# Abstract

At present, authentication techniques using fingerprint biometrics have been widely used in various fields because these techniques are safer and more comfortable than the traditional passwords. However, this biometric authentication, especially the templates stored in storage media both online and offline, still need to be protected. For the purpose of protection, a technique in the biometric cryptosystem is proposed in this thesis; it is called the fuzzy vault scheme.

Fuzzy vault scheme is one technique in biometric cryptosystems that secure data or messages (such as keys or secret messages) using the user's fingerprint data. Furthermore, some noise (chaff point) is also added to the database so that the user's fingerprint data can be disguised. Although the fingerprint data in the form of minutiae can be protected using a fuzzy vault scheme compared to traditional authentication systems, it can reduce user convenience. This is because the data stored in the database is the result of encryption data containing a combination of secret messages, fingerprint data and some chaff points (noise).

Previous studies proposed a distance-based method in the fuzzy vault scheme because it does not need to align and rotate the fingerprint image during registration or authentication. In addition, the distance-based method does not produce a helper data that can lead to information leakage that can be exploited by impostor. In this thesis, the distance-based method is proposed with several modifications,

namely minutiae filter process, several numbers of chaff point generation and the candidate points identification techniques. The experimental shows that the rate of false reject from the same finger with different impression (false rejection rate) and the rate of false accept from two different fingers (false acceptance rate) in the authentication process decrease. The previous method produced FRR 13.4375% and FAR 0.4515% and the proposed method produces FRR 8.9475% and FAR 0.3520%.

**Keywords:** *biometric cryptosystem*, *fuzzy vault scheme*, *minutiae filter*, *chaff point generation*, *candidate point identification*.