BYSM-2006 Symposium, 19-21 Sep.2006, Baltimore

Multilevel liveness verification for face-voice biometric authentication

Girija Chetty

School of ISE, University of Canberra

Australia

Overview: MLLV Framework

- MLLV framework for secure face-voice biometric person authentication
- Addresses Impostor and replay attacks in face-voice biometric domain
- Allows liveness verification based on novel feature extraction and fusion techniques.
- Experiments with three speaking face corpora
- Performance : DET curves and EER rates

Background

- Still stuck with passwords and ID which are clearly not adequate.
- Token based systems – vulnerable to theft and forgery.
- Biometrics- a better solution
- Which Biometric ? Voice, fingerprint, retina, face
- User acceptance and usability more important for diffusion of Biometrics in everyday life.
- user acceptance & usability.
- vulnerable to forgery

User acceptance and Usability !!

- Recent EU report in 2005 – proposed biometric diffusion by 2015
- Example everyday scenarios
  - (face/voice) biometric system at child care centers which unobtrusively scans parents when they ring the doorbell.
  - Over-65 bus pass holders with facial template on the smart cards which needs to be renewed every year
  - Computer games
  - Video rentals
  - Gas/cooking appliances (kitchen) avoid accidents with kids.
  - Replacing finger-print recognition in the car !!

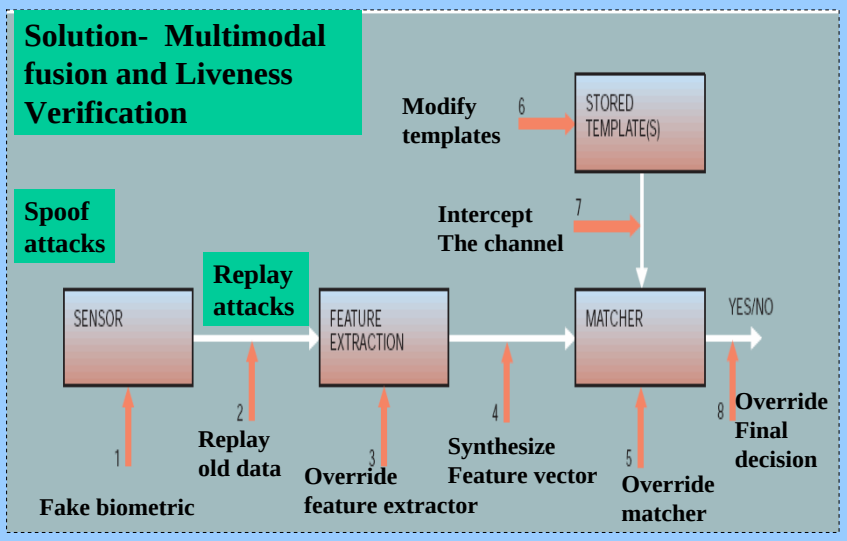
Face Voice Biometrics

- Rate high in terms of User acceptance and usability.
- But more vulnerable to forgery
  - Pre-recorded audio
  - Still photo
  - Pre-recorded video
  - Animated video from a still photo
- Vulnerable to environmental degradations
  - Acoustic noise effects
  - Visual artefacts

Multimodal biometrics

- Multimodal Fusion
  - Addresses environmental and background degradation problems
- Liveness Verification – addresses forgery
  - Exploit visual manifestation of speech in speaking faces.

Vulnerability of different stages to fraudulent attacks



Biometric security framework based on multimodal fusion

- Multi-level security framework based on
  - Multimodal Fusion of static and dynamic face-voice biometric information from **Speaking faces (kinematic-acoustic system and cannot be easily faked)**

    and
  - Liveness detection/verification of present novel fusion and feature-extraction techn **attacks)**
- Methodology
  - Bimodal Feature Fusion
  - Cross Modal Fusion
  - 3D Multi-modal Fusion
- Three data corpora

Multi-level security

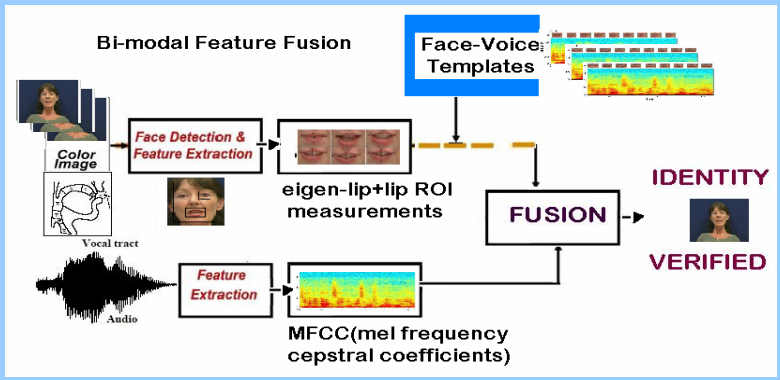
-Level 1 security: static attacks

Level 2 - video attacks

Level 3- synthetic speaking face attacks

Bi-Modal Feature Fusion (BMF)

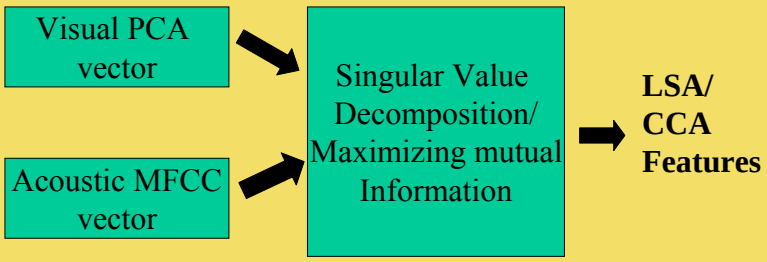
– Verify liveness by feature-level fusion of acoustic features + dynamic lip features from lip region



Cross-Modal Fusion (CMF)

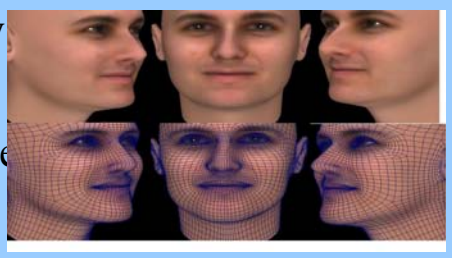
– Detect liveness of face-voice biometric data by extracting audio-visual synchrony based on:

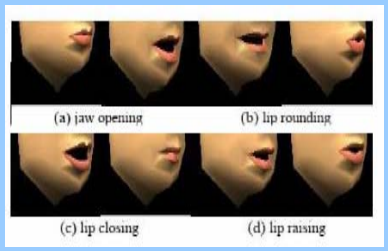
- Latent Semantic Analysis (LSA) features:
- Canonical Correlation Analysis (CCA) features:



3D Multi-modal Fusion (3MF)

- Detect Liveness by extracting depth information from face
- 3D Face models
- Rigid fusion
  - 3D Shape + texture +acoustic features

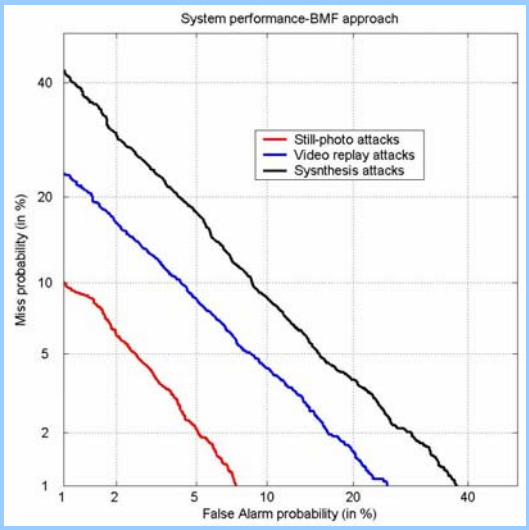




Experiments

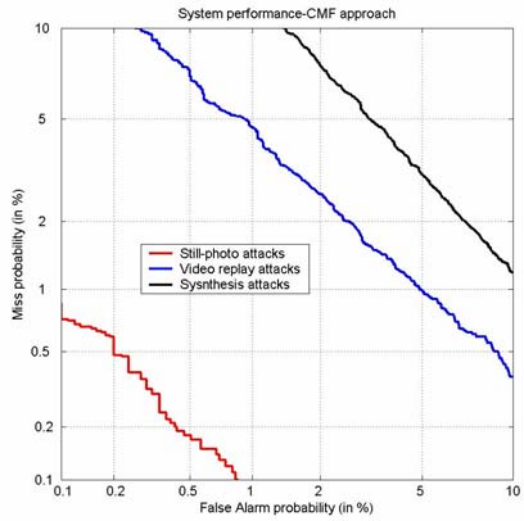
- Training phase:
- 10 mixture GMM speaker model from corpora.
- Test phase: clients' live test recordings were evaluated against a client's model λ by determining the log-likelihoods *(log p(X|λ))* of the time sequences *X* of audiovisual feature vectors.
- For testing replay attacks, three types of replay/synthetic attack experiments were conducted.
  - Still replay attacks
  - Video replay attacks
  - Synthetic replay attacks

Results- BMF approach



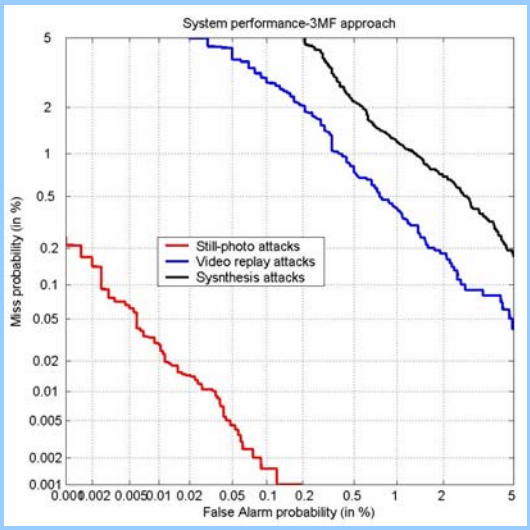
School of ISE, BLIS Division

Results-CMF approach



School of ISE, BLIS Division

Results – 3MF approach



School of ISE, BLIS Division

EER comparison

	Still	Video	Synthetic
• BMF	2.4 %	6.54 %	9.23 %
• CMF	0.29%	2.25%	3.96%
• 3MF	0.0155 %	.611%	1.18%

School of ISE, BLIS Division

Conclusions

- Multi-level security framework.
- Reported replay attacks only
- Similar performance in addressing basic impostor attacks
- Complete software oriented solution
- An extensible framework for addressing futurisitic forgery scenarios