

# BEYOND PERFORMANCE: EMERGING RESEARCHES FOR BIOMETRICS

**BIAN YANG**

**NORWEGIAN BIOMETRIC LABORATORY AT  
GJØVIK UNIVERSITY COLLEGE, NORWAY**

**DECEMBER 2011, LEUVEN**



## OUTLINE

---

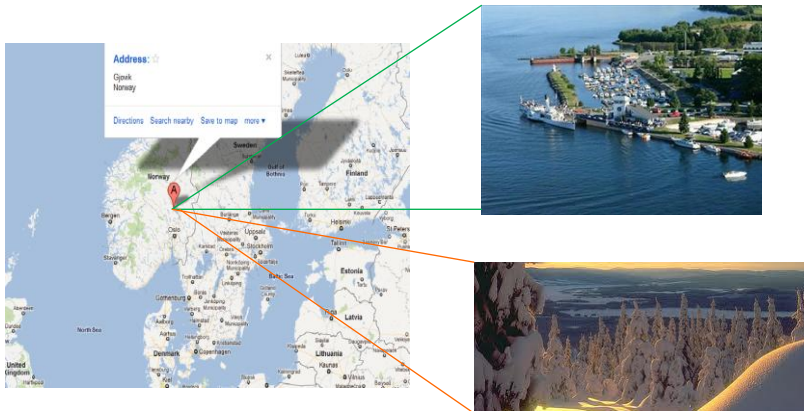
- GUC biometrics group – Norwegian Biometrics Laboratory
- Aspects other than technical performance, acceptability, and cost?
  - Privacy issues
  - Anti-spoofing
  - Convenience
  - Non-typical modalities and emerging novel application fields
- Remarks

# Norwegian Biometrics Laboratory



## NORWEGIAN BIOMETRICS LABORATORY

- Location: Gjøvik, Norway (1.5 hours drive north to Oslo)



## NORWEGIAN BIOMETRICS LABORATORY

---

- [http://nislabs.no/biometrics\\_lab](http://nislabs.no/biometrics_lab)
- Newly established in February 2011, led by Prof.Dr. Christoph Busch  
<http://www.christoph-busch.de/>
- Employee –
  - 5 full time professor / associate professor
  - 1 post-doc researcher, 6 Ph.D. students
- Research areas –
  - Fingerprint / finger vein, 2D/3D face, dental, ear and acoustic, signature, gait, keystroke, gesture, and mouse.
  - On-the-fly sensing and mobile biometrics
  - Privacy enhancement
- Projects
  - TURBINE (FP7, 2008-2011), BEST network (EU, 2009-2011), FIDELITY(FP7, 2012-)
  - NIST-BTP-metrics (NIST, 2010-2011), NIST-NFIQ2(NIST)
  - Hitachi vein recognition, IDEX fingerprint evaluation




---

Aspects other than technical performance, acceptability and cost?

## ASPECTS OTHER THAN TECHNICAL PERFORMANCE, ACCEPTABILITY, AND COST?

What are the most concerned in a biometrics-enabled system?

- Accuracy
  - Fingerprint: EER  $\approx$  0.1% (FVC-on-going)
  - Face: FRR  $\approx$  1~2.5% @ FAR = 0.1% (FRVT2006)
  - Iris: FRR  $\approx$  1.1~1.4% @ FAR = 0.1% (ICE2006)
- Processing rate
  - Fingerprint identification: 100,000,000 per second (MegaMatcher Accelerator by NeuroTechnology)
  - Automated Border Control: 17 seconds (vs. 45 secs by manually checking, Accenture report)
- Reliability
  - System robustness
  - Sample quality tolerance



## ASPECTS OTHER THAN TECHNICAL PERFORMANCE, ACCEPTABILITY, AND COST?

Some non-technical aspects

- Acceptability
  - Iris ?  
Could be difficult for the financial sector ... misunderstanding caused by movies ...



- Teeth



- Cost
  - Retina
  - DNA

and ... what aspects else might we concern?



## ASPECTS OTHER THAN TECHNICAL PERFORMANCE, ACCEPTABILITY, AND COST?

---

- Other aspects which are also important for practical deployment or future applications –
  - Privacy
  - Anti-spoofing
  - Convenience
  - New modalities and new application fields

---

Privacy

## PRIVACY

---

Story of "dry plate" based hand-held camera

- Invented in 1879
- Making camera portable and capturing instant



Privacy concerned over the instantly-taken portraits brought by this technological revolution

- portrait: exactly a privacy concern related to biometrics!!

## PRIVACY

---

“That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to **define anew** the exact nature and extent of such protection.”

- Samuel D. Warren, Louis D. Brandeis, The Right to Privacy, *Harvard Law Review*, Vol.IV, December 15, 1890, No.5.

- Privacy: a dynamic concept
- Kept in concern since ancient time till so far
- New technologies keep bringing challenges to privacy while help defining **new extent** of privacy

## PRIVACY

A modern biometrics-enabled system

Privacy concerns can be found in

- Data collection process (US airport X-ray scanning with **remote inspector**)



## PRIVACY

- Information linkage in storage (linkage between identity reference and biometric reference)



Secure binding of IR and BR using CI is recommended in ISO/IEC 24745 on Biometric Information Protection.

## PRIVACY

---

- Concern on CI – still linkable between IR and BR!
  - Yes, but can we anonymize this linkage?

A story from GUC100 database [www.nislab.no/guc100](http://www.nislab.no/guc100)

- multi-sensor fingerprint database, 6 sensors, 100 subjects, 12 sessions, 10 fingers
- collected in winter-spring time in Norway, 2008
- Authorized to use for the EU-FP7 project TURBINE
- One subject **requested to delete** his data after the TURBINE project ... and then we found it was really necessary to keep the namelist.



## PRIVACY

---

- Lesson from the GUC100 story:
  - Anonymization is not equal to privacy protection
  - Privacy includes the right to controlling the processing of own data, besides hiding the linkage
- Better solutions instead of a namelist:
  - Hashing the IR (name, DOB, ...)
  - Not enough entropy? Hashing the IR + PIN (personal secret)
  - ...



## PRIVACY

---

- Biometric references protection (a.k.a. biometric template protection)

- **Target**

to prevent original biometric characteristics from leakage (both inadvertently and maliciously)

- **Impacts of characteristics leakage**

- leakage of health and other personal information

- risk of profiling attack (linkage of different enrolled applications: bank records, financial records, transaction records, ...)

- faking samples

- ...

- **Two approaches to leakages**

- via prints from fresh samples (**hard to prevent practically**)

- via templates stored in databases (**preventable**)



## PRIVACY

---

- **vs. Anti-spoofing techniques**

- anti-spoofing: action after leakage

- biometric template protection: action to prevent leakage from the databases

- **what if anti-spoofing techniques only without BTP?**

- leakage of health and other personal information ;-(

- risk of profiling attack (linkage of different enrolled applications: bank records, financial records, transaction records, ...) ;-(

**Conclusion:** even if biometric characteristics are not able to change, we should make their templates **renewable** in case of biometric information leakage from templates.



## PRIVACY

### ISO/IEC JTC1 SC27 24745 on Biometric Reference Protection (IS, June 2011)

- **Security**

Confidentiality, Integrity, Renewability and revokability

- **Privacy**

Irreversibility (from the protected templates to their plaintexts)  
Unlinkability (among protected templates diversified from the same plaintext biometric feature)



## PRIVACY

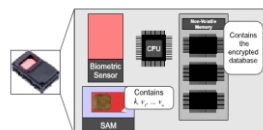
### Why not standard encryption and data authentication mechanisms ?

- **Comparison in the encrypted domain?**

Too fuzzy to be comparable after encryption.

- **Comparison after decryption?**

Need a secure comparison environment e.g., a Secure-Access-Module hardware . (J.Bringer, et al, (Sagem Security) BioID MultiComm2009)



(hardware dependent!!)



## PRIVACY

---

### Existing solutions for BTP

- alias {Helper Data Scheme (Philips), Pseudo Identities (TURBINE), Fuzzy commitment (RSA Lab), Cancelable Biometrics (IBM), Biometric encryption, Fuzzy Vault (RSA Lab), }, Shielding functions (Philips), Fuzzy extractors (NY Univ.), BIOCRYPTICS (GenKey), Random Projection (Yonsei Univ.), Secure sketch (Polytech. Univ. NY), Secure Syndrome (Mitsubishi), ...}
- Products:
  - Philips priv-ID
  - GenKey BIOCRYPTICS
  - Mitsubishi
  - Sagem Sécurité (Morpho)



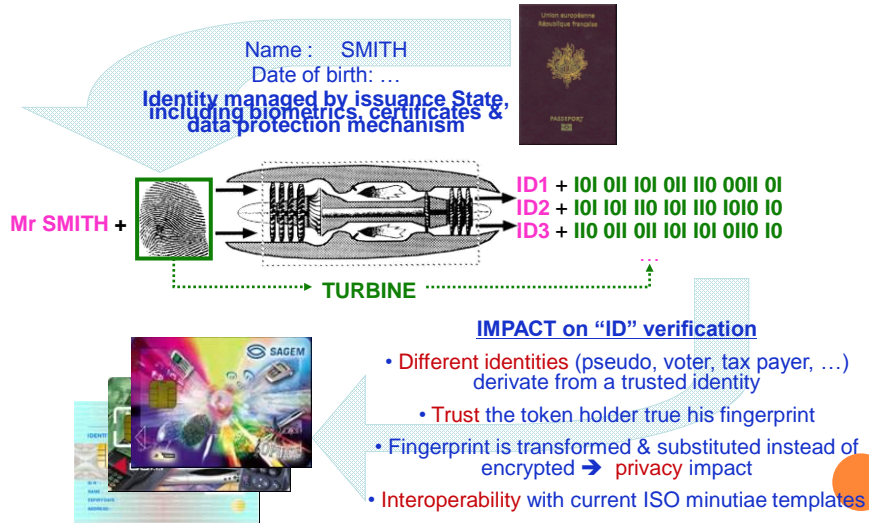
## PRIVACY

---

- TURBINE: TrUsted Revocable Biometric IdeNtitiEs
- <http://www.turbine-project.eu/>
- European 7th Framework Programme (Integrated Project)
- Duration: 3 years (2008.02-2011.01)
- Funding: 9.9 M€
- Target: provide secure authentication based on protected biometric templates (testing and application modality is currently concentrating on fingerprints)
- Performance target: FRR<1%@FAR=0.1% (**achieved in TURBINE**)



## PRIVACY



## Anti-spoofing

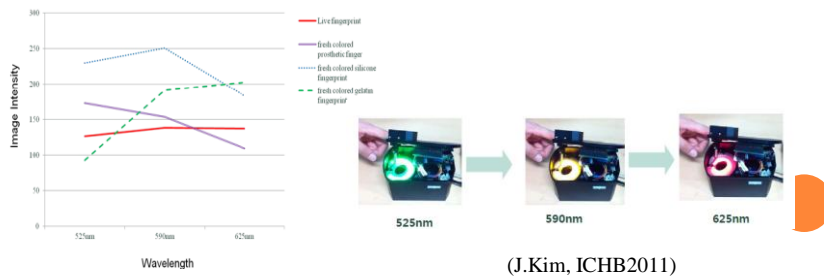
## ANTI-SPOOFING

### ○ Hardware based solutions

Application specific: blood pressure, temperature, odor, ...

### ○ Software based solutions

- pore number / perspiratory characteristics detection in fingerprint
- Ultra-sound based subsurface characteristics
- Color / multi-spectral imaging characteristics



## ANTI-SPOOFING

Note: anti-spoofing methods are **not theoretically secure** against spoofing attempts (like the embarrassing situation of anti/virus) ;-(

# Convenience



## CONVENIENCE

### Mobile computing platform

- Portable
- Enhanced privacy – sensor under subjects' control (psychologically?)
- General-purpose sensors (e.g., cell phone camera, acceleration meter)
- Modalities: finger, face, gait, teeth, ...



Left index finger performance

EER = 0.0% Nokia N95

EER = 8.5% HTC Desire

NeuroTechnology software used

(GUC experimental results)



## CONVENIENCE

### On-the-fly sensing

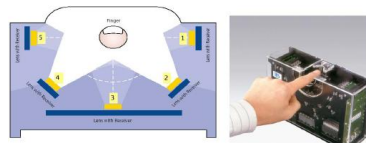
- Touchless
- At a variable distance
- On-the-move
- Uncontrolled data capturing environment
- Break-through sensing technologies



Fujitsu palm vein on-the-move sensor



AOptix InSight iris sensor

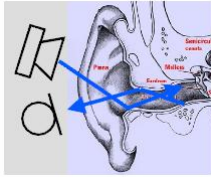


TBS touchless fingerprint sensor

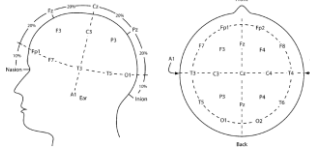
Un-typical modalities and  
emerging novel applications

## UN-TYPICAL MODALITIES

Some un-typical modalities GUC is working on -



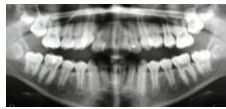
Ear accoustics



Brain wave (EEG)



Gait on mobile phone



teeth

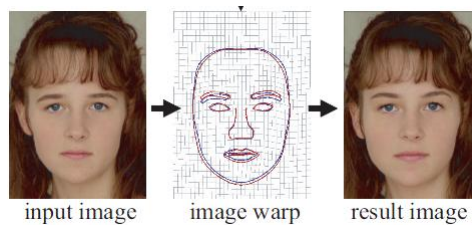


keystroke



## EMERGING NOVEL APPLICATIONS

### Beautification



(T. Leyvand, et al, SIGGRAPH '08)

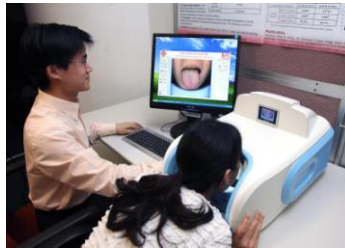
- Large face-lifting market in US and east Asia
- Problem for face recognition? (to be evaluated)



## EMERGING NOVEL APPLICATIONS

### Medical biometrics

- Heart sound
- Iris
- Tongue
- Pulse
- ...



Tongue based diagnosis by PolyU Hong Kong

Many features from TCM to be evaluated and verified.

## REMARKS

1. Besides technical performance, other aspects need our attention for practical deployment;
2. Privacy, as an old topic of concern, extends in scope by new technologies but able to protect by technologies as well;
3. Anti-spoofing is hard to achieve theoretical and general solutions;
4. Convenience is a technological trend;
5. New modalities and new applications makes biometrics more interesting and useful.

## THANK YOU

---

Thank You for Attention.

Contacts:

[bian.yang@hig.no](mailto:bian.yang@hig.no)

