MOBILE-HEALTH: MONITORING AND SECURITY

Dr. Nikolaos Bourbakis

Wright State University

Assistive Technologies Research Center

I would like to thank the
MobileHealth-2011 Organizers for the very successful meeting, but especially I would like to thank Professor Nikita for inviting me to share some of my views on
Health Monitoring-Security with you

Outline

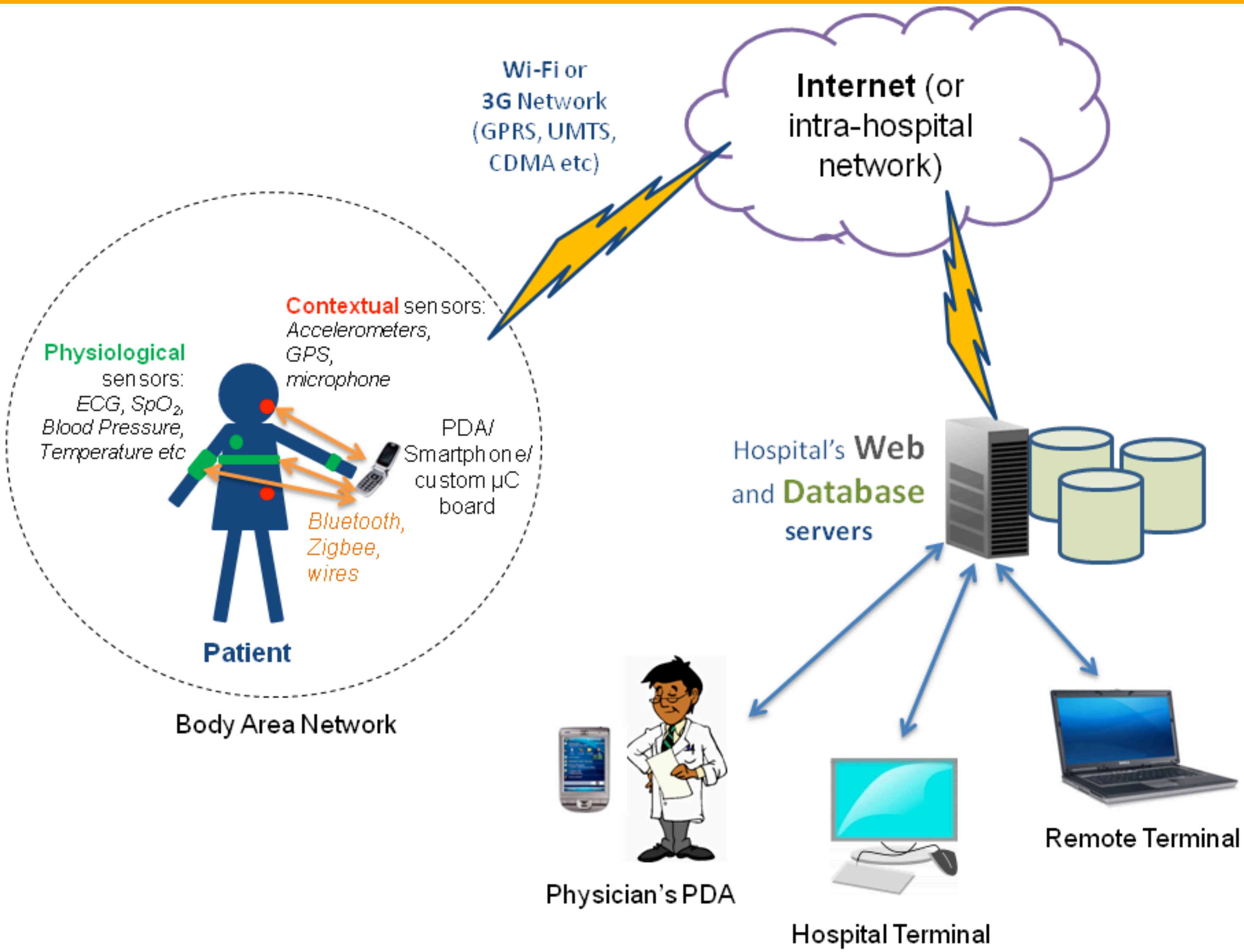
- **Motivation**
- **Health Monitoring**
  - **Health Information Exchange**
  - **WHMS**
- **Security-Privacy**
- **Protecting Health Information**
- **(Compression – Encryption – Hiding)**
- **Authentication-Authorization**
- **(Biometrics : Iris – Voice – Fingerprint)**
- **Conclusions**

Motivation: Technology and Reality

- The necessity of **continuous monitoring** of persons at risk and the increasing prevalence of chronic conditions among our aging population present great challenges for any healthcare system. Delays in diagnosis impede preventive treatments, and the associated complications are costly both for patients and taxpayers. For example, costs associated with elderly 'falls' are staggering. In 2000, direct costs of all fall injuries, for people 65 and older, exceeded $19B, (2020 → $54B). **Early diagnosis** with continuous monitoring systems clearly is critical to the economic sustainability of a healthcare system. High quality but low-cost treatments, including early diagnosis and prevention, will also significantly contribute to the well-being of persons at risk.
- Continuous monitoring of patient private health data with no secure protection is not acceptable in today's digital world of hijacking. Monitoring people at risk with mobile devices requires **a secure way of health information exchange** and a secure authentication/authorization access of these valuable data.

HEALTH INFORMATION EXCHENGE

MOBILE-HEALTH: Health Information Exchange



Health Monitoring Issues & Prognosis Prototype

- **Health demographics, IT-based health management solutions**
- **Wearable health monitoring systems** (WHMS)
- **The Prognosis WHMS system**
  - *The Prognosis WHMS architecture*
  - *Extraction of fuzzy symptoms from physiological data*
  - *Decision support based on a fuzzy regular language approach*
  - Use-Device Interaction and system simulation
  - A patient-adaptive health-learning strategy
  - System prototype based on off-the-shelf components

Some Health Demographics

- Fact: the **global population** is both **growing** and **ageing!**
- There are currently more than 650 million people over the age of 65. (there will be double as many within a decade)
- There has also been an **increase of chronic age-related diseases**, such as: congestive heart failure, dementia, sleep apnea, cancer, diabetes and chronic obstructive pulmonary disease.
- In addition to that, approximately 33% of persons over the age of 65 and 50% of persons over the age of 85 experience a **fall** each year.
- Health Monitoring **Children at Risk**
- **Health care costs** are increasing, quality of life and productivity are reclining and in many cases family members serve as primary care assistants

IT-based health management solutions

- Information and communication technologies are expected to provide the means to realize **personalized, low cost and citizen-centered healthcare solutions.**
- As a result, a variety of **health information networks** is being developed that link hospitals, healthcare professionals, care providers, laboratories and ultimately people's homes. (closed-loop health monitoring, management and delivery system)

Personal Health Monitors

- In the context of distributed health information networks, **personal health monitors** (PHS) can enable real-time physiological, activity and mental status monitoring.
- This can lead to **early detection** and diagnosis of critical health changes, which may not be observed during routine short-time check-up visits to doctors.
- Thus PHS could enable **prevention** of a variety of health hazards and risks while also saving billions of dollars annually.
- PHS constitute the front-end of the components of the health information network:
  - Secure collection of physiological data from the patient
  - Secure and reliable transmission of data to a remote monitoring location.

Personal Health Monitors

- Traditionally, "crude" and bulky monitoring devices have been employed to collect patient vital signs.
- For example, bed-side Monitors:

- *Problems* with such systems:
  - *Size & cost*
  - *Too many wires*
  - *Patient must be immobilized*
- Unsuitable for **ubiquitous, unobtrusive, long-term** and **low-cost** health monitoring
- **Small, low-weight, portable, autonomous** devices are required for this goal.

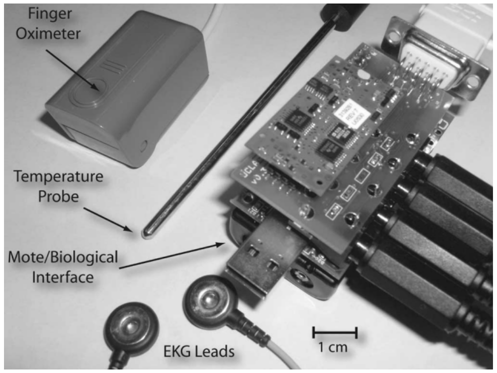
Wearable Health-Monitoring Systems (WHMS)

Wearable Health-Monitoring Systems (WHMS)

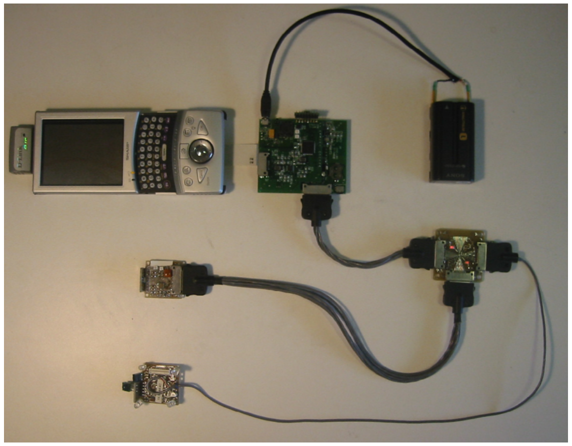
- Comprise a variety of miniature **wearable** and even **implantable sensors.**
- Realize **ambulatory monitoring** of the user's health condition.
- Enable **long-term** unobtrusive measurement of physiological parameters and vital signs (such as heart rate, blood pressure, body temperature, respiration rate, oxygen saturation, electrocardiogram (ECG) etc.) through daily activities.
- Provide **real-time** updates about the user's health status and possibly generate **alarms** in case of detected **emergencies.**
- Could lead to **consumer operated/based** health management and early risk detection & prevention.

R&D in WHMS – Research Prototypes

- **Category 1**: Systems based on a microcontroller board and/or on custom designed platforms



Bi-Fi (Univ. of California in LA)



LiveNet (MIT, Media Laboratory)

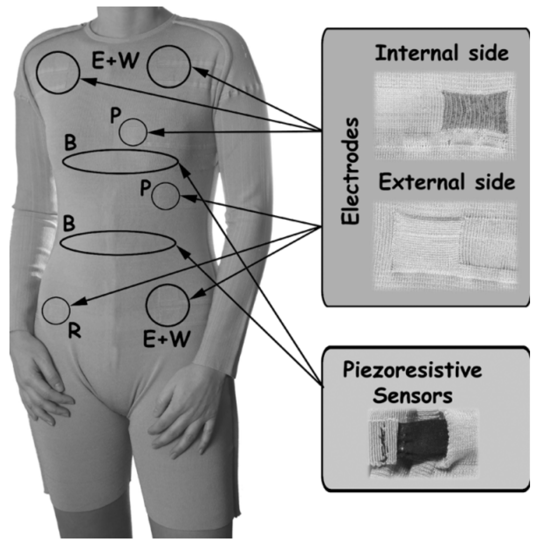
AMON (multiparameter monitor, wrist-worn device, EU-funded project)

RTWPMS (EE Dept., Nat. Taiwan Un.)

R&D in WHMS – Research Prototypes

- **Category 2:** WHMS based on "smart textiles".

HealthWear
(EU-funded
project)

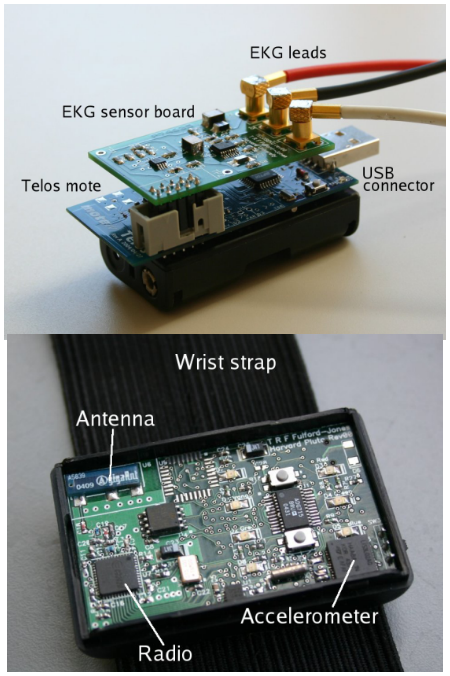


WEALTHY
(EU-funded
project)

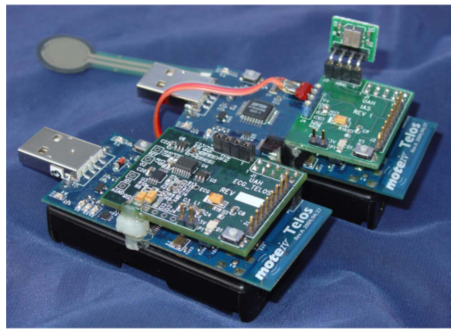
MERMOTH
(EU-funded
project)

R&D in WHMS – Research Prototypes

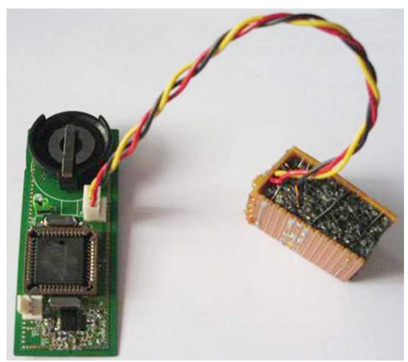
- **Category 3:** Mote-based Body Area Networks.



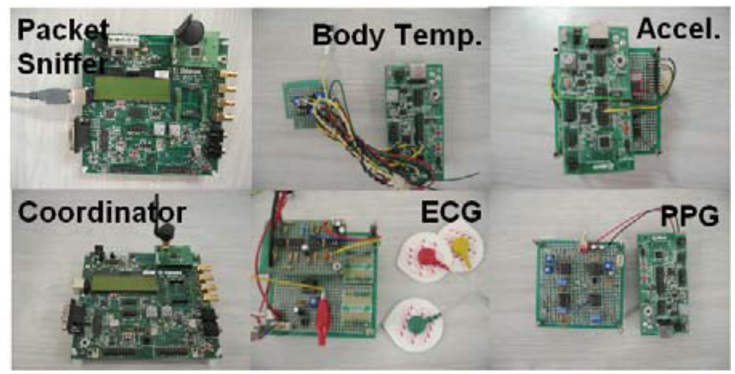
CodeBlue
(Harvard Univ.)



Univ. of Alabama in Huntsville



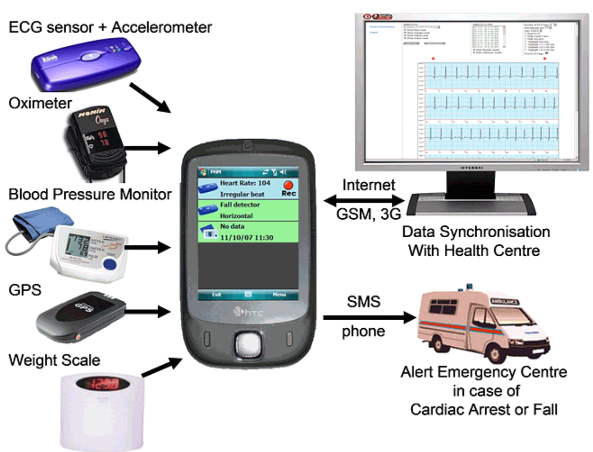
Univ. of Newcastle, AUS
(Medical Implant Band RF)



Hanyang Univ., South Korea

R&D in WHMS – Research Prototypes

- **Category 4:** WHMS based on commercial Bluetooth sensors and smart-phones.



Personal Health Monitor (Univ. of Tech., Syndey)

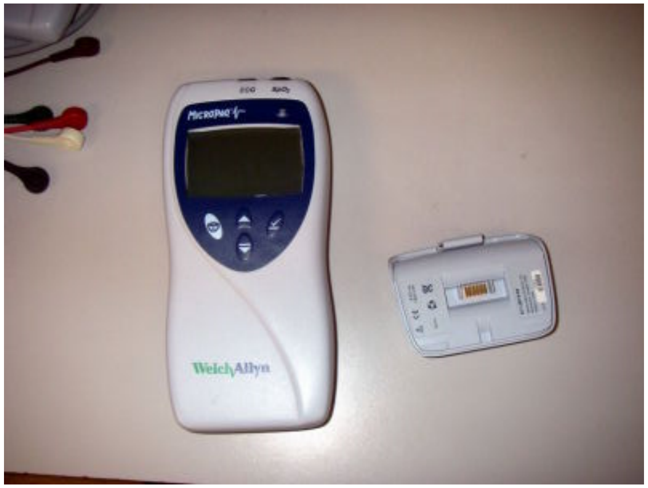
HeartToGo
(ACT Lab, Univ. of Pittsburgh)

Nat. Taipei Univ. of Tech, Taiwan

Commercially available WHMS

LifeShirt
(VivoMetrics)

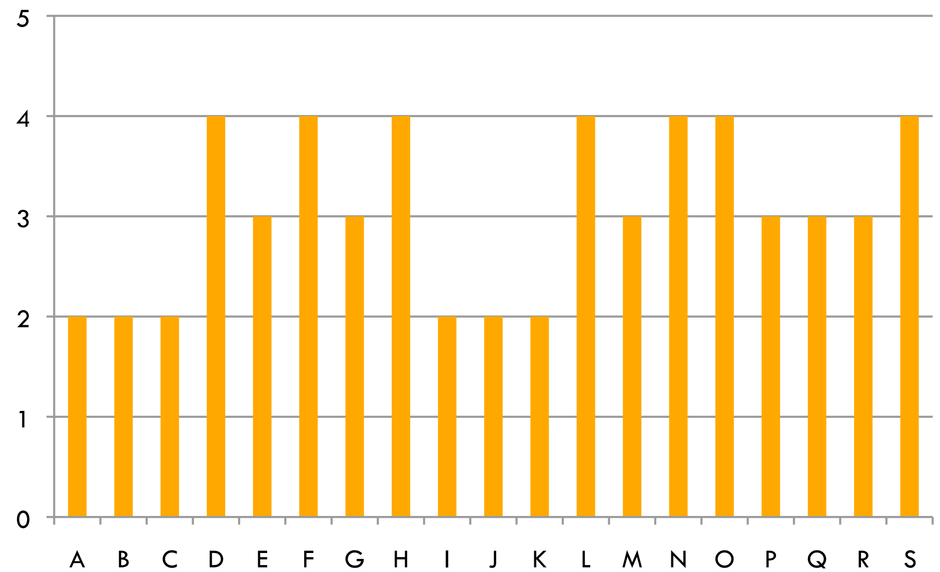
WristCare
(Vivago)



MicroPaq Monitor
(Welch Allyn)

Maturity Evaluation

	Patient's perspective	Physician's perspective	Manufacturer's perspective	Average
F1	3	2	1	2
F2	3	2	1	2
F3	3	1	2	2
F4	2	3	3	3
F5	3	2	2	2.3
F6	3	3	3	3
F7	3	2	2	2.3
F8	1	1	3	1.7
F9	3	2	1	2
F10	3	3	3	3
F11	3	3	3	3
F12	3	1	3	2.3
F13	2	3	2	2.3
F14	3	3	3	3
F15	2	2	2	2
F16	3	2	2	2.3



Maturity scores for the selected systems (1=low, 2=medium-low, 3=good, 4=high, 5=maximum)

- The above graph was produced as a **weighted average** of every graded feature.
- **Feature**-specific capabilities were **graded** as being {very low, low, medium, high, very high}

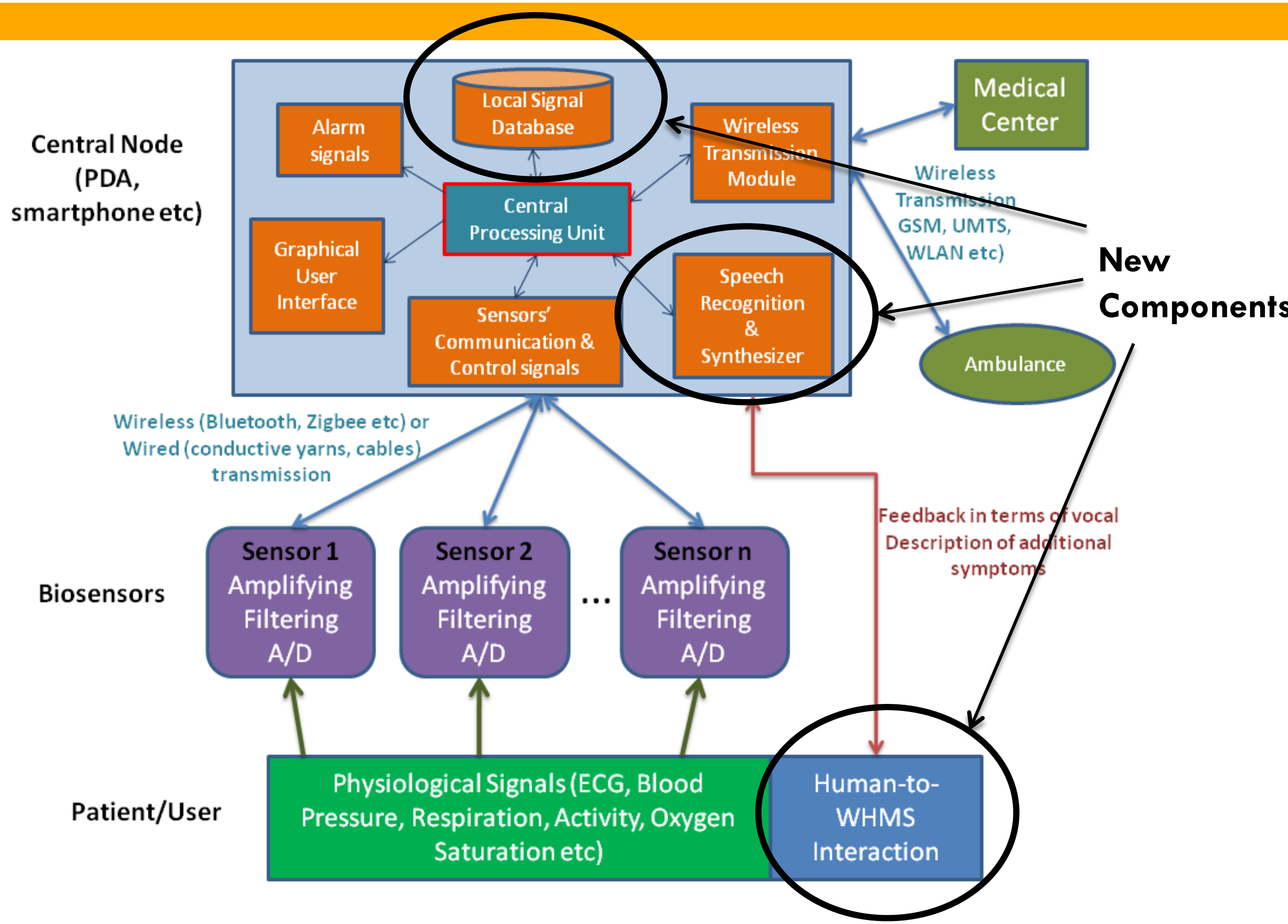
Discussion

- None of the systems reached maximum maturity score.
- Systems that reached high scores include:
  - Several smart textile-based systems (high wearability, user comfortableness, **reliability** due to good contact between the skin and the bio-sensors)
  - Some Bluetooth sensor + smart-phone –based systems (utilization of commercially available components + they constitute a first approach towards **interactive** or **patient-adaptive** WHMS)
- Several common issues have been identified in current WHMS prototypes and point out future challenges:
  - **Battery technologies and energy scavenging**
  - **Security of private information**
  - **Further improvements in sensor miniaturization and efficiency**
  - **Clinical validation**
  - **Standardization and cooperation at all levels**

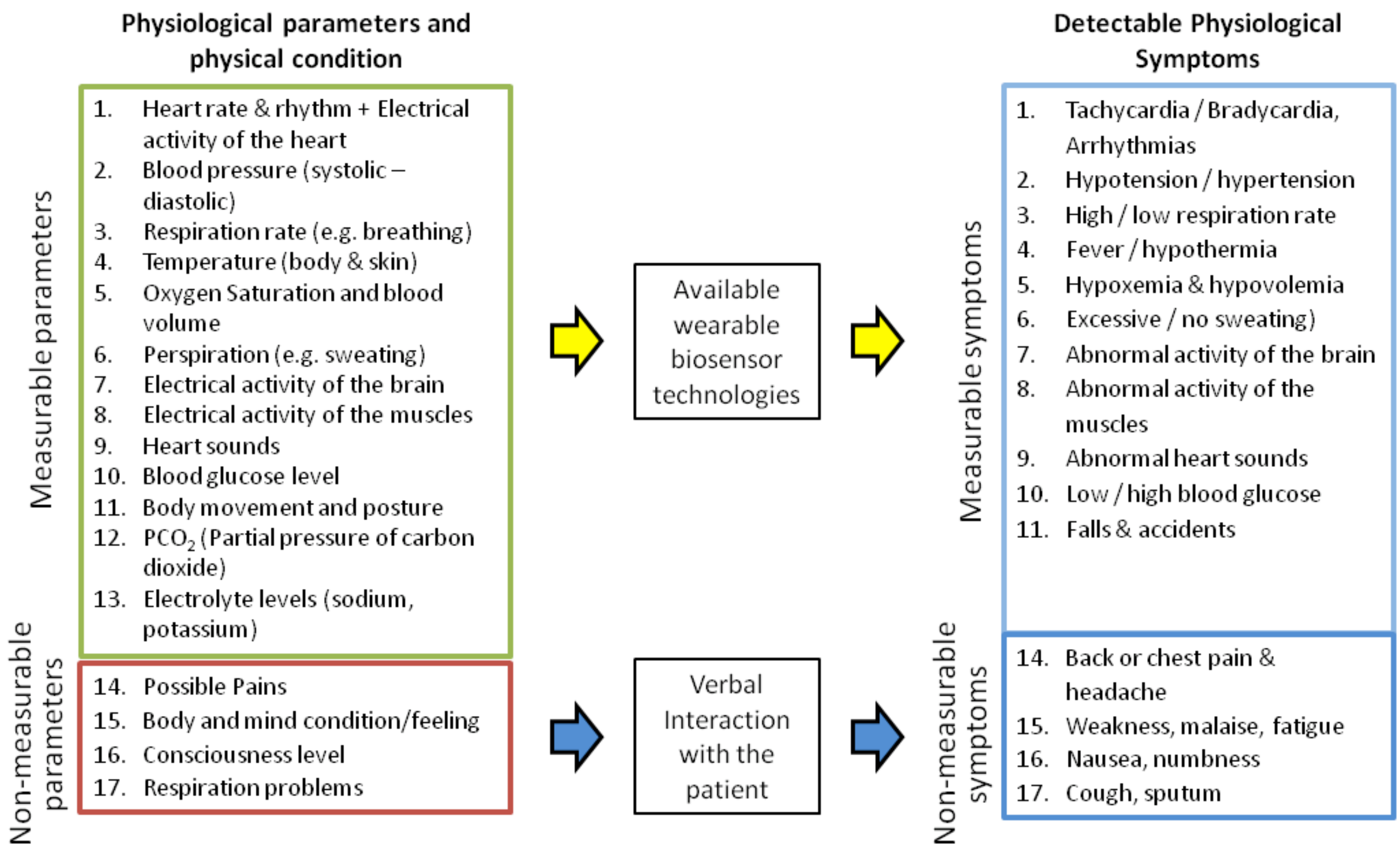
The Prognosis system-prototype

- Prognosis WHMS architecture
- Extraction of fuzzy symptoms from physiological data
- Decision support based on a fuzzy regular language approach

Prognosis WHMS architecture



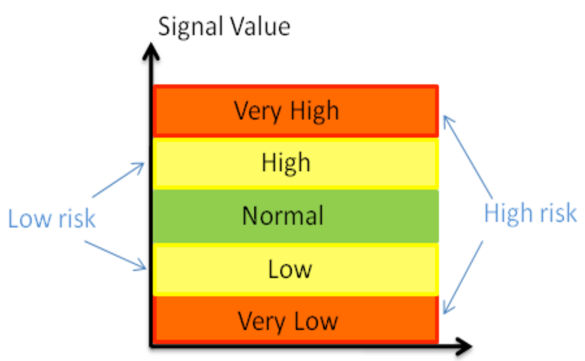
Symptoms and body signal correspondence



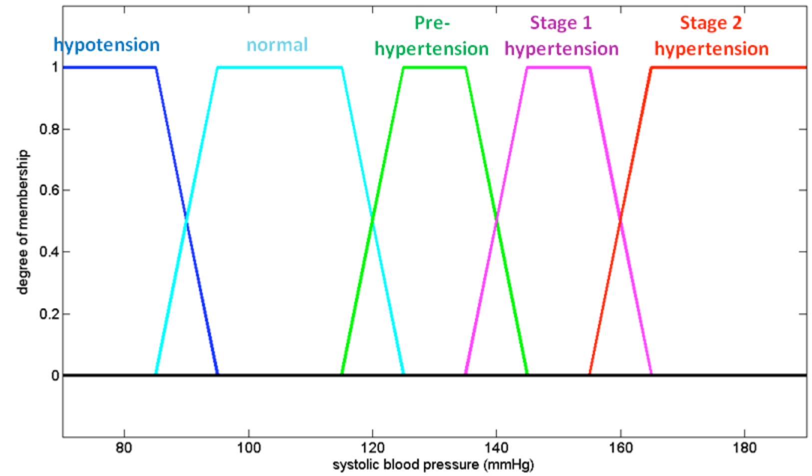
Fuzzy health symptoms

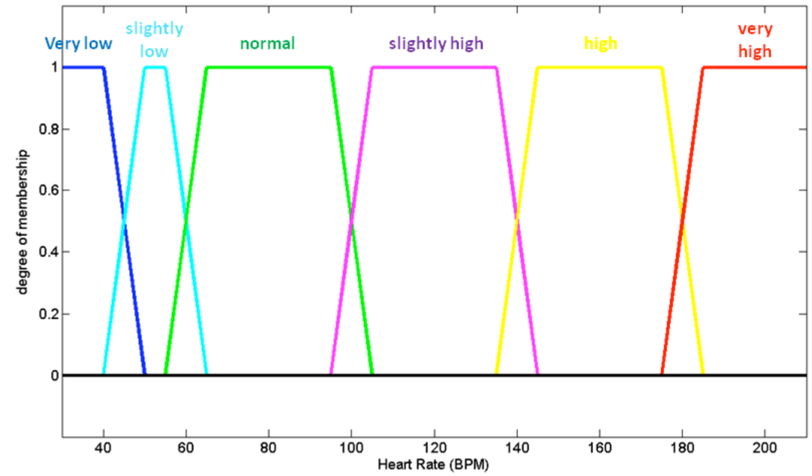
- The various bio-signals that can be captured by a WHMS can give rise to **normal** (benign) or **alarming** health states.
- **Co-occurrence** of specific symptoms under certain conditions can indicate the presence of a specific health risk.
- However the degree of dangerousness (or severity) and the degree of actual occurrence of a specific symptom is **fuzzy** in nature:
  - "Health is a matter of degree, illness is a matter of degree and disease is a matter of degree", *Kazem Sadegh-Zadeh, philosopher of medicine*

Extraction of fuzzy symptoms from scalar bio-signals



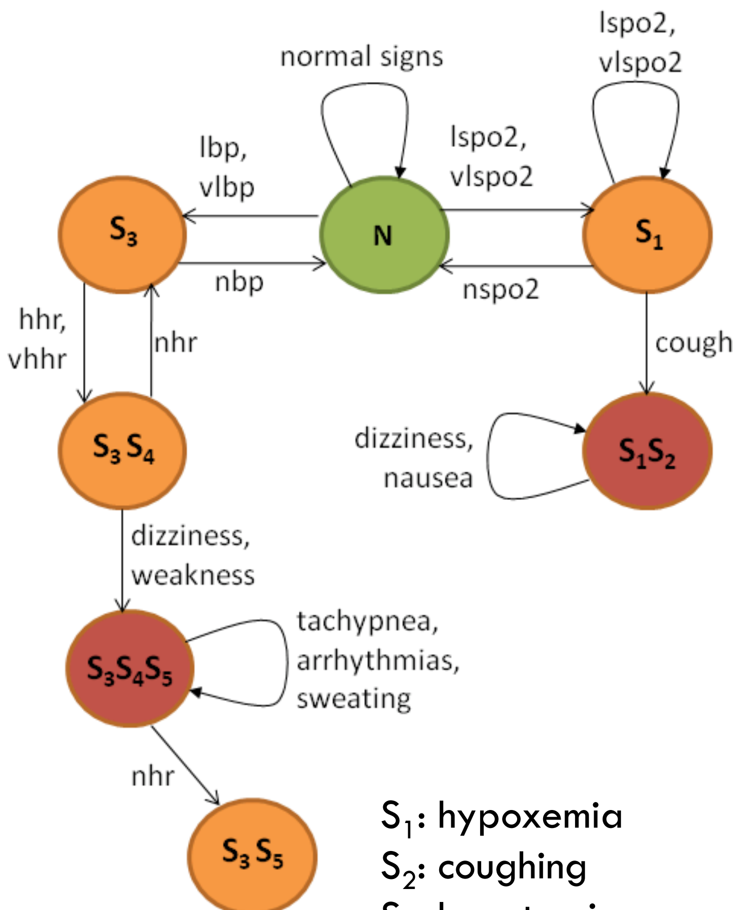
Crisp Symptoms





Fuzzy Symptoms

Prognosis Formal Approach



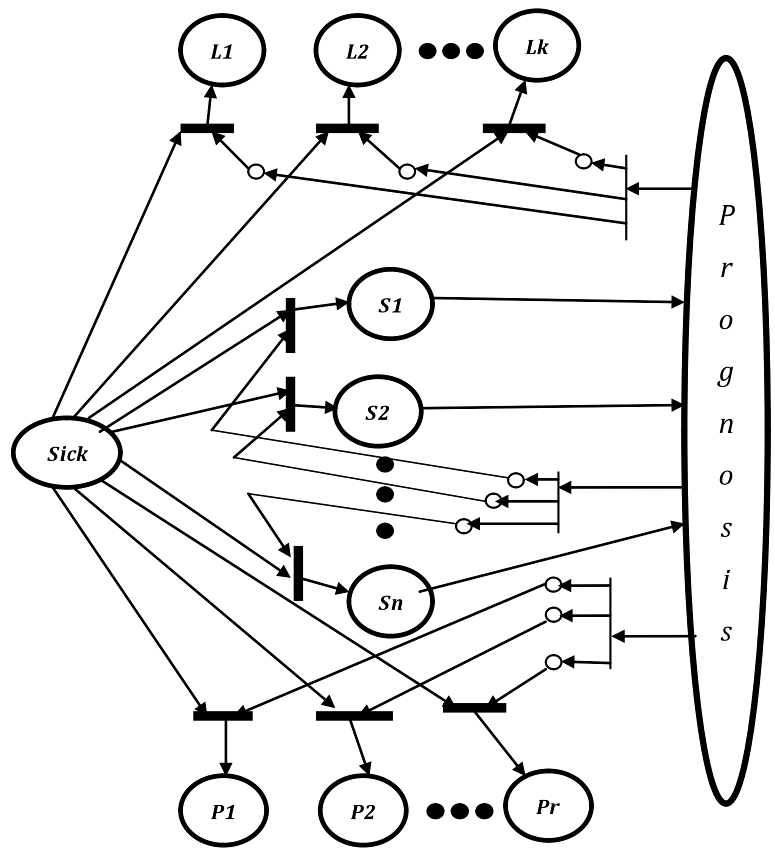
S_1: hypoxemia
S_2: coughing
S_3: hypotension
S_4: tachycardia
S_5: dizziness, weakness or nausea

Current State	HR	SpO2	BP	Resp Rate	VF	ECG
N 1.0	n 0.9	n 1	n 0.7	n 1	-	n 0.9
N 0.95	n 0.8	n 1	lbp 0.6	n 1	-	n 0.9
S_3 0.64	n 0.7	n 0.9	lbp 1	n 1	-	n 0.8
S_3 0.78	n 0.6	n 0.9	vlbp 0.6	n 0.9	-	n 0.9
S_3 0.79	hhr 0.6	n 0.9	vlbp 0.8	n 0.8	-	n 0.8
S_3S_4 0.61	hhr 0.9	n 0.8	vlbp 1	n 0.7	-	n 0.8
S_3S_4 0.73	vhhr 0.7	n 0.8	vlbp 1	n 0.6	-	n 0.7
S_3S_4 0.76	vhhr 0.9	n 0.8	vlbp 1	hrr 0.6	dizzy-ness	pvc 0.6
$S_3S_4S_5$ 0.57	vhhr 1	n 0.8	vlbp 1	hrr 0.7	-	pvc 0.6

User-Device Interaction and system simulation

<u>Prognosis *Interaction*</u>

- The user of the *Prognosis* wearable platform should be able to **interact** with the system in a meaningful and helpful manner:
  - This will help and hopefully also motivate the user to have an even more **active role** in his **personal health management**
  - Most importantly it will provide a greater **context** for physiological measurements which would have been otherwise impossible to capture in a remote and **unsupervised** health-monitoring **scenario**
- Sphinx-4 speech recognition software package is being used to model the Human-Device Interaction (**HDI**)



An HDI scenario

User: <Feels a slight chest discomfort and some of his vitals start to go out of range>

System: *Some of your vitals are out of regular range. Do you need immediate help?*

User: *No*

System: *Do you have any other symptoms?*

User: *Yes*

System: *Please describe your symptoms*

User: *I have slight chest discomfort.*

System: <the system does not acknowledge the user's phrase>

Please state your symptom again in a brief manner

User: *chest pain*

System: <Recognizes the symptom>

Is the symptom intermittent or continuous?

User: *continuous*

System: *Is the symptom instantaneous or persistent?*

User: *persistent*

System: *Is the pain radiating to your arms?*

User: *Yes*

System: *Is the pain aggravated by movement or breathing?*

User: *No*

System: *Are you experiencing any other symptoms, such as hemoptysis or sputum?*

User: *No*

System: *Describe your pain level on a scale from one until ten*

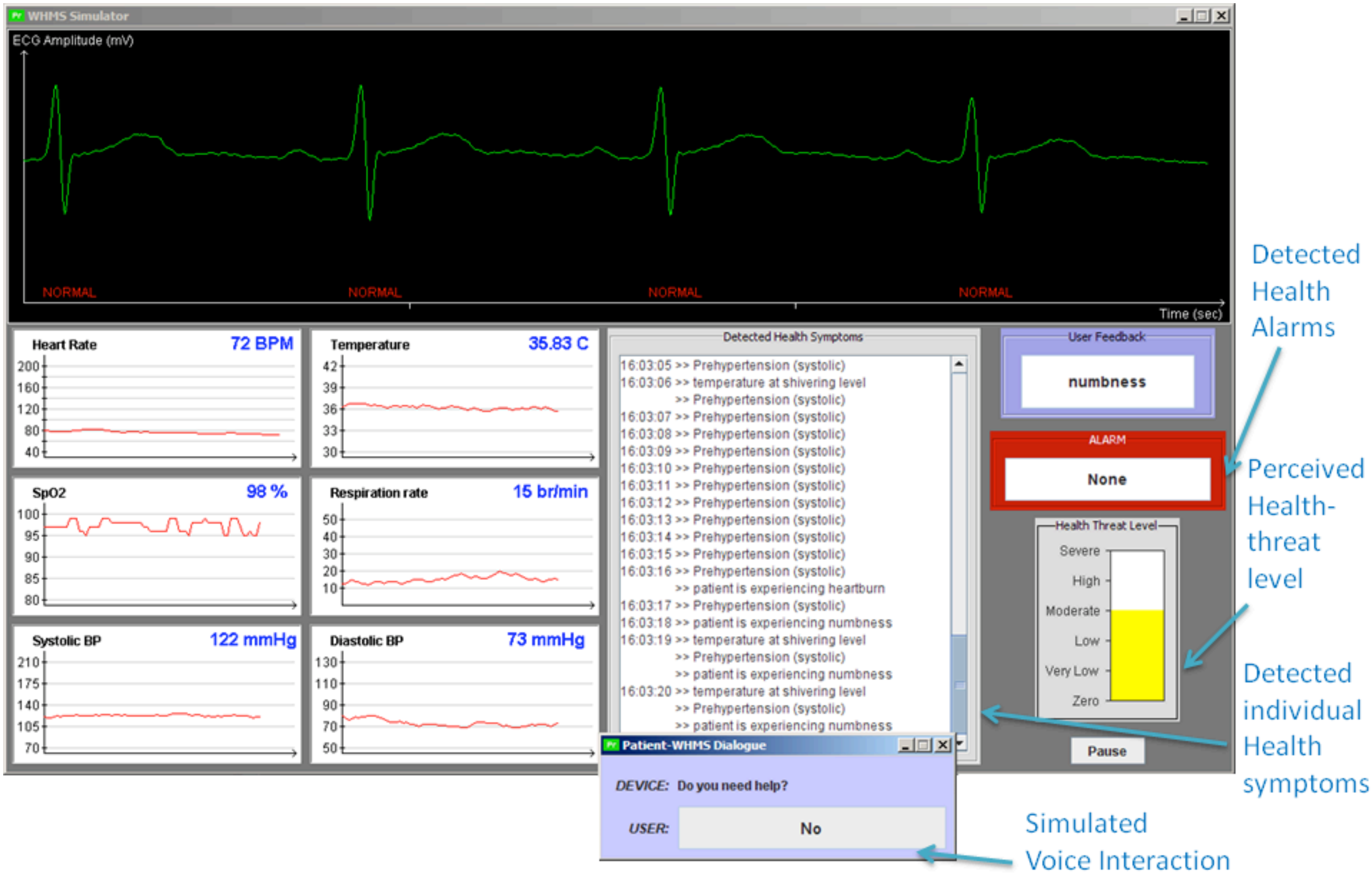
User: *five*

System: <decides that according to the user's answers and his recent vital signs the user could be in an alarming health condition>

< notifies the medical center by sending an alarm message via GPRS>

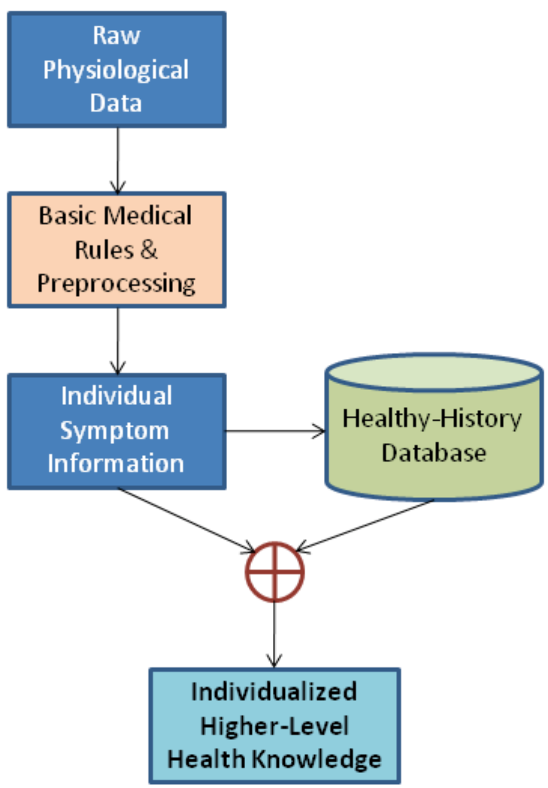
I have notified the medical center about your current condition

Simulator GUI



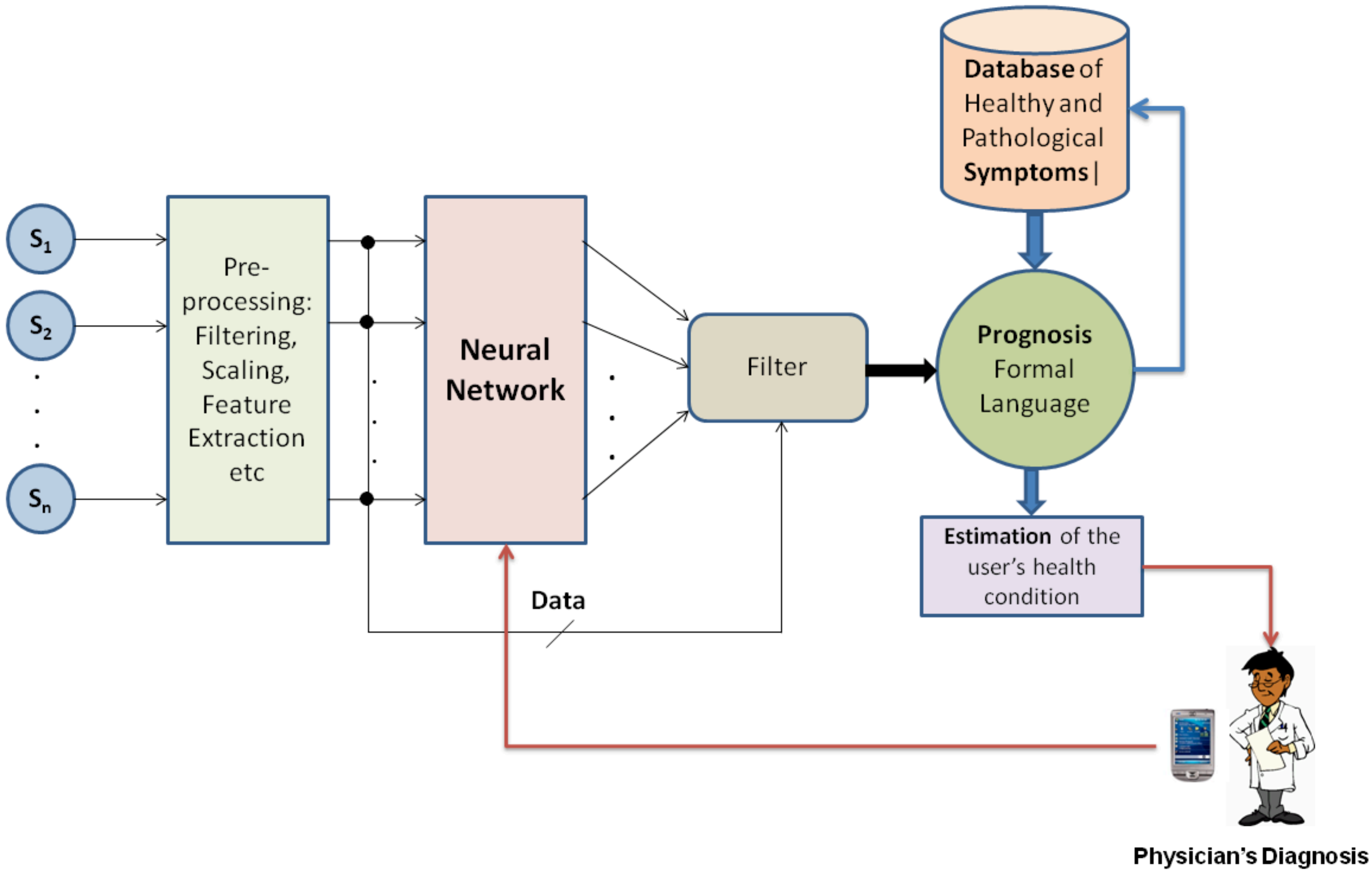
A patient-adaptive health-learning strategy

Healthy-history Database Concept



- We want the multi-sensor wearable health monitoring device to be able to extract **higher level of information** about the user from the recorded physiological data.
- For example:
  - HR under 60 BPM → bradycardia
  - HR over 100 BPM → tachycardia
  - What does a HR measurement of 130 BPM mean**?**
  - To answer the previous question, the user’s physiology, medical history and his current context need to be accounted for.

Patient-specific embedded decision support

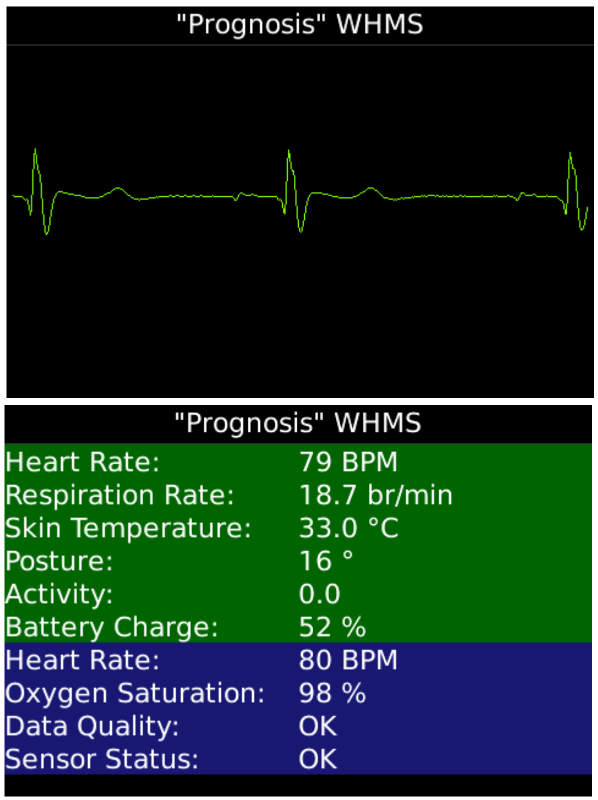


System-prototype based on off-the-shelf components

Prognosis *Prototype wearable platform*

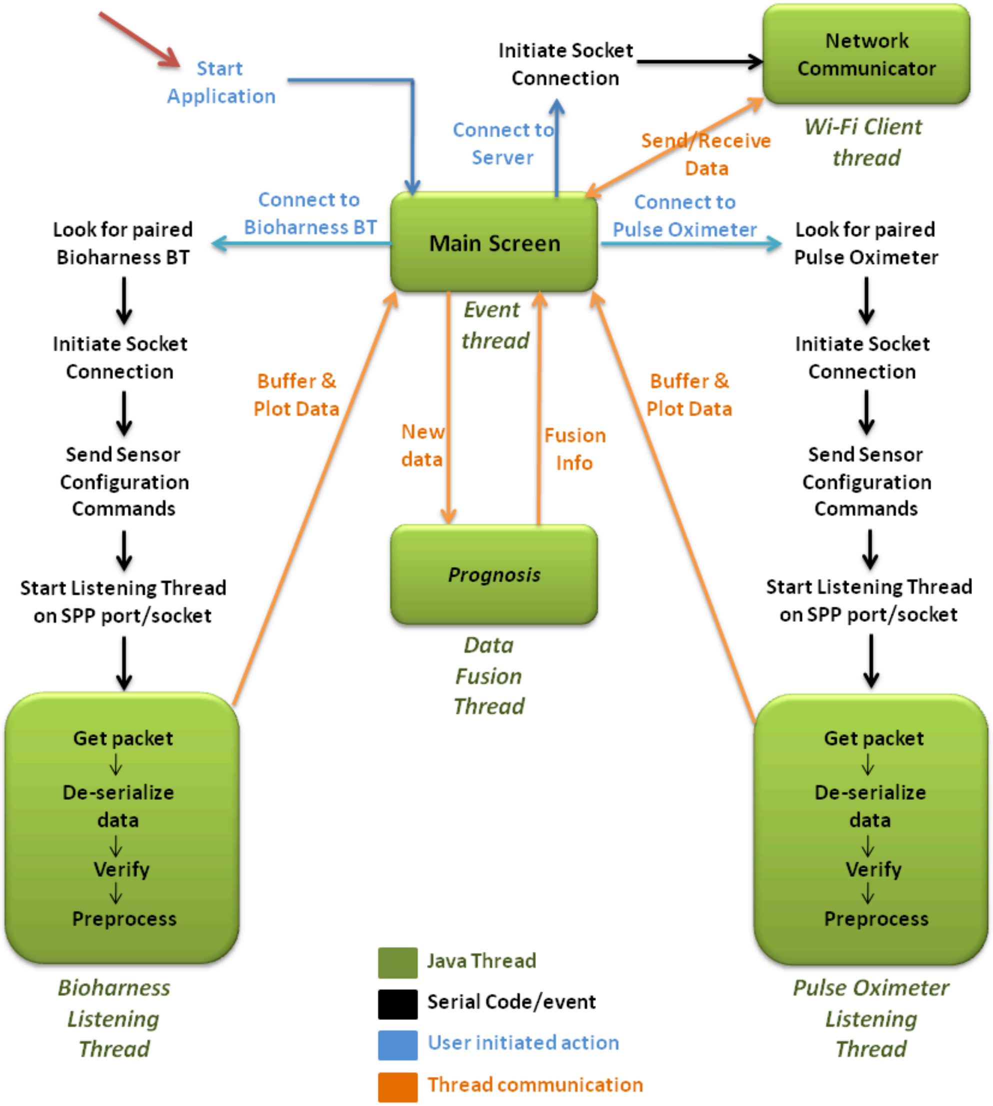
- System prototype is based on commercial **off-the-shelf** components:
  - **BlackBerry Bold** 9000 smart-phone (624 MHz processor, J2ME, multi-programming/multi-threading support, Bluetooth piconet support)
  - **Bioharness BT** (chest belt using dry contact electrodes & measuring ECG, heart rate, respiration rate, skin temperature, activity, posture)
  - **Nonin** Bluetooth **Pulse Oximeter** (measures pulse waveform, oxygen saturation, heart rate)
  - Bluetooth Blood Pressure and Glucose Monitors (to be added)

Prognosis System Operation



- Smartphone allows for multiple simultaneous Bluetooth connections (Serial Port Profile).
- Set up a Body Area Network, by initiating a separate **thread** to communicate with every individual bio-sensor:
  - Configures the sensor remotely.
  - Collects and de-serializes packets.
  - Verifies and preprocesses new data.
  - Sends the extracted data and features to the main thread for plotting and **data fusion**.
- The main thread will eventually fuse all collected physiological measurements within a certain time-frame to produce an estimate of the user's health condition (*Prognosis* formal language).

J2ME Software Architecture



GUI of the remote monitoring application

Conclusion

- This research attempts to establish an innovative interactive, self-adaptive and intelligent WHMS paradigm:
  - We defined a novel model based on a **fuzzy regular formal language** to describe the current state of health of the WHMS user, which considers symptom **ambiguity** and **causal relationships** between various disorders and symptoms to derive a thorough **estimation** with a certain degree of **confidence**.
  - It is hoped that such a solution can lead to **early detection** and hopefully also to prevention of health episodes by carefully following, capturing and describing the **health trends** recorded from physiological and contextual sensors.
  - System modeling based on SPNs and the corresponding simulation helped us define the operational framework of the Prognosis solution.
  - We have developed a patient-learning scheme, which through a learning phase will be able to embed
  - System implementation based on state-of-the-art components.

SECURITY : CRYPTO-BIOMETRIC SCHEMES

Outline

- Motivation and Other
- Why Secure Processors
- SCAN Secure Processor
- Compression-Encryption-Hiding
- Why Biometrics Authentication
- Voice-Iris-Fingerprint
- How to Secure Health Information Exchange
- Conclusion

MOTIVATION

The CSI Computer Crime and Security Survey analyzes important long term computer security trends every year:

- **Unauthorized use of computer systems**

- **Security related incidents from outside, as well as inside, an organization**

- **Types of attacks or misuse detected and Virus Immunity**

- Actions taken in response to computer intrusions

Why Secure Processors

SOFTWARE BASED SECURITY

- **Using serial code**
  - Causing piracy a little bit difficult, but not too much
- **Install/update anti-virus software**
  - Defend from only known viruses, limitations
- **Firewall/intrusion detection**
  - Configuration is not that easy
- **Secure software design**
  - Performance is an issue

Software based security is limited in capabilities and not safe from <u>determined hackers</u>!!!

A POSSIBLE SOLUTION

Host Computer Security – Information Security – Network Security

"A Secure processor operates on encrypted data using a dynamically encrypted instruction set;
The use of Secure processors may improve the security not only at the host computer level, but also at the information and network levels as well.

SCAN – SECURE PROCESSOR

Specs…

- **Instruction & Data Encryption & Decryption based on SCAN methodology**
  - Modified SparcV8 processor architecture (32 bit instructions)

- **Compiler Optimization**

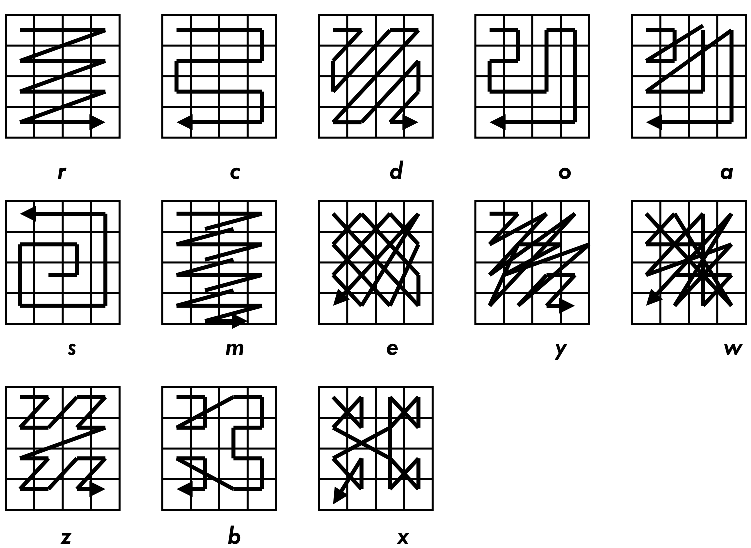
- **New instruction and FPGA co-proc set to handle**
  - Voice Biometric Authentication
  - Iris Biometric Authentication
  - Fingerprint Biometric Authentication

- **New instruction and FPGA co-proc set to handle**
  - Image compression
  - Image encryption and decryption
  - Information hiding and extraction

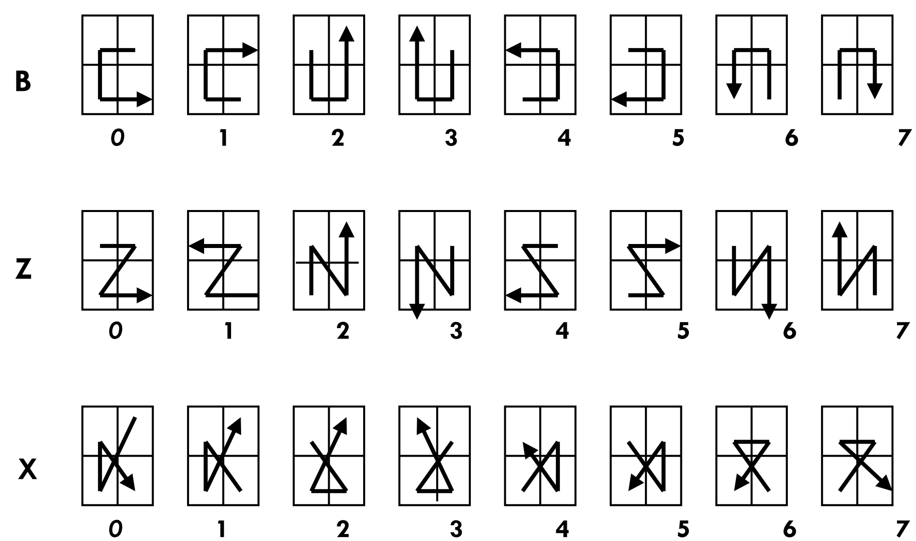
} FPGA co-processors

SCAN METHODOLOGY (1986 -)

- 2D spatial accessing methodology
- Can represent and generate a large number of scanning paths
- A set of basic scan patterns & a set of transformations
- A set of rules to compose simple scan patterns to obtain complex scan patterns



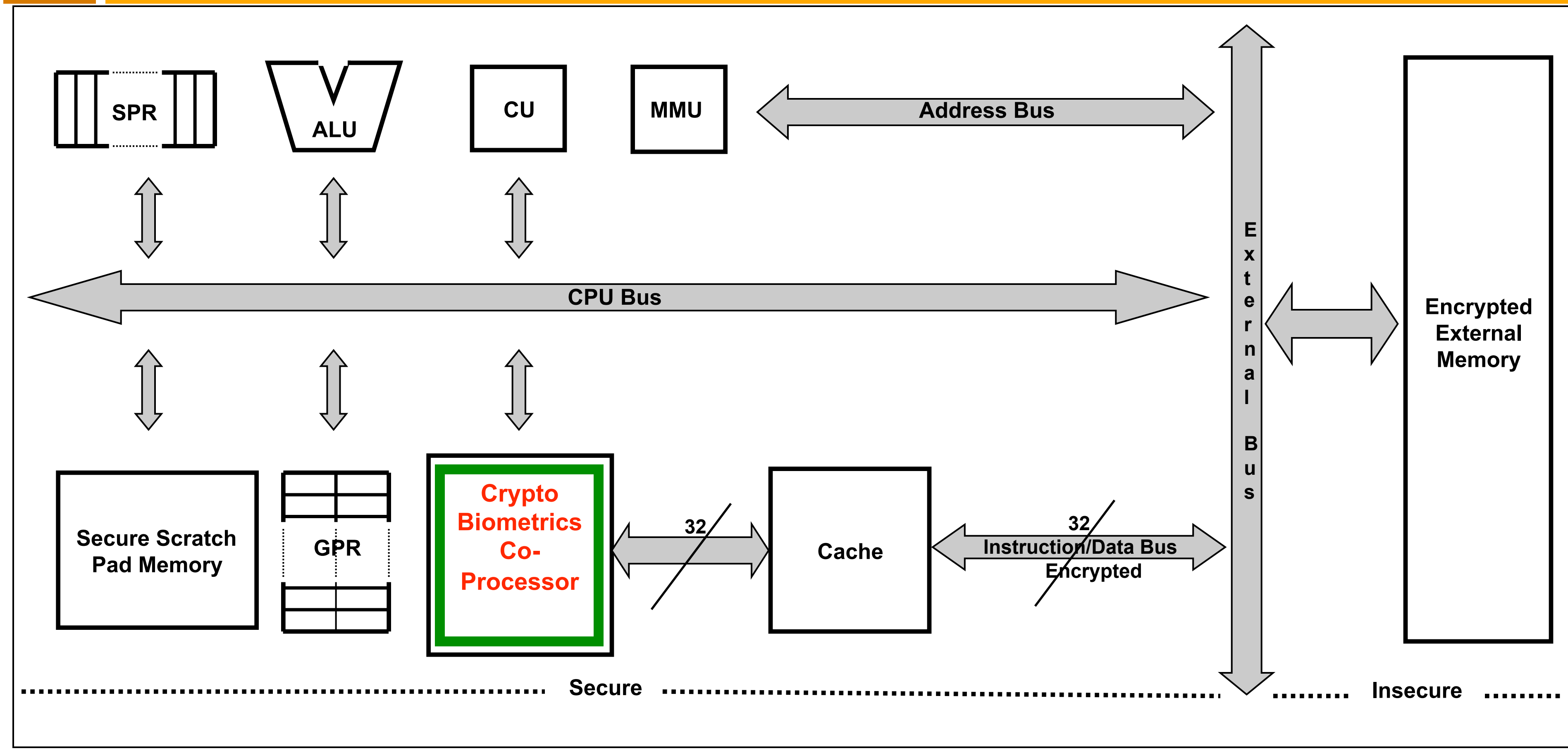
Basic scan patterns



Partition patterns and transformations

SCAN-SP ARCHITECTURE

SCAN-SP ARCHITECTURE



SCAN-SP:
CRYPTO CAPABILITIES

FPGA CRYPTO CO-PROCESSOR

SCAN methodology based information compression, information encryption and information hiding

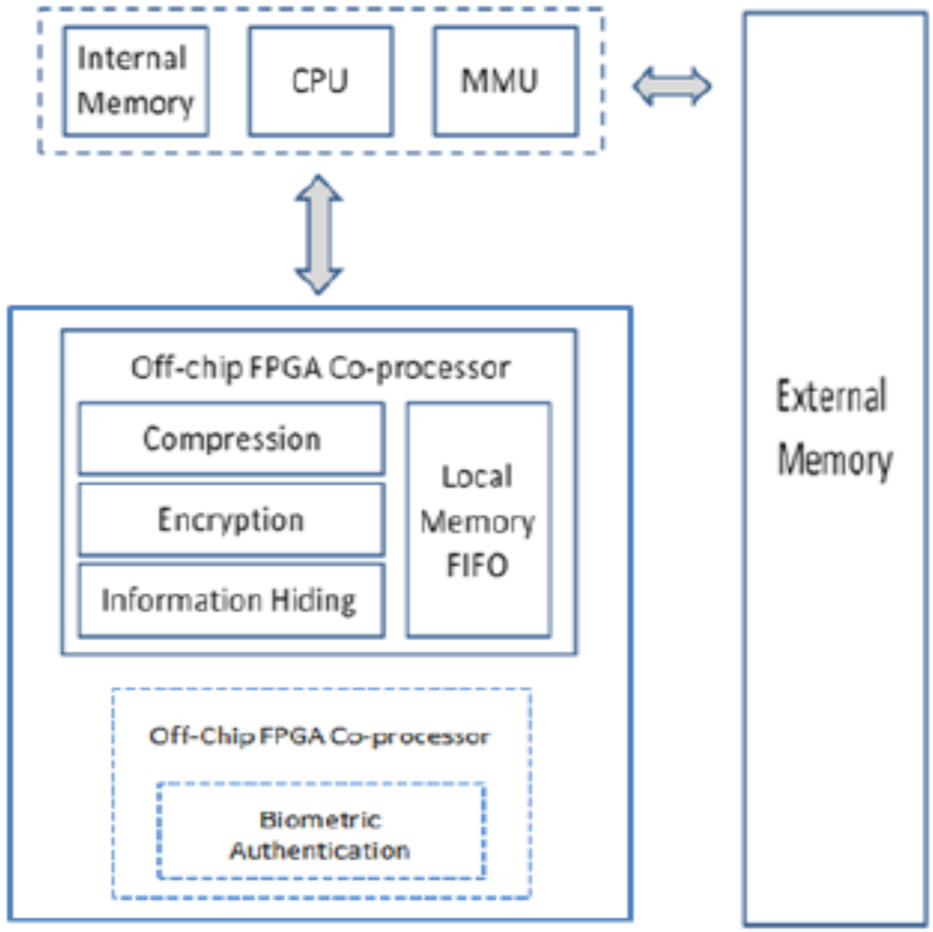
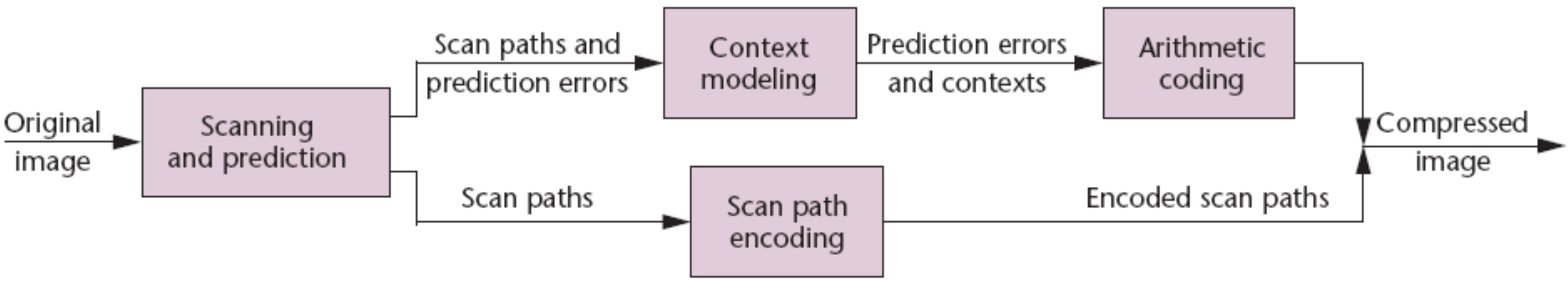


IMAGE COMPRESSION

The lossless image compression algorithm consists of four main steps…



SCAN methodology also offers a light-lossy compression associated with high-complexity secure encryption with a flat histogram!

IMAGE COMPRESSION RESULTS

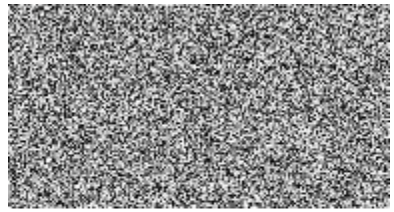
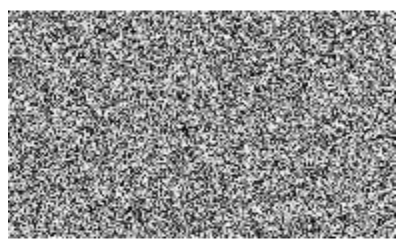
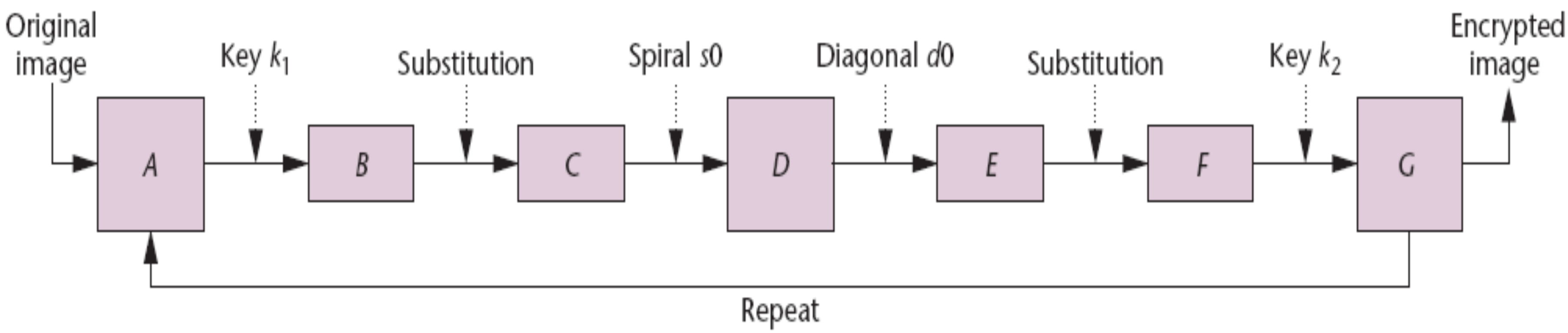
 Lena		**1.88145** **Latest** **1.9201**
 Camera Man		**2.49032**
 Mandrill		**1.70329**

IMAGE ENCRYPTION

SCAN encryption method is based on pixel value permutation and substitution. The substitution rule adds confusion and diffusion properties.

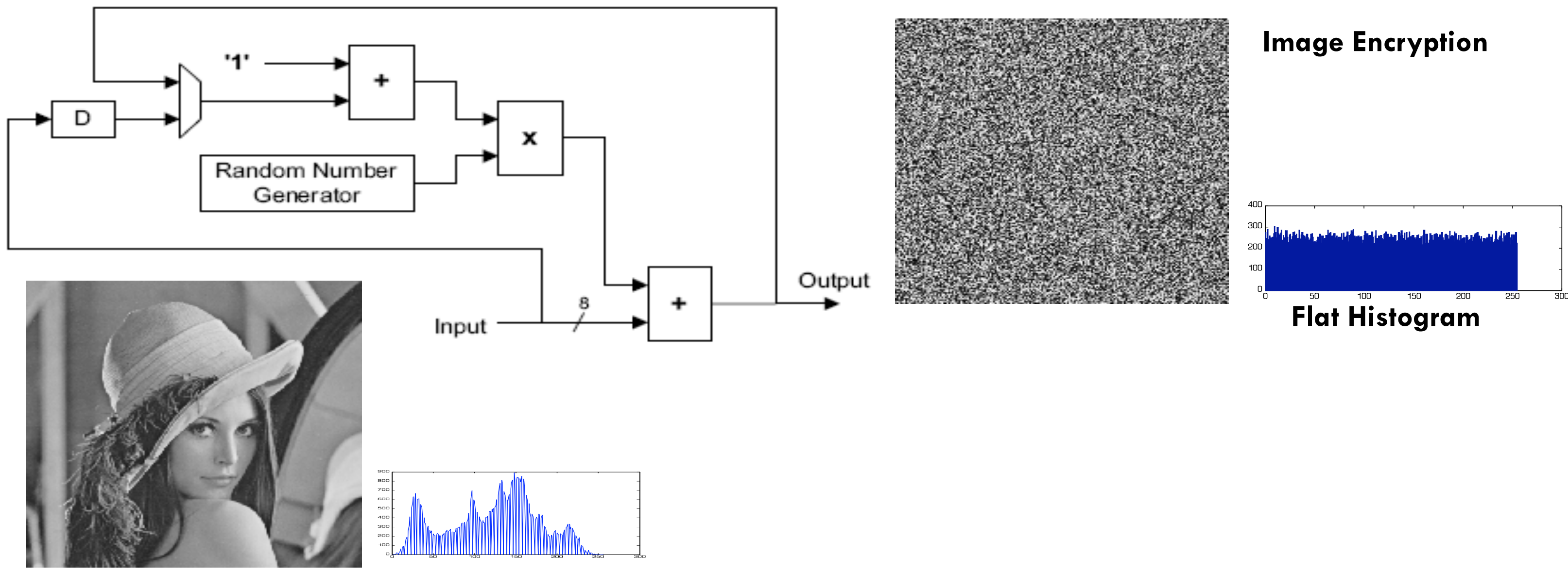


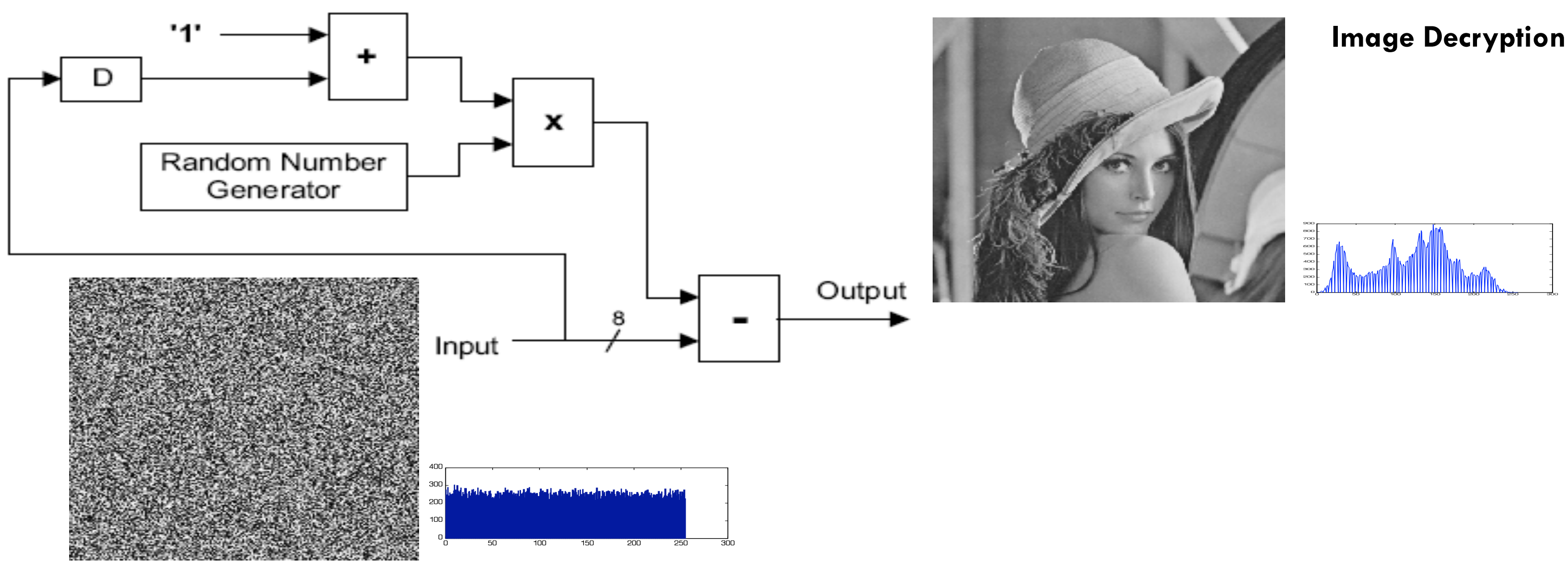
SCAN encryption methods' important features are:

- *Symmetric private-key encryption*
- *Iterated product cipher*
- *Key dependent permutation*
- *Large key space*
- *Variable-length keys*
- *Encrypting large blocks*

For an Image size 1024 × 1024, the number of encryption keys is $> 10^{304000}$

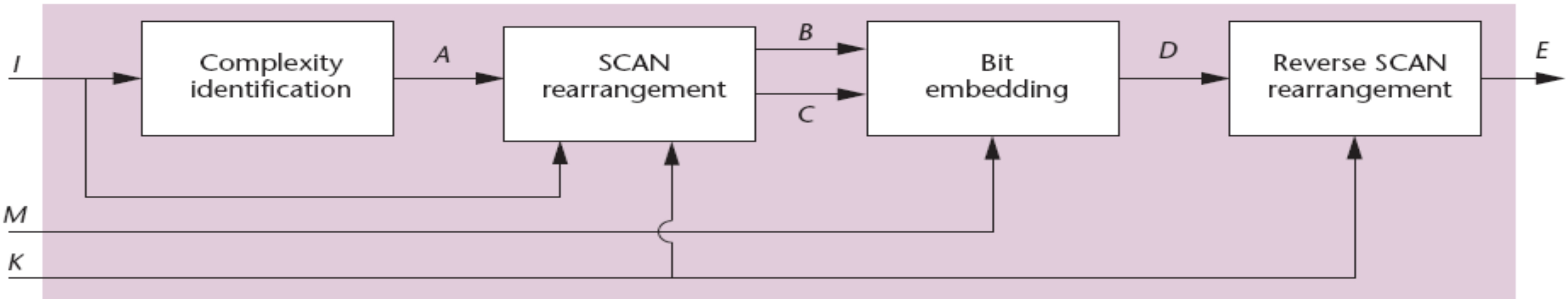
IMAGE ENCRYPTION RESULTS





INFORMATION HIDING

Embedding algorithm has of 4 main steps…

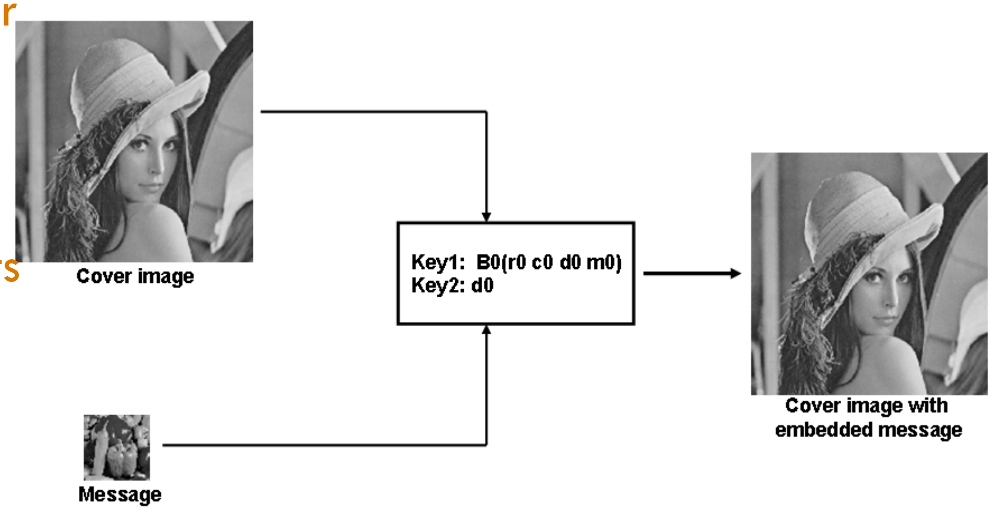


I - Cover image
M - Secret data
K - Secret key
E - Final Embedded image

A - Complexity matrix
B - Rearranged complexity matrix
C - Rearranged cover image
D - Rearranged embedded image

- Identify the complex noisy regions such as edges and textures of the cover image

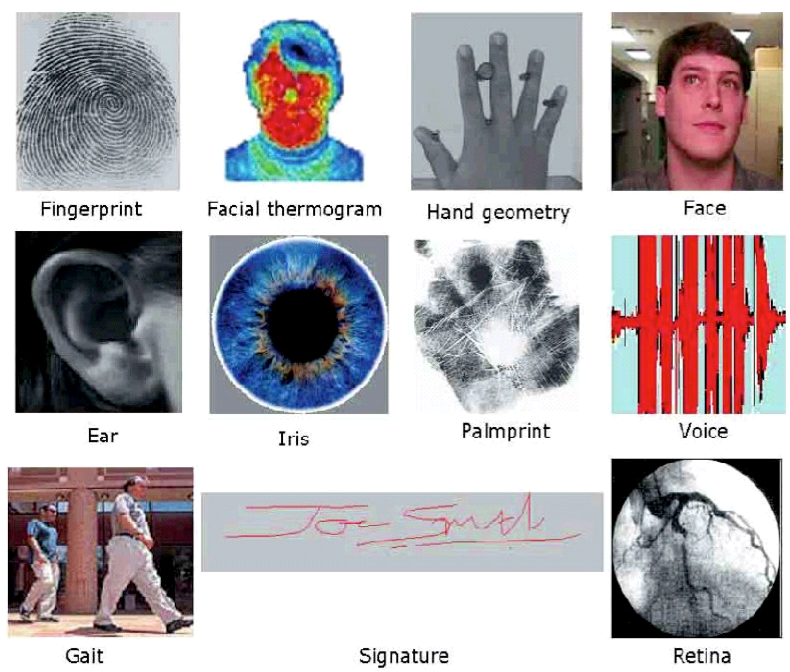
- Embed the secret data bits into a variable number of least-significant bits of the pixels in complex regions depending on their complexity, choosing a SCAN key



WHY BIOMETRICS AUTHENTICATION

BIOMETRICS

Biometrics is the study of methods for uniquely identifying or authenticating humans based on intrinsic physical or behavioral traits.



Multimodal biometric systems can improve the incompleteness of any unimodal biometric system!

TERMS IN BIOMETRICS

Identification: characteristics are selected from a database, to produce a list of possible or likely matches.

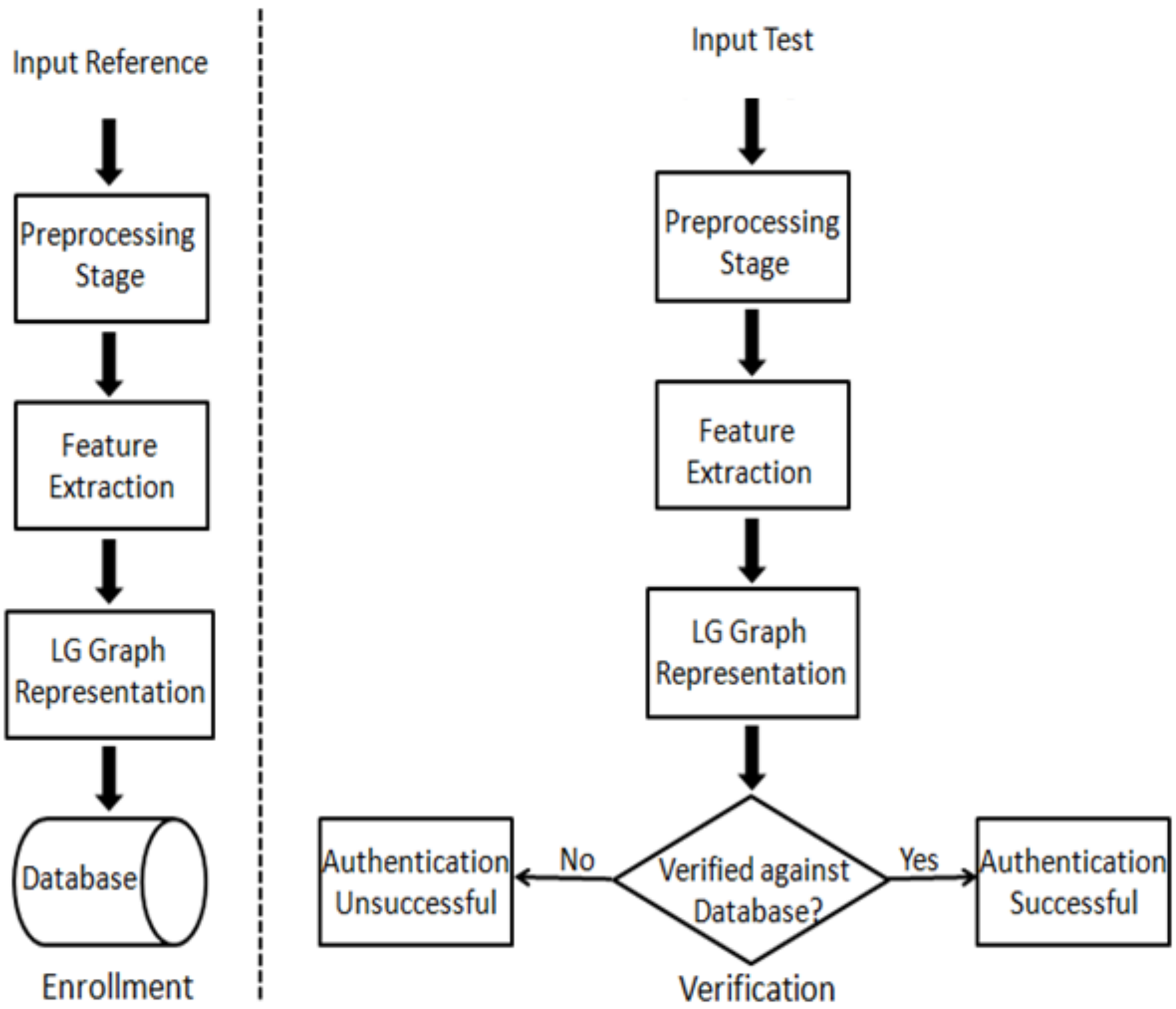
Authentication: when a person makes a claim that he or she is that specific person, just that specific person's characteristics are being checked to see if they match.

The two important operations in a biometric system are:

Enrollment: The biometric of the individual is stored as a database.

Test: The biometric information of the individual is detected and compared with the stored database.

Stages in Enrollment and Verification



Local Global Graph Method (1987)

- The LG graph describes the individual features of the signal/image in relation to the entire signal/image, thus offering a robust methodology for signal/image description & comparison.

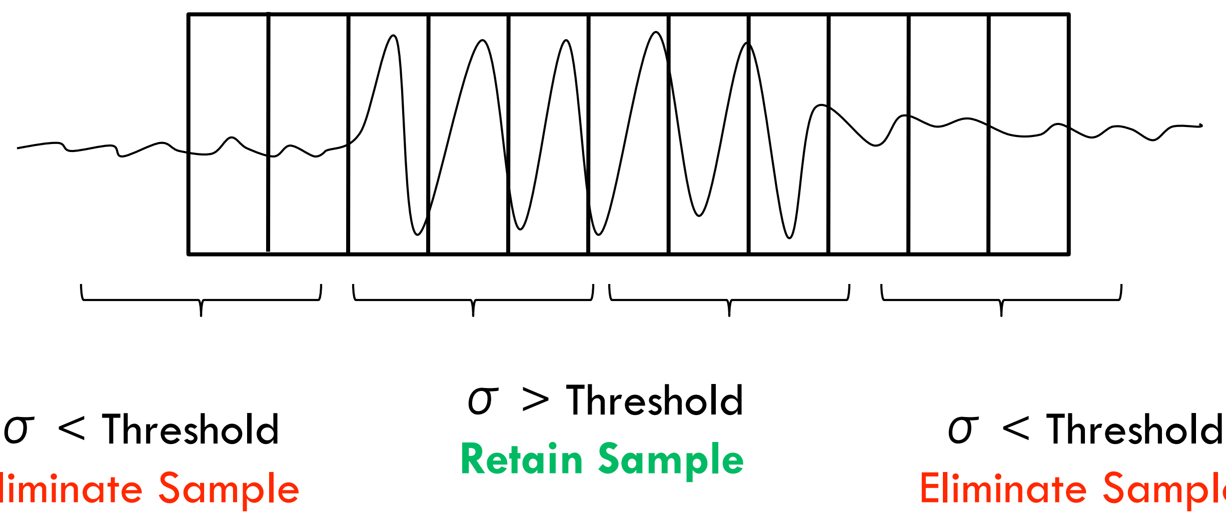
- LG graph features are extracted from a subject's biometric & stored in the system database.

- LG graph of the presented biometric is compared with the stored database to establish authenticity.

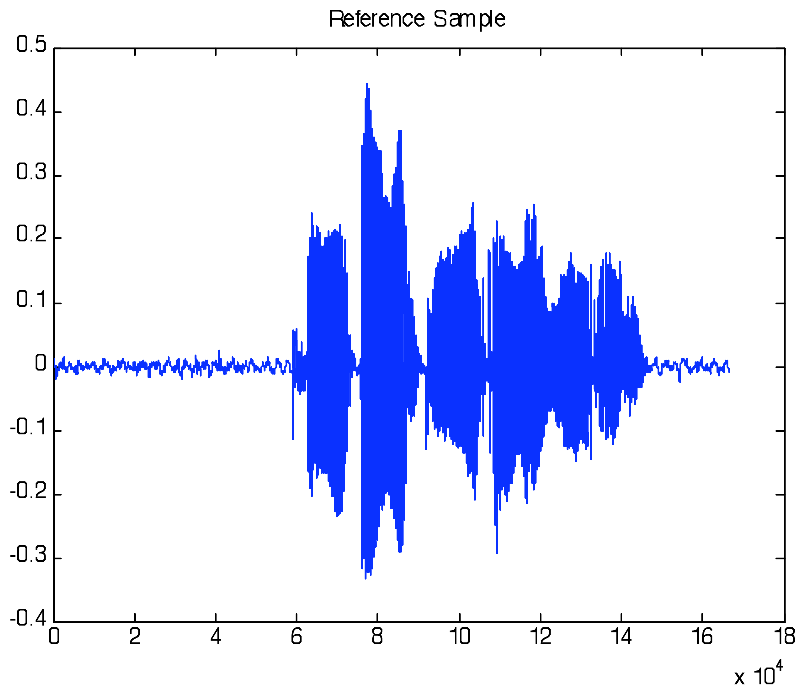
VOICE BIOMETRIC AUTHENTICATION

Pre-processing the speech signal

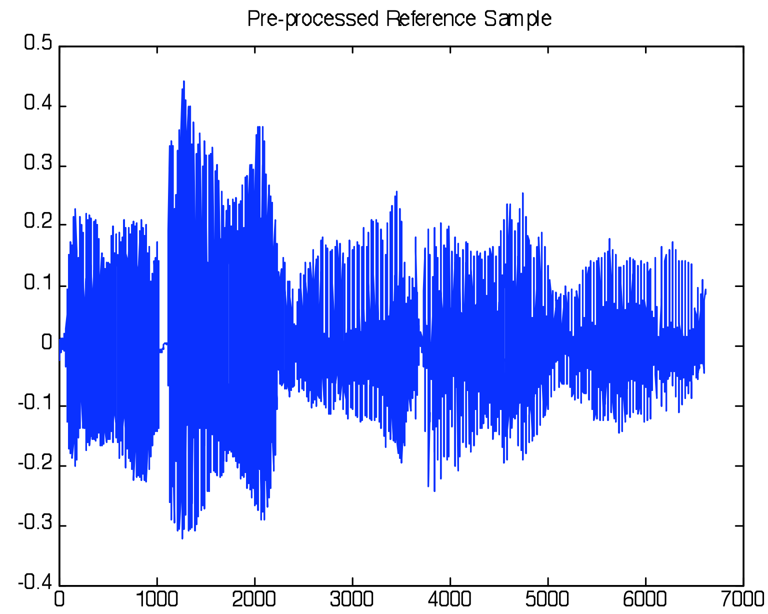
- Eliminate silence from input speech signal
- Align test and reference speech signal
  - using Standard Deviation (σ) of the samples of speech signal in a moving window



RESULTS OF PRE-PROCESSING



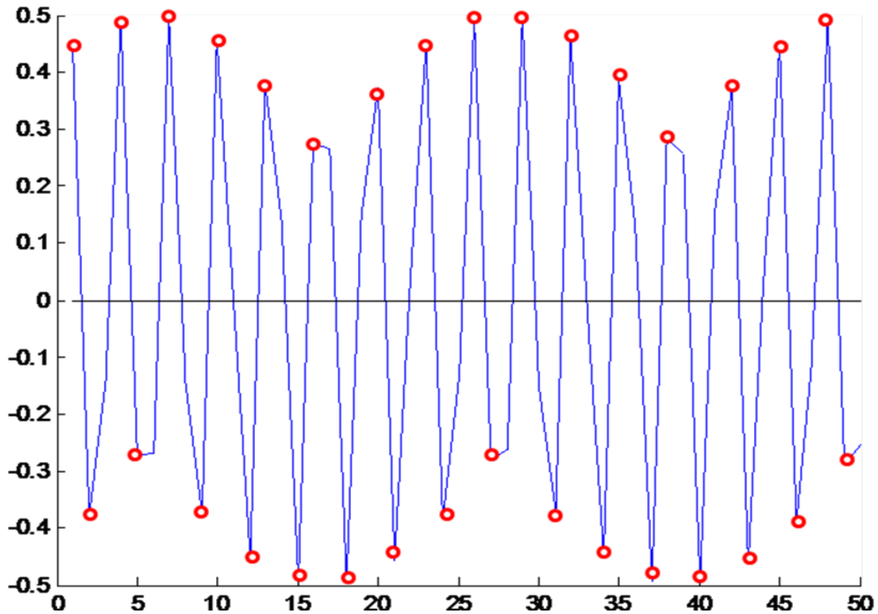
Speech sample



Pre-processed Speech sample

Step 1: Detect Maxima and Minima

- Find the slope of the straight line segments that form the signal
- Identify points where the slope of the signal changes



Step 2: Creation of Local Graphs

- Extract features from the nodes that occur in the signal approximated by the triangles. A node given by N_i is represented by:

  $N_i = \{SP_i, EP_i, ø_i, L_i\}$

  N_i stands for the i^{th} node

  SP_i stands for the starting point of a segment joining $Node_i$

  EP_i stands for the ending point of a segment joining $Node_i$

  $ø_i$ stands for the angle between $Node_i$ & the horizontal axis (slope)

  L_i stands for the length of segment joining $Node_i$

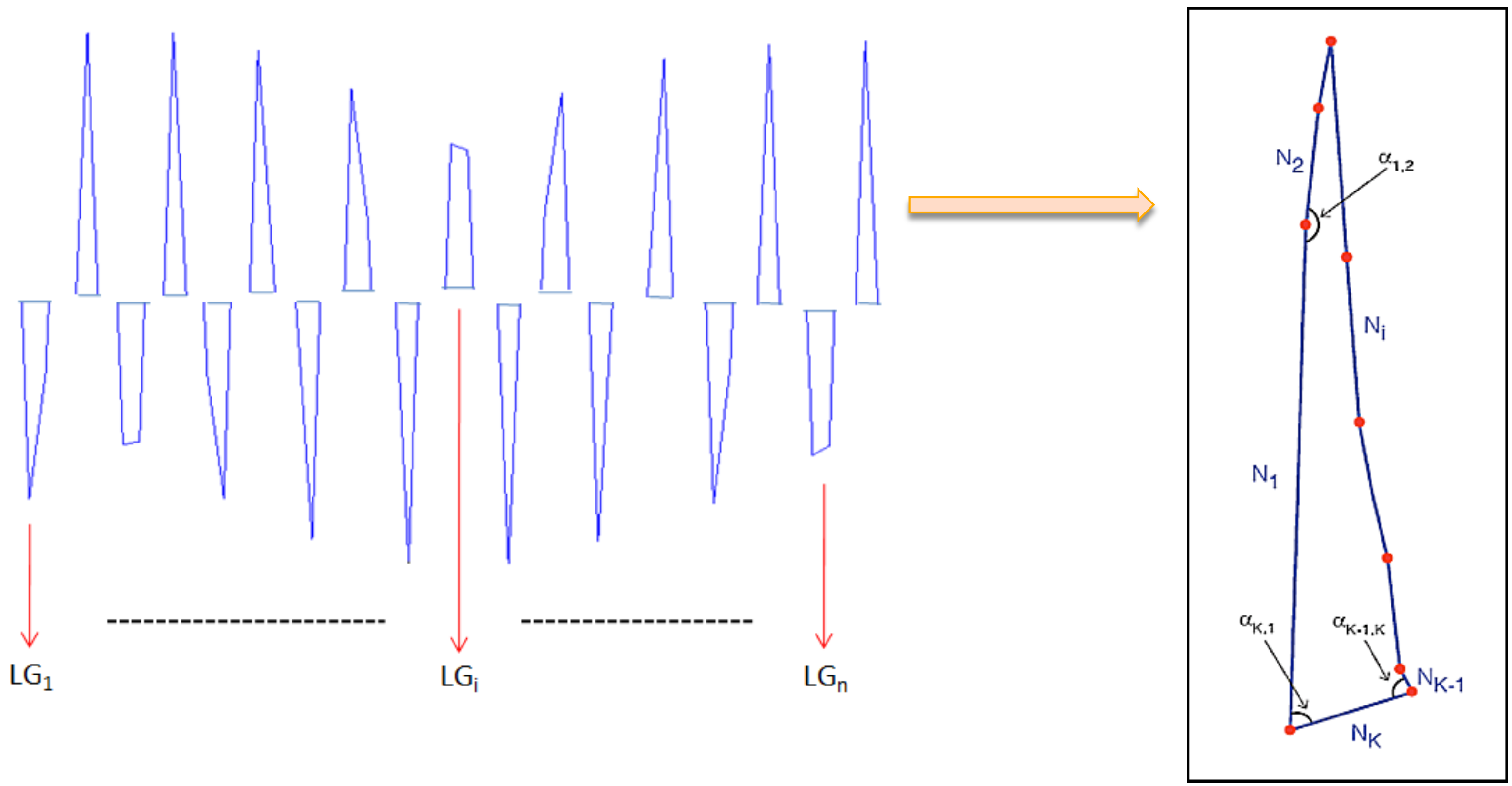
- The relationship between two nodes is given by α_{ij}.

  α_{ij} stands for $\{*N_i, \theta_{ij}, *N_j\}$, where,

  N_i & N_j stand for the two consecutive nodes that occur in the signal

  θ_{ij} stands for the angle “connecting” Nodes i & j

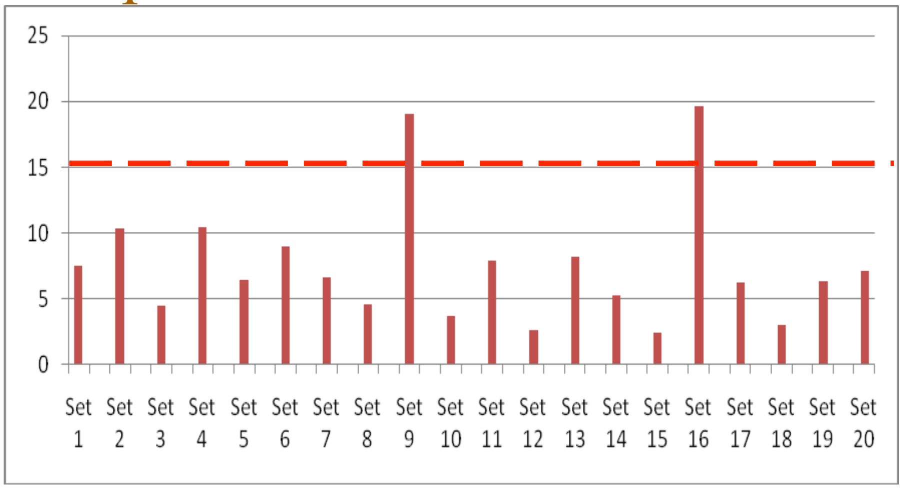
Step 3: Creation of LG Graphs



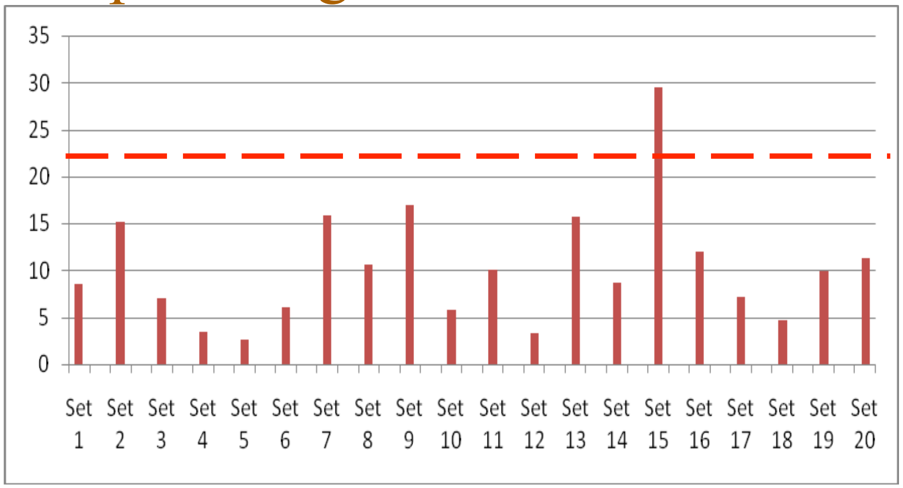
$$LG_i = N_1\alpha_{1,2}N_2\alpha_{2,3}N_3\alpha_{3,4}\ldots N_{K-1}\alpha_{K-1,K}N_K\alpha_{K,1}$$

Results – LG Graph Methodology

- The threshold ε is pre-determined experimentally, & is hard-coded in the program.
- Area and height features were calculated from the triangular representations of reference and test speech signals.



Minimizing distance between reference & test sample for "area" feature (threshold at 15, i.e. 75% of maximum)



Minimizing distance between reference & test sample for "height" feature (threshold at 22.5, i.e., 75% of maximum)

Results – LG Graph Methodology

- Threshold at 75% results in an accuracy of 90%.
- All the values less than the threshold are accepted as a match while values greater than the threshold are rejected.

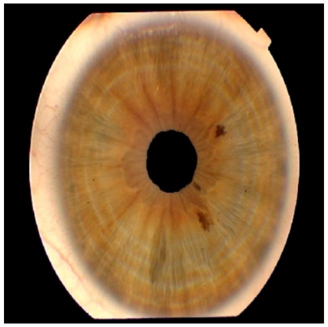
IRIS BIOMETRIC AUTHENTICATION

PRE-PROCESSING THE IRIS IMAGE

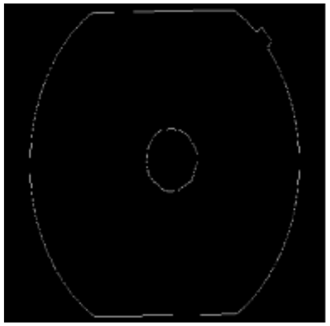
- Iris localization
- Image smoothing
- Log-polar transformation
- Image segmentation

IRIS LOCALIZATION

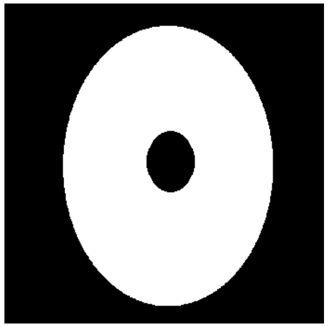
Using edge detection combined with Hough transform to localize iris in the acquired image



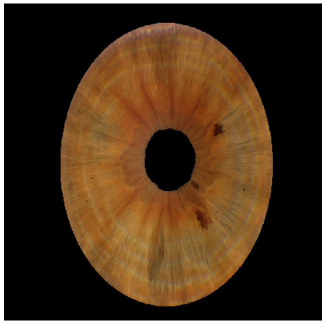
Acquired iris image



Edge image



Circular mask



Localization of iris

IMAGE SMOOTHING

Image smoothing is necessary to eliminate trivial regions that can appear in the segmented iris image.

A simple averaging filter of size 3x3 or 5x5 can be selected for smoothing the iris image.

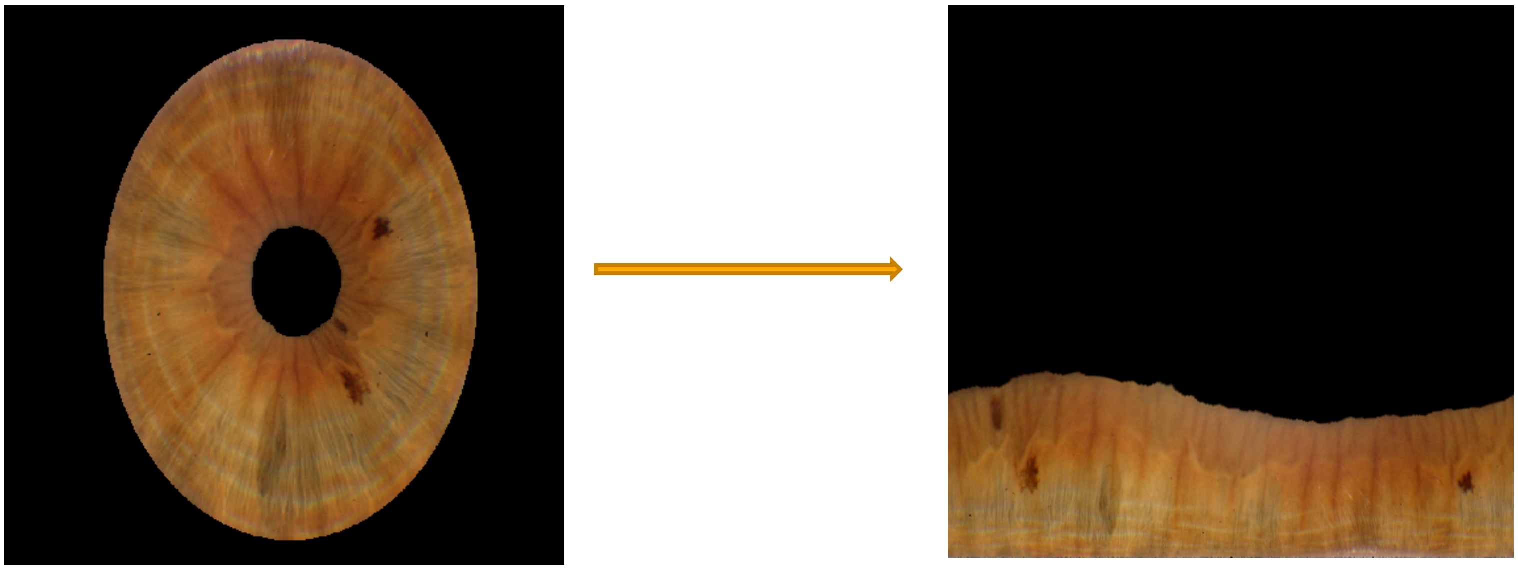
LOG-POLAR TRANSFORMATION

The log-polar transformation is a conformal mapping from the points on the Cartesian plane to points in the log-polar plane.

Advantages

- Data reduction.
- Embedding an implicit focus of attention in the center of the visual field.
- Image rotation in Cartesian plane results in translational shifts in the log-polar plane.

LOG-POLAR TRANSFORMATION



Log-Polar transformation after iris localization

IMAGE SEGMENTATION

Segmentation is a crucial part of the algorithm because the LG graph representation directly depends on the results of segmentation.

The segmentation algorithm must incorporate invariance to noise and rotation in the presented test image to enable reliable authentication.

K-means algorithm for image segmentation.

EXPERIMENTAL RESULTS

- With rotational variation ranging from 0 to 360 degrees, we obtained 92% accuracy in authentication.

- With rotational variation ranging from +/- 50 degrees, we obtain 100% accuracy in authentication.

FINGERPRINT BIOMETRIC AUTHENTICATION

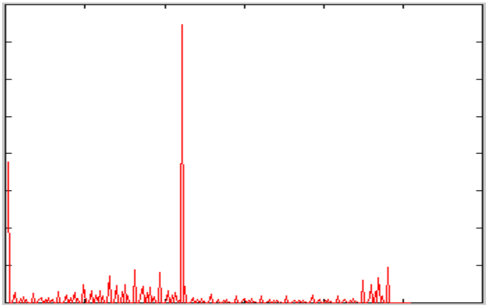
PRE-PROCESSING THE FINGERPRINT IMAGE

The important steps in preprocessing include :

- Binarization
- Skeletonization
- Elimination of spurious regions

BINARIZATION

The acquired fingerprint image has a bi-modal histogram as seen below, thus it is easy to set up a hard threshold to binarize and generate a negative of the acquired image.



Bi-modal histogram

Synthetic fingerprint

Binarized image

SKELETONIZATION

Skeletonization is achieved by implementing an *"OPEN"* operation on the binary image followed by thinning operation.

Skeletonization of the fingerprint image

ELIMINATING SPURIOUS REGIONS

Connected component labeling algorithm with 8 neighbor connectivity:

- Isolate different regions.

- Remove regions that have pixel count lesser than a threshold.

- Thus eliminating spurious regions.

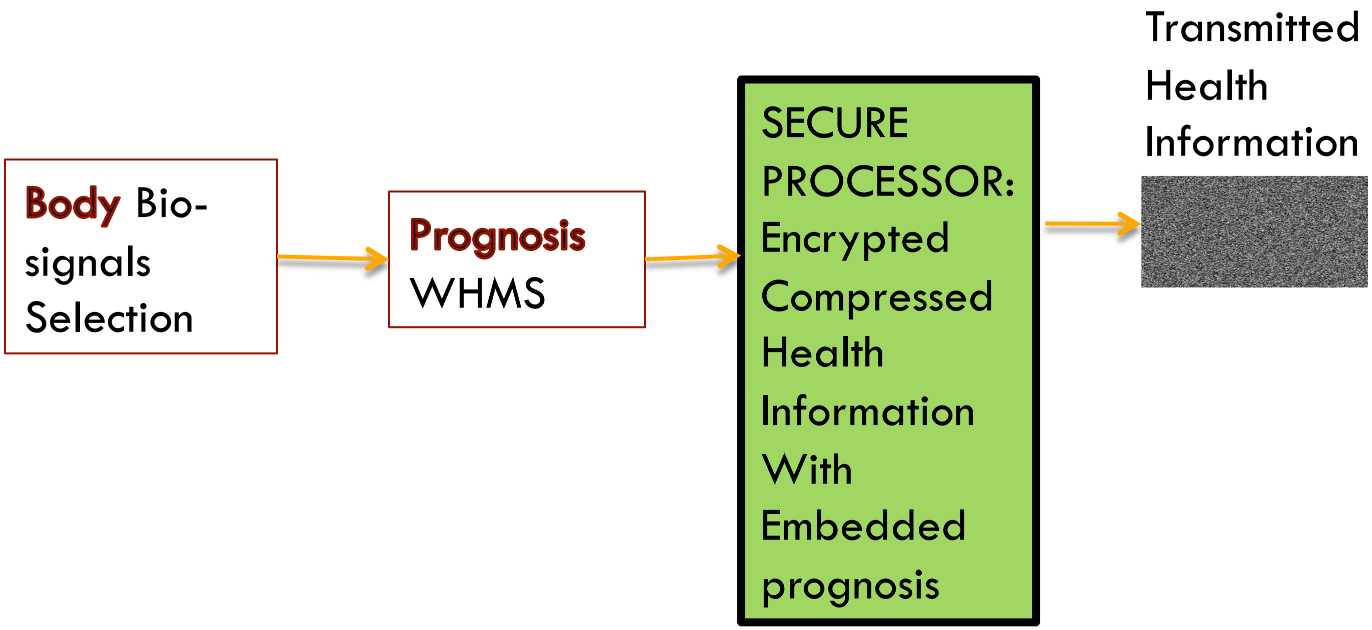
IDENTIFICATION OF REGION CENTROIDS

Isolation of a single ridge, its centroid, its end and start points

Centroids of different region (centroids highlighted as squares)

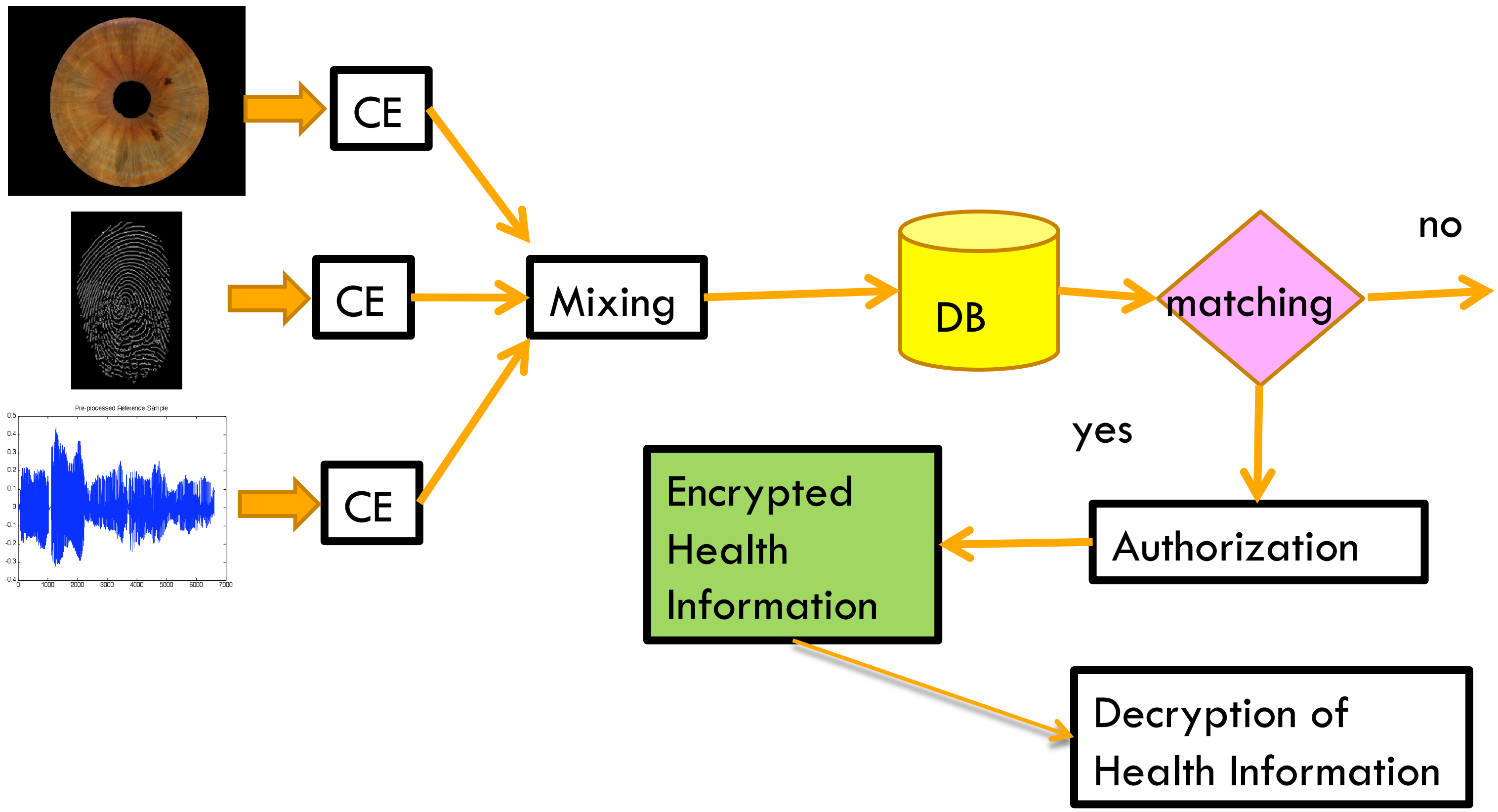
How to Secure HIEx

Clint Site:



How to Secure HIEx

MD site:



CONCLUSIONS

- WHMS will offer Monitoring Health Conditions and Secure Information Exchange
- Current Technological Devices for monitoring the health conditions of People at Risk do not offer accurate and reliable information yet.
- Implanted Devices and sensors could be a solution
- Every patient's case is different
- Health Information Exchange for making Decisions has to be associated with protection
- Security methodologies do not offer the silver bullet of perfect protection
- Implanted Sensors (People and FDA challenge)

Thank you!