Continuing Education Program
Center for Computing and Information
Technology
Faculty of Engineering
University of Indonesia

ISAS (Information Search and Analysis Skill)

“Face Recognition as Authentication Security”

Group 1

Muhamad Hudya Ramadhana

Mutia Ayu Dianita

Faculty :

Dudy Fathan Ali, S.Kom

Class : 4SC1 (PNJ)

Faculty of Engineering University of Indonesia

Depok 16424

PREFACE

First, Let us give praise to Allah S.W.T who give guidance to us untill we can complete our ISAS entitled “Face Recognition as Authentication Security”. As author write this article, author get a lot of support from various parties. Among others are :

1. Our parents, who always help in the form of spirit and material.
2. Dr. Aries Subiantoro, M.Sc as director of CCIT Faculty of Engineering, University of Indonesia.
3. Mr. Dudy Fathan Ali S.Kom, as our faculty who have provided guidance and support and referrals to us so that we can finish ISAS.
4. Our friends who always give the information that they know, exchange ideas and give encouragement to us in writing this article.

Author know that the results of this article is far from perfect and there are still many shortcomings, author hope readers will give comments and suggestions in building this article in order to become better. We hope this article can be useful for those who read or hear, especially for CCIT students of the Faculty of Engineering UI.

Our ISAS titled “Face Recognition as Authentication Security” is One of Technique to secure any action when accessing data. We hope with this ISAS people will understand about Face Recognition.

Depok, April 2017

Author

TABLE OF CONTENTS

CHAPTER I : INTRODUCTION

CHAPTER II : BASIC THEORY

CHAPTER III : PROBLEM ANALYSIS

CHAPTER IV : CONCLUSION AND SUGGESTION

TABLE OF FIGURES

CHAPTER 1

INTRODUCTION

I.1 Background

Data Security is one of concern for all user who using the internet network. Nowadays, hackers threat all data and hangs it like a Damocles sword. The transmission data through any communication channel needs strong encryption techniques in purpose of the data security. The trends of development in information technology is needed to safe, secure, and protect the transmission of data. Conventional encryption technique methods give failed desired result of data protection. However, unique ID and password, and combination between symbol, alphabets & numerical will give a good impact to account security.

There are many ways to save our account data. As example we can save it into a card, account with password, or with key. But those method are not good because the security at every method is insecure. The card and key can be stolen or missing in some place, and the account with password can be stolen or the owner can forget the password. So every scientist trying to do some research to make data with most secure level. Finally nowadays, Face Recognition born as one of method to implement and secure any information related with account details with only our anatomy face.

Face recognition is one of technique to secure the information data which takes the image of person and compares it with the recorded image in the database. The comparing obtained from technique that capture the representation of the faces structure like the shape of eyes, the distance between nose, eyes and mouth, the eyebrows, form of the forehead, and etc.

This paper will describe the definition about Face Recognition as Authentication Security and the method to save and secure the information via face anatomy. This paper also tell about the process and algorithm how to detect the landmarks of face, after that the landmarks will be process and detected the spot. After that this paper also tell about the process of comparing between two images to find the similarity spot for authentication using face recognition. This paper aim to tell about the authentication process of Face Recognition and the method how to get the spot at human face.

1.2 Writing Objective

The purpose of this ISAS are :

1. Definition of Security System.
2. Definition of Biometric Security.
3. Definition of Authentication.
4. Definition of Face Recognition.

1.3 Problem Domain

Accordance with the title of ISAS "Face Recognition" We will discuss about:

1. SWOT Analysis of Face Recognition
2. Authentication Process of Face Recognition

1.4 Writing Methodology

The method which used in this ISAS is the method of browsing from internet, reading online journal, and make a survey in problem domain.

1.5 Writing Framework

The paper was written by systematic as follows :

CHAPTER I : INTRODUCTION

1.1 Background

Discusses the briefly description about security system, description about biometric security, briefly description about authentication, description about face recognition.

1.2 Writing Objective

The purpose of this article is to understand about face recognition, biometric security, SWOT analysis, and authentication with Face Recognition.

1.3 Problem Domain

First, tell about the SWOT analysis of Face Recognition, it’s a comparison between Strength, Weakness, Opportunity and Threat. Second, tell about process of authentication with Face Recognition.

1.4 Methodology Writing

To get data which needed, this paper use the method of observing or direct observation techniques, author reads famous repository online journal.

1.5 Writing Framework

This paper Writing Framework consists of four Chapter, the first chapter is introduction which tells the background, writing objective, several problem domain, methodology writing and writing framework of this paper.

Chapter II Basic of Theory

In chapter II, paper written several sub chapter. The first sub chapter is to tell about briefly description of system security. The second sub chapter is to tell about Definition of Biometric System. The third sub chapter is to tell about briefly description of Authentication. The fourth sub chapter is to tell about definition of Face Recognition.

Chapter III Problem Analysis

Analyzing and solve the problem that contained in problem domain.

Chapter IV Conclusion and Suggestion

Conclude and suggest related to this paper.

CHAPTER II
BASIC THEORY

II.1 Briefly Description : Security System

Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

Security is critical for enterprises and organizations of all sizes and in all industries. Weak security can result in compromised systems or data, either by a malicious threat actor or an unintentional internal threat (Bhatia, 2013).

II.2 Biometric Security

Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. The past of biometrics includes the identification of people by distinctive body features, scars or a grouping of other physiological criteria, such like height, eye color and complexion. The present features are face recognition, fingerprints, handwriting, hand geometry, iris, vein, voice and retinal scan. The most recognized biometric technologies are fingerprinting, retinal scanning, hand geometry, signature verification, voice recognition, iris scanning and facial recognition.

A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below:

1. Identification (1: n) – One-to-Many: Biometrics can be used to determine a person's identity even without his awareness or approval. Such as scanning a crowd with the help of a camera and using face recognition technology, one can verify matches that are already store in database.

2. Verification (1:1) - One-to-One: Biometrics can also be used to verify a person's identity. Such as one can allow physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retina scan

Biometric Technology such as: fingerprint recognition, voice recognition, signature recognition, palm scan, iris scan, retina scan, hand geometry, signature scan, keystroke scan and face recognition (Bhatia, 2013).

II.3 Briefly Description : Identification and Authentication

Identification provides user identity to the security system. This identity is typically provided in the form of a user ID. The security system will typically search through all the abstract objects that it knows about and find the specific one for the privileges of which the actual user is currently applying. Once this is complete, the user has been identified.

Authentication is the process of validating user identity. The fact that the user claims to be represented by a specific abstract object (identified by its user ID) does not necessarily mean that this is true. To ascertain that an actual user can be mapped to a specific abstract user object in the system, and therefore be granted user rights and permissions specific to the abstract user object, the user must provide evidence to prove his identity to the system. Authentication is the process of ascertaining claimed user identity by verifying user-provided evidence

User identification and authentication are typically the responsibility of the operating system. Before being allowed to create even a single process on a computer, the individual must authenticate to the operating system. Applications and services may or may not honor authentication provided by the operating system, and may or may not require additional authentication upon access to them (Havighurst, 2007).

II.4 Face Recognition

In order to recognize a person, one commonly looks at faces, which differentiate one person to another. Face recognition is used to search for other images with matching features. Eyes in particular seem to tell a story not only about which somebody is, but also about how that person feels, where his/her attention is directed, etc. Face recognition records the spatial geometry of unique features of the face. Main focuses on key features of the face. Face recognition technique is used to identify terrorists, criminals, and other types of persons for law enforcement purposes. This is a non-intrusive, cheap technology. In face recognition 2d, recognition is affected by change in lighting, the person's hair, age, and if the people wear glasses, low resolution images

It requires camera as equipment for user identification; thus, it is doubtful to become popular until most peaces include cameras as standard equipment. United States used same technologies to prevent people from obtaining fake identification cards and driver's. Facial recognition is a form of computer vision that uses faces to attempt to identify a person or verify a person's claimed identity. (Bhatia, 2013)

II.5 SWOT Analysis

The SWOT analysis is a business analysis technique that your organization can perform for each of its products, services, and markets when deciding on the best way to achieve future growth. The process involves identifying the strengths and weaknesses of the organization, and opportunities and threats present in the market that it operates in. The first letter of each of these four factors creates the acronym SWOT.

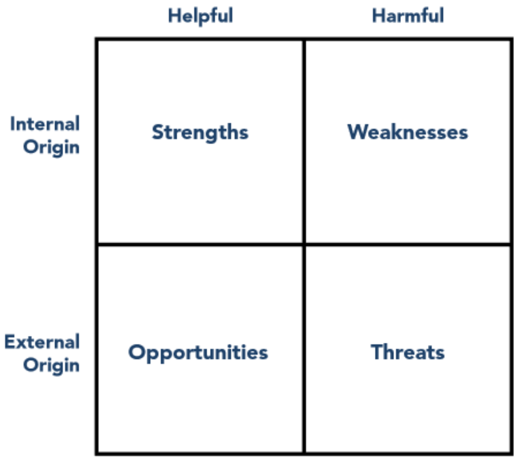

Figure 2.1 SWOT Analysis

The SWOT analysis is a popular and versatile tool, but it involves a lot of subjective decision making at each stage. It should always be used as a guide rather than as a prescription and it is an iterative process. There is no such thing as a definitive SWOT for any particular organization because the strengths, weaknesses, opportunities, and threats depend to a large extent on the business objective under consideration (Team FME, 2013).

.

CHAPTER III
PROBLEM ANALYSIS

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:

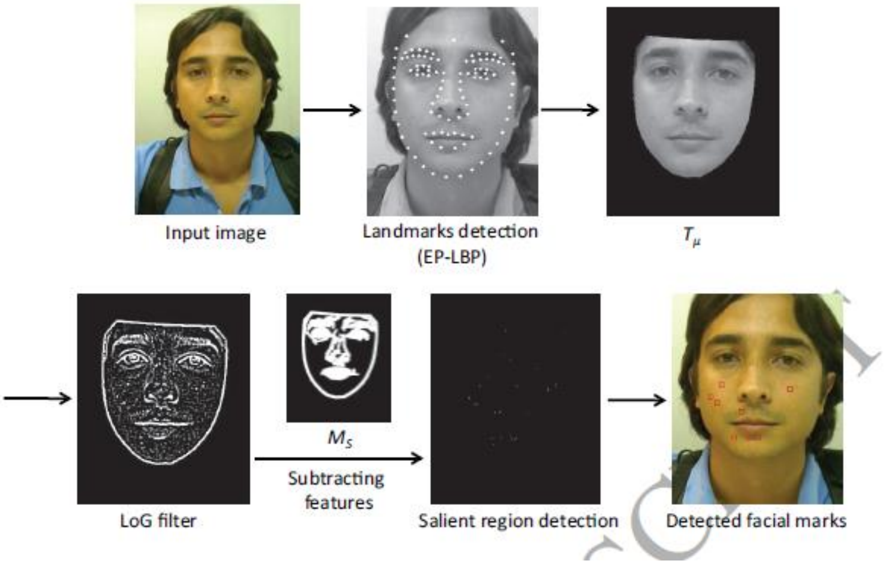

Figure 3.1 Face Detection Process

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

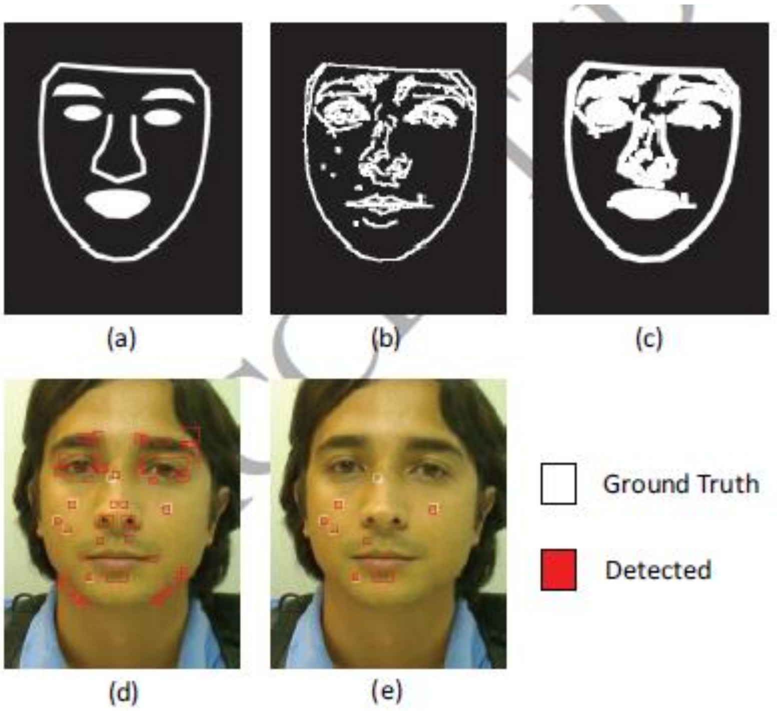

Fig 3.2 Detecting process of two images.

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).

III.2 SWOT Analysis of Face Recognition as Authentication

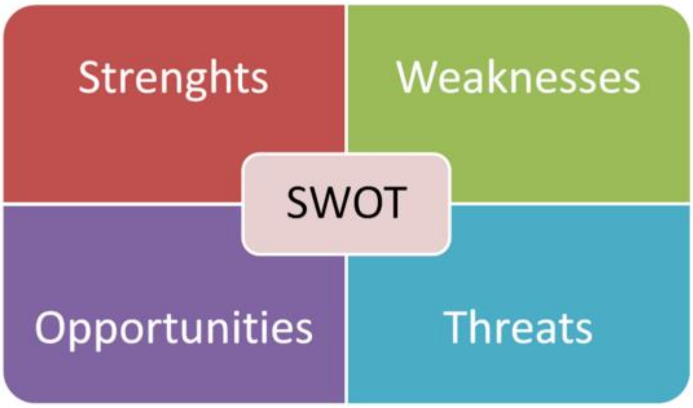

Figure 3.4 Swot Picture

(REF: 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. **Strength**

   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 compare 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.

CHAPTER IV
CONCLUSION AND SUGGESTION

IV. 1 Conclusion

Face Recognition is one of technique in information security to secure information through human face. Face recognition has several process in detecting the human face. The input image will be substracted to find the Salient Region spot. After that to compare between two images, the system will check the user specific mask and will be compared with face data in database. Face Recognition also has their own Strength, Weakness, Opportunities, and Threat that make Face Recognition Balance between in each point.

IV.2 Suggestion

1. Face Recognition is a good idea to store any information data but need good algorithm to secure the data.
2. Face Recognition can be used as authentication to handle the security.

BIBLIOGRAPHY

Bhatia, R. (2013). Biometrics and Face Recognition. *International Journal of Advanced Research in Computer Science and Software Engineering*, 92-94.

Havighurst, R. (2007). *User Identification and Authentification.* New York: Taylor & Francis Group, LLC.

Riera, F., Gonzalez, A., & Vazquez, H. (2017). Facial Marks for Improving Face Recognition. *Science Direct*, 6-7.

Team FME. (2013). *SWOT Analysis Strategy Skills.* www.free-management-ebooks.com.