CHAPTER 1
INTRODUCTION

"When knowledge is limited - it leads to folly... When knowledge exceeds a certain limit, it leads to exploitation."

■ *Abu Bakr (r.a)*

Due to internet era, the data exchange between one and another party is increased. The important aspect that should be guaranteed is the legality of the user. To ensure the legality of the user, authentication process is necessary. Fingerprints are often used to authenticating the legality of the user. However, lately fingerprint spoofing have break the fingerprint verification system. Therefore, this study is proposed to overcome the problem by strengthening the fingerprint verification system.

This chapter discusses the rationale in Section 1.1 that explain the background of this study and related problem situation. Theories and concept used to conceptualize this study are discusses in Section 1.2, while Section 1.3 discusses the variable related to the problem and their relationship to the paradigm of this study. The intended problem within this study is explained in Section 1.4. Section 1.5 discusses the proposed approach to solving the intended problem. Besides, this study describes some assumption in Section 1.6, while Section 1.7 describes the scope of works and delimitation. Finally, the contribution of this study is described in Section 1.8.

1.1 Rationale

The legitimacy of users is an important thing in data exchange, such that the authentication process is necessary to prove it. Nowadays, the authentication is not only done by offline means, but also done by online means, so it can be done anywhere

and anytime. However, there is no guarantee that the party involved in online authentication is the legal party, except if the involved one includes unique data that prove their identity.

The static biometric such as fingerprint, iris, and face are frequently used on the authentication process. Static biometrics have a permanent trait in each person, such that it is possible to attack the system by creating a fake biometric. Such an attack is called as spoofing attack. A Spoofing attack is done by creating fake fingerprint's texture using playdoh [1]–[3], creating a fake face using photo [4], creating fake iris using printer machine [5] or steal it directly from the database [6]. Spoofing is considered harmful because it can increase the risk of false acceptance, such that the adversary can be authenticated as the legitimate user. This condition explains that the fingerprint-based authentication system is vulnerable to spoofing attacks.

The proposed research designed a system to strengthen the fingerprint-based authentication system. The addition of dynamic biometrics to strengthen the fingerprint-based authentication system is used to minimize spoofing rates.

1.2 Theoretical Framework

A spoofing attack is done by making a fake fingerprint of the victim to break the fingerprint verification system. The threat model of this attack is to imitate the texture of fingerprint using unprofessional material such as wood glue, playdoh, and silicone. The permanent trait and universal make fingerprint easy to forge [3]. This study focuses to strengthen the fingerprint by adding dynamic biometric to improve its strength against spoofing attacks. Furthermore, this study used a dynamic voice to strengthen the fingerprint-based authentication system. Voice is a dynamic biometric because the physical and behavioral factors are capture together inside it [7]. The physical factor obtained from the articulation organ (mouth, lips, tongue, etc.) [8] while the behavioral factor obtained from the intonation, health condition, word are spoken, etc. [9]. The voice is represented in a voiceprint extracted from spectrogram

display. The spectrum analysis in spectrogram is implemented to obtained more accurate information of the voice.

1.3 Conceptual Framework

The physical and behavioral factors on the voice allow for multivariate analysis, such that it provides a more accurate analysis then static biometric [9]. The proposed authentication system used the voice from the syllable as a template, then those templates are combined to create new words, such that the new voice are produced by the users. Thus, the sound produced by the user has a large variation. This makes it difficult to spoofed because to conduct spoofing attack the adversary should be guessing the occurrence of the word during authentication.

1.4 Problem Statements

Based on the rationale of this study in Section 1.1, the legality of the user is necessary. To ensure the data is sent and received by a legal party, the authentication process is necessary. The authentication methods using biometric have been developed, one of them is fingerprint-based authentication system. However, the permanent character of fingerprint makes the texture easy to fake, such that the fingerprint-based authentication is vulnerable against spoofing attack. A study from K. Jain et. al [1] and Tsutomu Matsumoto et.al. [2] have successfully break the fingerprint-based system using fake fingerprint. The attack is conducted by duplicating the fingerprint's texture using playdough and silicon. Therefore, this study proposed a method to strengthen the fingerprint-based authentication system.

1.5 Hypotheses

J. Galbally et.al [4] mentioned the dynamic biometric can minimize the probability of successful the spoofing attack because . In addition, the behavior factor in dynamic biometric will be difficult to make a duplicate of the biometric itself [9].

For overcoming the spoofing attack proposed by Anil K. Jain [1] and Tsutomu Matsumoto et.al. [2], the proposed method introduces the dynamic voice instead of using fingerprint only. The dynamic voice is proposed because for forging it, large amount of guessing is necessary. This condition occurs because dynamic voice biometric has a lot of syllable combination such that the possibility to forge its low and the complexity of guessing the voice is high. To improve the security against spoofing attack, this study introduced voiceprint method to extract the dynamic voice feature [10] produced from the spectrogram of the voice signal.

1.6 Assumption

This study assumes that the inputs of the proposed system are as follows:

1. The fingerprint input is a thin fingerprint image with the minutia-based feature extraction
2. The voice input is a time domain-based voice signals produced of two syllable-based Indonesian words. The spectrogram-based voiceprint used to extract the voice feature.
3. The verification process is first based on fingerprint and continued with dynamic voice-based authentication if the fingerprint-based authentication is success
4. The data collection is conducted in a non-noisy environment

1.7 Scope and Delimitation

This study formulated the scope and delimitation are as follows:

1. The system is proposed to strengthen the fingerprint-based authentication
2. The output of the authentication process is a status that determine whether the user is legal (genuine) or not

1.8 Importance of the Study

Verification of the user's validity is necessary to ensure data exchange involved the legal party. Considering the data's urgency and the threat of spoofing attack on the current verification system justifies the need for increasing the security level. Thus, by applying the proposed approach derived from the result of this study, the security level of the authentication system can be improved.