An Overview of the Research Activities of the Pattern Recognition & Biometric Research Group at the Faculty of EE and Computing

Professor Slobodan Ribarić, Ph.D.
University of Zagreb
Faculty of Electrical Engineering and Computing (FER)
Unska 3, 10000 Zagreb, CROATIA
slobodan.ribaric@fer.hr

Overview

1. Pattern Recognition & Biometric Research Group
2. International Research Projects
3. Research Activities on the Field of Biometrics
4. Palmprint-based recognition systems
5. Biometric System Based on Fusion of Palmprint and Face Features
6. Hand Detection and Palmprint Localization from Video Sequences
7. Proposal for a new COST Action

1. Pattern Recognition & Biometric Research Group

(at the Department of Electronics, Microelectronics,Computer and Intelligent Systems)

- Full Professor
- Researcher (Ph.D.)
- Assistant
- Three Ph.D. students

National research project: **Autonomy Oriented Computer Structures (AOC)** applied on the Field of Pattern Recognition, Biometrics, Computer Vision and Knowledge Representation

Biometrics

- Biometrics is the science of identifying, or verifying the identity of a person based on physiological or/and behavioural characteristics.

- Biometrics – a new technology which deals with identification of individuals based on their physiological or/and behavioural characteristics.

physiological characteristics:

- DNA (DeoxyriboNucleic Acid)
- Body odour
- Skin reflectance
- Fingerprint
- Palmprint
- Hand and finger geometry
- Hand vein
- Face
- Iris
- Retinal scan

behavioural characteristics:

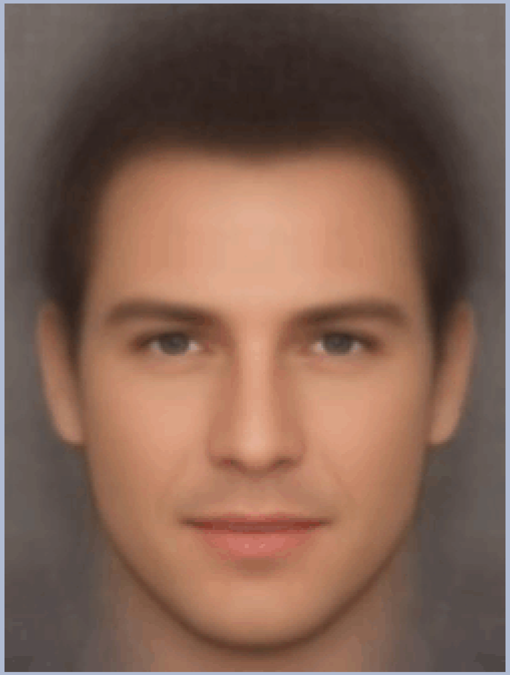
- Signature (static off-line, dynamic on-line)
- Keystroke dynamics
- Gait
- Lip motion
- Voice
- Gesture
- Grip

“soft” biometric characteristics:

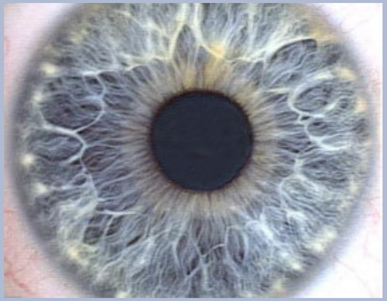
- Hair colour
- Weight
- Race
- Eye colour
- Height

Popular biometric characteristics (modalities)

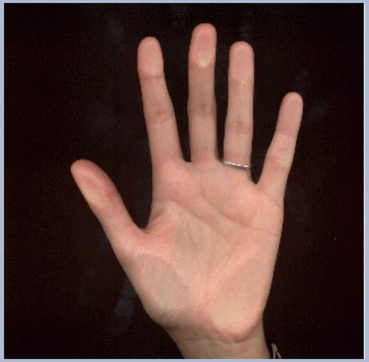
Fingerprint



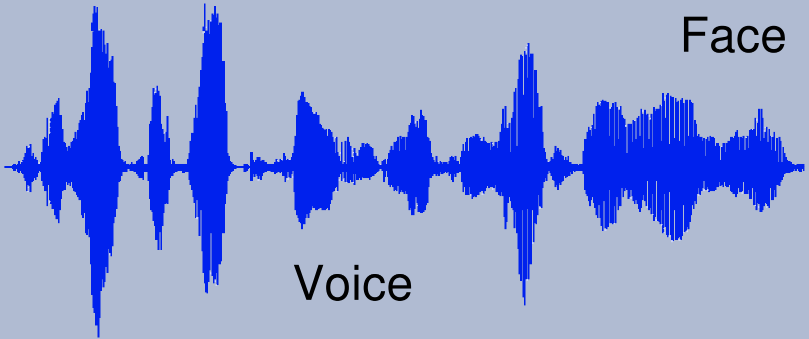
Face



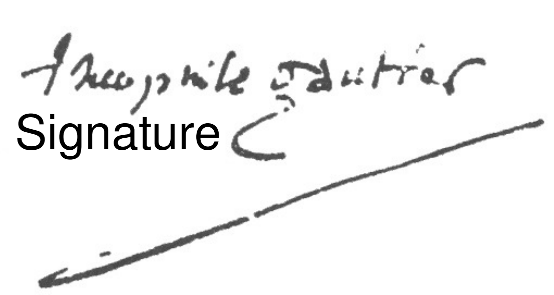
Iris



Hand



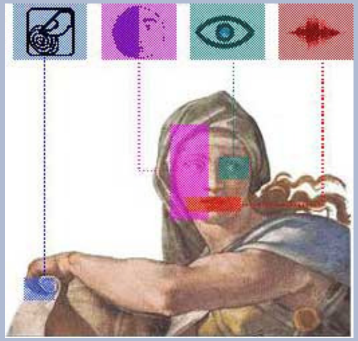
Voice



Signature

2. International Research Projects

- Biometrics on Internet – COST* 275 (EU project)



COST 275: Biometrics on the Internet

2001 – 2005

- Biosecure – Network of Excellence (EU project)

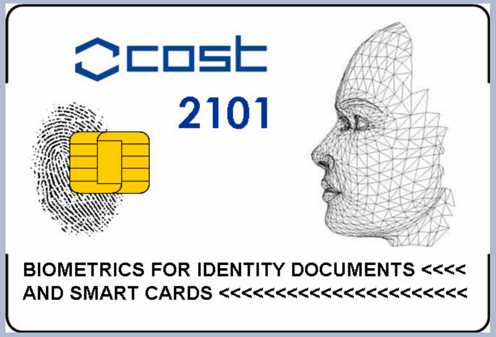
BIOSECURE

Network of Excellence: Biometrics for Secure Authentication

2004 – 2007

*COST – European Cooperation in Science and Technology

- Biometrics for Identity Documents and Smart Cards – COST 2101 (EU project)


cost
2101
BIOMETRICS FOR IDENTITY DOCUMENTS <<<<
AND SMART CARDS <<<<<<<<<<<<<<<<<<<<<<

COST 2101: Biometrics for Identity Documents

2006 – 2009

- Bilateral Research projects

Proposal for a new COST Action: De-identification for privacy protection in multimedia content

Brussels 10 September 2012

Slobodan Ribarić

University of Zagreb

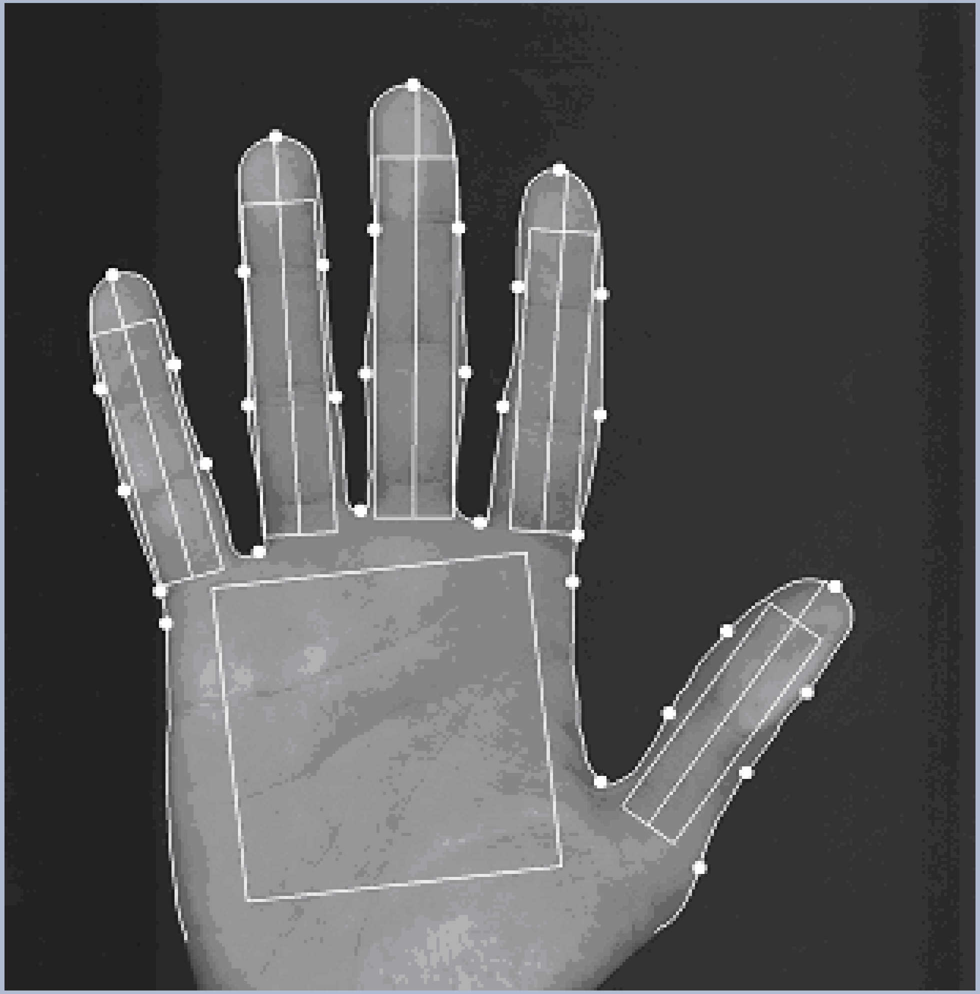
Faculty of Electrical Engineering and Computing

Croatia

4. Palmprint-based recognition systems

- Eigenfinger and Eigenpalm Based Identification System
- Biometric Authentication System Based on Eigenfingers and Finger-Geometry with Aliveness Detection
- Biometric Recognition System Based on Fusion of Fingerprints, Digitprints and Palmprints
- Palmprint Recognition System Based on Haralick Local Features
- Colour-based Palmprint Recognition System
- Biometric System Based on Fusion of Palmprint and Face Features
- Hand Detection and Palmprint Localization from Video Sequences

Eigenfinger and Eigenpalm Based Identification System

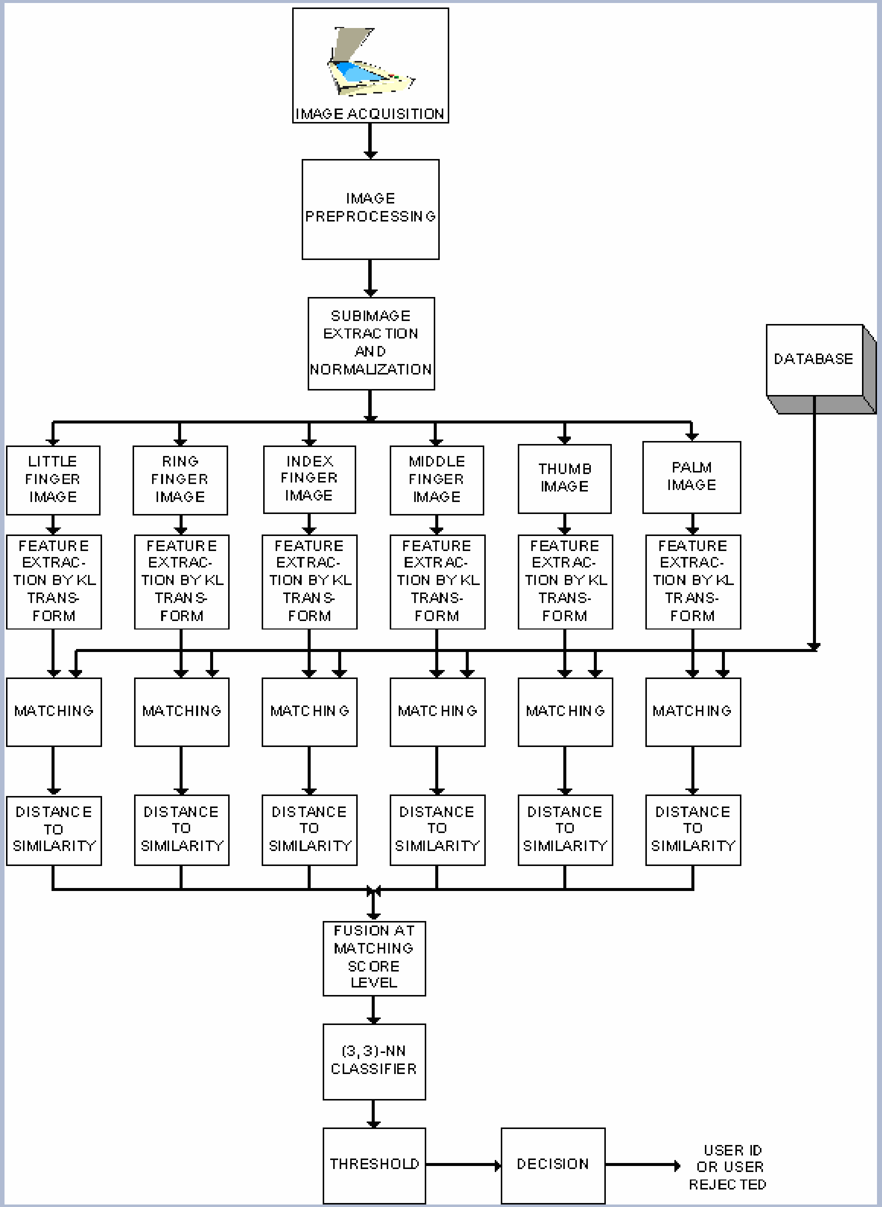


Our approach:

- Finger-strip region
- Palm-print region

Eigenfinger and Eigenpalm Based Identification System (cont.)

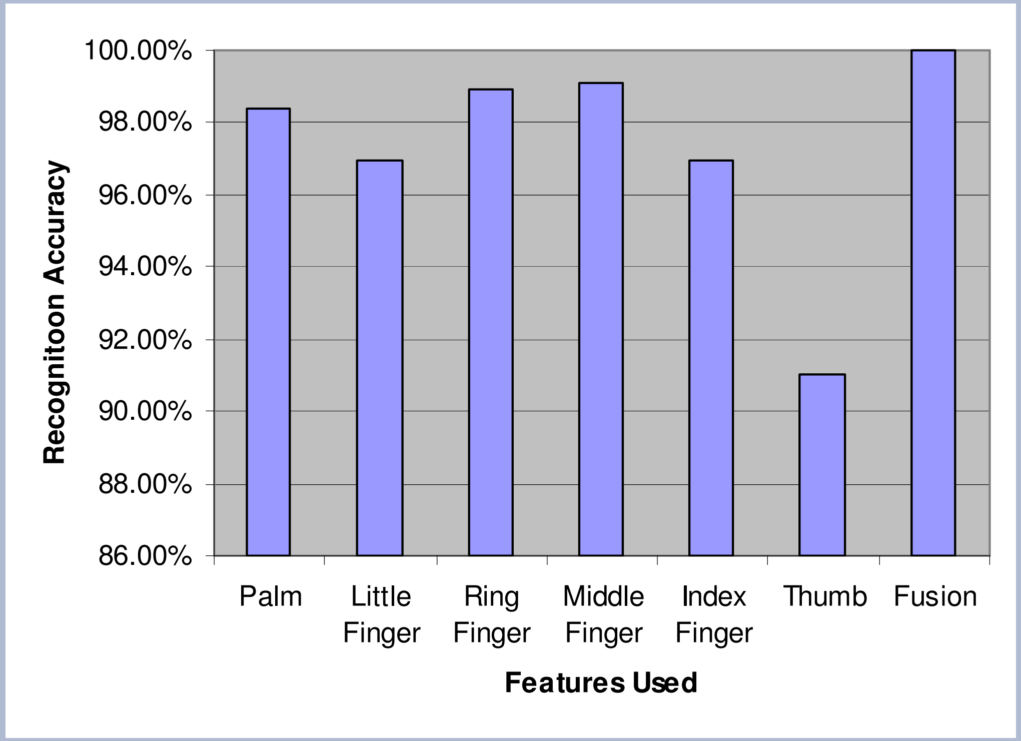
Block-diagram of the system



(S. Ribaric, I. Fratric, A Biometric Identification System Based on Eigenpalm and Eigenfinger Features, IEEE Trans. on PAMI, Nov. 2005, pp. 1698-1709)

Eigenfinger and Eigenpalm Based Identification System (cont.)

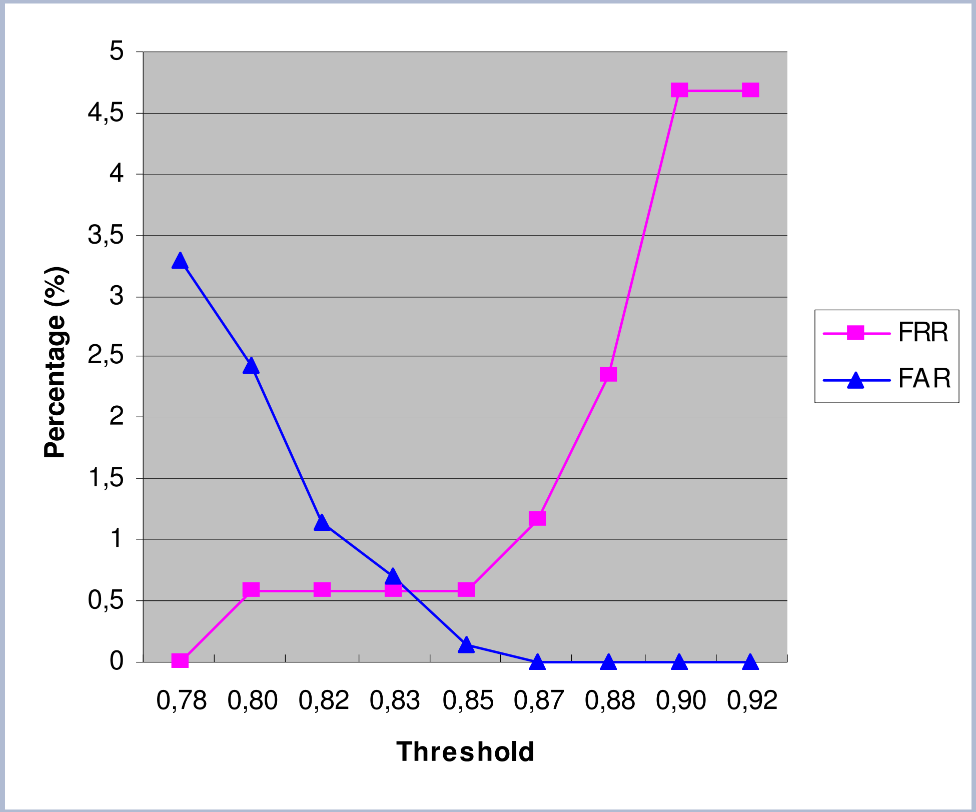
Recognition results



- high recognition accuracy for some of the fingers
- strip-like finger image – a novel biometric feature

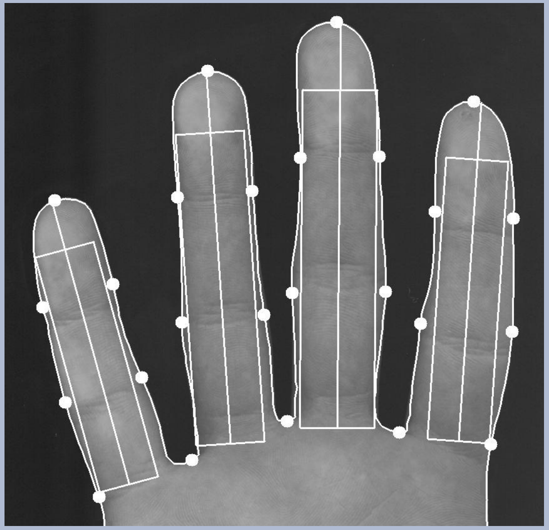
Eigenfinger and Eigenpalm Based Identification System (cont.)

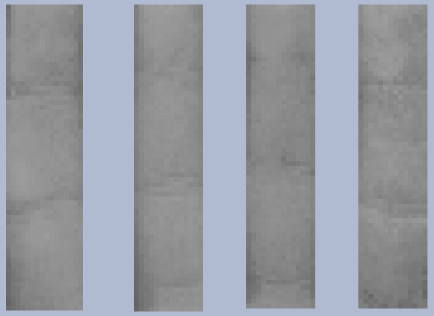
Identification test results

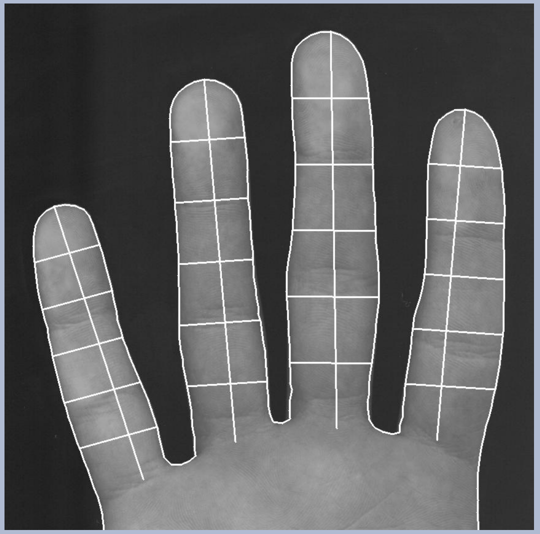


- EER (equal error rate) of FRR = FAR = 0.58% for threshold T = 0.83.
- A minimum TER (Total Error Rate, TER = FAR + FRR) of 0.72% is achieved with T = 0.85.

Finger-geometry and Eigenfinger-based System with Aliveness Detection

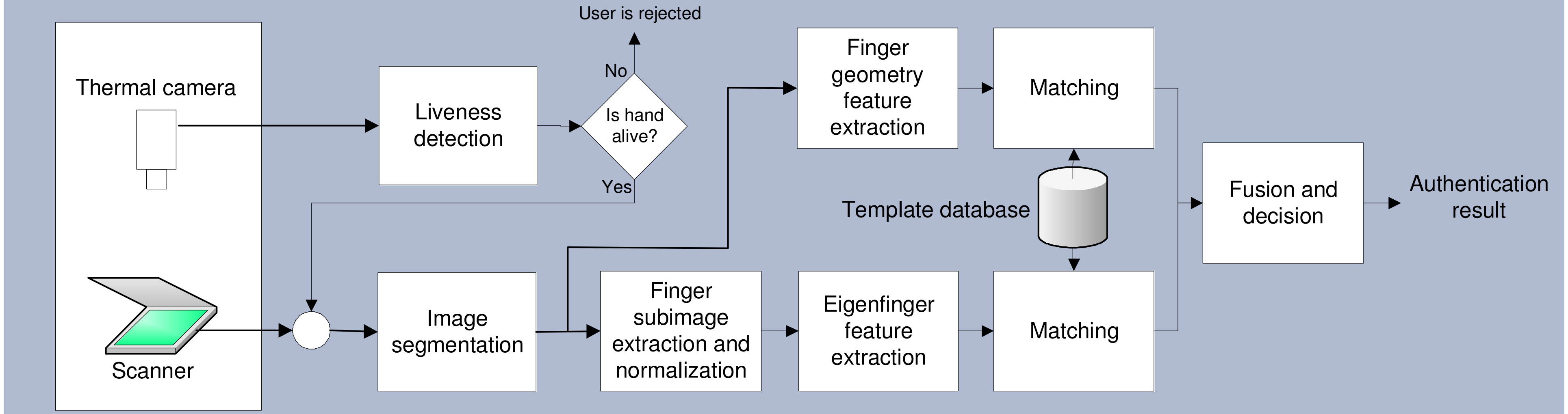






- Four strip–like regions of the fingers are localized
- PCA is used to extract the features from each of the finger subimages
- 100 eigenfingers were used in representing each finger
- Six geometry measurements are taken for each finger

Biometric Authentication System Based on Eigenfingers and Finger-Geometry with Aliveness Detection (cont.)

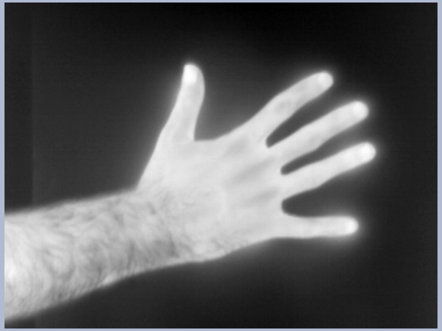


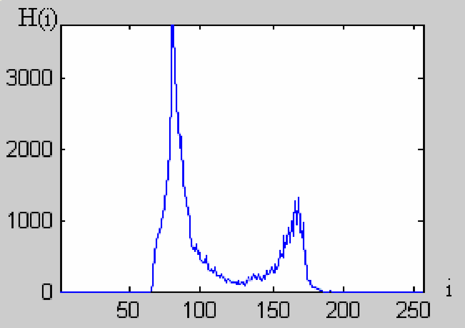
(S. Ribarić, I. Fratrić,
An Online Biometric Authentication System Based on Eigenfingers and Finger-Geometry // Proceedings of 13th European Signal Processing Conference. 2005.
N. Pavešić, T. Savič, S. Ribarić, I. Fratrić,
A multimodal hand-based verification system with an aliveness-detection module. // Annals of Telecommunications. 62 (2007) , 1-2; pp. 1655-1680)

Aliveness Detection

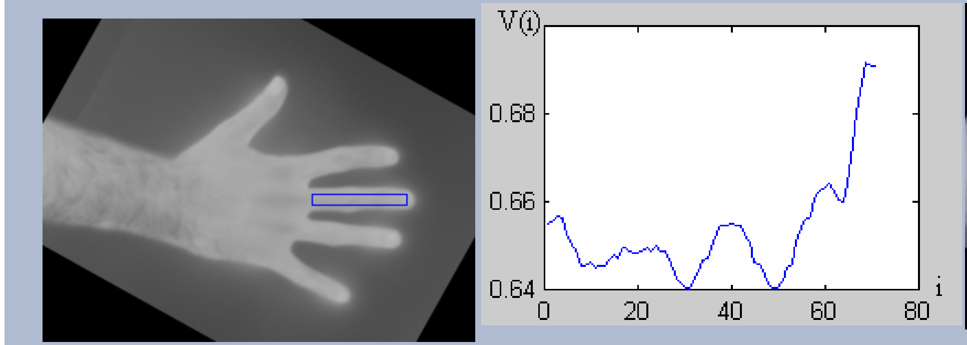
- Two kinds of features are proposed:

1. Histogram of the thermal hand image

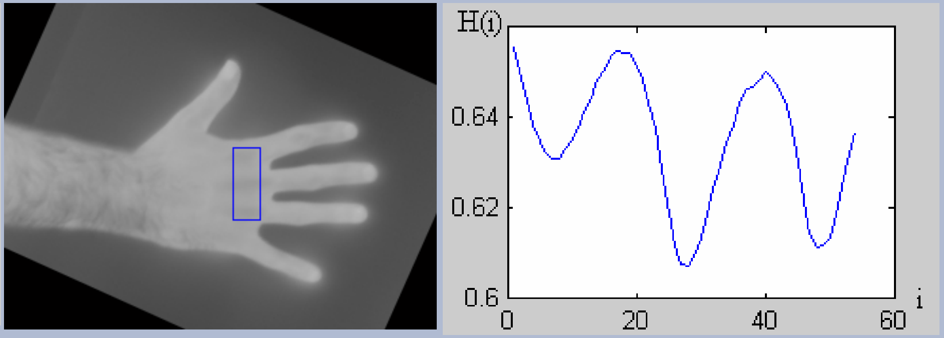




2. Temperature variations in the two characteristic regions of dorsal hand images

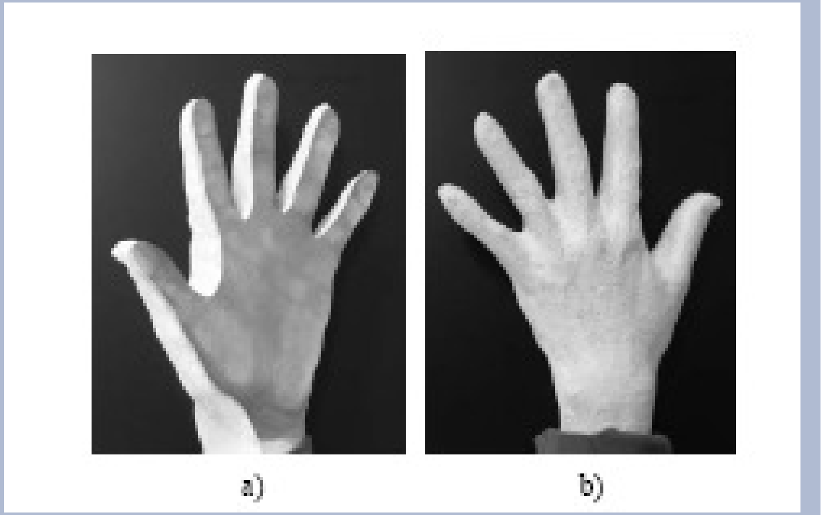


Vertical projection of the finger region

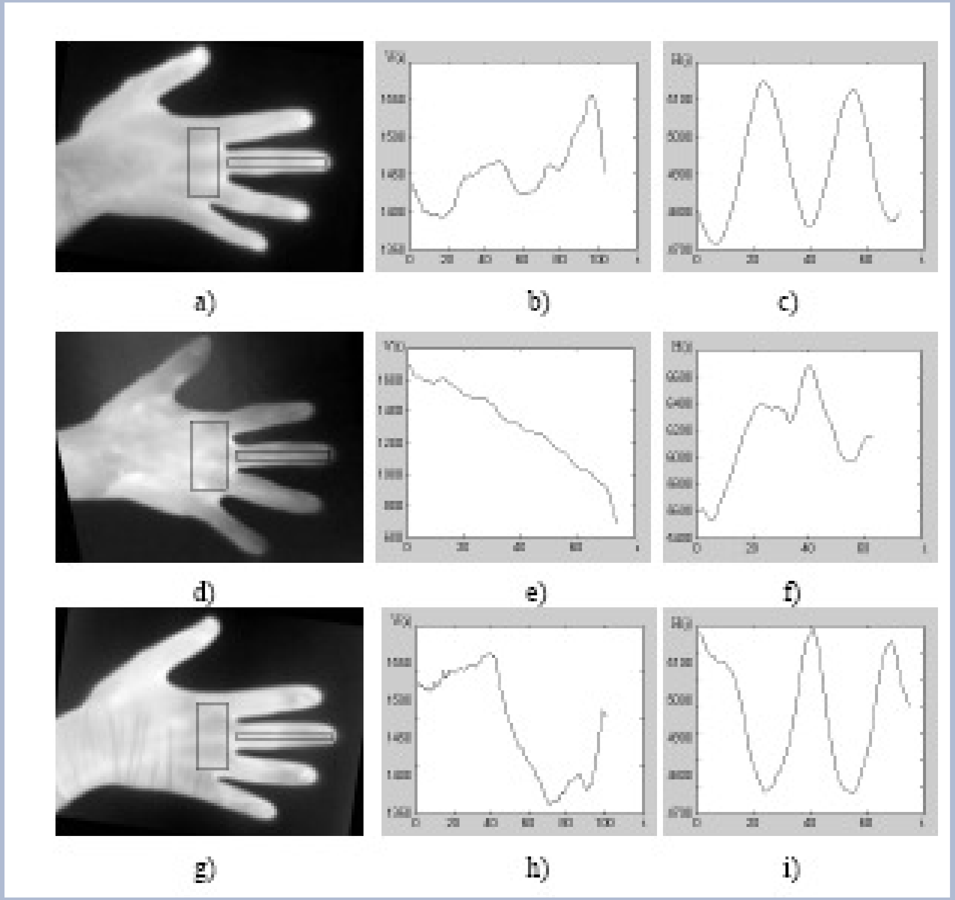


Horizontal projection

Aliveness detection



Artificial hand (Type I)



a) Infrared alive-hand image
b) Heated artificial hand image (Type I)
c) Heated artificial hand image (Type II)

Aliveness detection

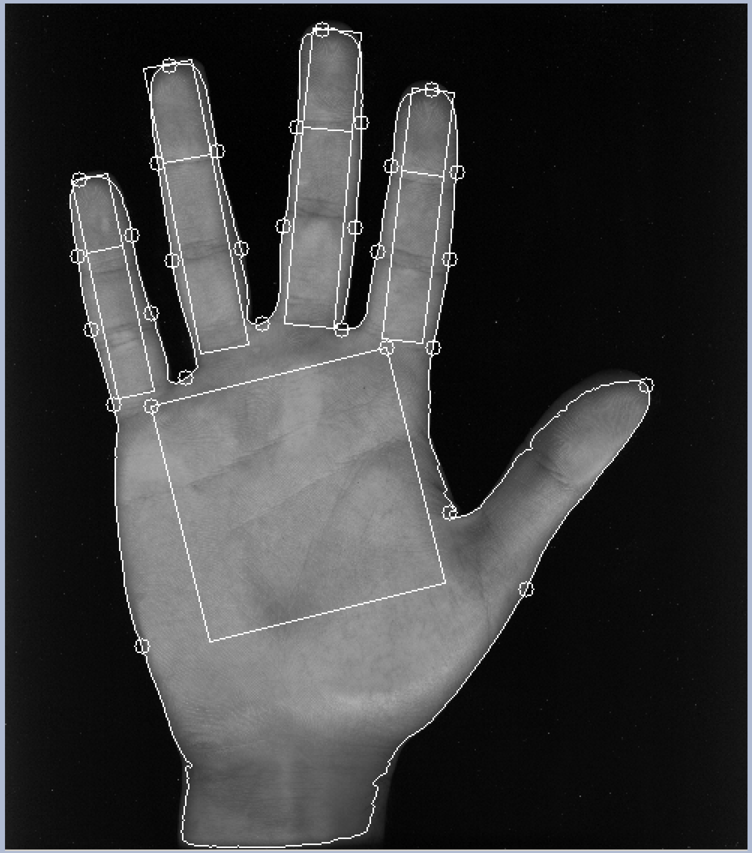
Classifier	Classification accuracy [%]
Linear kernel SVM	95.0
3-degree polynomial kernel SVM	100.0
RBF kernel SVM	100.0

Aliveness classification accuracy for different SVM-based classifiers

Biometric Recognition System Based on Fusion of Fingerprints, Digitprints and Palmprint

- 9 regions of interest (ROI) are detected:
  - 4 ROIs on tips of 4 fingers
  - 4 ROIs on 4 fingers between first and third phalanx (digitprint)
  - 1 ROI on palm

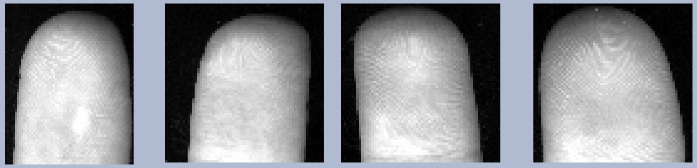
- ROIs represent hand biometric identifiers



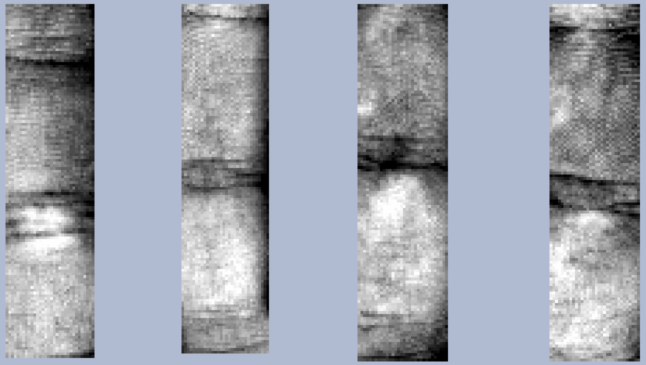
Hand contour,
reference points,
ROI rectangles

Biometric Recognition System Based on Fusion of Fingerprints, Digitprints and Palmprint (cont.)

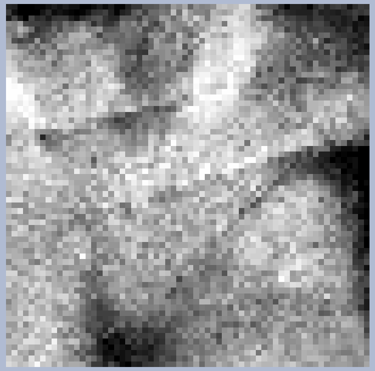
ROI’s sub-images:



fingerpints (64 x 64 pixels),



digitprints (128 x 32 pixels),

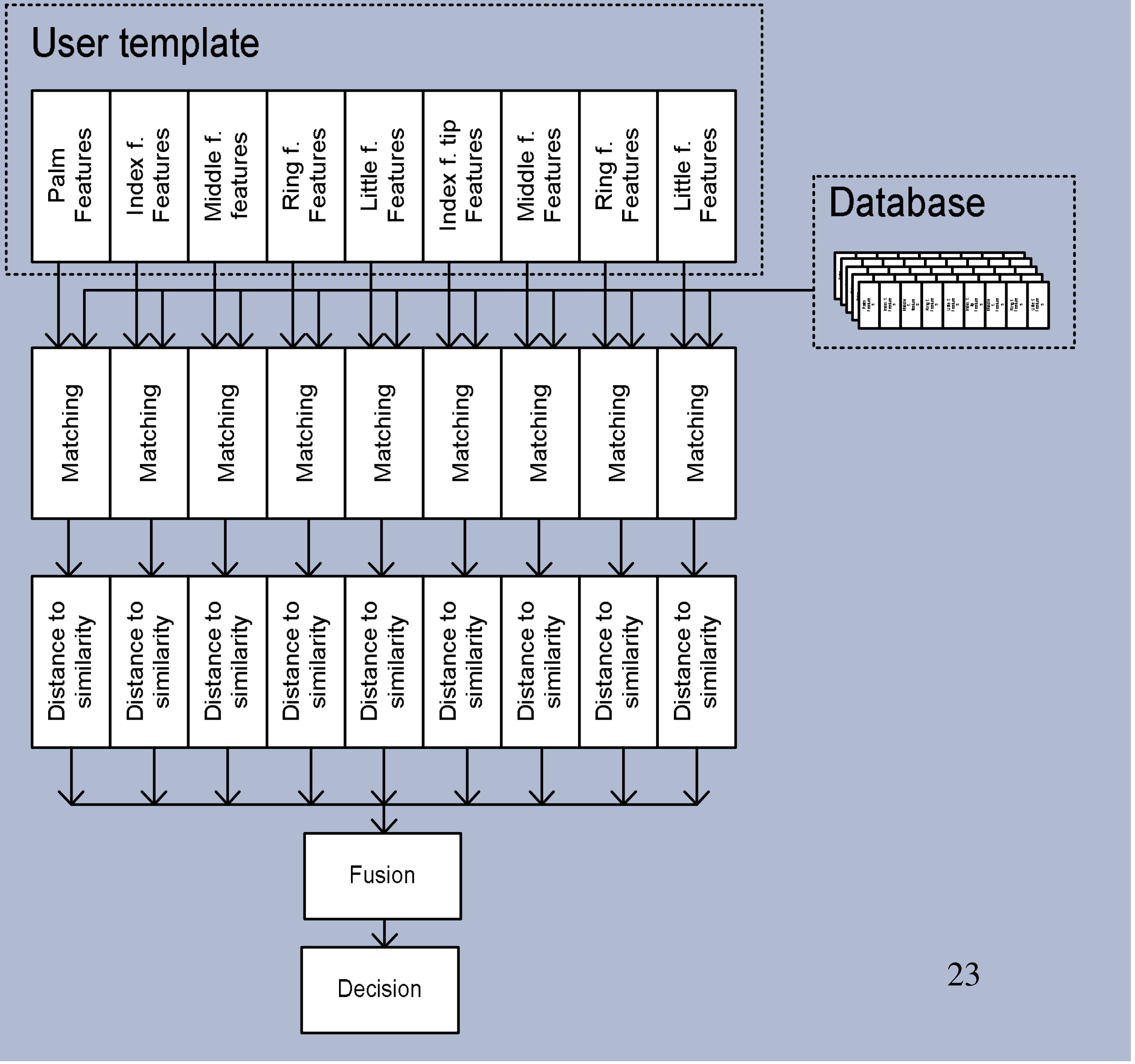


palm (64 x 64 pixels)

Biometric Recognition System Based on Fusion of Fingerprints, Digitprints and Palmprint (cont.)

System archtecture

- 1-NN (Nearest Neighbour) classification rule (Euclidean distance),
- Fusion at matching score level (Ribaric et al., 2002)



Biometric Recognition System Based on Fusion of Fingerprints, Digitprints and Palmprint (cont.)

Feature extraction based on:

- PCA (Principal Component Analysis)
- LDA (Linear Discriminant Analysis)
- MDF (Most Discriminant Features),
- RD-LDA (Regularised-direct LDA)

(N. Pavešić, Nikola; S. Ribarić, ; B. Grad, Finger-Based Personal Authentication: a Comparison of Feature-Extraction Methods Based on Principal Component Analysis, Most Discriminant Features and Regularised-Direct Linear Discriminant Analysis. // IET Signal Processing. 3 (2009) , 4; 269-281)

Biometric Recognition System Based on Fusion of Fingerprints, Digitprints and Palmprint (cont.)

Identification:

dimensions of the ROIs feature vectors:

100 PCA coefficients

183 MDF coefficients (based on N - c = 736 PCA coefficients)

183 MDF coefficients (based on c = 184 PCA coefficients)

183 RD-LDA coefficients

Rates of the average correct identification (for fusion-all ROIs)

99.5 %; 0.43 – PCA; *m* = 100 components

99.78 %; 0.24 – MDF; m = 183 (based on N - c = 736 PCA coefficients)

99.67 %; 0.30 – MDF; m = 183 (based on c = 184 PCA coefficients)

99.98 % 0.05 – RD-LDA; m = 183

Biometric Recognition System Based on Fusion of Fingerprints, Digitprints and Palmprint (cont.)

Database setup

- ten images of the right hands of 184 people (122 men and 62 women; average age of the tested population is 36 years; two separate sessions) – 1840 images (ten images per class);

Closed-set identification

- 5 images from each image class were chosen randomly and used in the enrolment stage (client database)
- remaining 5 images were used to test system;
- the total number of attempts in the identification test was 920;

Palmprint Recognition System Based on Haralick Local Features

Based on the normalized GLCM, Haralick has proposed 14 statistical features, called Haralick features, that can be calculated for each δ and Θ.

In our approach the local Haralick features are obtained from the normalized grey-level co-occurrence matrices (GLCMs) created on the d x d pixels overlapping subimages of the palmprint's D x D ROI, $d < D$ defined by a sliding window that slides on the palmprint's ROI with a translation step $t = d/2$ pixels

(S. Ribarić, M. Lopar, Palmprint Recognition Based on Local Haralick Features // 2012 IEEE Mediterranean Electrotechnical Conference, MELECON 2012. Yasmine Hammamet : IEEE, 2012. 657-660)

Palmprint Recognition System Based on Haralick Local Features (cont.)

- matching:

live template and the templates from a system database - Euclidean distance

- distance to similarity transformation

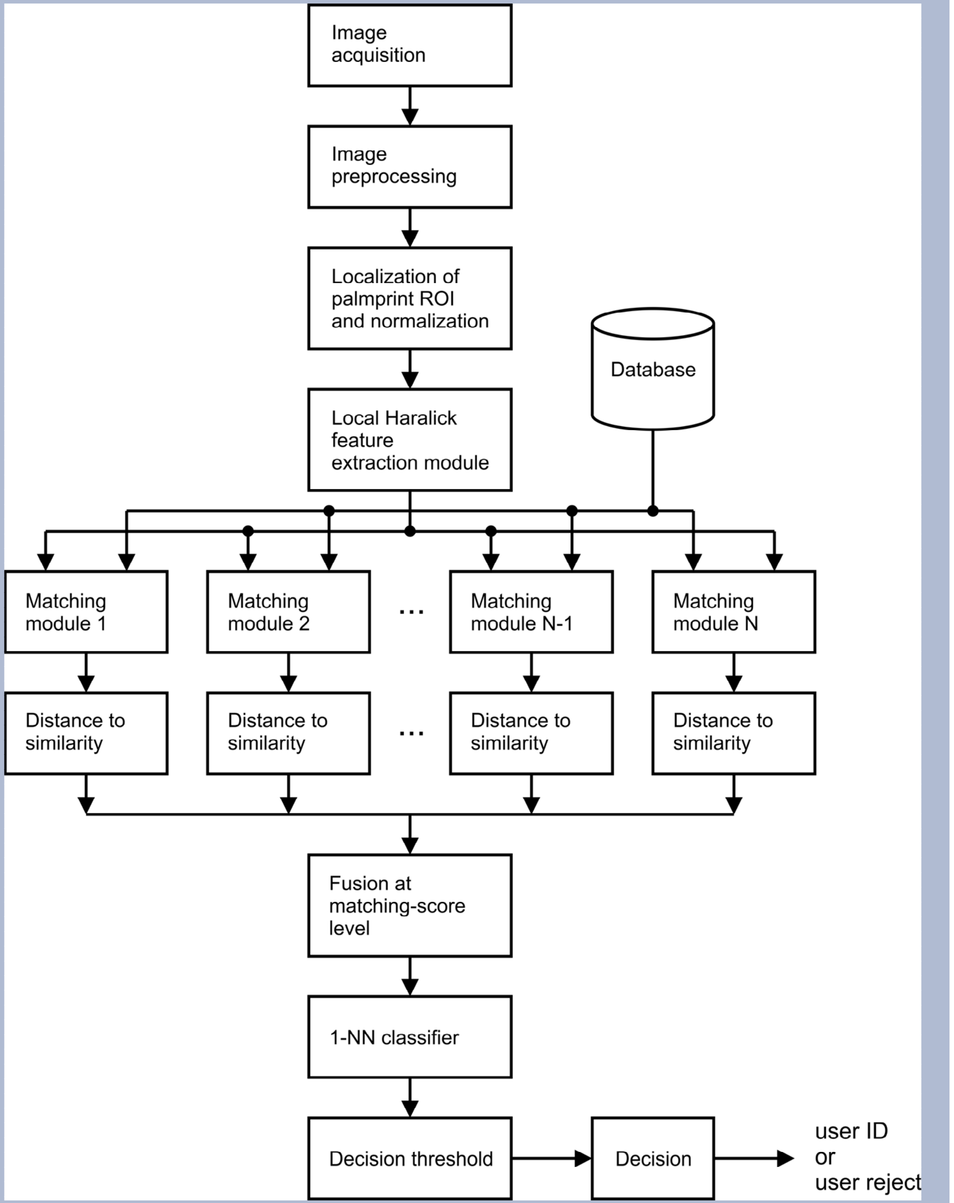
$$TSM_j = \sum_{i=1}^{N} w_i \, s_{ij}$$

- fusion at matching score level:

weighted-sum rule

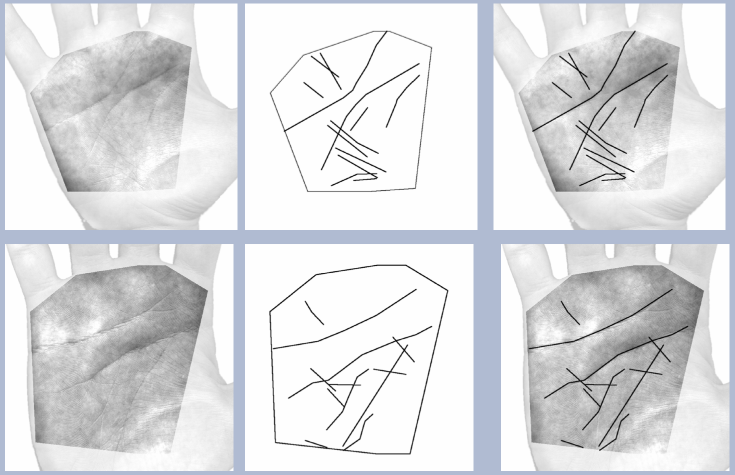
- classification:

1-NN classification rule

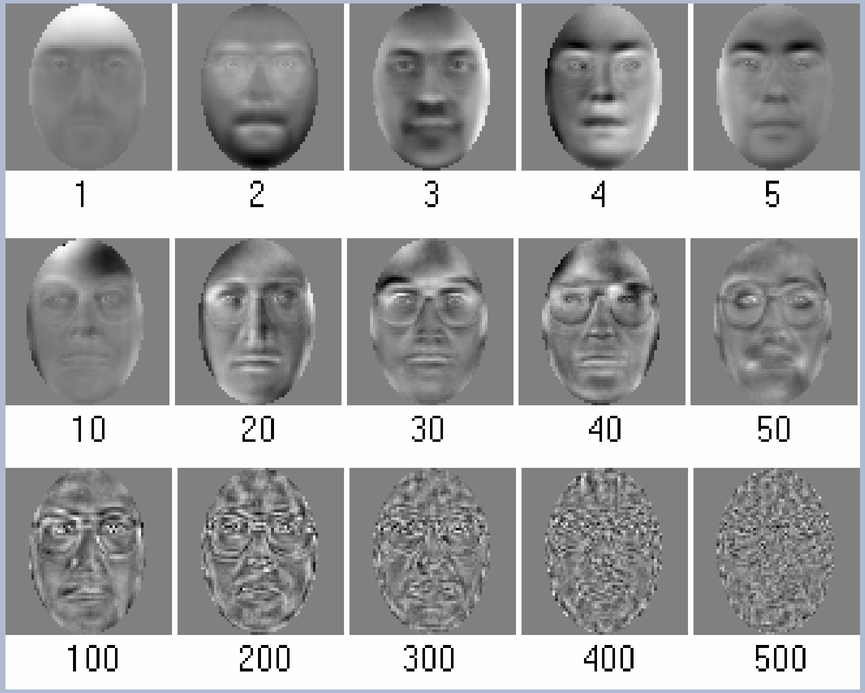


5. Biometric System Based on Fusion of Palmprint and Face Features

- Multimodal biometrics (fusion of face and palmprint / principal lines)



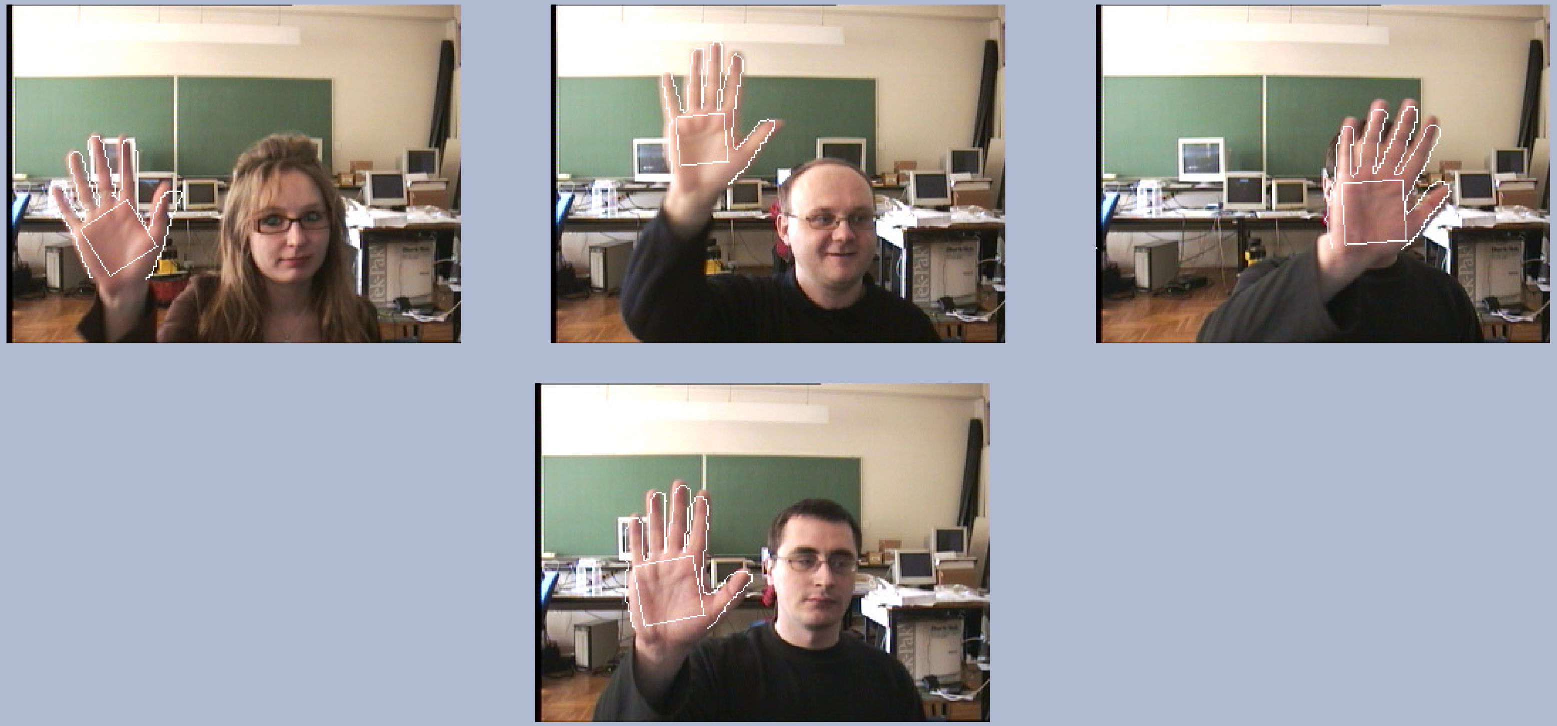
Principal lines



Eigenfaces

(Ribaric, S; Fratric, I; Kis, K.,
A novel biometric personal verification system based on the combination of palmprints and faces, INFORMATICA Volume: 19 Issue: 1 pp. 81-100, 2008.)

6. Hand Detection and Palmprint Localization from Video Sequences



(Fratrić, Ivan; Ribarić, Slobodan,
Local Binary LDA for Face Recognition // Lecture Notes in Computer Science, 6583 (2011) ; pp. 144-155)

European Cooperation in the field of
Scientific and Technical Research

Proposal for a new COST Action:

De-identification for privacy protection in multimedia content

Slobodan Ribarić

University of Zagreb

Faculty of Electrical Engineering and Computing

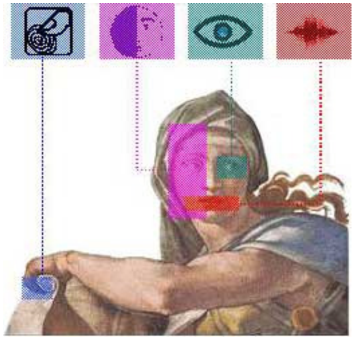
Croatia

History of the Proposal

COST 250

COST 250: Speaker Recognition in Telephony

1994 - 1999



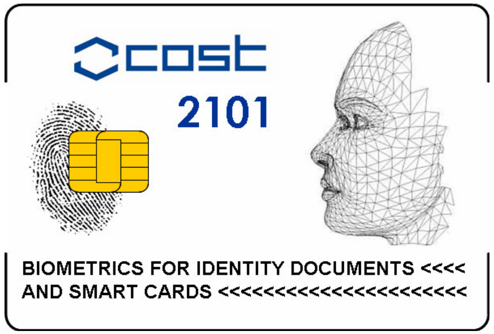
COST 275: Biometrics on the Internet

2001 – 2005

BIOSECURE

Network of Excellence: Biometrics for Secure Authentication

2004 – 2007

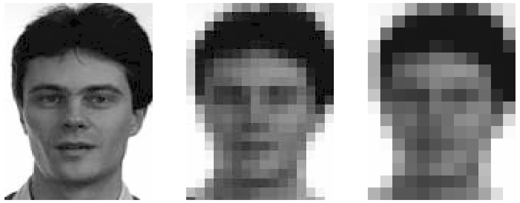

cost
2101
BIOMETRICS FOR IDENTITY DOCUMENTS <<<<
AND SMART CARDS <<<<<<<<<<<<<<<<<<<<<<

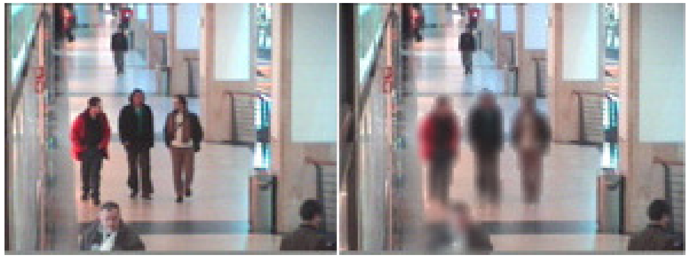
COST 2101: Biometrics for Identity Documents

2006 – 2009

Background and Motivation

- Privacy - the ability of an individual or group to have their personal information and affairs secluded from others, and to disclose them as they choose.
- Multimedia is media and content that uses a combination of different content forms (still images, audio, video, text, animation).
- De-identification in multimedia content - the process of concealing the identities of individuals captured in a given set of data (images, video, audio, text), for the purpose of protecting their privacy.





Background and Motivation

- A variety of scenarios to capture audio-video recordings of people, either for immediate inspection or for storage and subsequent analysis and sharing

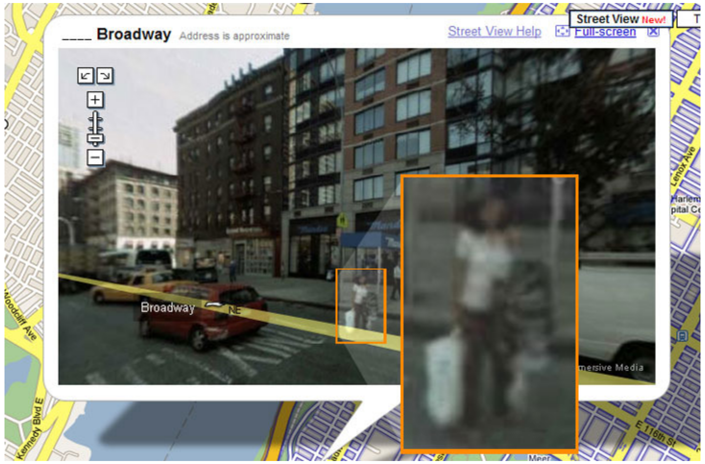
- The widespread use of video surveillance cameras and intelligent networks of sensors in public locations and the use of reliable biometric-based recognition software enable identification and tracking of people in real time

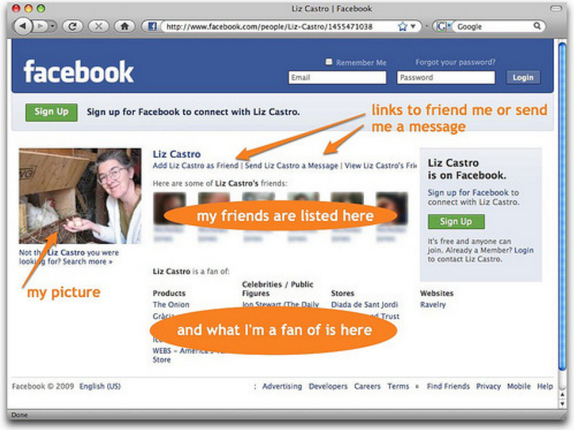
WARNING
THIS AREA IS UNDER 24 HOUR SURVEILLANCE BY PRIVATE SECURITY PERSONNEL

Background and Motivation

- Technologies like “Google Street View” and “EveryScape” provide an additional framework for the invasion of the individuals’ privacy

- Special attention needs to be given to develop de-identification technologies for Internet sites, and predominately social networks (Facebook, YouTube, Twitter)




Liz Castro | Facebook

http://www.facebook.com/people/Liz-Castro/1455471038

Sign up for Facebook to connect with Liz Castro.

Liz Castro

Add Liz Castro as Friend | Send Liz Castro a Message | View Liz Castro's Fri

Here are some of Liz Castro's friends:

Not the Liz Castro you were looking for? Search more »

Liz Castro is on Facebook.

Sign up for Facebook to connect with Liz Castro.

It's free and anyone can join. Already a Member? Login to contact Liz Castro.

Liz Castro is a fan of:

Products	Celebrities / Public Figures	Stores	Websites
The Onion	Jon Stewart (The Daily	Diada de Sant Jordi	Ravelry
Gràcia		Trust	
WEBS - America's Store			

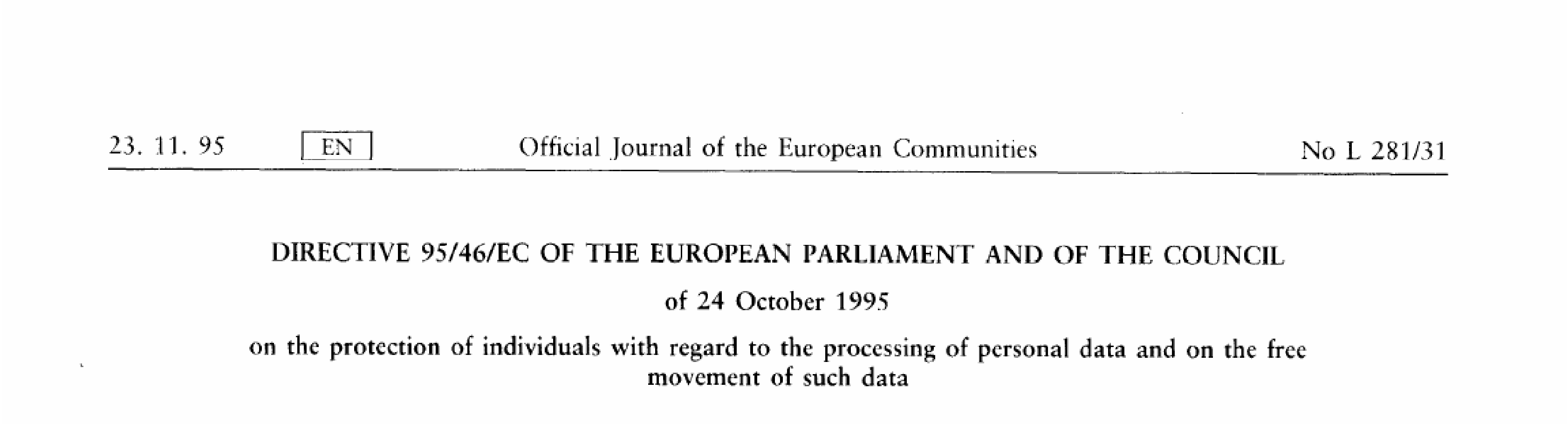
Facebook © 2009 English (US)

facebook
Remember Me
Forgot your password?
Email
Password
Login
Sign Up
Sign Up
links to friend me or send me a message
my friends are listed here
my picture
and what I'm a fan of is here
Advertising Developers Careers Terms Find Friends Privacy Mobile Help
Done

Background and Motivation

- The 1995 Data Protection Directive of the European Union (Directive 95/46/EC) is an operating basic model for handling personal data to protect private information.

- Six basic principles of the Fair Information Practices



23. 11. 95 EN Official Journal of the European Communities No L 281/31

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Background and Motivation

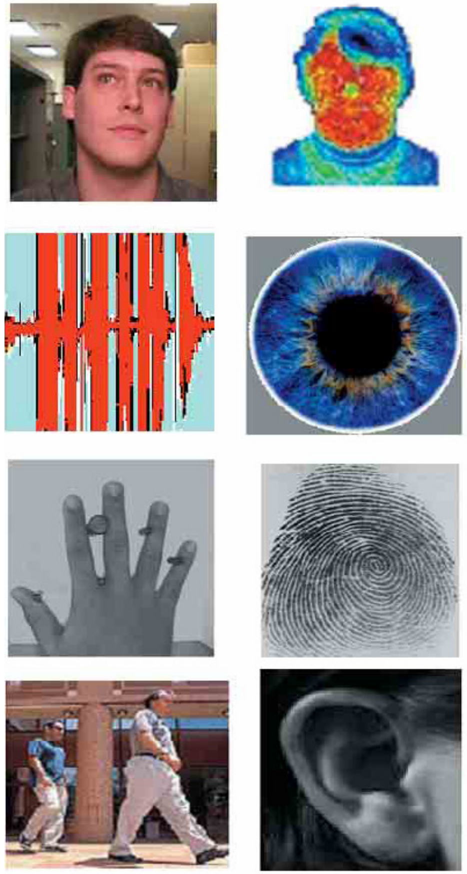
- Identity information extracted from multimedia documents can be of various forms including

  (i) physical biometric data

  (ii) behavioural biometric data

  (iii) soft biometric data

  (iv) non-biometric data (dressing style, hairstyle, speech context, specific social and political context, environment)



Background and Motivation

- De-identification is an interdisciplinary challenge, involving scientific areas:

  (i) image processing

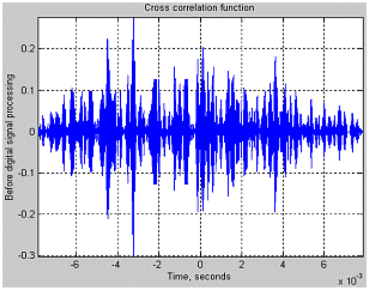
  (ii) pattern recognition

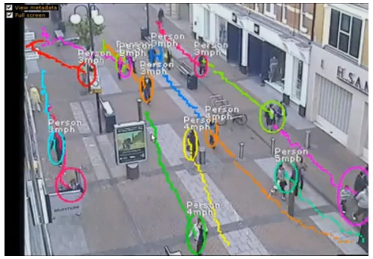
  (ii) speech analysis

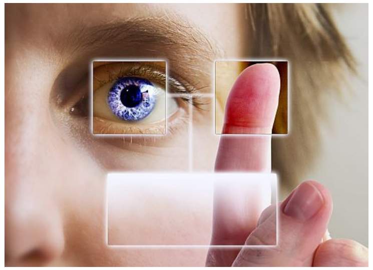
  (iii) video tracking

  (iv) biometrics

  In order to maximise the efficacy and employability of de-identification, the Action will provide the required insights and perspectives on social, ethical, legal aspects of privacy.







Aims and Objectives

- The aim of the Action is:

  (i) to facilitate and promote coordinated efforts in automated person de-identification in multimedia content through the provision of an effective and innovative approach to the integration of relevant European experts, institutions and organisations, as well as non-COST experts

  (ii) to provide the required insights and perspectives on social, ethical, legal aspects of privacy, and to facilitate self-sustaining links and cooperation amongst the researchers, the potential end-users, and system integrators

Aims and Objectives

- The main objectives:

(i) To establish mechanisms for sharing knowledge and technology among experts in different (usually complementary) fields related to automated de-identification and reversible de-identification

(ii) To provide innovative solutions for concealing, or removal of identifiers while preserving data utility and/or naturalness

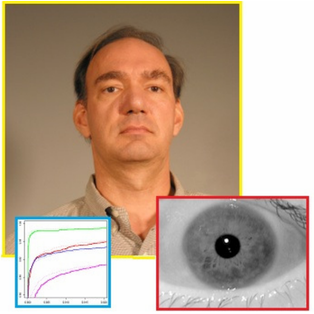
(iii) To investigate reversible de-identification and to provide a thorough analysis of security risks of reversible de-identification.

(iv) To provide a detailed analysis of legal, ethical and social repercussion of reversible/non-reversible de-identification.

(v) To promote and facilitate the transfer of knowledge to all stakeholders (scientific community, end-users, SME)

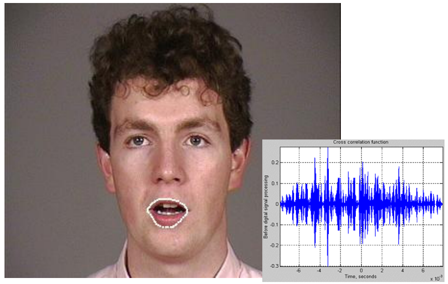
Innovation and Outcomes

(i) Development of novel de-identification methods for dealing with physical and behavioural biometric identifiers, which are simultaneously present in multimedia contents



Examples:

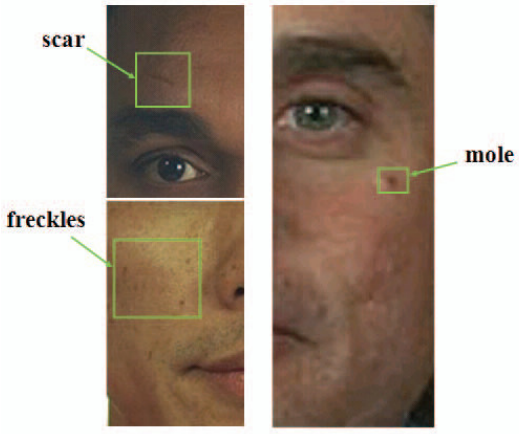
- De-identification methods for simultaneously present face, lip-motion and iris biometric identifiers
- De-identification methods for simultaneously present voice and lip-motion biometric identifiers
- De-identification methods for simultaneously present face and gait biometric identifiers



Precondition: Preserve the data utility and naturalness (eg. De-identification of individuals in videos captured in nursing homes)

Innovation and Outcomes

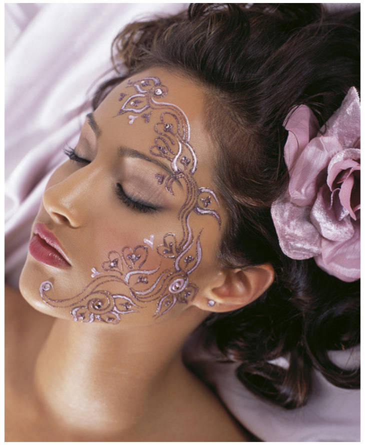
(ii) Development of novel de-identification methods for privacy protection by removing or concealing simultaneously present soft biometric data in multimedia contents



Examples:

- Methods for removing information related to eye colour, gender / age and race
- Methods for removing information related to moles, birthmarks and scars

Precondition: Preserve the data utility and naturalness



Innovation and Outcomes

(iii) Development of de-identification methods for non-biometric identifiers

Examples:

- Methods for removing information related to dressing style and/or hair style
- Methods for removing information about speech context; specific social and political context, and environment

Precondition: Preserve the data utility and naturalness (as much as possible)

Innovation and Outcomes

(iv) Societal aspects

Examples:

- Legal and ethical aspects of sharing and distribution of de-identified data and corresponding re-identification keys
- Redefining privacy protection in the context of de-identification
- Legal prerequisites of deploying de-identification technologies (e.g. notice signs)
- Comparison of social behaviour of people in the presence of surveillance technologies with and without de-identification

Innovation and Outcomes

- The outcomes and results of this Action could be exploited by:

  (i) a wide range of researchers across distinct technical and non-technical disciplines (biometrics, forensics, bioethics, ethics, legal and social disciplines)

  (ii) governmental institutions; companies; international standards organisations; policy makers; stakeholders involved in privacy protection and human rights

  (iii) social media website owners

  (iv) public transport companies

  (v) educational institutions for children, i.e. preschool, primary school, and high school

Applications

- The main classes of applications include:

  (i) Speech-based services

  (ii) Surveillance

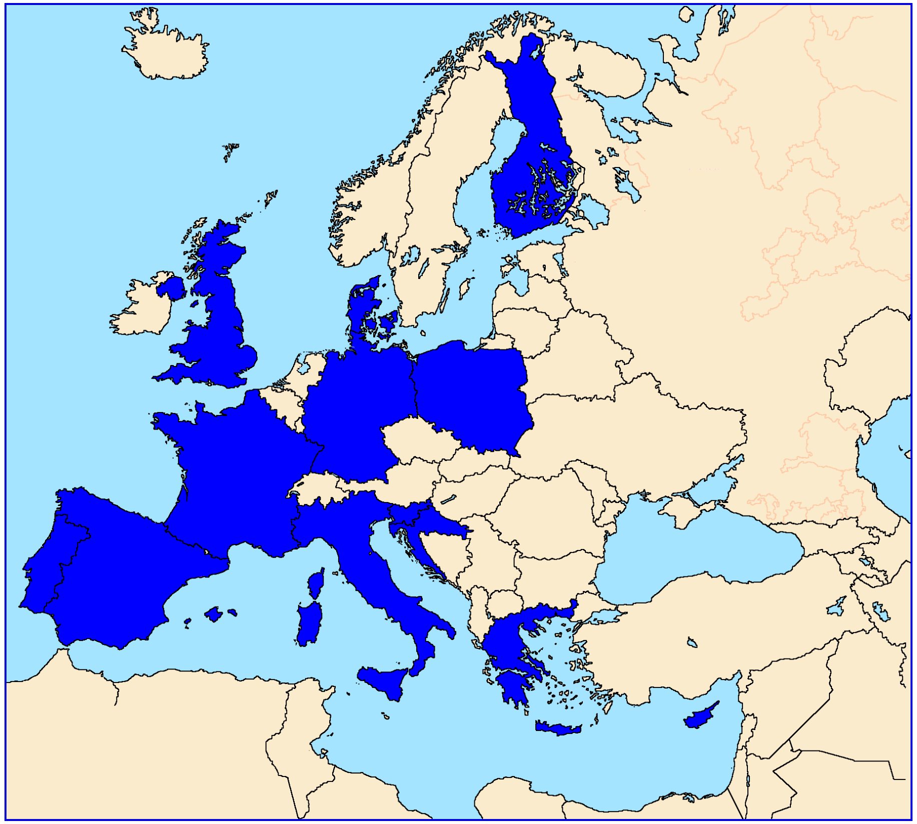
  (iii) Social media websites

- The Action aims to involve experts from ethics, bioethics, legal and social areas as consultants and advisors in all phases of developing de-identification and reversible de-identification methods for different application domains (for example, privacy protection of vulnerable groups: children, mentally and physically handicapped people)

Organization

At this moment:

- 24 institutions from 16 countries of which 2 are non-COST countries (USA and China)
- 33 experts from different scientific domains
- Both academic and industrial partners



Organization

Four working groups:

- **WG1**: De-identification methods for biometric identifiers
- **WG2**: De-identification methods for soft- and non-biometric identifiers
- **WG3**: Applications and added value of de-identified data
- **WG4**: Ethical, bioethical, societal and legal aspects and guidelines for de-identification and reversible de-identification

Organization

Milestones:

- Setting up and maintaining the Action web site
- Creating liaisons with the other COST Actions
- Establishing links with appropriate organisations
- Organising the Action Workshops
- Organizing the training schools
- Activation of inter-partner STSM visits
- Presenting scientific papers at workshops and conferences
- Scientific activities related to networking in the areas of de-identification, reversible de-identification and privacy protection (for example joint research papers, special sessions, common projects)

Organization

Monitoring and evaluation criteria

- Number of partner countries and participating institutions
- Number of national and international projects originating from the Action
- Number of STSMs, Training schools, Workshops,
- Thematic events and participation of ESRs
- Number of access registrations to the Action website
- New directives, guidelines and policy recommendations
- Number of joint papers
- Citation reports

Key to Success

- We are delighted to have received such positive and encouraging comments through EEP Consensus
- Novel area of research with strong multidisciplinarity
  - New technical and societal challenges
  - Importance for the society in general (Data Protection Directive of the European Union)
- Strong networking of researchers and institutions from different technical and societal areas of expertise
- Involvement of the leading EU experts in domain of social and ethical aspects of biometrics and data protection law
- Established cooperation between research groups
- Collaboration with other complementary COST actions and projects within European Framework Programs
- Involvement of ESRs is an essential contributor to the sustainable success