CHAPTER III
PROBLEM ANALYSIS

III.1 SWOT Analysis of Face Recognition as Authentication

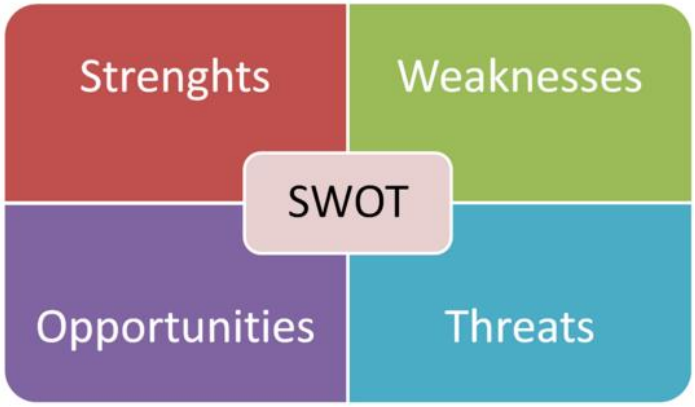

Figure 3.1 Swot Picture

(REF: [www.research-methodology.net)](www.research-methodology.net)

Face Recognition definitely has their own strength and weakness. Otherwise Face Recognition also has their Opportunities and Threats from external side.

1. Strengths

   Face Recognition is a simple method to secure any information. Scientist believe Face Recognition is better than any method.

   Because with Face Recognition we can store any data easily rather than other method. As example with Face Recognition people can easily do authentication via a security door. In movie, there are some interaction between door and human via authentication. The authentication which used is Face Recognition. It's proven that authentication using Face Recognition is better than other method.

2. Weakness

   In facing the weakness or challenges, there are several points that should be anticipated:

a. Pose

When taking the picture, the images of a face vary due to the relative camera face pose (frontal, tilted, profile, upside down).

b. Facial Expression and emotions

The appearance of faces is based on person facial expression and emotion. Without good algorithm, system can't detect between the images want to be compared and the images which stored in database. As example if the first photo is taken with calm face and the second one compared with smile face, without good algorithm computer can't compare the face line between calm and smile face. It's based on the face behavior.

c. Imaging Conditions

When the image is stored, any factor should be distraction when the system want to compared with the new images. As example if the stored image with good lightning and the image which want to be compared with bad lightning it can't be hard to detected except the algorithm of stored image already improved and can recognize well the image which want to be compared with lightning exception.

d. Age

Age can be a major problem of face recognition. Along with increase of age, the line and wrinkles on face will change slowly. If the algorithm can't handle the exception of older face it should be compared with images 20 year ago. It could be the big problem when authenticating with Face Recognition.

3. Opportunities

In face recognition, this case has several opportunities. As example, nowadays if a city using face recognition. The city can be change to modern city or smart city. Because any information will be stored in resident face. Government will has their own database that containing the resident information. Any transaction or authentication can be easily detected with

only face authentication. Otherwise if criminal activity happened the CCTV or Camera can capture the images of the criminal and the data will be compared with the data inside the database. Face Recognition can also integrated with health facility. As example we can integrated the face of resident and will detected with an algorithm to detect the disease.

4. Threat

   Face Recognition can be the treatment of resident information data. From the game called watchdog, the hacker can hack the system information and stole any information via database. When hacker already stole information, the information data will not be secure anymore. And the hacker can access any information of someone account. As example with face recognition, resident store bank, bill, and other account information. The data will be stolen and the hacker will has freedom access to the data.

III.1 Authentication Process of Face Recognition

1. Mask Construction

   Face Recognition will authentication the stored image and the image which want to be compared. This is the steps of detecting the image:

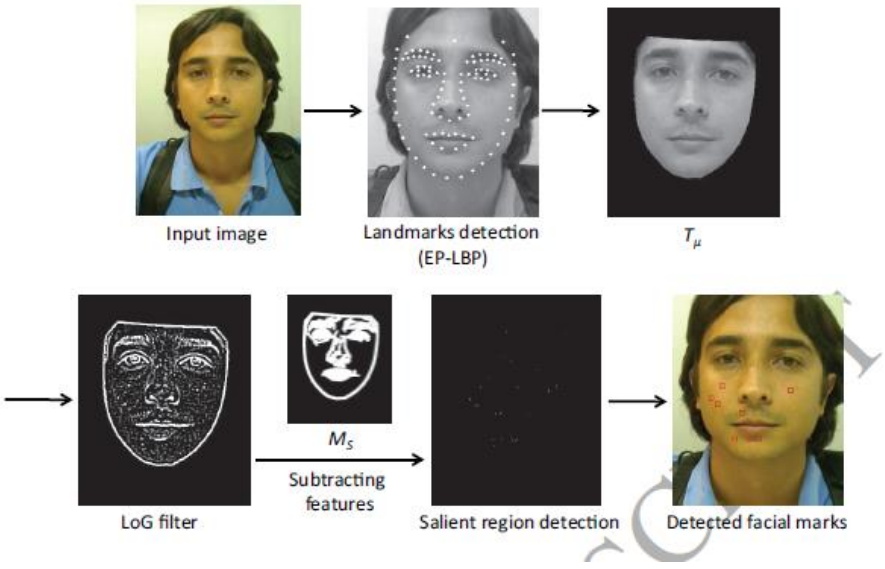

Figure 3.2 Face Detection Process

a. Input the image which want to be detected.
b. Algorithm will detect the landmark of face and detect the pixel and detect limit of face landmark.
c. After that the detected landmark will be cut and saved as T variable.
d. Detected landmark will filtered with black and white filtered to process the marked pixel at detected landmark.
e. After that, the detected landmark will be subtracted.
f. The real pixel of detection of face will be detected called Salient Region.
g. The algorithm will recognize that spot pixel as detected facial marks.
h. The image will be stored in database.

2. Detection of Facial Marks

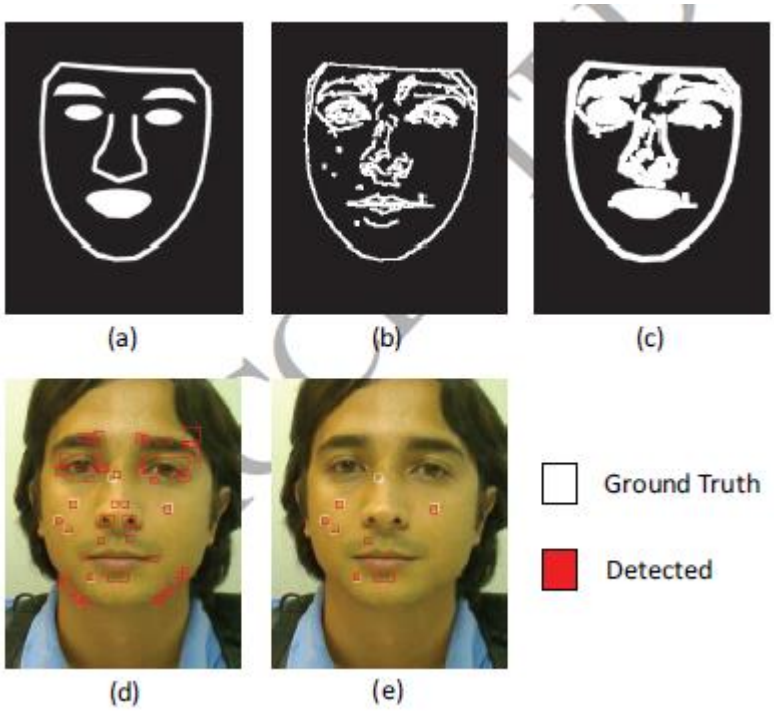

Fig 3.3 Detecting process of two images.

Process of detecting can be process with below method:

a. The image will be input and get the landmark face.
b. The algorithm will check and obtained the edge.
c. The algorithm will check user specific mask.

d. The red spot are the pixel in landmark which detected via landmark face.
e. The detected face spot pixel will be compared with the image in database, and the image will check as much as ground truth and detected spot between those pictures.
f. If the compared image are similar, it will process to next step.

Matching two images I_1 and I_2, and N_1, N_2 are their detected marks. Respectively the similarity between I_1 and I_2 can be determined below.

$$FMM = \frac{\sum_{i=0}^{|N_1|} \min D(n_i, n_j)}{|N_1|}, \forall n_j \in N_2 | (x_j, y_j) \in R_i$$

Fig 3.3 Equation of comparing image.

For each mark $nj \in, xj$ and yj are its spatial central coordinates. For each mark $ni \in N1$, a rectangular region R_i was built around its central coordinates in I2, as an area of potential matching. This ensure a spatial coherence in the matching of the marks, i.e, very distant facial marks are not verified (Riera, Gonzalez, & Vazquez, 2017).