Lecture on Fingerprint Sensing & Pattern Recognition

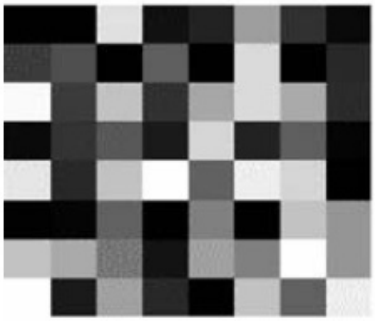
Nanang Syahroni
EEPIS – Surabaya - Indonesia
(JICA Expert on Digital Communication)
nanang@eepis-its.edu

Electronics & Telecommunication Department - Tumba College of Technology - Rwanda

Image Processing

- Image digitization is a process that converts a pictorial form to numerical data.
- A digital image is an image f(x, y) that has been discretized in both *spatial coordinates* (x,y) and *brightness* (intensity or gray-level quantization).
- The image is divided into small regions called picture elements or pixels.
- The number at each pixel represents the brightness or darkness (generally called the intensity) of the image at that point.

- In figure below shows a digital image of size 8x8 with 1 byte per pixel as used in fingerprint pattern as decribed more details in previous training session.
- In figure below we have seen a digital image and its numerical representation.

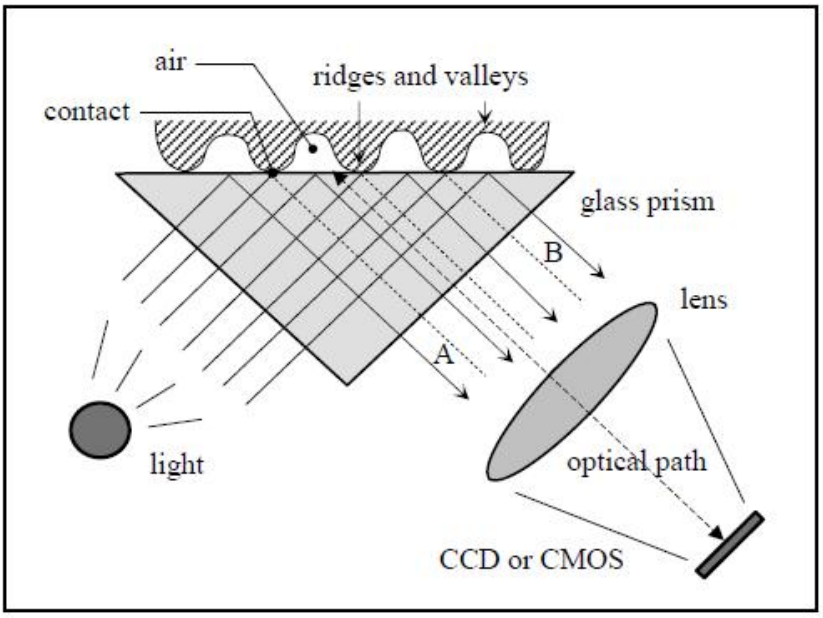


1	8	219	51	69	171	81	41
94	108	20	121	17	214	15	74
233	93	197	83	177	215	183	78
41	84	118	62	210	71	122	38
222	73	197	248	125	226	210	5
35	36	127	5	151	2	197	165
196	180	142	52	173	151	243	164
254	62	172	75	21	196	126	224

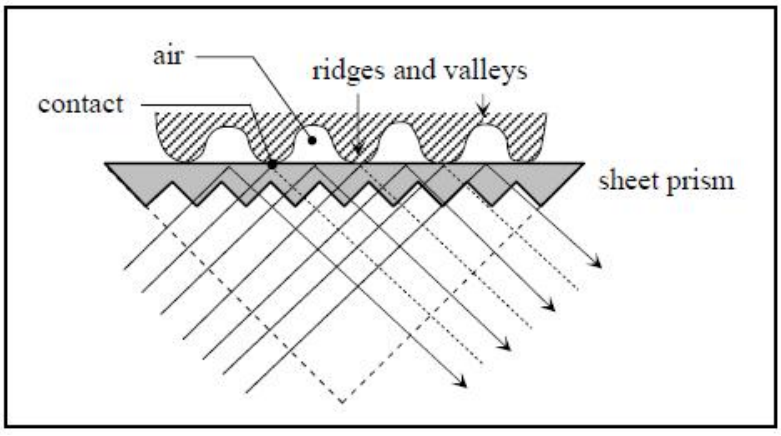
Fingerprint Scanner

- The general structure of a typical fingerprint scanner is consists of:
  - Sensor reads the ridge pattern on the finger surface.
  - A/D converter converts the analog reading in the digital form.
  - Interface module is responsible for communicating (sending images, receiving commands, etc.) with external devices (personal computer).

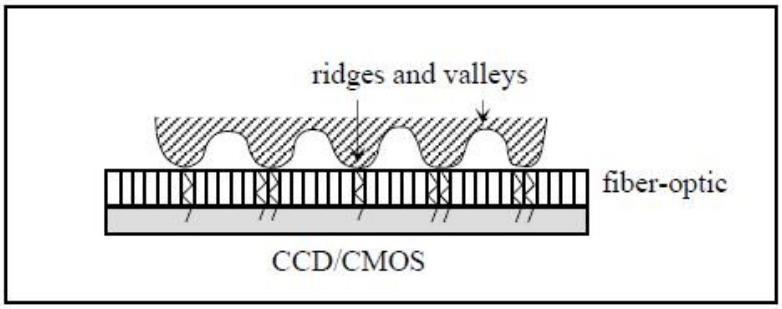
Frustrated Total Internal Reflection (FTIR)



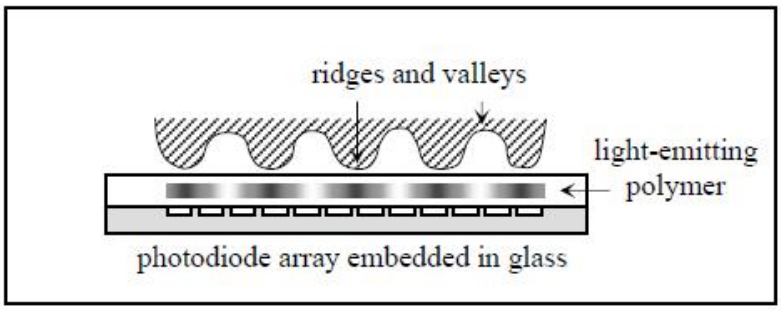
Sheet Prism FTIR



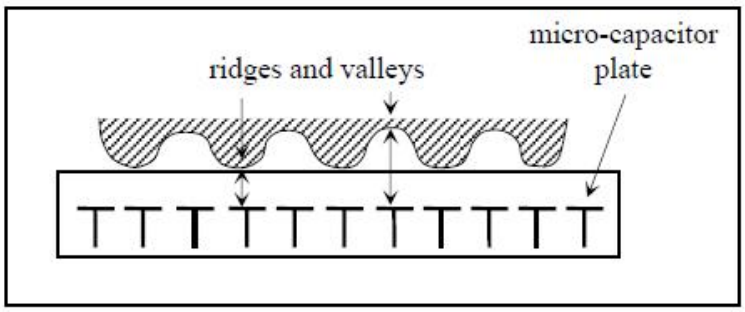
Micro-optical Guides CCD/CMOS



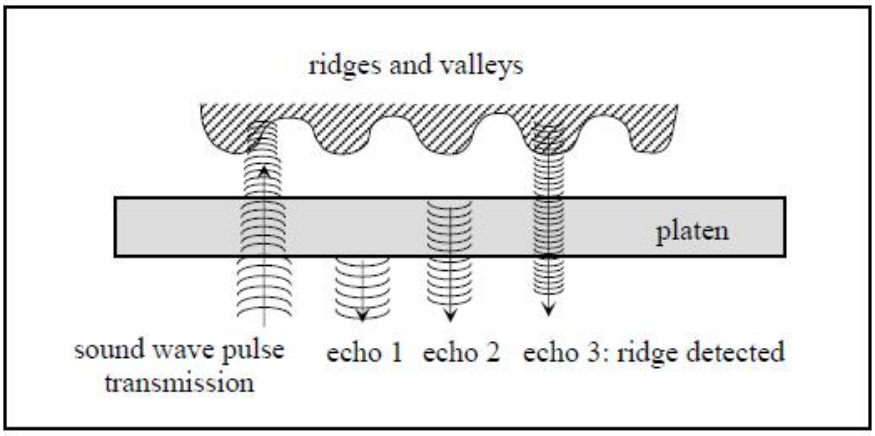
Electro-optical Sensor



Capasitif Sensor



Ultrasonic Sensor



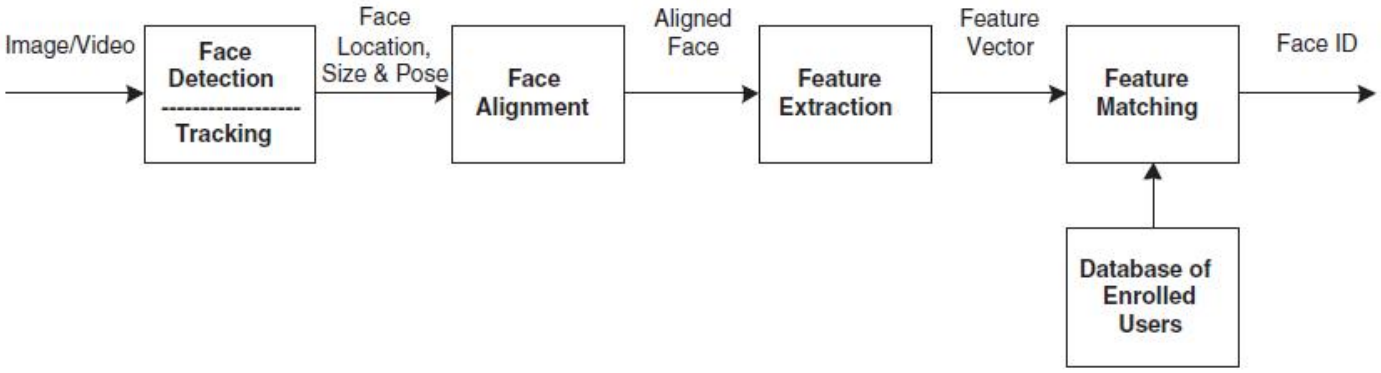
Face Recognition

- A face recognition system is expected to identify faces present in images and videos automatically.
- It can operate in either or both of two modes:
  1. Face verification (or authentication)
  2. Face identification (or recognition)
- Face verification involves a one-to-one match that compares a query face image against a template face.
- Face identification involves one-to-many matches that compares a query face image against all the template images in the database to determine the identity of the query face.

Face Recognition Processing

- A face recognition system generally consists of four modules: detection, alignment, feature extraction, and matching.
- After a face is normalized geometrically and photometrically, feature extraction is performed to provide effective information that is useful for distinguishing between faces of different persons.
- For face matching, the extracted feature vector of the input face is matched against those of enrolled faces in the database.

Face Recognition Processing Flow



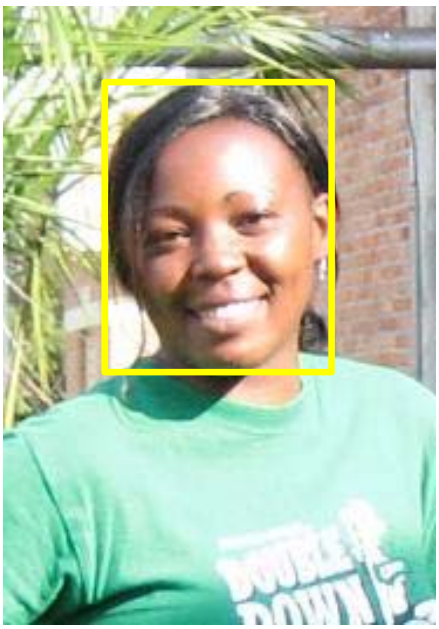
Face Detection

- Face detection can be performed based on several cues:
  - Skin color (for faces in color images
  - and videos)
  - Motion (for faces in videos)
  - Facial/head shape
  - Facial appearance, or a combination of these parameters.

Face Windowing

- Most successful face detection algorithms are appearance-based without using other cues.
- The processing is done as follows:
  - An input image is scanned at all possible locations and scales by a subwindow.
  - Face detection is posed as classifying the pattern in the subwindow as either face or nonface.
  - The face/nonface classifier is learned from face and nonface training examples using statistical learning methods.

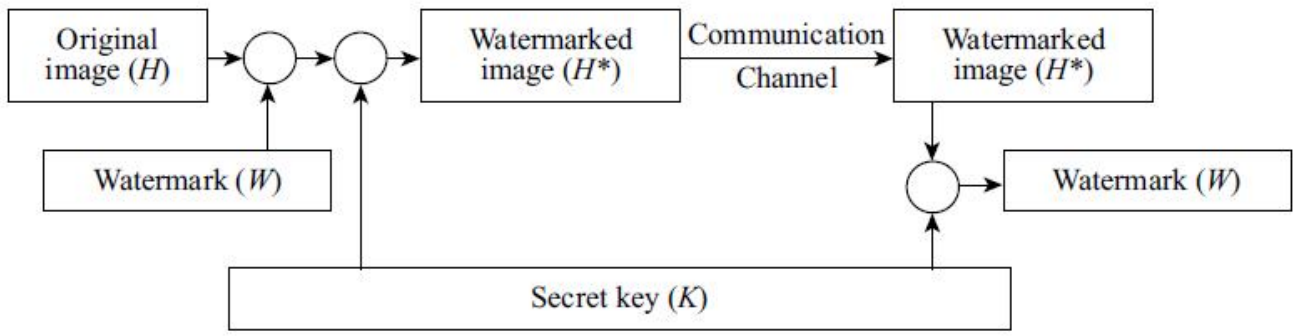
Typical of Frontal Face Detection Examples



Watermarking

- A watermark is a pattern of bits inserted into a digital medium that can identify the creator or authorized users.
- The digital watermark, unlike the printed visible stamp watermark, is designed to be invisible to viewers.
- The bits embedded into an image are scattered all around to avoid identification or modification.

- A watermark message ***W*** is embedded into a media message, which is defined as the host image ***H***. The resulting image is the watermarked image ***H****.
- In the embedding process, a secret key ***K***, for example, a random number generator, is sometimes involved to generate a more secure watermark.
- The watermarked image ***H**** is then transmitted along a communication channel.
- The watermark can be detected or extracted later by the receiver.



References

1. Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar (editors), *Handbook of Fingerprint Recognition*, 2nd edition, Springer-Verlag, London, 2009.
2. Stan Z. Li and Anil K. Jain (editors), *Handbook of Face Recognition*, Springer, 2005.
3. Frank Y. Shih, *Image processing and pattern recognition : fundamentals and techniques*, IEEE & John Wiley & Sons, 2010.

Morakoze