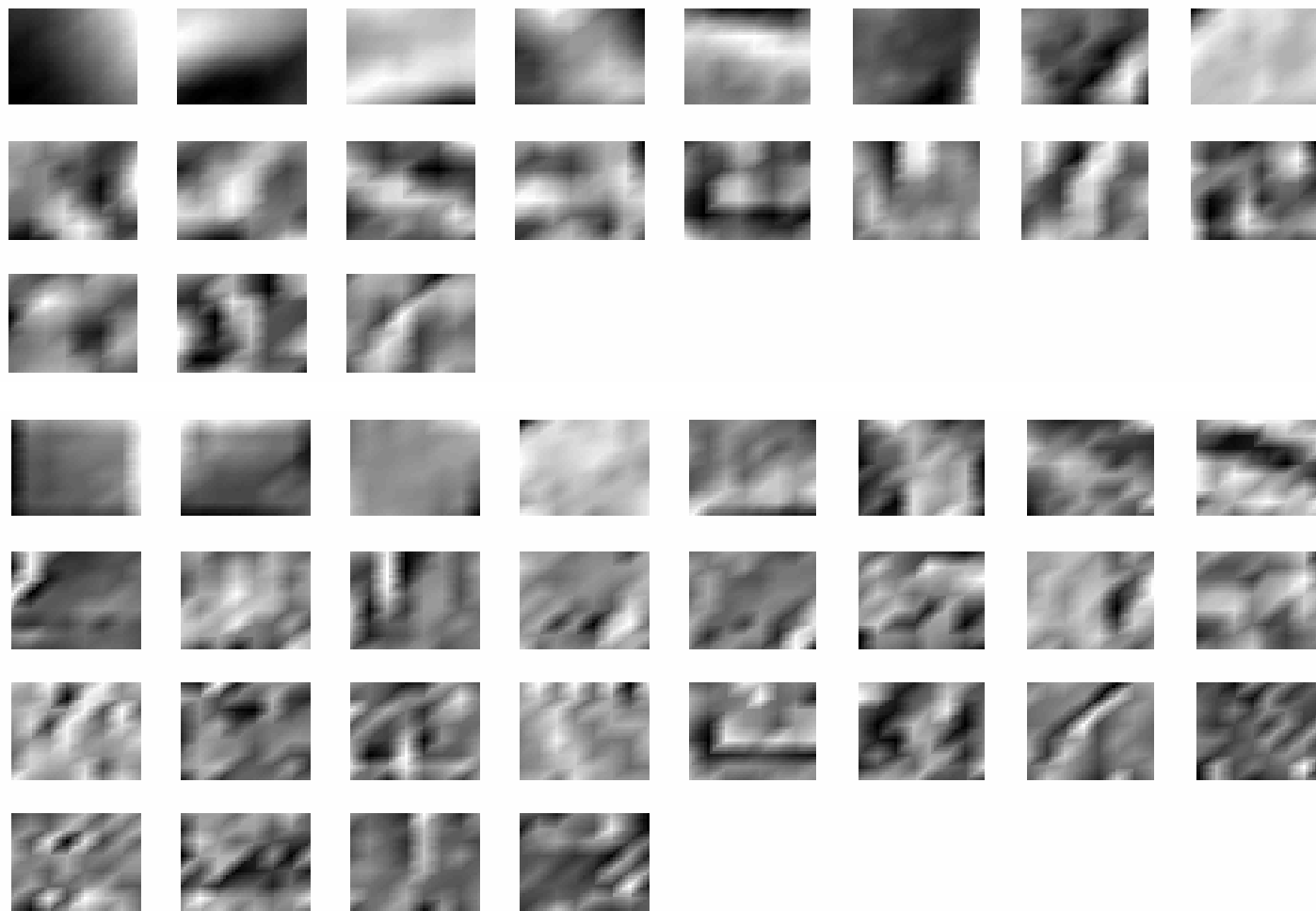
Source: MIT Photobook/Eigenfaces Demo



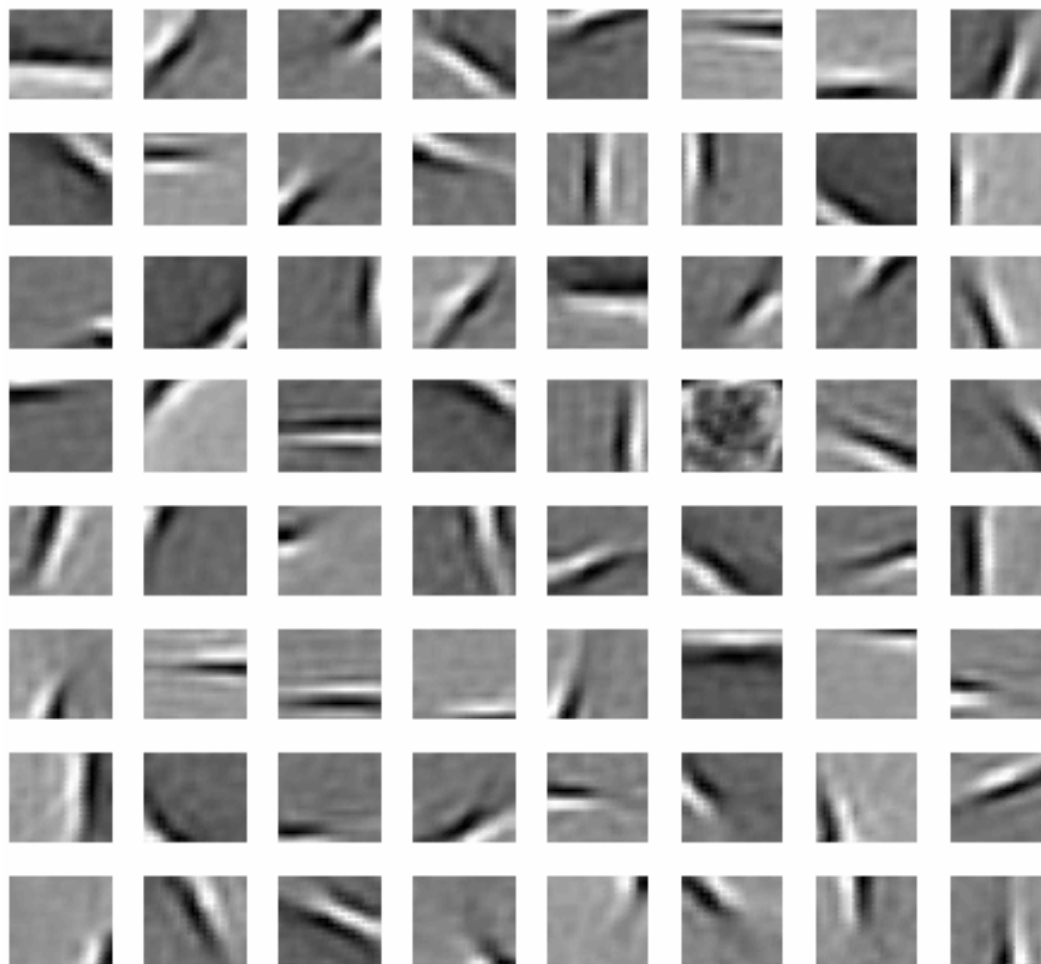
Physiologically Plausible?

- PCA is not the favoured model of feature extraction in the primary visual cortex
 - Current “sparse coding” models are non-orthogonal (Olshausen & Field, 1996)
 - Best results achieved by filtering input data (lateral geniculate nucleus = whitening filter)
 - E.g., whitening local face segments produces a more even apportionment of variance between principal components
 - Greater potential for distinctiveness

Orthogonal Models

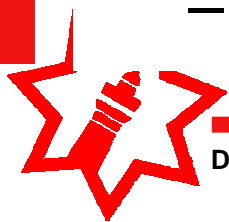


Non-Orthogonal Models



Problems with Face Recognition

- Systems that work well in the lab may fail in the real world
 - Reliable feature extraction relies on environmental control
- Systems that work well on small data sets don't scale
 - Especially for verification, where thousands/millions of subjects are enrolled
- Biometric authentication not well integrated into existing authentication infrastructure
 - Where does it fit in the PKI?



Real World Requires 3 Factors

- CIO Today report
 - Gartner (2005) claim that 2.5 million Internet banking users have lost money in phishing attacks
 - US Federal regulators looking at biometric standards for Internet banking
 - UK standards available for biometric data format (BS ISO/IEC 19794)
 - What about standards for biometric authentication services?



Biometrics Research at Macquarie

- How to find facial features in a natural scene?
- Can classifiers tolerate ageing?
 - Biometric passport – 10 year lifetime
- Designing secure protocols and data formats for biometric authentication into the enterprise
- Developing demonstrators (e.g., Internet banking)



Finding the Eyes

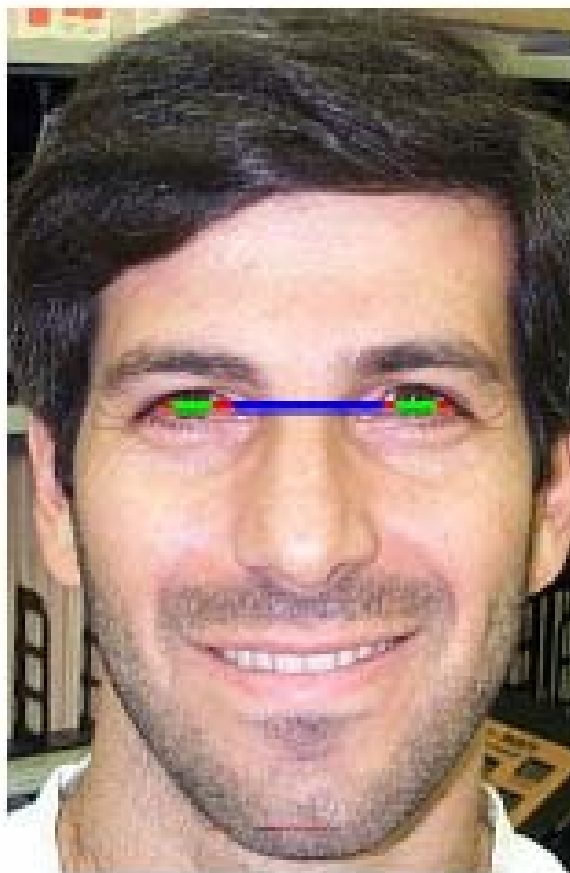
- Attempt to identify a sequence of colours (“colour contour”) that is unique to the face
 - The sequence is a horizontal line of pixel values that crosses the middle of both eyes
 - Regions marked using sclera colours, iris/pupil, and skin
 - Ideally, contour should be unique to faces (but isn’t always!)
 - Size/consistency of contours can eliminate false positives

Finding the Eyes

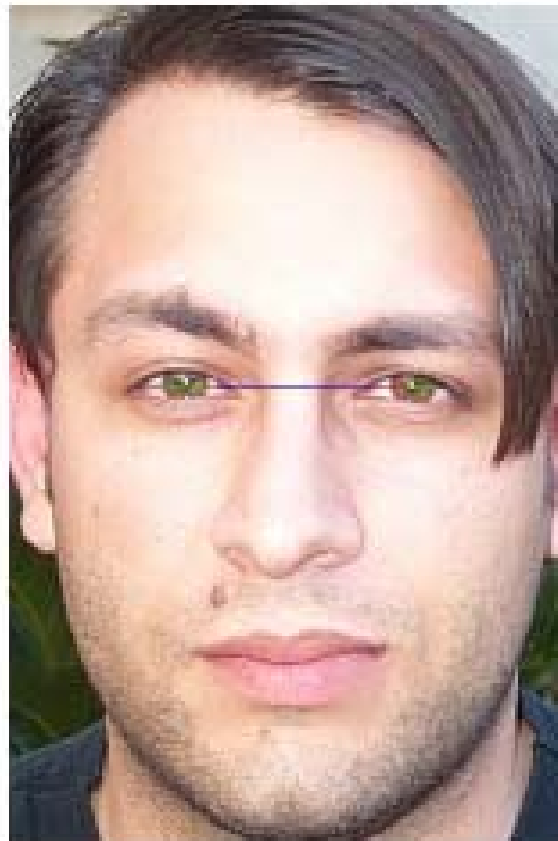
- Our technique is very fast
 - 1280x1024 pixel face detected in ~2s using a Java application on Athlon 2.6GHz (faster using C)
 - Each pixel row is scanned (could double performance by scanning every 2nd row)
 - The area with the greatest number of matches contains the eyes



Multiple Row detection



Single Row Detection



Issues

- Limited ability to tolerate rotation
 - Could rotate X, Y if no match found (e.g., head tilted)
 - Faces must be fairly close to the camera (not in the distance)
 - Must be facing the camera
 - Some eyes are harder to detect than others
 - Wide and tall eyes, consistent skin colour, lots of sclera, is best



Rotation



Difficult Faces



Biometric/Cryptographic Integration

- Possibilities
 - Generating a key from a biometric template
 - Can be revoked and reissued
 - Multiple keys can be generated from the same template
 - BUT how to deal with the variability of biometric data since cryptography requires certainty?

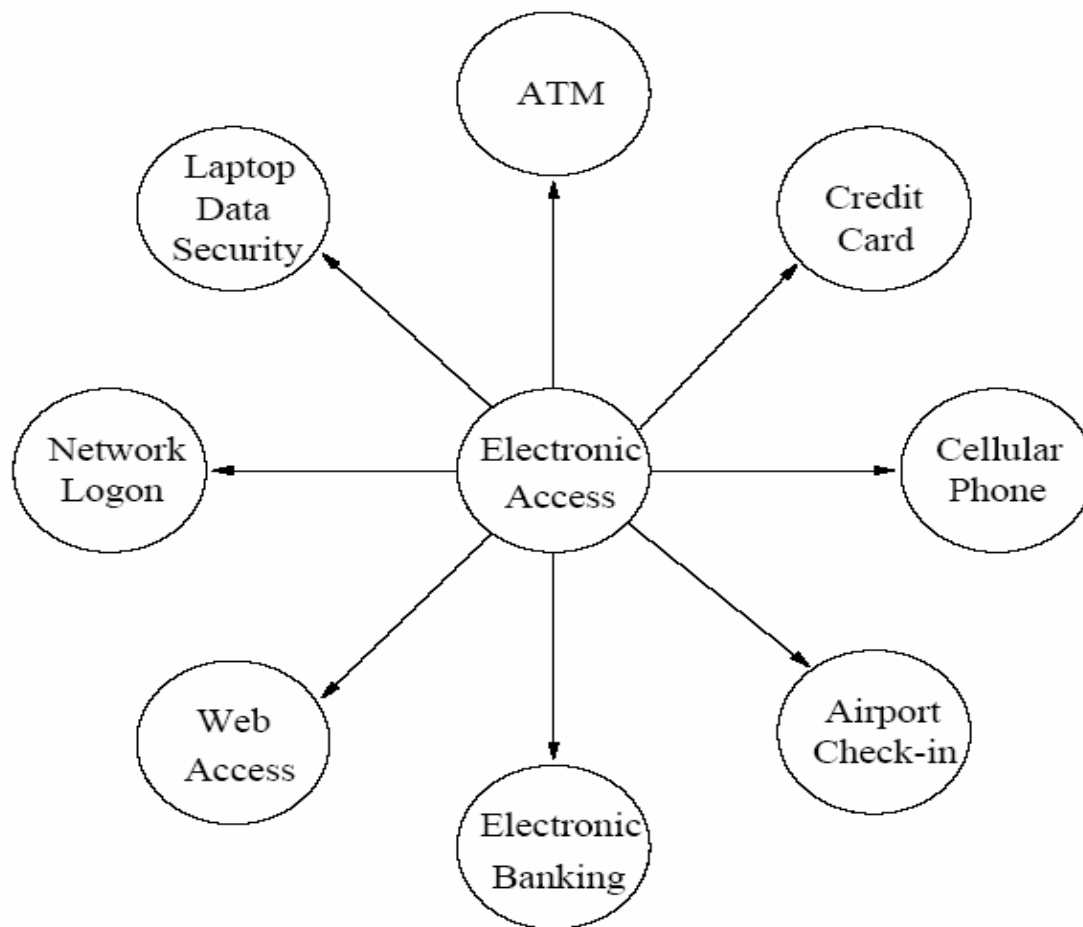
Are Biometric Systems Ready?



- Certainly in Korea...
 - Korean discount store LG Mart has begun using a fingerprint payment system to remove the need for customers to use credit cards in the settlement process
 - Woori Bank deploys fingerprint biometrics at ATMs and 15,000 Internet banking users
- Also at high levels in the US financial markets
 - United Bankers Bank (representing 1,200 community banks) uses fingerprint authentication (http://www.digitalpersona.com/news/clippdfs/0904_DigitalID.pdf)



Real World Applications



Demonstrator



- Scenario: Future Internet banking system that uses biometric authentication
 - Application uses XML Web Services
 - Broker provides fingerprint recognition and authentication services, also using XML Web Services
- XML
 - Provides platform-independent data formatting standards
- Web Services
 - Provides platform-independent service invocation standards using XML
 - Distributed, cross-platform authentication service



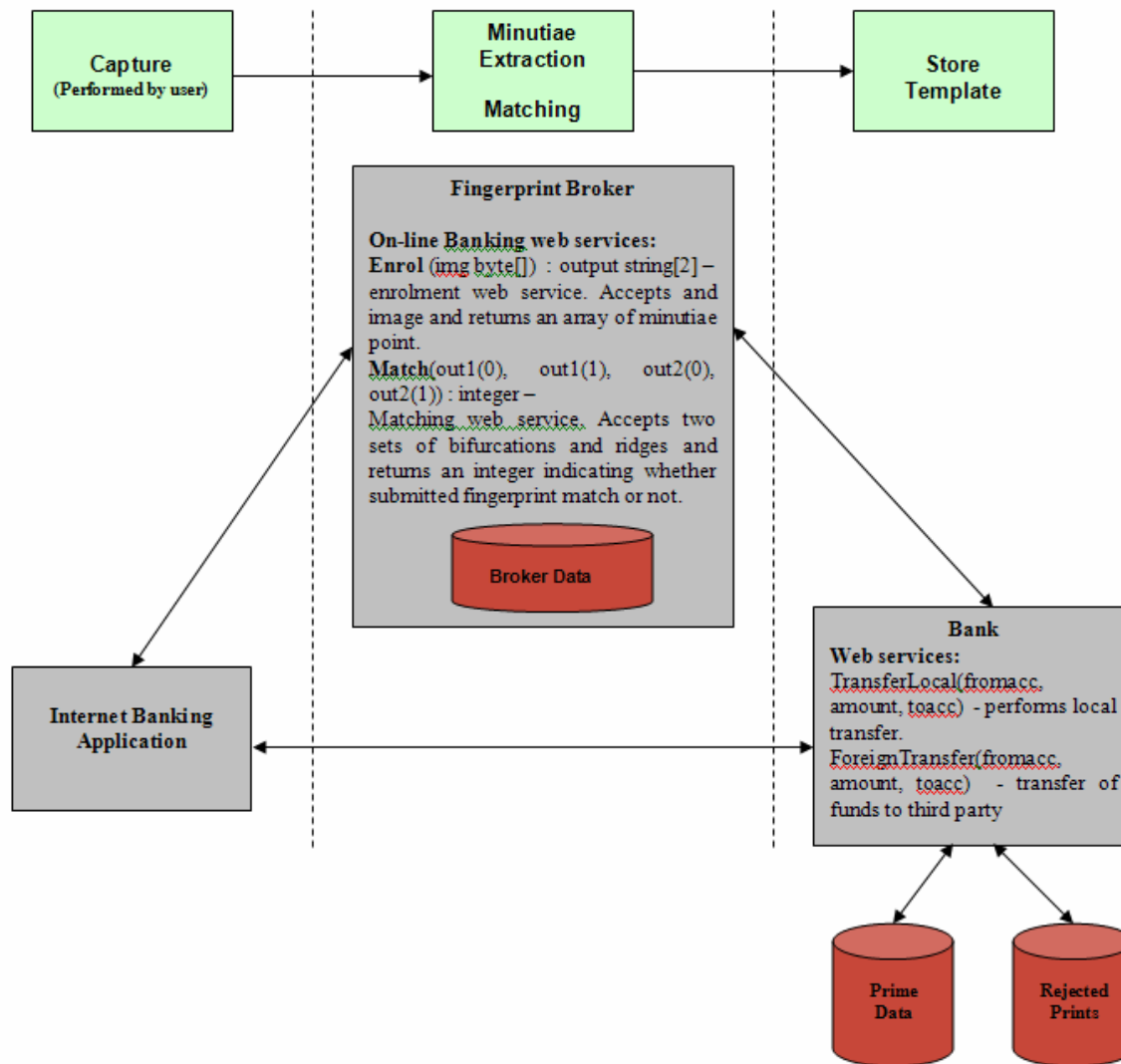
Authentication Broker

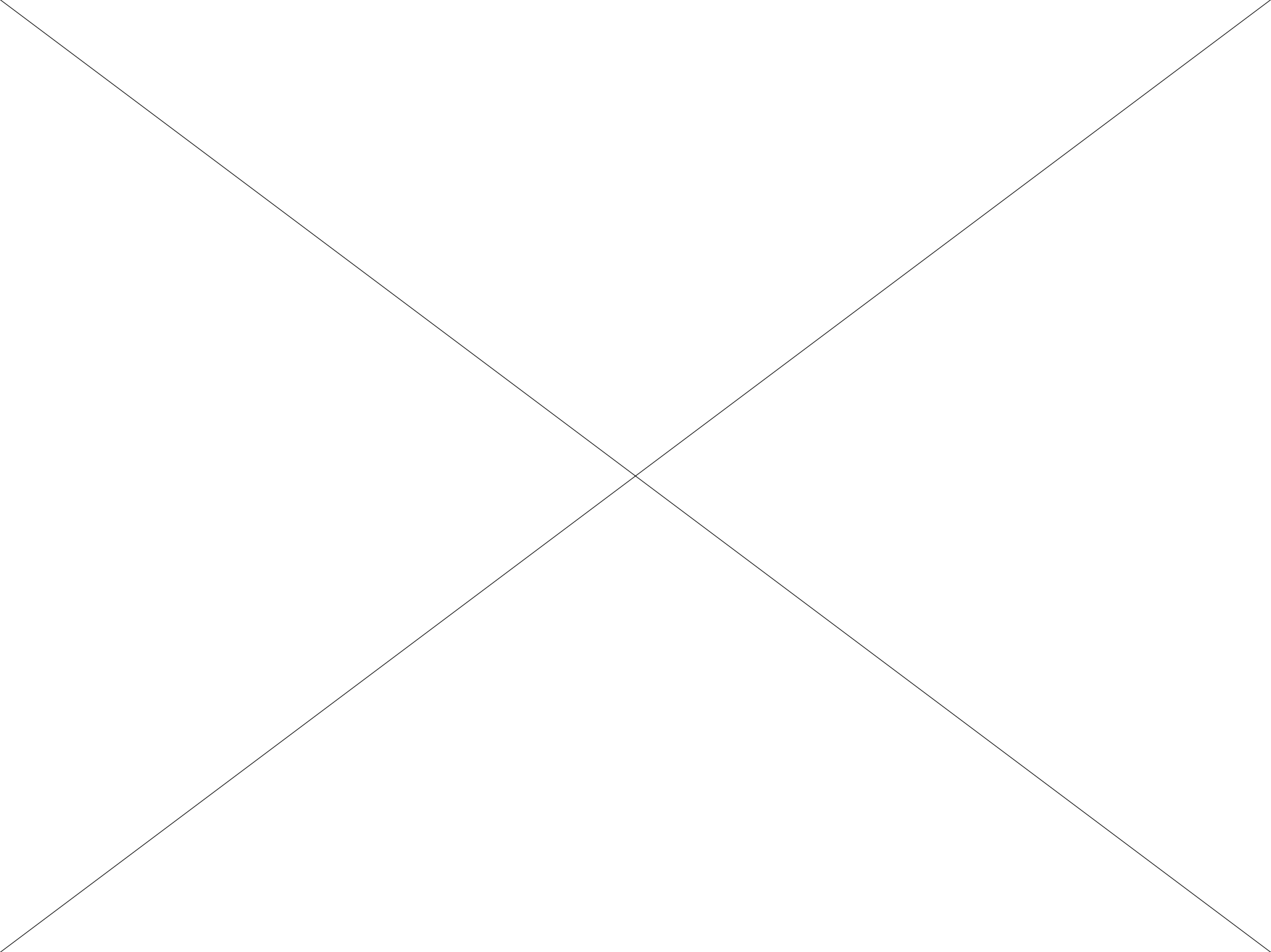


- On-line fingerprint services have been envisaged for some time ...
 - Automated Fingerprint Identification Systems (AFIS) already widely deployed
 - Extension to existing distributed authentication services (like Passport)
 - Our solution doesn't require any proprietary APIs or specific hardware
 - Support for different fingerprints for different services



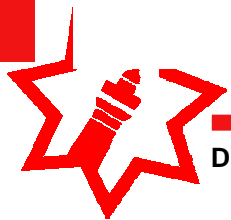
System Architecture





Summary

- Significant challenges remain in the development of feature identification and extraction
- Scale-up and real-time constraints are important obstacles
- Current work focusing on demonstrating how to secure future banking systems using biometrics



Biometrics Research Team (2005)

- Brock Henry – Reliable identification of facial features
- Wai Han Ho – Investigation of ageing in feature extraction and recognition
- Zeng Zhou – Incorporation of biometric data into digital certificates and signatures
- Oksana Bacchurina – Development of biometric-based banking systems using XML Web Services
- Xiang Li – Risk assessment of secure biometric-based banking systems using XML Web Services

