OTP USING IMAGE PROCESSING AND EXTRACTION-SELECTION TECHNIQUE

Mrs Latha D U[1], Sanath S[2], Lavanya A P[3], Sanjay B R[4], Megha B H[5]
[1]Assistant professor, [2345]UG Students
Dept of Computer Science and Engineering
BGS Institute Of Technology, B G Nagar, Mandya-571448

Abstract: ***In this paper, we present an iris-based access control protocol that is resistant to iris-based replay attacks. This new style of biometric-based access control protocol is similar to the so called, 'one time password' approach used by some conventional username/password access protocols. 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. The Genetic and Evolutionary Feature Extraction(GEFE) is a feature extraction technique that can be used to optimize feature extractors for uniquely biometric images. 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 genetic-based 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.***

Keywords: Evolutionary Computation; Cyber Security; Periocular Recognition; Biometrics; Feature Selection; Feature extraction

I. INTRODUCTION

Biometric is the field of research devoted to identification using physiological and behavioral characteristics [1]. Biometric based feature extraction is main module in a biometric base access control system. The 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. Biometric system is mainly used in social media sites and high security sectors like government, hospital, banking, etc, the 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. 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. [5]. Shelton et al. proposed two biometric-based access control protocols that used disposable Feature Extractors (FEs) an their associated feature vectors (FVs) to mitigate replay attacks on a facial biometric recognition system. Their results showed that GEFE [4] technique created FEs and FVs that were unique from each other and that achieved high recognition accuracy. Because of this, they could be used to mitigate replay attacks by not allowing the use of a particular FE or FV more than once. However, GEFE will eventually begin to evolve FEs similar to previously evolved FEs. The greater the number of common FEs, the more likely a successful biometric replay attack will occur. The feature extraction technique used in this work is Genetic and Evolutionary Feature Extraction (GEFE) [5]. GEFE is used to optimize feature extractors using Genetic and Evolutionary Computation (GEC) [5]. GECs are a machine learning techniques that simulates Darwinian components to evolve solutions for problems, GEFE traditionally evolves texture based feature extractors for identification. GEFE has been shown to have a superior identification and verification performance than traditional texture based techniques like Local Binary Patterns (LBP) method. In this work proposes the Genetic and Evolutionary Feature Selection (GEFeS) method for optimizing masks for improved recognition [6]. This work uses a hybrid of GEFE, GEFEmany and GEFeS [4-6] to mitigate replay attacks by using a unique Feature vector (FV) and corresponding unique mask to represent an individual. The hybrid is applied to the data set of smart phone periocular images taken from the iPhone5[7]. The remainder of this paper is as follows. In Section 2, we describe the approaches used in this work such as using GEFE, GEFEmany, GEFeS for mitigating replay attacks in detail, evolving genetic masks and applying masks for mitigating replay attacks. In Section 3, we present our experiment, and in Section 4, we present our results. Finally, in Section 5, we provide our` conclusions and future work.

II. GEFE MANY AND GEFES FOR MITIGATING ATTACKS

This section describes the feature extraction techniques used for this experiment. The presented approach is the GEFE and evolved GEFEmany approach. We also used GEFeS on each presented feature extraction technique for feature selection.

A. Local Binary Patterns

The Local Binary Pattern (LBP) feature extraction method is a technique proposed by Ojala et al. [3], [4]. This technique can be used to classify textures patterns in images and uses these textures to create feature vectors (FVs) with images. For facial recognition, the LBP technique works by segmenting the image into uniform sized, non-overlapping regions, as shown in Fig. 1. Each region has a histogram associated with it, where the bins in the histogram correspond to the texture patterns found in each region. A FV is created by concatenating the histograms from all regions of a segmented image.

B. Genetic and Evolutionary Feature extraction

One of the most important modules of any biometric system is the feature extraction module given a sample it is important for the feature extraction method to extract a rich set of features that can be used for identity recognition. For facial recognition, the LBP method works by segmenting the image into uniformly sized, non-overlapping regions [7].

The Genetic and Evolutionary Feature Extraction (GEFE) uses Genetic and Evolutionary Computation to optimize the feature extraction. FEs are trained on some data set of images. Multiple images of a subject are separated into a probe and gallery set. The probe set simulates images from the client side of a system, while the gallery set simulates a database of previously enrolled samples. The fitness (fi) associated with the candidate FE (fei), is described as the total number false positive matches made when comparing each probe to the gallery set, added to the percentage of patches activated in a FE. GEFEmany compares every instance in a training set to one another i.e N:N matching where as traditional GEFE compares only one instance of each subject to every other instance i.e 1:N matching. Replay attacks occur when a template is captured during the transmission across a network. Using disposable FEs mitigates replay attacks because if the template is captured: (a) the exact FE used to extract the appropriate template will not be known to the hacker, and/or (b) the captured template from one authentication session will not match the expected template for a future authentication session. The FEs are unique as well as the templates (FVs) extracted by the FEs, as the results of our experiments demonstrated in [3]. Figure 1 demonstrates the modules in a biometric system and how an attacker can capture data to replay attack. To gain access to an asset, users will provide a biometric sample and the system will select a FE and apply it to the sample. Using the FE a feature vector (FV), a template, is extracted. The FV, and/or FE, are then passed over the network and compared with the previously enrolled templates associated with the FE used to create the template [3]. GEFE and GEFE many can be used to create disposable FE. Unlike conventional authentication systems, which enroll a single template for each subject allowed access, an authentication system using disposable FEs may enroll numerous templates for each subject (one template associated with each FE). To gain access to an asset, users will provide a biometric sample and the system will select a FE and apply it to the sample. Using the FE a feature vector (FV), a template, is extracted. The FV, and/or FE, are then passed over the network and compared with the previously enrolled templates associated with the FE used to create the template [3].

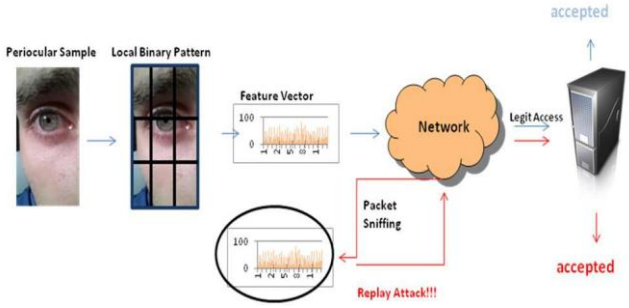


Fig. 1. Biometric System undergoing a replay attack

C. Genetic and Evolutionary Feature Selection

Genetic and Evolutionary Feature Selection (GEFeS) is feature selection technique that is based on simulated evolution. GEFeS is used to evolve feature masks (FMs) in an effort to discover high-performing sub-feature sets. The FMs are used to 'mask out' non-salient features of the FVs that are extracted by the four baseline ARSs.

The evolutionary process of GEFeS is as follows. Initially, a random population of FMs is created. FMs are represented as a string of real values between 0 and 1 and the lengths of these FMs are equivalent to the lengths of the FVs. If a FM value is less than 0.5, then the corresponding FV value is masked out; otherwise, the FV value is used. Each FM is then evaluated on a sub-dataset (training and/or validation) of blog samples, represented as FVs, to determine its fitness. The fitness evaluation function is ten times the number of FVs incorrectly classified plus the percentage of the features used.

III. EXPERIMENT

This research applied the GEFE+GEFeS and GEFE many+GEFeS hybrid techniques to periocular images. The BIPLab MICHE image database (BIPLab) [7] was used to obtain images. The hybrid techniques is the process of evolving FEs using GEFE, and then evolving FMs on the vectors created by the GEFE FEs. Both FEs and FMs are optimized on a training set and evaluated on a mutually exclusive test set. There were 30 FEs optimized for periocular recognition and 30 FMs optimized on each FE.

From the BIPLab database, we used a training set of 35 subjects. For the test set we used 20. The images from the database were taken from an iPhone5 FaceTime HD camera of 1.2 megapixels (MP) . All images were taken 10cm away from the device, and was taken indoors using artificial light. The images also are 72 dots per inch (dpi). Four periocular samples were used for each subject in each dataset.

IV. RESULTS

In Table 1, the performances of LBP, GEFE, GEFEmany and the GEFeS hybrids are shown. The result includes the identification accuracy of each method and the percentage of patches activated as well as the percentage of features used. For the GEFeS hybrids, 30 FMs were evolved for 30 FEs each. The method 'Avg' denotes the average performance of

all 30 sets of FMs on their respective FEs. The method 'Best' denotes the average identification of the set with the highest accuracy. The fourth column denotes the percentage of features used by each technique. For GEFE, LBP, and GEFEmany, the features were measured by the number of patches used. For the GEFeS approaches, the percentage of features was the amount not masked out by the masking values. The GEFEmany technique used slightly more patches than GEFE on average, but GEFeS required fewer features on

GEFEmany FEs than GEFE FEs. There were several sets with the same accuracy, but the best was selected based on the minimal percentage of features. Results show on the test set an average accuracy increase from GEFE to GEFE+GEFeS with 81.00% and 82.07%, respectively. We also recorded and

increase from GEFEmany to GEFEmany+GEFeS with 86.16% to 86.24%. On the best FEs for GEFE+GEFeS and GEFEmany+GEFeS there was an average accuracy of 86.16% and 94.00% respectively with a best accuracy of 100.00% for both GEFeS hybrids.

Table 1. Results of LBP , GEFE and GEFEmany for Identification

Dataset	Methods	Average Feature Percentage	Average Accuracy	Best Accuracy
iPhone5 (Testset)	LBP	(2 * 3) = 6	-	94.67%
	GEFE	2.5	81.00%	95.00%
	GEFE+GEFeS (Avg)	40.20%	82.07%	90.03%
	GEFE+GEFeS (Best)	47.34%	86.16%	100.0%
	GEFEmany	2.66	86.16%	100.0%
	GEFEmany+GEFeS (Avg)	38.09%	86.24%	91.17%
	GEFEmany+GEFeS (Best)	38.24%	94.00%	100.0%

In Fig. 2, the best performing FEs are shown in Receiver Operator Characteristic (ROC) curves. The ROC curve plots the True Accept Rate (TAR) and the False Accept Rate (FAR) of subjects. As previously reported in [5], the LBP algorithm has a TAR of 0.5619 at a FAR of 0.00028. GEFE was also reported to have a TAR of 0.6271 at a FAR of 0.00089. GEFE+GEFeS has an initial TAR of 0.5833 at a FAR of 0.000877. GEFE many has a TAR of 0.9318 at a FAR of 0.0032. GEFE many+GEFeS has an initial TAR of 0.6500 at a FAR of 0.002. Both GEFeS hybrids have a poorer performance in regards to verification but as shown in Fig. 3, the increase in unique representations makes this approach preferable for mitigating replay attacks.

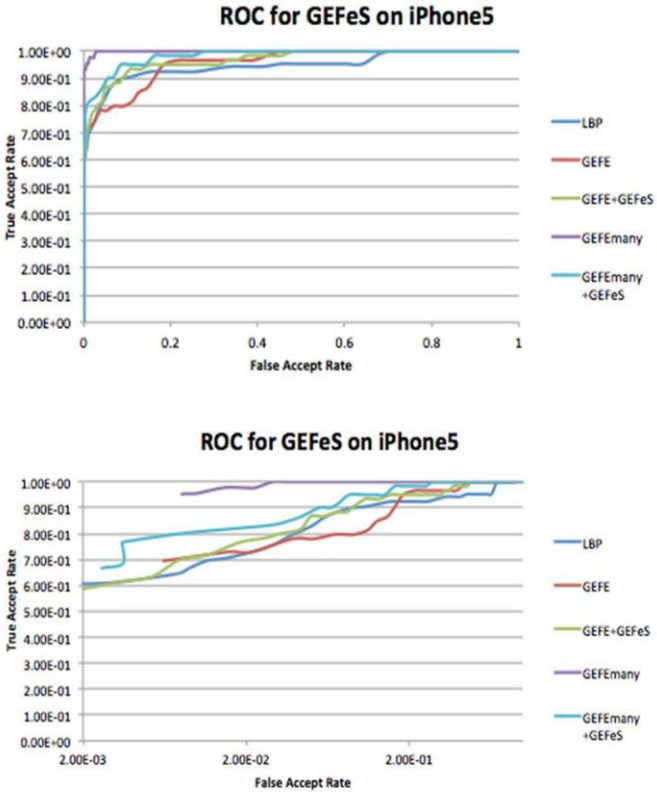
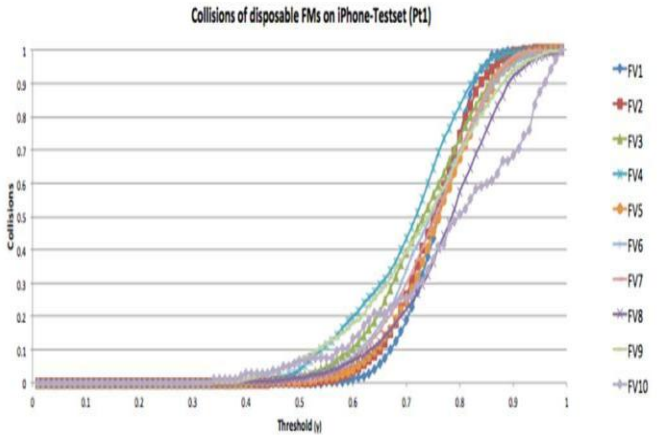


Fig. 2. ROC curves on Iphone5 (top) and Log Scaled (Bottom)

The results in Fig. 3 below show the percentage of collisions for all activated histograms (y-axis) over an increasing threshold (x-axis). Each series represent the collisions for different disposable FEs. As shown below, collisions of histograms from disposable FMs start to rise around a threshold of 0.58 on average. A 100% collision rate is reached on average at a threshold of 0.96. A collision rising at a lower threshold indicates that permutations of histograms for FVs are not unique, and are more likely to allow a successful replay attack.



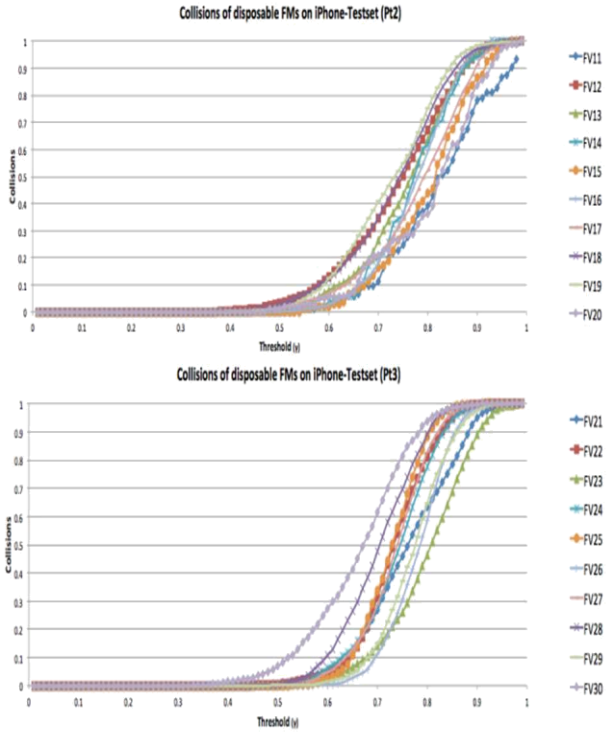


Fig. 3. Collision Graphs for Feature Masks on Iphone5

Figure 4 shows sample FEs evolved by GEFE many and placed overtop of periocular images taken from the iPhone 5. This selection of four FEs chosen at random appear to all be different, in regards to the location, dimensions and numbers of patches. It stands to reason that each FE will produce a unique FV, though the image may be exactly the same. Regardless, every FE has a higher identification performance than LBP alone.

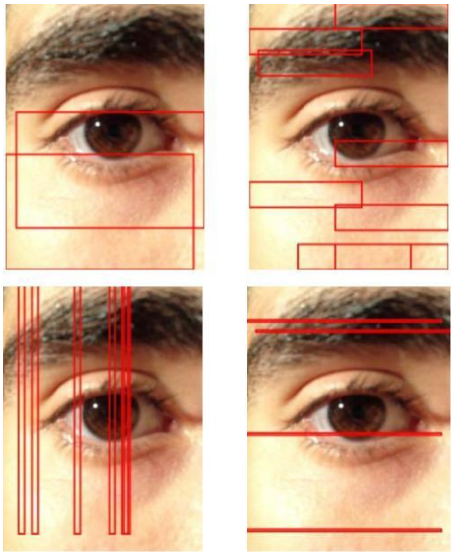


Fig. 4. GEFE many Feature Extractors

V. CONCLUSION

In this work, FEs and FMs were evolved that created unique FVs which were exclusive from one another. This was done to address the issue of a number of unique representations of one's biometric data to mitigate replay attacks. The masks were primarily used for different representations, but the average accuracy of every FE was improved with the optimized masks. The GEFEmany approach had a better identification performance than traditional GEFE, and the feature selection technique improved both extractions.

Future work will be devoted towards evolving FEs specifically for anti-spoofing. We will be implementing a combination of deep learning approaches that includes convolutional neural network architecture.

ACKNOWLEDGMENT

This research is based upon work supported by the Army Research Office (Contract No. W911NF-15-1-0524).

REFERENCES

[1] Davis, L. (1991). Handbook of genetic algorithms. New York: Van Nostrand Reinhold.

[2] Shelton, J., Dozier, G., Bryant, K., Smalls, L., Adams, J., Popplewell, K., Abegaz, T., Woodard, D., & Ricanek, K. (2011). "Comparison of Genetic-based Feature Extraction Methods for Facial Recognition," Proceedings of the 2011 Midwest Artificial Intelligence

[3] Shelton, J., Bryant, K., Abrams, S., Small, L., Adams, A., Leflore, D., Alford, A., Ricanek, K. & Dozier, G. (2012). "Genetic & Evolutionary Biometric Security: Disposable Feature Extractors for Mitigating Biometric Replay Attacks". The 2012 Proceedings of the 10th Annual Conference on Systems Engineering Research.

[4] Shelton. J., Roy, K., O'Connor, B., & Dozier, G. (2014). "Mitigating Iris-Based Replay Attacks". The International Journal on Machine Learning and Computing (IJMLC), Vol. 4, No. 3, pp. 204 – 209.

[5] Jenkins, J., Shelton, J., Roy, K. (2016). "A Comparison of Genetic Based Extraction Methods for Periocular Recognition", in The 6th International Conference on Information Communication and Management (ICICM)

[6] Abegaz, T., Dozier, G., Bryant, K., Adams, J., Baker, B., Shelton, J., Ricanek, K., and Woodard, D. L. (2011) Genetic-Based Selection and Weighting for LBP, oLBP, and Eigenface Feature Extraction, Proceedings of the 22nd Midwest Artificial Intelligence and Cognitive Science Conference (MAICS), Cincinnati, OH, pp. 221-224

[7] BIPLab, University of Salerno. http://biplab.unisa.it/MICHE/database/.

[8] Ojala, T., Pietikainen, M., & Maenpaa, T. (2002). "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns". IEEE Transactions on Pattern Analysis and Machine Intelligence IEEE Trans. Pattern Anal. Machine Intell., pp. 971-987.

