BIOMETRICS ON KEYSTROKE DYNAMICS LOGGING WITH VERIFICATION

Ritik Ramaiya | Boominathan P| SCOPE

Introduction

The main contribution of this study was the evaluation of the text-input performance as a function after training on the longest keystroke samples available. Most of the studies show that biometric systems cause many ambiguities due to false authentication of users. Pressing and releasing times of keys are the main factor to take into consideration which will help us to determine the genuine user, as well as taken the total time to login which is not covered by other studies. Also training data is quite efficient in this case as it creates a wide range for the user when attempting to login.

Motivation

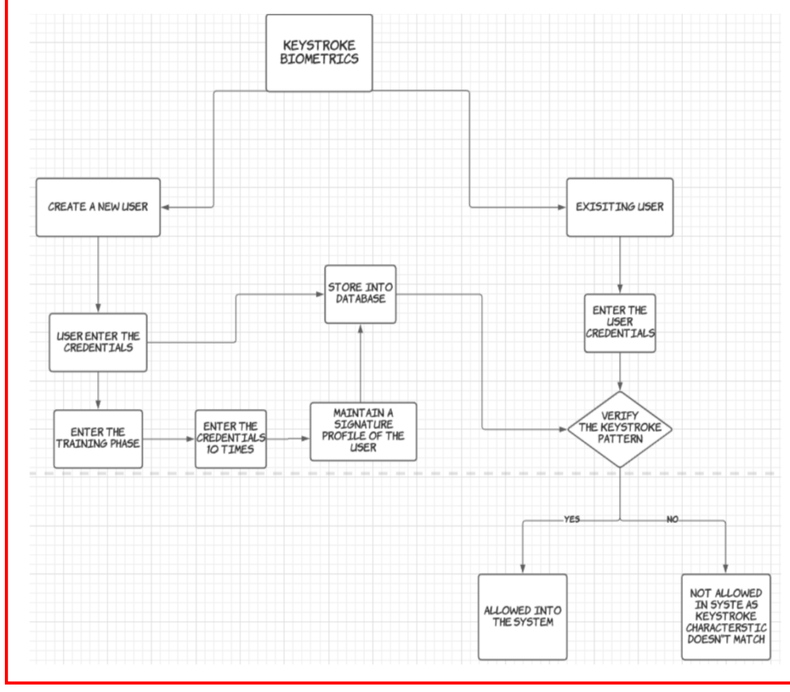
A lot of brute force attacks have been initiated in past years in the area of keystroke biometric system which allows intruders to login into various systems and destroy them. Our aim in this paper is to introduce a model which will provide an extra layer of security by authenticating different users and putting in place a mechanism to eradicate false logins without proper authentication.

Scope of the Project

The scope of this project is to develop a fully automatic secure biometric keystroke dynamic system which yields the Lowest equal error rate which is the main goal for all biometric system. Our goal is to achieve a better and lower equal error rate than all other algorithms implemented. The standard measurements that are utilized in keystroke dynamics research are between key idleness and key hold-time. The application should uphold different clients attempting to login and distinguishing regardless of whether they are approved to login by contrasting their composing qualities and the idleness normal and standard deviation taken by the quantity of preliminaries which for our situation is 10, so in view of those values the entrance is allowed or denied.

Methodology

In the initial phase the system starts with a simple user interface where by you have to prompt whether you are a new user or an existing user. If you are a new user then it asks for your name and password for the first time in order to register you in the system. Once it has taken the new user details from you, it will prompt you to enter the details 10 times so as it can train the data against your typing patterns which are the pressing and releasing times of the keys you type and captures the time and calculates a average which we call latency mean and calculate the standard deviation which will help it determine the existing user is genuine or trying to replicate the original user. On the other hand if you choose Existing user instead of new user, it asks for your name and password and a general phrase so that it can match your typing characteristics against the database in which your timings for pressing and releasing the keys are stored. The claimed user will then have to pass the verification test which is get the typing pattern correctly and within the time stored in the system which is the latency mean time and the standard deviation.



Architectural Diagram

Results

Data input plays a very huge role as if the characters are widely spaced on the keyboard the results might be vague sometimes as the user might try to find the keys if they purchase a new machine and try to login. This causes some ambiguities as biometric systems are a behavioural trait. Nature of client design directly influences the introduction of a check system, in this way, arranging a fair and discriminative keystroke incorporate profile is a fundamental cycle that should not be subverted. Generally speaking, as per the performed research, it is sensible that biometric recognition on cell phones can be acted, in actuality, applications taking advantage of the particular attributes of every client's composing patters. Having the option to accomplish such objective would be exceptionally advantageous for incorporating KD-based recognition frameworks into the entrance control components previously utilized while utilizing cell phones.

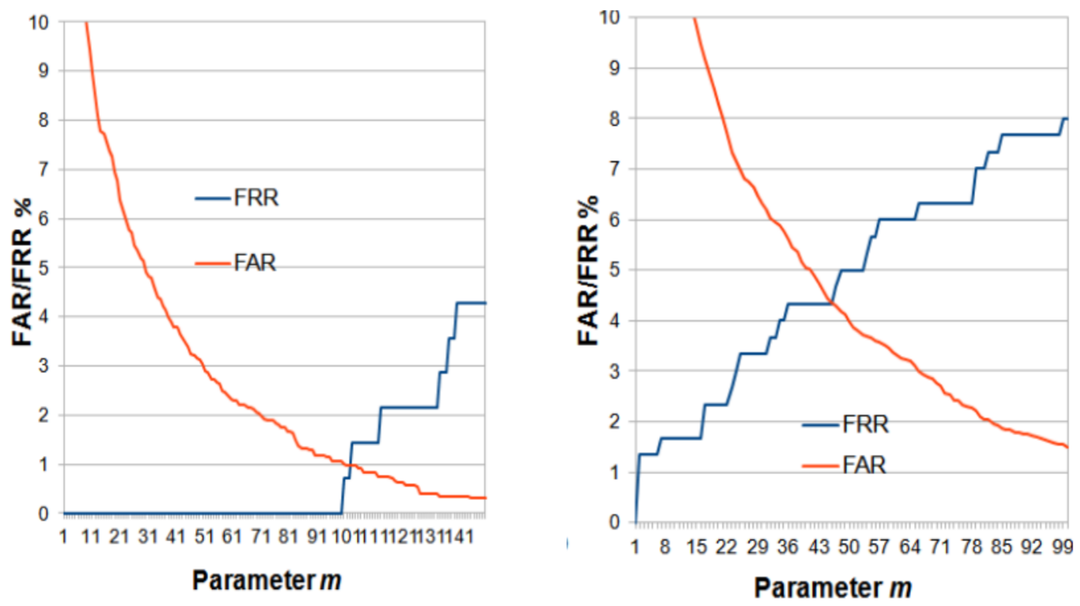


Figure showing achieved EER's with different populations

As we can see the Figures above on the Left side has an EER of 1% with a large number of keystrokes, on the left side we can observe that the EER is roughly 4% with a smller population which indicates that large population provides a much better authentication mechanism.

From previous studies done by other researchers using a random forest classifier, they achieved an equal error rate (EER) of 8.6%. Bakelman's results were not as robust as the results obtained by the team at Carnegie Mellon when used in conjunction with the features used in the Carnegie Mellon study, obtaining an EER of 10.5%. However, when Bakelman's and team ran their experiments using their own feature data, they recorded an EER of 6.1%. However we have managed to get much better results of about 4% with small population and much better results i.e almost 1% with our proposed model.

Conclusion

The above results demonstrate to us the properties which are required for the system in order to authenticate the system aggressively without any stopping. This biometric grants "continuous authentication" of a singular's character over a meeting after the individual logs in utilizing a more grounded biometric like finger impression or iris so go about as dynamic biometric framework.

These create the basis of a potentially effective way of enhancing overall security rating by playing a significant role in part of a larger multifactor authentication mechanism. E-commerce and E-payment are at a large threat in the modern world now, keystroke biometric can highly be useful in those scenarios.

References

- S. J. Shepherd, "Continuous authentication by analysis of keyboard typing characteristics," in *Proceedings of the 1995 European Convention on Security and Detection.*

- M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: a review," *Applied Soft Computing Journal*.