# One-time Password for Biometric Systems: Disposable Feature Templates

## OBJECTIVE:

Main objective of the system is The features extracted are from an improved geneticbased extraction technique that performed well on periocular images. The results in this manuscript show that the improved extraction technique coupled with the feature selection technique has an improved identification performance compared with the traditional genetic based extraction approach.

## ABSTRACT:

Biometric access control systems are becoming more commonplace in society. However, these systems are susceptible to replay attacks. During a replay attack, an attacker can capture packets of data that represents an individual's biometric. The attacker can then replay the data and gain unauthorized access into the system. Traditional password based systems have the ability to use a one-time password scheme. This allows for a unique password to authenticate an individual and it is then disposed. Any captured password will not be effective. Traditional biometric systems use a single feature extraction method to represent an individual, making captured data harder to change than a password. There are hashing techniques that can be used to transmute biometric data into a unique form, but techniques like this require some external dongle to work successfully. The proposed technique in this work can uniquely represent individuals with each access attempt. The amount of unique representations will be further increased by a genetic feature selection technique that uses a unique subset of biometric features. The features extracted are from an improved geneticbased extraction technique that performed well on periocular images. The results in this manuscript

show that the improved extraction technique coupled with the feature selection technique has an improved identification performance compared with the traditional genetic based extraction approach. The features are also shown to be unique enough to determine a replay attack is occurring, compared with a more traditional feature extraction technique.

## INTRODUCTION:

Dependable user authentication is increasingly important in a world with the internet of things. If an individual's authentication is compromised, it could have consequences ranging from loss of privacy to secure information being used to harm or steal. From the commercial use level (social media sites) to high security sectors (government, banking, etc…), hackers will attempt to attack an authentication system using a variety of techniques. One such attack is a biometric replay attack. Replay attacks are data being replayed into a system by an attacker to grant access to the attacker. Previous research has suggested using genetic and evolutionary computation (GEC) approaches for optimized biometric recognition. This technique is known as Genetic and Evolutionary Feature Extraction (GEFE) . GEFEmany was implemented to further improve the performance of GEFE Whereas GEFE trained on a traditional 1:N identification system, GEFEmany trained on a N:N system, allowing for more training comparisons and more effective extractors. Shelton et al. proposed two biometric-based access control protocols that used disposable feature extractors (FEs) and their associated feature vectors (FVs) to mitigate replay attacks on a facial biometric recognition system. Their results showed that GEFE technique created FEs and FVs that were unique from each other and that achieved high recognition accuracy.